Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής
Πρόγραμμα Μεταπτυχιακών Σπουδών
«Προηγμένα Συστήματα Πληροφορικής»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**«Ανάλυση και Διαχείριση Επικινδυνότητας στα Πληροφοριακά Συστήματα - Υλοποίηση Μεθοδολογίας σε Επιχειρησιακό Περιβάλλον»**
Ονοματεπώνυμο Φοιτητή	**Γεωργίου Σοφία**
Πατρώνυμο	**Ιωάννης**
Αριθμός Μητρώου	**ΜΠΠΛ/ 09066**
Επιβλέπων	**Δέσποινα Πολέμη, Επίκουρος Καθηγήτρια**

Ημερομηνία Παράδοσης **03/2012**

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Πολέμη Δέσποινα Επικουρος Καθηγήτρια	Δουληγέρης Χρήστος Καθηγητής	Κοτζανικολάου Παναγιώτης Λέκτορας

Επιτελική Σύνοψη

Καθώς οι περισσότεροι οργανισμοί βασίζουν πλέον ένα μεγάλο μέρος της λειτουργίας τους σε πληροφοριακά συστήματα, η ανάγκη για κατάλληλη ασφάλεια αυξάνεται. Δυστυχώς, είναι δύσκολο να γίνει επιλογή των μέτρων ασφαλείας που χρειάζονται για να επιτευχθεί ικανοποιητική ασφάλεια.

Μεγάλες ποσότητες πόρων ξοδεύονται με σκοπό την αποφυγή αποτυχιών. Παρόλα αυτά, τελικά είναι αδύνατο να υπάρξει η εγγύηση ότι το ΠΣ είναι τέλειο, όπως είναι επίσης αδύνατο να προβλεφθεί και να εξαλειφθεί κάθε τι από τον εξωτερικό κόσμο που πιθανόν να απειλήσει το ΠΣ.

Αυτό που όμως είναι δυνατό να επιτευχθεί, είναι η μείωση της πιθανότητας εμφάνισης κινδύνου, η οποία θα επιφέρει και ελάττωση της αβεβαιότητας. Προϋπόθεση για την επίτευξη αυτής της ελάττωσης αποτελεί η εφαρμογή μιας κατάλληλης διαχείρισης επικινδυνότητας ώστε να επιτευχθεί επαρκής αναγνώριση και αποτελεσματική αντιμετώπιση των διαφόρων κινδύνων που απειλούν το σύστημα.

Αν η επικινδυνότητα θεωρηθεί ως το γενικότερο πλαίσιο που αναφέρεται σε πολιτικούς, τεχνικούς και διαχειριστικούς παράγοντες που απειλούν ένα ΠΣ ή την επιτυχία των έργων λογισμικού, η διαχείρισή της αποτελεί τη διαδικασία αναγνώρισης και ανάλυσης αυτών των απειλών, ποσοτικοποίησης των επιπτώσεών τους και εφαρμογής σχεδίων που θα ελαττώσουν ή θα εξουδετερώσουν τις αρνητικές τους συνέπειες.

Αυτή η μεταπτυχιακή διατριβή ασχολείται με την ανάλυση κινδύνων, διαδικασιών και μεθοδολογιών που αναγνωρίζουν τα προβλήματα ασφαλείας, τα ταξινομούν με βάση την σημαντικότητα τους και τέλος προτείνουν λύσεις για την επίλυση τους. Παρουσιάζονται οι διαφορετικοί τρόποι ανάλυσης κινδύνων, οι κυριότερες μέθοδοι που χρησιμοποιούνται σήμερα, τα πακέτα λογισμικού που κυκλοφορούν στην αγορά. Στο τέλος, υλοποιείται μια εφαρμογή ανάλυσης κινδύνων σε πολυεθνική εταιρεία τηλεπικοινωνιών με το λογισμικό της NRisk. Μέσα από αυτή τη προσπάθεια, διαφαίνεται η αξία της διαχείρισης επικινδυνότητας για τον έλεγχο του λογισμικού, ενώ παράλληλα προκύπτουν ορισμένοι σημαντικοί παράγοντες που επηρεάζουν άμεσα το ποσοστό κινδύνου που απομένει μετά την ολοκλήρωση της φάσης, καθώς και μια συνολική διαδικασία διαχείρισης επικινδυνότητας.

Πιο αναλυτικά, στην αρχή παρουσιάζονται κάποιες βασικές έννοιες σχετικές με τον κίνδυνο και τη διαχείρισή του στα ΠΣ. Στη συνέχεια, παρουσιάζονται και αναλύονται κάποιες από τις πιο γνωστές μεθοδολογίες Ανάλυσης, Αξιολόγησης και Διαχείρισης της επεικυνδυνότητας στα ΠΣ. Παρακάτω, γίνεται λόγος για άλλες μεθόδους ή καλύτερα διαδικασίες για την Διαχειριση της επικυνδυνότητας σε έργα λογισμικού. Στο τέλος αυτών παρουσιάζεται ένα εργαλείο/διαδικασία κλειστού κώδικα που χρησιμοποιείται μόνο στα πλαίσια μιας μεγάλης εταιρείας ανάπτυξης και ελέγχου λογισμικού τηλεπικοινωνιών και πώς αυτό λειτουργεί.

Παρατίθεται, δηλαδή, μία διαδικασία η οποία διαχειρίζεται και παρακολουθεί την επικινδυνότητα στο λογισμικό, η εφαρμογή της οποίας προϋποθέτει την ύπαρξη συγκεκριμένης πολιτικής από την πλευρά των υπευθύνων για την ανάπτυξη του λογισμικού, έτσι ώστε να παρέχεται μια βάση για τη λήψη αποφάσεων σχετικών με το επιτρεπτό επίπεδο της μετά τον έλεγχο εναπομείνασας επικινδυνότητας.

Η παρούσα εργασία, παρέχει μια καλή βάση πάνω στην οποία μπορεί να στηριχθεί περαιτέρω έρευνα του πεδίου που προκύπτει από τη συσχέτιση των εννοιών της διαχείρισης επικινδυνότητας λογισμικού και του ελέγχου που διεξάγεται σε αυτό. Τέλος, αυτό που είναι σημαντικό να επιτευχθεί είναι ένας κατάλληλος ποιοτικός, αλλά κυρίως ποσοτικός συνδυασμός της επικινδυνότητας του λογισμικού με τα διάφορα κριτήρια ποιότητας που το χαρακτηρίζουν,

όπως είναι για παράδειγμα η αξιοπιστία ή η ασφάλεια, ώστε να παρέχεται στον ενδιαφερόμενο μια πληρέστερη και ακριβέστερη εικόνα του.

Executive Summary

As most organizations are now based much of their operation in information systems, the need for proper security increases. Unfortunately, it is difficult to select the security measures needed to achieve adequate security.

Large amounts of resources spent to avoid failures. However, it is ultimately impossible to guarantee that the IS is perfect, it is also impossible to predict and eliminate anything from the outside world that might threaten the IS.

But what can be achieved is to reduce the likelihood of risk, which will also lead to reduction of uncertainty. Prerequisite for achieving this reduction is the application of appropriate risk management to achieve adequate recognition and effective treatment of various threats to the system.

If risk is seen as the context that refers to political, technical and management factors that threaten a IS or success of software projects, its management is the process of identification and analysis of these threats, quantifying their impact and implementation of projects to be reduce or eliminate the negative consequences.

This thesis deals with risk analysis, procedures and methodologies that identify security problems, the rank based on their importance and then propose solutions to resolve them. It shows the different ways of risk analysis, the main methods used today, the software packages on the market. In the end, carried out a risk analysis application to a multinational R&D Telecommunications company's software NRisk. Through this effort, it seems the value of risk management for software control, while deriving some important factors that directly affect the rate of risk remaining after the completion phase, and an overall risk management process.

More specifically, at the beginning it presents some basic concepts of risk and its management in IS. Then some of the most popular methods of Analysis, Assessment and risk Management in IS are presented and analyzed. Afterwards, we talk about other methods or procedures for better management of software projects in epikyndynotitas. At the end of these presents a tool / process closed code used only in a large company growth and control telecommunications software and how it works.

Listed, ie, a process that manages and monitors risk in the software, the application of which requires a specific policy on the part of those responsible for developing the software, so as to provide a basis for decisions on the admissibility level remaining after controlling risk.

This paper provides a good basis on which it could further research the field resulting from the correlation of the concepts of risk management and control software run at it. Finally, what is important is to achieve an appropriate quality, but rather a combination of quantitative risk of various software quality standards that govern it, such as for example the reliability or safety, to give the person a complete and accurate picture of.

Πίνακας Περιεχομένων

1 Εισαγωγή

Οι αποτυχίες λογισμικού είναι ο εφιάλτης της εποχής της πληροφορίας. Τεράστιες ποσότητες πόρων ξοδεύονται σε όλες τις σχετικές με τη τεχνολογία λογισμικού βιομηχανίες με σκοπό την καταπολέμηση αυτού του εφιάλτη. Παρόλα αυτά, τελικά είναι αδύνατο να υπάρξει η εγγύηση ότι το λογισμικό είναι τέλειο, όπως είναι επίσης αδύνατο να προβλεφθεί και να εξαλειφθεί κάθε τι από τον εξωτερικό κόσμο που πιθανόν να απειλήσει το λογισμικό όσο αυτό εκτελείται.

Αυτό που όμως είναι δυνατό να επιτευχθεί, είναι η μείωση της πιθανότητας αποτυχίας του έργου λογισμικού, η οποία θα επιφέρει και ελάττωση της αβεβαιότητας που ενυπάρχει σε αυτό. Προϋπόθεση για την επίτευξη αυτής της ελάττωσης αποτελεί η εφαρμογή μιας κατάλληλης διαχείρισης επικινδυνότητας καθόλη τη διάρκεια της ανάπτυξης του λογισμικού. Άλλωστε η επικινδυνότητα και η διαχείριση αυτής, έχουν αναδειχθεί σε θέματα μεγάλου ενδιαφέροντος, ιδιαίτερα μάλιστα κατά τη διάρκεια των τελευταίων ετών, όπου έχουν προκύψει νέες προοπτικές και ευκαιρίες, ενώ παράλληλα έχει οξυνθεί και ο ανταγωνισμός στη βιομηχανία λογισμικού.

Οι διάφορες προσεγγίσεις που έχουν κατά καιρούς αναπτυχθεί και εφαρμόζονται, εξετάζουν το θέμα της διαχείρισης της επικινδυνότητας λογισμικού, κατά τη διάρκεια όλων των φάσεων του κύκλου ζωής ανάπτυξης λογισμικού, χωρίς καμία ιδιαίτερη εστίαση σε κάποια συγκεκριμένη φάση. Αυτή η άποψη περί εφαρμογής της διαχείρισης επικινδυνότητας από τη στιγμή που ξεκινά να αναπτύσσεται το λογισμικό, έως τη στιγμή που παραδίδεται και συντηρείται, είναι απόλυτα ορθή και δικαιολογημένη. Διότι σε διαφορετική περίπτωση δεν θα μπορούσε να επιτευχθεί επαρκής αναγνώριση και αποτελεσματική αντιμετώπιση των διαφόρων κινδύνων που απειλούν το σύστημα λογισμικού.

Ο βασικός στόχος της ασφάλειας των πληροφοριακών συστημάτων είναι η στήριξη της αποστολής του οργανισμού. Όλοι οι οργανισμοί εκτίθενται σε αβεβαιότητες, μερικές από τις οποίες έχουν αντίκτυπο στην οργάνωση με ένα αρνητικό τρόπο. Για να υποστηρίξουν την οργάνωση, οι επαγγελματίες της ασφάλειας πρέπει να είναι σε θέση να βοηθήσουν τη διαχείριση των οργανισμών τους με το να κατανοήσουν και να τις διαχειριστούν αυτές τις αβεβαιότητες.

Ο κύριος λόγος για τη διαχείριση κινδύνων σε μια οργάνωση είναι να προστατεύσει την αποστολή και τα περιουσιακά στοιχεία της οργάνωσης. Ως εκ τούτου, η διαχείριση του κινδύνου πρέπει να είναι μια λειτουργία διαχείρισης και όχι τεχνική λειτουργία. Είναι ζωτικής σημασίας για τη διαχείριση των κινδύνων για τα συστήματα. Η κατανόηση των κινδύνων, και ειδικότερα, η κατανόηση των συγκεκριμένων κινδύνων για το σύστημα επιτρέπει στον ιδιοκτήτη του συστήματος για την προστασία του πληροφοριακού συστήματος ανάλογα με την αξία του στην οργάνωση. Το γεγονός είναι ότι όλοι οι οργανισμοί έχουν περιορισμένους πόρους και ο κίνδυνος δεν μπορεί ποτέ να μειωθεί στο μηδέν. Έτσι, η κατανόηση των κινδύνων, ιδίως το μέγεθος του κινδύνου, επιτρέπει στους οργανισμούς να δώσουν προτεραιότητα σε σπάνιους πόρους.

Η διαχείριση των αβεβαιοτήτων που δεν είναι εύκολο έργο. Οι περιορισμένοι πόροι και ένα συνεχώς μεταβαλλόμενο τοπίο των απειλών και των τρωτών σημείων κάνουν αδύνατο τον μετριασμό όλων των κινδύνων. Ως εκ τούτου, οι επαγγελματίες για την ασφάλεια των πληροφοριακών συστημάτων πρέπει να έχουν ένα σύνολο εργαλείων για να ώστε να μοιράζονται μια κοινώς κατανοητή αντίληψη με τους διευθυντές επιχειρήσεων και πληροφοριακών συστημάτων, σχετικά με τις πιθανές επιπτώσεις των διαφόρων σχετικών με την ασφάλεια απειλών για την αποστολή τους. Αυτό το σύνολο εργαλείων πρέπει να είναι σταθερό, επαναλαμβανόμενό, συμφέρον από πλευράς κόστους και να μειώνουν τους κινδύνους σε ένα λογικό επίπεδο.

Η διαχείριση του κινδύνου δεν είναι κάτι καινούργιο. Υπάρχουν πολλά εργαλεία και τεχνικές που διατίθενται για την οργανωτική διαχείριση των κινδύνων. Υπάρχουν ακόμη διάφορα εργαλεία και τεχνικές που εστιάζουν στην διαχείριση των κινδύνων για τα πληροφοριακά συστήματα.

2 Αξιολόγηση, Ανάλυση Επικινδυνότητας και Διαχείριση Κινδύνων στα πληροφοριακά συστήματα

Η διαχείριση του κινδύνου είναι η διαδικασία κατά την οποία προσδιορίζεται ο κίνδυνος, γίνεται η αξιολόγησή του, και λαμβάνονται μέτρα για τη μείωση του κινδύνου σε ένα αποδεκτό επίπεδο. Η προσέγγιση της διαχείρισης κινδύνου καθορίζει τις διαδικασίες, τις τεχνικές, τα εργαλεία, τους ρόλους και τις αρμοδιότητες της ομάδας για ένα συγκεκριμένο έργο. Το σχέδιο διαχείρισης των κινδύνων περιγράφει τον τρόπο που θα είναι δομημένη η διαχείριση του κινδύνου και την εκτέλεση του έργο. Κατά την ανάλυση του κινδύνου βρίσκουμε, αναλύουμε τις επιπτώσεις, τις απειλές και τις αδυναμίες.

Όσον αφορά τα πληροφοριακά συστήματα, η διαχείριση του κινδύνου είναι η διαδικασία της κατανόηση και την αντιμετώπισης των παραγόντων που μπορεί να οδηγήσουν σε αποτυχία της εμπιστευτικότητας, της ακεραιότητας ή της διαθεσιμότητας ενός πληροφοριακού συστήματος. Κίνδυνος, εδώ, για την ασφάλεια είναι η βλάβη σε μια διαδικασία ή οι σχετικές πληροφορίες που προκύπτουν ένα σκόπιμο ή τυχαίο συμβάν που επηρεάζει αρνητικά την διαδικασία ή τις σχετικές πληροφορίες.

2.1 Βασικοί Ορισμοί

2.1.1 Κίνδυνος

Κίνδυνος είναι η δυνητική ζημία που μπορεί να προκύψει από κάποια υφιστάμενη διαδικασία ή από κάποιο μελλοντικό γεγονός. Ο κίνδυνος είναι παρών σε κάθε πτυχή της ζωής μας και πολλοί διαφορετικοί κλάδοι επικεντρώνονται σε αυτόν, δεδομένου ότι εφαρμόζεται σε αυτούς.

Επικινδυνότητα είναι η πιθανότητα μια συγκεκριμένη απειλή να εκμεταλλευτεί μια συγκεκριμένη ευπάθεια. Εναλλακτικά ο κίνδυνος, ο οποίος εκφράζει το ενδεχόμενο για απώλεια, μπορεί να εκφραστεί καλύτερα με την απάντηση των τεσσάρων παρακάτω ερωτήσεων:

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

Στον τομέα της ασφάλειας, ο βασικός τύπος που αποτελεί την ανάλυση της Επικινδυνότητα (Ε) ορίζεται ως το γινόμενο της Πιθανότητας (Π) πραγματοποίησης ενός επεισοδίου ασφάλειας επί το (οικονομικό ή άλλο) Κόστος (Κ) που θα επιφέρει, δηλαδή **Ε=Π*Κ** [1]ή αλλιώς **Β>Ρ*L** όπου Β = Το κόστος για την πρόληψη μιας απώλειας, Ρ = Η πιθανότητα να συμβεί μια απώλεια και L = Το συνολικό κόστος μιας απώλειας.

Κίνδυνος, όπως είπαμε, είναι μια λειτουργία της πιθανότητας μιας συγκεκριμένης απειλής που ασκεί ιδιαίτερη ευπάθεια, καθώς και οι επιπτώσεις του εν λόγω δυσμενούς γεγονότος στην οργάνωση. Το νόημα του τύπου είναι ότι όταν το κόστος της πρόληψης μιας απώλειας είναι μεγαλύτερο από το γινόμενο του κόστους της απώλειας επί την πιθανότητα να συμβεί αυτή τότε η υλοποίηση του μέτρου πρόληψης κρίνεται ως υπερβολική. Στην αντίθετη περίπτωση το μέτρο πρόληψης συμφέρει να υλοποιηθεί. Συνήθως τα μεγέθη υπολογίζονται σε ετήσιες απώλειες και ετήσια πιθανότητα να συμβεί ένα γεγονός. Ο τύπος αυτός αντικατοπτρίζει

[1] **Σωκράτης Κ. Κάτσικας,** *"Ανάλυση, Αποτίμηση και Διαχείριση Επικινδυνότητας Πληροφοριακών Συστημάτων".*

την κεντρική ιδέα πίσω από κάθε ανάλυση κινδύνων, όχι μόνο για πληροφοριακά συστήματα. Την ιδέα του υπολογισμού της πιο συμφέρουσας λύσης.

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

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

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

2.1.2 Απειλή

Ένα μη επιθυμητό γεγονός που μπορεί να προκαλέσει μη διαθεσιμότητα του συστήματος και των υπηρεσιών, τυχαία ή με πρόθεση τη μετατροπή των δεδομένων, την καταστροφή των δεδομένων ή του συστήματος και τέλος μη εξουσιοδοτημένη αποκάλυψη ευαίσθητων πληροφοριών είναι απειλή. Πιο απλά, απειλή είναι το ενδεχόμενο μια πηγή απειλής να ασκήσει (να ενεργοποιηθεί κατά λάθος ή σκόπιμα) μια συγκεκριμένη ευπάθεια. Αν επεκτείνουμε λίγο την έννοια της απειλής, έχουμε την Απειλή-Πηγή (threat-sources). Με τον όρο αυτό εννοούμε είτε την πρόθεση και τη μέθοδο με στόχο την σκόπιμη εκμετάλλευση μιας ευπάθειας ή μια κατάσταση και μια μέθοδο που μπορεί να προκαλέσει κατά λάθος μια ευπάθεια.

Η απειλή είναι απλώς η δυνατότητα για την άσκηση μιας συγκεκριμένης ευπάθειας. Οι ίδιες οι απειλές δεν είναι ενέργειες. Οι απειλές πρέπει να συνδυαστούν με τις απειλές-πηγές για να γίνουν επικίνδυνες. Πρόκειται για μια σημαντική διάκριση, κατά την αξιολόγηση και τη διαχείριση κινδύνων, δεδομένου ότι κάθε απειλή-πηγή μπορεί να σχετίζεται με μια διαφορετική πιθανότητα, η οποία, επηρεάζει την εκτίμηση των κινδύνων και τη διαχείριση τους. Συχνά είναι σκόπιμο να συγκεντρωθούν οι απειλές-πηγές σε απειλές. Κάποιες (αλλά όχι όλες) από τις πιθανές απειλές για τα πληροφοριακά συστήματα είναι οι εξής:

Η Τυχαία Γνωστοποίηση (Accidental Disclosure): Η άνευ αδείας ή τυχαία ελευθέρωση των διαβαθμισμένων, προσωπικών ή ευαίσθητων πληροφοριών.

Οι πράξεις της Φύσης (***Acts of Nature):*** Όλα τα είδη φυσικών φαινομένων (π.χ. σεισμοί, τυφώνες, ανεμοστρόβιλοι) που μπορούν να βλάψουν ή να επηρεάσουν το σύστημα / εφαρμογή. Οποιαδήποτε από αυτές τις πιθανές απειλές θα μπορούσε να οδηγήσει σε μερική ή ολική διακοπή λειτουργίας, επηρεάζοντας έτσι τη διαθεσιμότητα.

Η Τροποποίηση του Λογισμικού (Alteration of Software): Μία εκ προθέσεως τροποποίηση, προσθήκη, διαγραφή του λειτουργικού συστήματος ή των προγραμμάτων του συστήματος εφαρμογής, από εξουσιοδοτημένο χρήστη ή μη, που θέτει σε κίνδυνο το απόρρητο, τη διαθεσιμότητα, ή την ακεραιότητα των δεδομένων, τα προγράμματα, το σύστημα, ή τους πόρους που ελέγχονται από το σύστημα. Αυτό περιλαμβάνει κακόβουλο κώδικα, όπως είναι οι «λογικές βόμβες», οι «δούρειοι ίπποι», οι «καταπακτές», και οι ιοί (logic bombs, Trojan horses, trapdoors, and viruses).

Η Χρήση εύρους ζώνης (Bandwidth Usage): Η τυχαία ή εσκεμμένη χρήση του εύρους ζώνης των επικοινωνιών για άλλους σκοπούς εκτός αυτών για τους οποίους προορίζεται.

Οι Ηλεκτρικές παρεμβολές / Διακοπές (Electrical Interference/Disruption)*:* Μια παρέμβαση ή διακύμανση μπορεί να προκύψει ως αποτέλεσμα μιας διακοπής ρεύματος. Αυτό μπορεί να προκαλέσει άρνηση εξυπηρέτησης στους εξουσιοδοτημένους χρήστες (ανεπάρκεια) ή τροποποίηση των δεδομένων (διακυμάνσεις).

Η Σκόπιμη αλλοίωση των δεδομένων (Intentional Alteration of Data): Μια σκόπιμη τροποποίηση, προσθήκη, ή διαγραφή των δεδομένων, από εξουσιοδοτημένο χρήστη ή μη, θέτει σε κίνδυνο την εμπιστευτικότητα, τη διαθεσιμότητα ή την ακεραιότητα των δεδομένων που παράγονται, μεταποιούνται, ελέγχονται, ή αποθηκεύονται από συστήματα επεξεργασίας δεδομένων.

Το Σφάλμα Ρυθμίσεων του Συστήματος (τυχαία)(System Configuration Error (Accidental): Μια τυχαία λάθος ρύθμιση παραμέτρων κατά την αρχική εγκατάσταση ή αναβάθμιση του υλικού, του λογισμικού, του εξοπλισμού επικοινωνίας ή του λειτουργικού περιβάλλοντος.

Η Δυσλειτουργία / Διακοπή Τηλεπικοινωνιών (Telecommunication Malfunction/Interruption): Κάθε σύνδεση επικοινωνίας, μονάδα ή βλάβη στοιχείου αρκεί για να προκαλέσει διακοπές στη μεταφορά δεδομένων διαμέσων τηλεπικοινωνιών μεταξύ τερματικών ηλεκτρονικών υπολογιστών, απομακρυσμένων ή κατανεμημένων επεξεργαστών, και των τοπικών εγκαταστάσεων υπολογιστών.

2.1.3 Ευπάθεια (Αδυναμία)

Μια αδυναμία ή σχεδιαστική ατέλεια σε ένα σύστημα, εφαρμογή ή υποδομή που μπορεί να γίνει αιτία για την παραβίαση της ασφάλειας και της ακεραιότητας του συστήματος. Ευπάθεια είναι ένα ελάττωμα ή μια αδυναμία στις διαδικασίες ασφάλειας του συστήματος, το σχεδιασμό, την υλοποίηση, ή τους εσωτερικούς ελέγχους που θα μπορούσαν να ασκηθούν (κατά λάθος ή εσκεμμένα) και έχουν ως αποτέλεσμα την παραβίαση της ασφάλειας ή την παραβίαση της πολιτικής ασφάλειας του συστήματος.

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

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

• Να μην έχουν οριστεί με σαφήνεια οδηγίες και διαδικασίες έκτακτης ανάγκης.

• Η έλλειψη ενός δοκιμασμένου, σαφούς, σχεδίου έκτακτης ανάγκης.

• Η απουσία επαρκούς τυπικής εκπαίδευσης έκτακτης ανάγκης.

• Η έλλειψη αντιγράφων ασφαλείας των πληροφοριών (δεδομένων και λειτουργικού συστήματος).

• Οι ανεπαρκείς διαδικασίες ανάκτησης πληροφοριών του συστήματος, για όλους τους χώρους επεξεργασίας (συμπεριλαμβανομένων των δικτύων).

• Η έλλειψη εναλλακτικών τοποθεσιών επεξεργασίας ή αποθήκευσης.

• Η έλλειψη εναλλακτικών υπηρεσιών επικοινωνίας.

2.1.4 Αντίμετρο

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

2.2 Ανάλυση και Αξιολόγηση Κινδύνου

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

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

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

Ένας κίνδυνος αξιολογείται με τον εντοπισμό απειλών και των τρωτών σημείων, στη συνέχεια, με τον προσδιορισμό των πιθανοτήτων και των επιπτώσεων για κάθε κίνδυνο. Δυστυχώς, η εκτίμηση των κινδύνων είναι μια περίπλοκη επιχείρηση, συνήθως βασισμένη σε ελλιπή ενημέρωση (σχήμα 1). Υπάρχουν πολλές μεθοδολογίες με στόχο η επιτρεπόμενη αξιολόγηση των κινδύνων να είναι επαναληφθεί, και να δίνουν συνεπή αποτελέσματα.

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

2.2.1 Ποσοτική αξιολόγηση των κινδύνων

Η *Ποσοτική* εκτίμηση των κινδύνων αξιοποιεί τις μεθοδολογίες που χρησιμοποιούνται από οικονομολογικά ιδρύματα και ασφαλιστικές εταιρείες. Αναθέτοντας τιμές στις πληροφορίες, τα συστήματα, τις επιχειρηματικές διαδικασίες, το κόστος ανάκτησης, κ.λπ., οι επιπτώσεις και επομένως ο κίνδυνος, μπορούν να μετρηθούν από άποψη άμεσων και έμμεσων δαπανών.

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

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

ALE = SLE * ARO[2], όπου SLE (Single Loss Expectancy-Ενιαίο Προσδόκιμο Απώλειας) και ARO (Annualized Rate of Occurrence-Ετησιοποιημένος Ρυθμός εμφάνισης).

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

Ως εκ τούτου, ένα μεγάλο περιθώριο λάθους είναι συνήθως συνυφασμένο με την ποσοτική εκτίμηση του κινδύνου στα πληροφοριακά συστήματα. Αυτό μπορεί να μη συμβαίνει πάντα η στο μέλλον. Δεδομένου ότι το σώμα των στατιστικών στοιχείων είναι διαθέσιμο, οι τάσεις μπορούν να επεκτείνουν την εμπειρία του παρελθόντος. Οι ασφαλιστικές εταιρείες και τα χρηματοοικονομικά ιδρύματα κάνουν άριστη χρήση αυτών των στατιστικών προκειμένου να εξασφαλίσουν ότι η ποσοτική αξιολόγησή του κινδύνου τους έχει νόημα, είναι επαναλαμβανόμενη και συνεπής. Τυπικά, δεν είναι οικονομικά αποδοτική για να εκτελέσει μια ποσοτική εκτίμηση του κινδύνου σε ένα πληροφοριακό σύστημα, λόγω της σχετικής δυσκολίας απόκτησης ακριβών και πλήρη πληροφοριών. Ωστόσο, εάν η πληροφορία θεωρείται αξιόπιστη, μια ποιοτική εκτίμηση κινδύνου αποτελεί ένα εξαιρετικά ισχυρό εργαλείο για την ανακοίνωση του κινδύνου σε όλα τα επίπεδα της διοίκησης. Η Ποσοτική μέτρηση του κινδύνου είναι η τυπική.

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

1) οι δυσκολίες στον προσδιορισμό και την απόδοση αξίας των κεφαλαίων, και

2) η έλλειψη στατιστικών πληροφοριών που θα καθιστούσαν δυνατό τον προσδιορισμό της συχνότητας.

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

2.2.2 Ποιοτική αξιολόγηση των κινδύνων

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

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

Τα βήματα της ποιοτικής αξιολόγησης των κινδύνων είναι τα ακόλουθα:

[2] **Steve, Elky**. "*An Introduction to Information System Risk Management".* May 31, 2006

2.2.2.1 Εντοπισμός Απειλών

Τόσο οι πηγές των απειλών όσο και οι απειλές πρέπει να εντοπιστούν. Οι απειλές πρέπει να περιλαμβάνουν τις πηγές για να εξασφαλιστεί η ακριβής εκτίμηση. Μερικές κοινές πηγές απειλών περιλαμβάνουν:

• **Φυσικές απειλές:** πλημμύρες, σεισμοί, τυφώνες

• **Ανθρώπινες Απειλές:** απειλές που προκαλούνται από τον άνθρωπο, συμπεριλαμβανομένων τόσο των ακούσιων (Ακούσια εισαγωγή δεδομένων) όσο και των σκόπιμων ενεργειών (επιθέσεις στο δίκτυο, προσβολή από τον ιό, πρόσβαση χωρίς άδεια)

• **Περιβαλλοντικές Απειλές:** διακοπή ρεύματος, ρύπανση, χημικές ουσίες, η ζημία των υδάτων.

Τα άτομα που καταλαβαίνουν την οργάνωση, τη βιομηχανία ή τον τύπο του συστήματος (ή ακόμη καλύτερα και τα τρία) είναι βασικά για τον εντοπισμό απειλών. Μόλις ο γενικός κατάλογος των απειλών συνταχθεί, οι γνώστες του συστήματος, της οργάνωσης ή της βιομηχανίας τον αναθεωρούν και συντάσσουν ένα κατάλογο απειλών που ισχύει για το σύστημα.

Είναι χρήσιμο να συνταχθεί ένας κατάλογος απειλών που υπάρχουν σε όλη την οργάνωση και να χρησιμοποιηθεί ως βάση για όλες τις δραστηριότητες διαχείρισης κινδύνου. Καθώς ένας σημαντικός παράγοντας της διαχείρισης του κινδύνου είναι το να εξασφαλίζει τη συνοχή και την επαναληψιμότητα, η χρησιμότητα οργανωτική λίστα απειλών είναι ανεκτίμητη.

2.2.2.2 Εντοπισμός Αδυναμιών

Οι αδυναμίες μπορούν να προσδιοριστούν με πολλούς τρόπους. Διάφορα συστήματα διαχείρισης των κινδύνων προσφέρουν διαφορετικές μεθοδολογίες για τον προσδιορισμό των αδύναμων σημείων. Αρχικά, ξεκινάμε με κοινούς καταλόγους αδυναμιών ή περιοχές ελέγχου. Στη συνέχεια, σε συνεργασία με τους ιδιοκτήτες του συστήματος ή άλλων προσώπων με γνώση του συστήματος ή του οργανισμού, εντοπίζουμε τα τρωτά σημεία που ισχύουν για το σύστημα. Ειδικά τρωτά σημεία μπορούν να βρεθούν μέσω της αναθεώρησης των ιστοσελίδων των προμηθευτών και των δημοσίων αρχείων των τρωτών σημείων, όπως Common Vulnerabilities and Exposures (CVE) ή το National Vulnerability Database (NVD).

Επιπλέον, ενώ τα ακόλουθα εργαλεία και τεχνικές χρησιμοποιούνται συνήθως για την αξιολόγηση της αποτελεσματικότητα των ελέγχων, μπορούν επίσης να χρησιμοποιηθούν για τον εντοπισμό των αδύναμων σημείων:

• **Σαρωτές Ευπάθειας** - Λογισμικό που μπορεί να εξετάσει ένα λειτουργικό σύστημα, μια δικτυακή εφαρμογή ή έναν κώδικα για γνωστά ελαττώματα, συγκρίνοντας το σύστημα (ή το σύστημα απαντά σε γνωστά ερεθίσματα) με μια βάση δεδομένων ελαττωματικών υπογραφών.

• **Δοκιμή Εισχώρησης** - Μια προσπάθεια από τις αναλυτές ασφαλείας να ασκήσουν τις απειλές κατά του συστήματος. Αυτό περιλαμβάνει επιχειρησιακές αδυναμίες, όπως είναι η κοινωνική μηχανική.

• **Έλεγχος των λειτουργικών και διαχειριστικών ελέγχων** - Μια εμπεριστατωμένη επανεξέταση των επιχειρησιακών ελέγχων και των ελέγχων διαχείρισης μέσω της σύγκριση της τρέχουσας τεκμηρίωσης με τις βέλτιστες πρακτικές (όπως η ISO 17799) και από τη σύγκριση των πραγματικών πρακτικών έναντι των τρεχουσών τεκμηριωμένων διαδικασιών.

Είναι πολύτιμο να έχουμε μια βασική λίστα των τρωτών σημείων που λαμβάνονται πάντα υπ' όψιν κατά τη διάρκεια κάθε αξιολόγησης κινδύνων σε μια οργάνωση. Η πρακτική αυτή εξασφαλίζει ένα τουλάχιστον ελάχιστο επίπεδο συνεκτικότητας μεταξύ των εκτιμήσεων επικινδυνότητας. Επιπλέον, οι αδυναμίες που διαπιστώθηκαν κατά τις προηγούμενες αξιολογήσεις του συστήματος θα πρέπει να περιλαμβάνονται σε όλες τις μελλοντικές εκτιμήσεις. Κάνοντας αυτό επιτρέπει στη διοίκηση να κατανοήσουν ότι οι προηγούμενες δραστηριότητες διαχείρισης κινδύνου ήταν αποτελεσματικές.

2.2.2.3 Σχέση Απειλών - Αδυναμιών

Μια από τις πιο δύσκολες δραστηριότητες της διαδικασίας διαχείρισης κινδύνου είναι η συσχέτιση μιας απειλής με μια αδυναμία. Παρ 'όλα αυτά, η θέσπιση αυτών των σχέσεων είναι μια υποχρεωτική δραστηριότητα, αφού ο κίνδυνος ορίζεται ως η άσκηση της απειλής κατά της αδυναμίας. Αυτό ονομάζεται συχνά αντιστοίχιση απειλής-ευπάθειας (T-V). Υπάρχουν πολλές τεχνικές για την εκτέλεση αυτού του καθήκοντος.

Δεν μπορεί κάθε απειλή να ασκηθεί εναντίον κάθε ευπάθειας. Για παράδειγμα, μια απειλή της «πλημμύρας» προφανώς ισχύει και για μια αδυναμία «έλλειψης σχεδιασμού έκτακτης ανάγκης», αλλά όχι σε μια ευπάθεια «αδυναμίας αλλαγής προεπιλεγμένων επικυρωτών.

Αν και λογικά φαίνεται ότι ένα τυποποιημένο σύνολο ζευγών απειλής-ευπάθειας θα ήταν ευρέως διαθέσιμα και χρησιμοποιούμενα. Παρόλα αυτά, δεν είναι εύκολα διαθέσιμα. Αυτό μπορεί να οφείλεται στο γεγονός ότι οι απειλές και ειδικότερα οι αδυναμίες συνεχώς ανακαλύπτονται και ότι τα ζεύγη απειλής-ευπάθειας θα αλλάζουν αρκετά συχνά.

Παρ 'όλα αυτά, ένας οργανωτικός πρότυπος κατάλογο των ζευγών θα πρέπει να θεσπιστεί και να χρησιμοποιηθεί ως αρχική τιμή. Η ανάπτυξη του καταλόγου ζευγών απειλής-ευπάθειας επιτυγχάνεται με την αναθεώρηση του καταλόγου αδυναμιών και την αντιστοίχιση μιας αδυναμίας σε κάθε απειλή που εφαρμόζεται, στη συνέχεια, και εξασφαλίζοντας ότι όλα τα τρωτά σημεία στα οποία η απειλή θα μπορούσε να ενεργήσει ενάντια έχουν εντοπιστεί. Για κάθε σύστημα, ο τυποποιημένος κατάλογος ζευγών απειλής-ευπάθειας θα πρέπει να προσαρμόζεται στη συνέχεια.

2.2.2.4 Καθορισμός Πιθανοτήτων

Ο καθορισμός των πιθανοτήτων είναι αρκετά απλός. Είναι η πιθανότητα μια απειλή που προκαλείται από απειλή-πηγή να συμβεί ενάντια σε ένα θέμα ευπάθειας. Προκειμένου να διασφαλίσει ότι οι εκτιμήσεις κινδύνου είναι συνεπείς, μπορεί να χρησιμοποιηθεί ένας τυπικός ορισμός της πιθανότητας για κάθε αξιολόγηση κινδύνου.

Το πιο σημαντικό πράγμα είναι να βεβαιωθούμε ότι η ορισμοί είναι σταθερά χρησιμοποιούμενοι, έχουν κοινοποιηθεί σαφώς, συμφωνήθηκαν και έγιναν κατανοητοί από την ομάδα εκτέλεση της αξιολόγησης και με την οργανωτική διαχείριση.

2.2.2.5 Καθορισμός Επιπτώσεων

Για να εξασφαλιστεί η επαναληψιμότητα, η επίπτωση ορίζεται καλύτερα από άποψη επιπτώσεων ανάλογα με τη διαθεσιμότητα, επιπτώσεις για την αξιοπιστία και τον αντίκτυπο επί εμπιστευτικότητας. Ο Πίνακας 1 απεικονίζει μια εφικτή προσέγγιση για την αξιολόγηση των επιπτώσεων, εστιάζοντας την προσοχή στις τρεις πτυχές της ασφάλειας των πληροφοριών. Ωστόσο, για να έχουν νόημα, να είναι επαναχρησιμοποιήσιμα και εύκολα ανακοινώσιμα, θα πρέπει να γίνονται συγκεκριμένες αξιολογήσεις για το σύνολο του οργανισμού.

	Εμπιστευτικότητα	Ακεραιότητα	Διαθεσιμότητα
Χαμηλός (Low)	Απώλεια του απορρήτου οδηγεί σε περιορισμένα αποτελέσματα σχετικά με την οργάνωση	Η απώλεια της ακεραιότητας οδηγεί σε περιορισμένο αντίκτυπο στην οργάνωση.	Απώλεια της διαθεσιμότητας οδηγεί σε περιορισμένο αντίκτυπο στην οργάνωση.
Μέτριος (Moderate)	Απώλεια του απορρήτου οδηγεί σε σοβαρά αποτελέσματα σχετικά με την οργάνωση	Η απώλεια της ακεραιότητας οδηγεί σε σοβαρό αντίκτυπο στην οργάνωση.	Απώλεια της διαθεσιμότητας οδηγεί σε σοβαρό αντίκτυπο στην οργάνωση.
Υψηλός (High)	Απώλεια του απορρήτου οδηγεί σε πολύ σοβαρά αποτελέσματα σχετικά με την οργάνωση	Η απώλεια της ακεραιότητας οδηγεί σε πολύ σοβαρό αντίκτυπο στην οργάνωση.	Απώλεια της διαθεσιμότητας οδηγεί σε πολύ σοβαρό αντίκτυπο στην οργάνωση.

Πίνακας 1: Δείγμα Καθορισμού των Επιπτώσεων

2.2.2.6 Αξιολόγηση Κινδύνων

Η εκτίμηση κινδύνου είναι η διαδικασία προσδιορισμού της πιθανότητας η απειλή να ασκηθεί κατά της ευπάθεια και των συνακόλουθων επιπτώσεων από ένα επιτυχή συμβιβασμό. Κατά την αξιολόγηση των πιθανοτήτων και των επιπτώσεων, πρέπει να λαμβάνεται υπόψη το τρέχον περιβάλλον των απειλών και των ελέγχων. Οι πιθανότητες και οι επιπτώσεις αξιολογούνται για το σύστημα όπως λειτουργεί κατά τη στιγμή της αξιολόγησης. Το δείγμα Πίνακα Προσδιορισμού των κινδύνων που φαίνεται στον Πίνακα 2 μπορεί να χρησιμοποιηθεί για να αξιολογηθεί ο κίνδυνος κατά τη χρήση συστήματος αξιολόγησης τριών επιπέδων.

		Επιπτώσεις		
		Υψηλός (High)	Μέτριος (Moderate)	Χαμηλός (Low)
Πιθανότητα	Υψηλός (High)	Υψηλός (High)	Υψηλός (High)	Μέτριος (Moderate)
	Μέτριος (Moderate)	Υψηλός (High)	Μέτριος (Moderate)	Χαμηλός (Low)
	Χαμηλός (Low)	Μέτριος (Moderate)	Χαμηλός (Low)	Χαμηλός (Low)

Πίνακας 2: Δείγμα Πίνακα Προσδιορισμού των Κινδύνων

Σε μια ποιοτική αξιολόγηση του κινδύνου, είναι καλύτερα να μην χρησιμοποιούνται αριθμοί κατά την εκτίμηση του κινδύνου. Τα διευθυντικά στελέχη, ιδιαίτερα τα στελέχη υψηλότερου επιπέδου που λαμβάνουν αποφάσεις σχετικά με την κατανομή των πόρων, συχνά λαμβάνουν μεγαλύτερη ακρίβεια από αυτή που μεταφέρεται στην πραγματικότητα κατά την επανεξέταση της έκθεσης της αξιολόγησης του κινδύνου που περιέχει αριθμητικές τιμές. Σε μια ποιοτική αξιολόγηση του κινδύνου, η πιθανότητα και η οι τιμές των επιπτώσεων βασίζονται στις βέλτιστες διαθέσιμες πληροφορίες, οι οποίες δεν είναι συνήθως καλά θεμελιωμένες σε τεκμηριωμένα προηγούμενα περιστατικά.

Η ποιοτική ανάλυση δεν προσπαθεί να δώσει ακριβείς αριθμητικές τιμές στις συνιστώσες της ανάλυσης κινδύνου. Αντιθέτως αρκείται να τις χαρακτηρίζει με εκφράσεις όπως πχ. μεγάλο, μέτριο, μικρό ή να δίνει τιμές από μια προαποφασισμένη κλίμακα. Με την λογική αυτή παρακάμπτονται οι πολύπλοκοι υπολογισμοί. Αν και οι κίνδυνοι δεν υπολογίζονται επακριβώς, επιτυγχάνεται η ταξινόμηση τους και επομένως η προτεραιότητα για την αντιμετώπιση τους. Η ποιοτική ανάλυση βασίζεται στην εμπειρία των ανθρώπων που συμμετέχουν για τον προσδιορισμό των κινδύνων. Πρόκειται προφανώς για μια υποκειμενική μέθοδο. Προσπαθεί να εκμεταλλευτεί την γνώση των ατόμων που συμμετέχουν ώστε να φτάσει σε αποδεκτά προσεγγιστικά αποτελέσματα στον ελάχιστο δυνατό χρόνο και με την ελάχιστη προσπάθεια, παρακάμπτοντας το πολύπλοκο μαθηματικό κομμάτι της ανάλυσης. Έχει αποδειχτεί με τον καιρό ότι η ποιοτική ανάλυση παράγει ικανοποιητικά αποτελέσματα όταν τα άτομα που συμμετέχουν έχουν την απαιτούμενη γνώση και εμπειρία για το πληροφοριακό σύστημα που εξετάζεται.

Η έννοια του να μην παρέχεται πλέον granularity στις εκθέσεις αξιολόγησης των κινδύνων απ' ότι ήταν διαθέσιμη κατά τη διάρκεια της διαδικασίας αξιολόγησης είναι κατά προσέγγιση ανάλογη με τη χρήση δεκαδικών ψηφίων στη φυσική και τη χημεία. Χοντρικά, σημαντικά ψηφία είναι τα ψηφία που είναι αξιόπιστη σε μια μέτρηση. Ως εκ τούτου, είναι αδύνατο να έχουμε περισσότερη ακρίβεια στο αποτέλεσμα από ό, τι ήταν διαθέσιμη από τα αρχικά δεδομένα. Ακολουθώντας αυτή τη λογική, αν η πιθανότητα και οι επιπτώσεις αξιολογήθηκαν σε Χαμηλή, Μέτρια, Υψηλή βάση, ο κίνδυνος θα είναι επίσης Ήπιος, Μέτριος ή Υψηλός.

Εάν η έκθεση αξιολόγησης κινδύνων, δεν επικοινωνεί με σαφήνεια το κατάλληλο επίπεδο διακριτότητας, ο αριθμός των επιπτώσεων και τα επίπεδα διαβάθμισης της πιθανότητας θα πρέπει να αυξηθούν. Ορισμένοι οργανισμοί προτιμούν τη χρήση τεσσάρων ή ακόμη και πέντε επίπεδων διαβάθμιση των επιπτώσεων και πιθανοτήτων. Ωστόσο, οι ατομικές επιπτώσεις και τα επίπεδα κινδύνου πρέπει να ορίζονται ακόμη συνοπτικά.

Στην πραγματικότητα οι περισσότερες τεχνικές που χρησιμοποιούνται σήμερα είναι μια μίξη ποσοτικής και ποιοτικής ανάλυσης. Τον χαρακτηρισμό ποιοτική ή ποσοτική ανάλυση την παίρνουν ανάλογα με ποια ανάλυση προσεγγίζουν καλύτερα.

Κατά τη διεξαγωγή της ανάλυσης των επιπτώσεων, το κύριο πλεονέκτημα της ποιοτικής ανάλυσης του αντίκτυπου είναι ότι δίνει προτεραιότητα στους κινδύνους και προσδιορίζει τους τομείς για την άμεση βελτίωση στην αντιμετώπιση των τρωτών σημείων. Το μειονέκτημα της ποιοτικής ανάλυσης είναι ότι δεν παρέχει συγκεκριμένες ποσοτικές μετρήσεις του μεγέθους των επιπτώσεων, ως εκ τούτου μια ανάλυση κόστους-οφέλους των συνιστώμενων ελέγχων είναι δύσκολη.

Το σημαντικότερο πλεονέκτημα μιας ποσοτικής ανάλυσης του αντίκτυπου είναι ότι παρέχει μια μέτρηση του μεγέθους των επιπτώσεων, η οποία μπορεί να χρησιμοποιηθεί για την ανάλυση κόστους-οφέλους των συνιστώμενων ελέγχων. Το μειονέκτημα είναι ότι, ανάλογα με τις αριθμητικές κλίμακες που χρησιμοποιούνται για να εκφράσουν τη μέτρηση, την έννοια της ποσοτικής ανάλυσης των επιπτώσεων ενδέχεται να είναι ασαφής, απαιτώντας το αποτέλεσμα να ερμηνεύεται κατά τρόπο ποιοτικό. Πρόσθετοι παράγοντες συχνά πρέπει να θεωρηθεί ότι καθορίζουν το εύρος των επιπτώσεων.

Στον παρακάτω πίνακα φαίνονται συγκεντρωτικά τα πλεονεκτήματα και τα μειονεκτήματα της ποιοτικής και ποσοτικής ανάλυσης:

	Πλεονεκτήματα	Μειονεκτήματα
Ποσοτική Ανάλυση των Κινδύνων	Τα αποτελέσματα έχουν το κύρος της μαθηματικής απόδειξης	Οι υπολογισμοί μπορεί να είναι πολύπλοκοι
	Τα αποτελέσματα μπορούν να εκφραστούν σε γλώσσα κατανοητή από τους διαχειριστές (managers) του οργανισμού	Η ανάλυση χρειάζεται πολύ χρόνο για να ολοκληρωθεί
	Η ανάλυση κόστους/οφέλους (cost/benefit) είναι πιο εύκολη και άμεση	Χρειάζεται μεγάλη ποσότητα προκαταρτικής εργασίας
	Η αξία των περιουσιακών στοιχείων του πληροφοριακού συστήματος (όσον αφορά την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα) γίνεται καλύτερα κατανοητή όταν εκφράζεται σε χρηματικά ποσά. Αυτό βοηθάει στην μεγαλύτερη αποδοχή της ασφάλειας	Η καθοδήγηση των συμμετεχόντων στην ανάλυση δεν μπορεί να γίνει εύκολα. Έτσι συνήθως χρειάζεται η συμμετοχή έμπειρων στην ποσοτική ανάλυση ατόμων
		Ιστορικά, η ποσοτική ανάλυση λειτουργεί καλά μόνο με την χρήση κάποιου αυτοματοποιημένου εργαλείου συνδεδεμένου με μια γνωστική βάση (knowledge base).

Ποιοτική Ανάλυση των Κινδύνων	Αποφεύγονται πολύπλοκοι υπολογισμοί	Είναι υποκειμενικής φύσεως
	Δεν είναι απαραίτητος ο αριθμητικός υπολογισμός της αξίας των κεφαλαίων	Δεν γίνεται μεγάλη προσπάθεια για την αναγνώριση της αντικειμενικής αξίας των κεφαλαίων. Έτσι, η αντίληψη της αξίας μπορεί να μην αντικατοπτρίζει την πραγματική αξία κατά τον υπολογισμό του κινδύνου.
	Είναι ευκολότερη η συμμετοχή ατόμων που δεν έχουν σχέση με την ασφάλεια και την πληροφορική.	Η ποιότητα των αποτελεσμάτων βασίζεται εξ' ολοκλήρου στην γνώση και την εμπειρία των ατόμων που συμμετέχουν στην ανάλυση
	Η ποιοτική ανάλυση χρειάζεται λιγότερο χρόνο και λιγότερους πόρους σε σχέση με την ποσοτική	Η ανάλυση κόστους/οφέλους (cost/benefit) δεν βασίζεται σε μαθηματική απόδειξη
	Η διαδικασία της ανάλυσης είναι πιο ευέλικτη	

Πίνακας 3: Πλεονεκτήματα και Μειονεκτήματα της ποσοτικής και ποιοτικής ανάλυσης.

2.3 Διαχείριση Κινδύνου

Η *Διαχείριση Κινδύνων (Risk Management)* περιλαμβάνει τρεις διαδικασίες: εκτίμηση των κινδύνων, μείωση των κινδύνων, και την αξιολόγηση:

Η διαδικασία εκτίμησης κινδύνου περιλαμβάνει τον προσδιορισμό και την αξιολόγηση των κινδύνων και των επιπτώσεων των κινδύνων, καθώς και τη σύσταση της μείωσης του κινδύνου μέτρων.

Η μετρίαση του κινδύνου αναφέρεται στην καθορισμό προτεραιοτήτων, την εκτέλεση και τη διατήρηση των κατάλληλων μέτρων μείωσης των κινδύνων που συνιστώνται από την διαδικασία αξιολόγησης του κινδύνου.

Η συνεχή διαδικασία αξιολόγησης και τα κλειδιά για την εφαρμογή ενός επιτυχημένου προγράμματος διαχείρισης κινδύνων.

Η *Διαχείριση Κινδύνων (Risk Management)* είναι η διαδικασία που επιτρέπει στους διαχειριστές να εξισορροπήσουν τα λειτουργικά και οικονομικά κόστη των μέτρων προστασίας και να πετύχουν κέρδη για τη δυνατότητα της αποστολής με το να προστατεύουν τα Πληροφοριακά συστήματα και τα δεδομένων που υποστηρίζουν τις αποστολές των οργανώσεών τους. Η διαδικασία αυτή δεν είναι μοναδική στον κλάδο των Πληροφοριακών συστημάτων.

Η *Εκτίμηση Κινδύνων (Risk Assessment)* είναι η πρώτη διαδικασία στην μεθοδολογία διαχείρισης κινδύνων. Οι διάφοροι οργανισμοί χρησιμοποιούν την εκτίμηση κινδύνων για να καθορίσουν την έκταση των δυνητικών απειλών και των κινδύνων που συνδέονται με ένα πληροφοριακό σύστημα σε όλο τον κύκλο ζωής του. Το αποτέλεσμα αυτής της διαδικασίας βοηθά στον εντοπισμό κατάλληλων ελέγχων για τη μείωση ή την εξάλειψη των κινδύνων κατά τη διάρκεια της διαδικασίας μείωσης τους.

Για να προσδιοριστεί η πιθανότητα μιας μελλοντικά ανεπιθύμητης ενέργειας, οι απειλές για ένα πληροφοριακό σύστημα θα πρέπει να αναλυθούν σε συνδυασμό με τις αδυναμίες και τους ελέγχους σε ισχύ για το πληροφοριακό σύστημα. Με τον όρο *Επιπτώσεις* αναφερόμαστε στο μέγεθος της βλάβης που θα μπορούσε να προκληθεί από την άσκηση μιας απειλή για μια ευπάθειας. Το επίπεδο του αντίκτυπου διέπεται από τις δυνητικές επιπτώσεις της αποστολής και στη συνέχεια παράγει μια σχετική τιμή για τις επιπτώσεις του πληροφοριακού συστήματος στο κεφάλαιο και τους πόρους.

Εν ολίγοις, η επιτυχής και αποτελεσματική διαχείριση των κινδύνων αποτελεί τη βάση της επιτυχούς και αποτελεσματικής ασφάλειας των πληροφοριακών συστημάτων. Λόγω της πραγματικότητας των περιορισμένων πόρων και σχεδόν απεριόριστων απειλών, πρέπει να ληφθεί μια λογική απόφαση σχετικά με την κατανομή των πόρων για την προστασία των συστημάτων. Οι πρακτικές διαχείρισης κινδύνου επιτρέπουν στην οργάνωση να προστατεύσει τις πληροφορίες και τις επιχειρηματικές της διαδικασίες ανάλογα με την αξία τους. Για να εξασφαλιστεί η μέγιστη τιμή της διαχείρισης των κινδύνων, πρέπει να είναι συνεπής και επαναλαμβανόμενη, ενώ εστιάζει στην μετρήσιμη μείωση του κινδύνου. Η καθιέρωση και η χρήση μιας αποτελεσματικής, υψηλής ποιότητας διαδικασία διαχείρισης κινδύνων και με βάση τις δραστηριότητες ενός οργανισμού για την ασφάλεια των πληροφοριών του σχετικά με τη διαδικασία αυτή οδηγούν σε μια αποτελεσματικό πρόγραμμα ασφάλειας των πληροφοριών του οργανισμού.

2.3.1 Διαχείριση Κινδύνων στα πληροφοριακά συστήματα

Ο σκοπός της αξιολόγησης κινδύνου είναι να βοηθήσει τη διαχείριση στον καθορισμό του που να κατευθύνει τους πόρους. Υπάρχουν τέσσερις βασικές στρατηγικές για τη διαχείριση κινδύνων: μετριασμός, μεταβίβαση, αποδοχή και τη αποφυγή.

Στην έκθεση αξιολόγησης κινδύνων, πρέπει να σχεδιαστεί μια στρατηγική διαχείρισης κινδύνου που να μειώνει τον κίνδυνο σε αποδεκτό επίπεδο για το αποδεκτό κόστος για κάθε κίνδυνο. Για κάθε στρατηγική διαχείρισης κινδύνων, πρέπει επίσης να καθοριστούν το κόστος που συνδέεται με τη στρατηγική και τα βασικά βήματα για την υλοποίηση της στρατηγικής της (γνωστό ως Σχέδιο Δράσης & Σταθμοί ή POAM).

2.3.1.1 Μετριασμός

Ο Μετριασμός είναι η πιο συχνή στρατηγική διαχείρισης κινδύνων. Ο μετριασμός περιλαμβάνει τον καθορισμό των αδυναμιών ή την παροχή κάποιου είδους αντισταθμιστικού ελέγχου για τη μείωση της πιθανότητας ή των επιπτώσεων που συνδέονται με την αδυναμία. Μια κοινή μείωση για μια τεχνική αδυναμία ασφαλείας είναι η εγκατάσταση ενός «μπαλώματος» (patch) που παρέχεται από τον πωλητή. Μερικές φορές η διαδικασία καθορισμού των στρατηγικών για το μετριασμό των επιπτώσεων ονομάζεται *ανάλυση ελέγχου*.

2.3.1.2 Μεταβίβαση

Μεταβίβαση είναι η διαδικασία που επιτρέπει σε ένα άλλο μέρος να αποδεχθεί τον κίνδυνο για λογαριασμό μας. Αυτό είναι δεν γίνεται ευρέως για τα συστήματα πληροφορικής, αλλά ο καθένας το κάνει όλη την ώρα στην προσωπική του ζωή. Το αυτοκίνητο, η υγεία και η ασφάλιση ζωής είναι όλα τρόποι μεταφοράς των κινδύνων. Στις περιπτώσεις αυτές, ο κίνδυνος μεταφέρεται από το άτομο σε ένα σύνολο κατόχων, συμπεριλαμβανομένων της ασφαλιστικής εταιρείας. Αυτό δε σημαίνει ότι έτσι μειώνονται οι πιθανότητες ή διορθώνονται τυχόν ατέλειες, αλλά μειώνει τον συνολικό αντίκτυπο (κυρίως οικονομικό) στον οργανισμό.

2.3.1.3 Αποδοχή

Αποδοχή είναι η πρακτική όπου απλά επιτρέπεται στο σύστημα να λειτουργεί με ένα γνωστό κίνδυνο. Πολλοί χαμηλοί κίνδυνοι είναι απλά αποδεκτοί. Οι κίνδυνοι που έχουν εξαιρετικά υψηλό κόστος για τον περιορισμό είναι επίσης συχνά αποδεκτοί. Πρέπει να δίνεται

προσοχή οι υψηλοί κίνδυνοι να γίνουν αποδεκτοί από τη διοίκηση. Πρέπει να διασφαλιστεί ότι η στρατηγική αυτή είναι γραπτή και έχει γίνει αποδεκτή από τους διαχειριστές που λαμβάνουν τις αποφάσεις. Συχνά οι κίνδυνοι γίνονται αποδεκτοί ενώ δε θα έπρεπε, και στη συνέχεια, όταν η εισχώρηση του συμβαίνει, το προσωπικό ασφαλείας ΤΠ είναι υπεύθυνο. Τυπικά, οι διευθυντές επιχειρήσεων, όχι το προσωπικό ασφαλείας ΤΠ, είναι εξουσιοδοτημένοι να αποδέχονται τον κίνδυνο για λογαριασμό ενός οργανισμού.

2.3.1.4 Αποφυγή

Αποφυγή είναι η πρακτική αφαίρεσης των ευάλωτων πτυχών του συστήματος ή ακόμα και το ίδιο το σύστημα. Για παράδειγμα, κατά τη διάρκεια της αξιολόγησης των κινδύνων, ένας δικτυακός τόπος αποκαλύφθηκε ότι αφήνει τους πωλητές να δουν τα τιμολόγια, χρησιμοποιώντας ένα αναγνωριστικό προμηθευτή ενσωματωμένο στο όνομα του αρχείου HTML ως ταυτότητα και όχι ως πιστοποίηση ή εξουσιοδότηση ανά πωλητή. Όταν ενημερώνονται για τις ιστοσελίδες και τον κίνδυνο στον οργανισμό, η διαχείριση αποφασίζει να αφαιρέσει τις ιστοσελίδες και να παρέχει τα τιμολόγια στον πωλητή μέσω άλλου μηχανισμού. Στην περίπτωση αυτή, ο κίνδυνος απεφεύχθη με την αφαίρεση των ευάλωτων ιστοσελίδων.

2.3.1.5 Γνωστοποίηση των κινδύνων και στρατηγικών διαχείρισης κινδύνου

Ο κινδύνου πρέπει επίσης να γνωστοποιείται. Μόλις ο κίνδυνος γίνει κατανοητός, οι κίνδυνοι και οι στρατηγικές διαχείρισης κινδύνου πρέπει να γνωστοποιηθούν στη διαχείριση του οργανισμού, με εύκολα κατανοητή διατύπωση. Οι διευθυντές είναι συνηθισμένοι στη διαχείριση κινδύνων, το κάνουν κάθε μέρα. Άρα το κλειδί είναι να παρουσιαστούν οι κίνδυνοι κατά τρόπο που θα καταλάβουν. Δε πρέπει να χρησιμοποιηθεί ο «φόβος, η αβεβαιότητα και η αμφιβολία». Αντί αυτού, πρέπει να παρουσιαστεί ο κίνδυνος όσον αφορά τις πιθανότητες και τις επιπτώσεις. Όσο πιο συγκεκριμένοι είναι οι όροι, τόσο πιο πιθανό είναι η οργανωτική διαχείριση να κατανοήσει και να αποδεχτεί τα πορίσματα και τις συστάσεις.

Με μια ποσοτική μεθοδολογία αξιολόγησης του κινδύνου, οι αποφάσεις της διαχείρισης του κινδύνου βασίζονται κατά κανόνα στη σύγκριση του κόστους του κινδύνου έναντι του κόστους της στρατηγική διαχείρισης κινδύνων. Η επιστροφή στην ανάλυση επενδύσεων είναι ένα ισχυρό εργαλείο για να συμπεριληφθεί στην έκθεση αξιολόγησης κινδύνων. Αυτό είναι ένα εργαλείο που χρησιμοποιείται ευρέως στις επιχειρήσεις για να δικαιολογήσουν τη λήψη ή μη λήψη ορισμένων μέτρων. Οι διευθυντές είναι πολύ εξοικειωμένοι με τη χρήση ROI (Return On Investment) για τη λήψη αποφάσεων.

Με μια ποιοτική μεθοδολογία εκτίμησης κινδύνου, η δουλειά είναι κάπως πιο δύσκολη. Ενώ το κόστος των στρατηγικών είναι συνήθως γνωστό, το κόστος της μη εφαρμογής των στρατηγικών δεν είναι, κι αυτός είναι ο λόγος που έγινε μια ποιοτική και όχι ποσοτική εκτίμηση των κινδύνων. Συμπεριλαμβανομένου μιας φιλικής ως προς την διαχείριση περιγραφής των επιπτώσεων και της πιθανότητας με κάθε κίνδυνο, η στρατηγική διαχείρισης κινδύνου είναι εξαιρετικά αποτελεσματική . Μια άλλη αποτελεσματική στρατηγική παρουσιάζει τον υπολειπόμενο κίνδυνο που θα είναι αποτελεσματικός αφού τεθεί σε ισχύ η στρατηγική διαχείρισης κινδύνων.

Κίνδυνος	Περιγραφή Κινδύνου	Επιπτώσεις	Πιθανότητα	Στρατιγική Διαχείρισης Κινδύνου	Κόστος	Υπολειπόμενος Κίνδυνος μετά την εφαρμογή της Στρατηγικής Διαχείρισης Κινδύνου
Μέτριος	Η αποτυχία στο περιβαλλοντικό σύστημα (π.χ. κλιματισμός) καθιστά το σύστημα μη διαθέσιμο.	Η αποτυχία στον περιβαλλοντικό έλεγχο θα μπορούσε να καταστίσει το σύστημα μη διαθέσιμο για περισσότερες από 48 ώρες	Το παρελθόν των δεδομένων υποδεικνύει ότι αυτό συμβαίνει 1-2 φορές ετησίως	Εφαρμογή ενός εφεδρικού σε κάποια άλλη τοποθεσία	250.000 ευρώ	Χαμηλός

Πίνακας 4: Δείγμα Πίνακα Διαχείρισης Κινδύνου

2.3.1.6 Εφαρμογή στρατηγικών διαχείρισης κινδύνου

Ένα Σχέδιο Δράσης & Οροσήμων (Plan Of Action & Milestones - POAM) θα πρέπει να αποτελεί μέρος της έκθεσης αξιολόγησης κινδύνου που παρουσιάζεται στη διαχείριση. Το POAM είναι ένα εργαλείο για να ενημερώνεται η διαχείριση σχετικά με την ολοκλήρωση της υλοποίησης των προτεινόμενων και τις τρεχουσών στρατηγικών για τη διαχείριση του κινδύνου.

Το πρώτο βήμα για την υλοποίηση στρατηγικών διαχείρισης κινδύνου είναι να εγκρίνει η διαχείριση το POAM. Στη συνέχεια, τα διάφορα άτομα και ομάδες υποβάλλουν εκθέσεις για την πρόοδο τους. Αυτές με τη σειρά τους αναφέρονται στη διοίκηση, και παρακολουθούνται στο πλαίσιο της συνεχιζόμενης διαδικασίας διαχείρισης κινδύνων.

Στον Πίνακα 5 (Δείγμα POAM) απεικονίζεται ένα τυπικό POAM. Το POAM περιέχει τον κίνδυνο, τη στρατηγική για τη διαχείριση κινδύνου, το σημείο επαφής (POC) που είναι αρμόδιο για την εφαρμογή της στρατηγικής, τους απαιτούμενους πόρους και τα διάφορα στάδια που συνθέτουν την εφαρμογή. Για κάθε ορόσημο, εισάγεται μια ημερομηνία «στόχος» ολοκλήρωσης και μια πραγματική ημερομηνία. Το POAM είναι ένα εργαλείο για την επικοινωνία με τη διαχείριση, και όχι για ένα σχέδιο διαχείρισης ενός έργου.

Κίνδυνος	Στρατιγική Διαχείρισης Κινδύνου	Σημείο Επαφής (POC)	Απαιτούμενοι Πόροι	Ορόσημο	Επιθυμητή Ημερ/νία Ολοκλήρωσης	Πραγματική Ημερ/νία Ολοκλήρωσης
Η αποτυχία στο περιβαλλοντικό σύστημα (π.χ. κλιματισμός) καθιστά το σύστημα μη διαθέσιμο.	Εφαρμογή ενός εφεδρικού σε κάποια άλλη τοποθεσία	Γεωργίου Σοφία	100.000 κόστος υλικού,50.000 κόστος λογισμικού,100.000 κόστος εργασίας	* Προμήθεια υλικού&λογισμικού * Εγκατάσταση υλικού * Εγκατάσταση λογισμικού * Διαμόρφωση συστήματος * Δοκιμή του συστήματος	*9/1 *9/15 *10/1 *10/15 *11/1	

Πίνακας 5: Δείγμα POAM

3 Μερικές κοινές Μεθοδολογίες και Εργαλεία για την Αξιολόγηση και τη Διαχείριση των κινδύνων σε Πληροφοριακά συστήματα

Οι παρακάτω μεθοδολογίες και τα εργαλεία αναπτύχθηκαν για τη διαχείριση των κινδύνων στα πληροφοριακά συστήματα:

3.1 Βασικές Μεθοδολογίες

3.1.1 Μεθοδολογία NIST - National Institute of Standards & Technology

Η NIST Special Publication (SP) 800-30, *Risk Management Guide for Information Technology Systems* είναι πρότυπο της Ομοσπονδιακής κυβέρνησης των ΗΠΑ. Η μεθοδολογία αυτή είναι κυρίως σχεδιασμένη για να είναι ποιοτική και βασίζεται σε εξειδικευμένους αναλυτές ασφαλείας που εργάζονται με τους ιδιοκτήτες του συστήματος και εμπειρογνώμονες τεχνικούς για τον εις βάθος εντοπισμό, την αξιολόγηση και τη διαχείριση του κινδύνου στα πληροφοριακά συστήματα . Η διαδικασία είναι εξαιρετικά περιεκτική, καλύπτοντας τα πάντα, από τον προσδιορισμό των απειλών-πηγές μέχρι και τη συνεχή αξιολόγηση και εκτίμηση.

Η μεθοδολογία NIST αποτελείται από 9 βήματα:

***Βήμα 1 -* Χαρακτηρισμός Συστήματος:** Το πρώτο βήμα είναι να καθοριστεί η έκταση της προσπάθειας. Σε αυτό το βήμα, εντοπίζονται τα όρια του πληροφοριακού συστήματος, μαζί με τους πόρους και τις πληροφορίες που συνθέτουν το σύστημα. Με τον χαρακτηρισμό ενός πληροφοριακού συστήματος καθιερώνεται η έκταση της προσπάθειας εκτίμησης του κινδύνου, σκιαγραφούνται τα όρια της επιχειρησιακής άδειας (ή διαπίστευσης), και παρέχονται πληροφορίες (π.χ., υλικό, λογισμικό, συνδεσιμότητα του συστήματος, και αρμόδιο τμήμα ή προσωπικό υποστήριξης) θεμελιώδους σημασίας για τον καθορισμό του κινδύνου.

***Βήμα 2 -* Εντοπισμός Απειλής:** Μια απειλή είναι η δυνατότητα για μια συγκεκριμένη απειλή-πηγή για να εξασκηθεί με επιτυχία μια συγκεκριμένη αδυναμία. Μια ευπάθεια είναι μια αδυναμία που μπορεί να ενεργοποιηθεί κατά λάθος ή να γίνει εκμεταλλεύσιμη σκοπίμως. Μια απειλή-πηγή δεν παρουσιάζει κίνδυνο, όταν δεν υπάρχει ευπάθεια που μπορεί να ασκηθεί. Κατά τον καθορισμό της πιθανότητας μιας απειλής, πρέπει να ληφθούν υπόψη οι απειλή-πηγές, οι αδυναμίες, και τα υπάρχοντα στοιχεία ελέγχου.

***Βήμα 3 -* Προσδιορισμός Αδυναμιών:** Η ανάλυση της απειλής σε ένα σύστημα πληροφορικής πρέπει να περιλαμβάνει μια ανάλυση των τρωτών της σημείων που συνδέονται με το περιβάλλον του συστήματος. Ο στόχος αυτού του βήματος είναι να συντάξει έναν κατάλογο των τρωτών σημείων του συστήματος (ελαττώματα ή αδυναμίες) που θα μπορούσαν να αξιοποιηθούν από τις πιθανές πηγές των απειλών.

Συνιστώμενες μέθοδοι για τον προσδιορισμό των τρωτών σημείων του συστήματος είναι η χρήση των πηγών ευπάθειας, οι επιδόσεις των δοκιμών ασφαλείας του συστήματος, καθώς και την ανάπτυξη της ασφάλειας απαιτήσεις καταλόγου ελέγχου. Θα πρέπει να σημειωθεί ότι τα είδη των τρωτών σημείων που θα υπάρχουν, καθώς και η μεθοδολογία που απαιτείται για την καθοριστεί αν υπάρχουν τρωτά σημεία, συνήθως ποικίλει ανάλογα με τη φύση των πληροφοριακών συστημάτων και τη φάση στην οποία είναι, στα SDLC:

- Αν το πληροφοριακό σύστημα δεν έχει ακόμη σχεδιαστεί, η αναζήτηση των αδύναμων σημείων πρέπει να επικεντρωθεί στις πολιτικές ασφάλειας του οργανισμού, στις προγραμματισμένες διαδικασίες ασφαλείας, και στους ορισμούς των απαιτήσεων του συστήματος, καθώς και στους πωλητές ή προγραμματιστές ανάλυσης της ασφάλειας των προϊόντων (π.χ. white papers).
- Αν το πληροφοριακό σύστημα έχει τεθεί σε εφαρμογή, ο προσδιορισμός των σημείων αδυναμίας πρέπει να διευρυνθεί ώστε να περιλαμβάνει πιο συγκεκριμένες πληροφορίες, όπως τα προγραμματισμένα χαρακτηριστικά ασφαλείας που περιγράφονται στα σχετικά έγγραφα για το σχεδιασμό της ασφαλείας καθώς και τα αποτελέσματα των δοκιμών της πιστοποίησης του συστήματος και της αξιολόγησης.

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

***Βήμα 4* - Ανάλυση Ελέγχου:** Ο στόχος αυτού του βήματος είναι να γίνει ανάλυση των ελέγχων που έχουν υλοποιηθεί, ή προγραμματιστεί για την εφαρμογή, από τον οργανισμό για την ελαχιστοποίηση ή την εξάλειψη της πιθανότητας μια απειλή να ασκήσει μια ευπάθεια στο σύστημα.

Για να προκύψει μια συνολική εκτίμηση κινδύνου που υποδεικνύει την πιθανότητα ότι μια πιθανή ευπάθεια μπορεί να ασκηθεί κατά την κατασκευή του συναφούς απειλητικού περιβάλλοντος (Βήμα 5 παρακάτω), πρέπει να ληφθεί υπόψη η εφαρμογή των εν εξελίξει ή προβλεπόμενων ελέγχων. Για παράδειγμα, μια ευπάθεια (π.χ., αδυναμία του συστήματος ή διαδικαστική αδυναμία) δεν είναι πιθανό να ασκηθεί, ή η πιθανότητα είναι μικρή, αν υπάρχει ένα χαμηλό επίπεδο ενδιαφέροντος απειλής-πηγής ή ικανότητας ή, εάν υπάρχουν αποτελεσματικές διαδικασίες ασφαλείας που μπορεί να εξαλείψουν ή να μειώσουν το μέγεθος της βλάβης.

***Βήμα 5* - Προσδιορισμός Πιθανοτήτων:** Για να προκύψει μια συνολική εκτίμηση κινδύνου που υποδεικνύει την πιθανότητα μια πιθανή ευπάθεια να ασκηθεί κατά την κατασκευή του συναφούς απειλητικού περιβάλλοντος, οι ακόλουθοι παράγοντες πρέπει να ληφθούν υπόψη:

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

***Βήμα 6* - Ανάλυση των επιπτώσεων:** Το επόμενο σημαντικό βήμα για τη μέτρηση του επιπέδου του κινδύνου είναι να προσδιοριστούν οι δυσμενείς επιπτώσεις που προκύπτουν από μια επιτυχημένη άσκηση απειλής μιας ευπάθειας. Πριν αρχίσει η ανάλυση των επιπτώσεων, είναι αναγκαίο να έχουμε λάβει τις ακόλουθες απαραίτητες πληροφορίες:

• Η αποστολή του συστήματος (π.χ., οι διαδικασίες που εκτελούνται από το πληροφοριακό σύστημα)
• Η κρισιμότητας του συστήματος και των δεδομένων (π.χ., η αξία ή η σημασία ενός συστήματος σε μια οργάνωση)

• Η ευαισθησίας του συστήματος και των δεδομένων

Η αρνητική επίδραση της εκδήλωσης της ασφάλειας μπορεί να περιγραφεί από την άποψη της απώλειας ή υποβάθμισης ή τον συνδυασμό οποιωνδήποτε από τους ακόλουθους τρεις στόχους ασφαλείας: την ακεραιότητα, τη διαθεσιμότητα και την εμπιστευτικότητα.

- **Απώλειας της ακεραιότητας**: Η ακεραιότητα του συστήματος και των δεδομένων αναφέρεται στην απαίτηση να προστατεύονται τα δεδομένα από ακατάλληλη τροποποίηση. Η ακεραιότητα χάνεται αν πραγματοποιούνται ανεξουσιοδότητες αλλαγές στα δεδομένα ή το πληροφοριακό σύστημα είτε από σκόπιμη ή ακούσια πράξη. Αν η απώλεια της ακεραιότητας του συστήματος ή των δεδομένων δεν διορθωθεί, η συνεχιζόμενη χρήση του μολυσμένου συστήματος ή των αλλοιωμένων δεδομένων θα μπορούσε να οδηγήσει σε ανακρίβεια, απάτη, ή λανθασμένες αποφάσεις. Επίσης, η παραβίαση της ακεραιότητας μπορεί να είναι το πρώτο βήμα για μια επιτυχημένη επίθεση κατά της διαθεσιμότητας ή της εμπιστευτικότητας του συστήματος. Για όλους αυτούς τους λόγους, η απώλειας της ακεραιότητας μειώνει την διασφάλιση ενός πληροφοριακού συστήματος.
- **Απώλεια Διαθεσιμότητας:** Αν ένα πληροφοριακό σύστημα με κρίσιμη αποστολή δεν είναι διαθέσιμο στους τελικούς χρήστες του, η αποστολή του οργανισμού μπορεί να επηρεαστεί. Η απώλεια λειτουργικότητας και επιχειρησιακής αποτελεσματικότητας του συστήματος, για παράδειγμα, μπορεί να οδηγήσει σε απώλεια παραγωγικού χρόνου, εμποδίζοντας έτσι τις επιδόσεις των τελικών χρηστών κατά την εκτέλεση των καθηκόντων τους για την υποστήριξη της αποστολής της οργάνωσης.

- **Απώλεια της εμπιστευτικότητας:** Η εμπιστευτικότητα του συστήματος και των δεδομένων αναφέρεται στην προστασία των δεδομένων από ανεπίτρεπτη αποκάλυψη. Ο αντίκτυπος της άνευ αδείας κοινολόγησης εμπιστευτικών πληροφοριών μπορεί να ποικίλλει από το να τεθεί σε κίνδυνο η εθνική ασφάλεια μέχρι το να αποκαλυφθούν τα προσωπικά δεδομένα δράσης. Απροσδόκητη αναρμόδια, ή ακούσια δημοσιοποίησή τους θα μπορούσε να οδηγήσει σε απώλεια εμπιστοσύνης του κοινού, αμηχανία, ή δικαστική δίωξη κατά του οργανισμού.

Μερικά από τις συνέπειες μπορούν να μετρηθούν ποσοτικά όπως η απώλεια εσόδων, το κόστος επισκευής του συστήματος, ή το επίπεδο της προσπάθειας που απαιτείται για τη διόρθωση των προβλημάτων που προκαλούνται από μια επιτυχημένη δράση απειλή. Άλλες επιπτώσεις δεν μπορούν να μετρηθούν σε συγκεκριμένες μονάδες, αλλά μπορούν να θεωρηθούν ή να περιγραφούν με τους όρους της υψηλή, μεσαία και χαμηλή επιπτώση.

***Βήμα 7* - Προσδιορισμός Κινδύνων:** Ο σκοπός αυτού του βήματος είναι να αξιολογήσει το επίπεδο του κινδύνου για το πληροφορικό σύστημα. Ο προσδιορισμός του κινδύνου για ένα συγκεκριμένο ζεύγος απειλής / ευπάθειας μπορεί να εκφραστεί ως συνάρτηση:

- Της πιθανότητας μια συγκεκριμένη απειλή-πηγή να επιχειρήσει να ασκήσει μια συγκεκριμένη ευπάθεια
- Του μεγέθους των επιπτώσεων που θα πρέπει να ασκήσει μια απειλή-πηγή με επιτυχία κατά της ευπάθειας
- Της επάρκειας των ισχυουσών ή προβλεπόμενων ελέγχων ασφαλείας για τη μείωση ή την εξάλειψη του κινδύνου.

Για τη μέτρηση του κινδύνου πρέπει να αναπτυχθούν μια κλίμακα κινδύνου και ένας πίνακας του επιπέδου των κινδύνων. Ο τελικός προσδιορισμός του κινδύνου προκύπτει από τον πολλαπλασιασμό της εκτίμησης για την πιθανότητα απειλής και των επιπτώσεων της απειλής. Ο πίνακας που ακολουθεί είναι μια 3 x 3 μήτρα της πιθανότητας κινδύνου (Υψηλή, Μέση και Χαμηλή) και της επίπτωσης της απειλή (Υψηλή, Μέση και Χαμηλή). Το δείγμα της μήτρας που φαίνεται στον πίνακα 6 δείχνει πώς προκύπτουν τα συνολικά επίπεδα κινδύνου (Υψηλό, Μέσο και Χαμηλό επίπεδο). Ο καθορισμός αυτών των επιπέδων κινδύνου μπορεί να είναι υποκειμενικός. Το σκεπτικό για αυτήν την αιτιολόγηση μπορεί να εξηγηθεί στα πλαίσια της πιθανότητας που έχει δωθεί για κάθε ενδεχόμενο κίνδυνου και της τιμής που έχει δωθεί για κάθε επίπεδο επιπτώσεων.

	Επίπτωση Απειλής		
Πιθανότητα Απειλής	Χαμηλή (10)	Μέτρια (50)	Υψηλή (100)
Υψηλή (1.0)	Χαμηλό 10 x 1.0 = 10	Μεσαίο 50 x 1.0 = 50	Μεσαίο 100 x 1.0 = 100
Μέτρια (0.5)	Χαμηλό 10 x 0.5 = 5	Μεσαίο 50 x 0.5 = 25	Μεσαίο 100 x 0.5 = 50
Χαμηλή (0.1)	Χαμηλό 10 x 0.1 = 1	Χαμηλό 50 x 0.1 = 5	Χαμηλό 100 x 0.1 = 10

Πίνακας 6: Δείγμα μήτρας δείχνει πώς προκύπτουν τα συνολικά επίπεδα κινδύνου

Παρακάτω περιγράφονται τα επίπεδα κινδύνου που φαίνονται στον παραπάνω πίνακα. Αυτή η κλίμακα κινδύνου, με αξιολογήσεις ως Υψηλό, Μέσο και Χαμηλό, αντιπροσωπεύει το βαθμό ή το επίπεδο του κινδύνου στον οποίο ένα σύστημα πληροφορικής αν ασκηθεί μια συγκεκριμένη ευπάθεια. Η κλίμακα κινδύνου παρουσιάζει επίσης τα μέτρα που πρέπει να λάβουν ανώτερα διοικητικά στελέχη για κάθε επίπεδο κινδύνου.

- **Υψηλό Επίπεδο κινδύνου:** Εάν μια παρατήρηση ή εύρημα αξιολογείται ως υψηλού κινδύνου, υπάρχει μεγάλη ανάγκη για λήψη διορθωτικών μέτρων. Ένα υπάρχον σύστημα μπορεί να συνεχίσει να λειτουργεί, αλλά ένα διορθωτικό σχέδιο δράσης πρέπει να τεθεί σε εφαρμογή το συντομότερο δυνατό.
- **Μεσαίο Επίπεδο κινδύνου:** Εάν μια παρατήρηση βαθμολογείται ως μέσου κινδύνου, χρειάζονται διορθωτικές ενέργειες και πρέπει να αναπτυχθεί ένα σχέδιο για να ενσωματωθούν αυτές οι ενέργειες μέσα σε εύλογο χρονικό διάστημα.
- **Χαμηλό Επίπεδο κινδύνου:** Εάν μια παρατήρηση περιγράφεται ως χαμηλού κινδύνου, η Αρμόδια Αρχή Έγκρισης του συστήματος πρέπει να καθορίσει αν οι διορθωτικές ενέργειες απαιτούνται ακόμη ή να αποφασίσει να αποδεχτεί τον κίνδυνο.

***Βήμα 8* - Συστάσεις Ελέγχου:** Σε αυτό το βήμα της διαδικασίας, παρέχονται οι έλεγχοι που θα μπορούσαν να μετριάσουν ή να εξαλείψουν τους κινδύνους που εντοπίστηκαν, όπως αρμόζει στις δραστηριότητες της οργάνωσης. Ο στόχος των προτεινόμενων ελέγχων είναι να μειώσουν το επίπεδο του κινδύνου για το πληροφοριακό σύστημα και τα δεδομένα του σε ένα αποδεκτό επίπεδο. Οι ακόλουθοι παράγοντες πρέπει να εξετάζονται κατά τη σύσταση των ελέγχων και των εναλλακτικών λύσεων για την ελαχιστοποίηση ή την εξάλειψη των εντοπιζόμενων κινδύνων:

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

• Νομοθεσία και κανονιστικές ρυθμίσεις

• Οργανωτική πολιτική

• Επιχειρησιακές επιπτώσεις

• Ασφάλεια και αξιοπιστία

Οι συστάσεις ελέγχου είναι τα αποτελέσματα της διαδικασίας αξιολόγησης του κινδύνου και συμβάλλουν στη διαδικασία μείωσης των κινδύνων, κατά τη διάρκεια της οποίας η συνιστώμενος διαδικαστικός και τεχνικός έλεγχος ασφαλείας αξιολογούνται, παίρνουν προτεραιότητα, και υλοποιούνται.

Δεν είναι δυνατό να μπορούν να εφαρμοστούν όλοι οι συνιστώμενοι έλεγχοι για τη μείωση των ζημιών. Για να προσδιοριστούν ποιοι έλεγχοι απαιτούνται και είναι κατάλληλοι για ένα συγκεκριμένο οργανισμό πρέπει να γίνεται μια ανάλυσης κόστους-οφέλους, για τους προτεινόμενους συνιστώμενους ελέγχους, ώστε να αποδειχθεί ότι το κόστος της εφαρμογής των ελέγχων μπορεί να δικαιολογηθεί από τη μείωση του επιπέδου του κινδύνου. Επιπλέον, οι επιχειρησιακές επιπτώσεις (π.χ. επιπτώσεις στην απόδοση του συστήματος) και η σκοπιμότητα (π.χ., τεχνικές προδιαγραφές, αποδοχή των χρηστών), της εισαγωγής της προτεινόμενης επιλογής πρέπει να αξιολογηθεί προσεκτικά κατά τη διάρκεια της διαδικασίας μείωσης του κινδύνου.

***Βήμα 9* - Τεκμηρίωση Αποτελεσμάτων**: Αφού η αξιολόγηση των κινδύνων έχει ολοκληρωθεί, τα αποτελέσματα πρέπει να τεκμηριωθούν με επίσημη έκθεση ή ενημέρωση.

Μια έκθεση αξιολόγησης των κινδύνων είναι μια έκθεση διαχείρισης που βοηθά ανώτερα διευθυντικά στελέχη, τους κατόχους της αποστολής, στη λήψη αποφάσεων σχετικά με την πολιτική, τα διαδικαστικά, τον προϋπολογισμό, και το σύστημα λειτουργίας και διαχείρισης των αλλαγών. Αντίθετα από την έκθεση ελέγχου ή έρευνας, η οποία αναζητά αδικίες, η έκθεση αξιολόγησης κινδύνου δεν θα πρέπει να παρουσιάζεται με κατηγορητικό τρόπο, αλλά ως μια συστηματική και αναλυτική προσέγγιση για την εκτίμηση κινδύνου, έτσι ώστε τα ανώτερα διοικητικά στελέχη να κατανοήσουν τους κινδύνους και να διαθέσουν πόρους για τη μείωση και τη διόρθωση ενδεχόμενων απωλειών. Για το λόγο αυτό, μερικοί άνθρωποι προτιμούν να αντιμετωπίζουν τα ζευγάρια απειλής / ευπάθειας ως παρατηρήσεις αντί για διαπιστώσεις στις εκθέσεις αξιολόγησης κινδύνου.

Τα βήματα 2, 3, 4, και 6, μπορούν να διεξάγονται παράλληλα αφού το Βήμα 1 ολοκληρωθεί.

3.1.2 Μεθοδολογία Cramm

Η μέθοδος CRAMM αναπτύχθηκε από την κεντρική υπηρεσία πληροφορικής και τηλεπικοινωνιών της Μ. Βρετανίας (Central Computer and Telecommunications Agency). Αποτελεί πρότυπη μέθοδο και έχει αναπτυχθεί με σκοπό να εφαρμοστεί κυρίως σε μεγάλους οργανισμούς, όπως είναι δημόσιοι οργανισμοί, τράπεζες, νοσοκομεία, επιχειρήσεις κοινής ωφέλειας κτλ.

Η μέθοδος CRAMM καλύπτει όλες τις συνιστώσες της ασφάλειας ΤΠΕ περιλαμβανομένων των τεχνικού θεμάτων, των διαδικασιών, της φυσικής ασφάλειας, του προσωπικού, της εκπαίδευσης κ.λ.π. Η μεθοδολογία υποστηρίζεται από αυτοματοποιημένο εργαλείο λογισμικού το οποίο υποστηρίζει όλα τα στάδια της εφαρμογής της.

Τα βασικά στάδια της μεθοδολογίας είναι τα ακόλουθα:

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

Ο συνδυασμός των τριών παραγόντων δίδει το βαθμό επικινδυνότητας του ΠΣ, έτσι ώστε να επιλεγούν τα κατάλληλα αντίμετρα:

- αξία αγαθών - επίπτωση (impact)
- επίπεδο απειλών (threat level)
- επίπεδο αδυναμιών (vulnerability level).

Πιο συγκεκριμένα η επικινδυνότητα προκύπτει ως εξής:

Απειλή x Αδυναμία = Πιθανότητα
Πιθανότητα x Επίπτωση = Επικινδυνότητα

Στάδιο 1^{ο}: Προσδιορισμός και αποτίμηση αγαθών (identification and valuation of assets)

Βήμα 1: Προσδιορισμός επιμέρους πληροφοριακών και επικοινωνιακών αγαθών: Προσδιορίζονται τα στοιχεία των Πληροφοριακών Συστημάτων που απαιτούν προστασία (Φυσικά αγαθά (κτήρια, υπολογιστικά συστήματα κτλ), Αγαθά λογισμικού, Αγαθά Δεδομένων). Επίσης, γίνεται εκτίμηση των άμεσων (οικονομικών) συνεπειών όπως είναι το κόστος επαναγοράς, και έμμεσων συνεπειών όπως η παρεμπόδιση λειτουργίας, οι νομικές συνέπειες κ.ά.

Βήμα 2: Αποτίμηση αγαθών: Η αξία κάθε ομάδας / κατηγορίας δεδομένων αποτιμάται με βάση την Επίπτωση (impact) που θα είχε η απώλειά της.

Βήμα 3: Επιβεβαίωση και επικύρωση αποτίμησης: Η σχετική έκθεση των αποτελεσμάτων περιλαμβάνει τον ορισμό του προς ανάλυση συστήματος και των ορίων του, τη μέθοδο εργασίας που ακολουθήθηκε, την αποτίμηση των περιουσιακών στοιχείων των Π.Σ. και τέλος τα γενικά συμπεράσματα.

Στάδιο 2^{ο}: Ανάλυση πληροφοριακού κινδύνου ή επικινδυνότητας (risk analysis)

Βήμα 1: Προσδιορισμός απειλών που αφορούν κάθε Αγαθό (asset)

Βήμα 2: Εκτίμηση απειλών (threat assessment) και αδυναμιών (vulnerability assessment)

Βήμα 3: Υπολογισμός επικινδυνότητας συνδυασμών Αγαθό – Απειλή – Αδυναμία: Ο βαθμός επικινδυνότητας είναι από 1 έως 7

Βήμα 4: Επιβεβαίωση και επικύρωση βαθμού επικινδυνότητας: Η ομάδα μελέτης μπορεί να χρησιμοποιήσει τις αναφορές που παράγει το λογισμικό της CRAMM. Οι αναλυτές έχουν τη δυνατότητα είτε να αλλάξουν τις τιμές της επικινδυνότητας, είτε να αλλάξουν τις τιμές

που έχουν προκύψει από την εκτίμηση των απειλών και αδυναμιών ή να υπολογίσουν εκ νέου την επικινδυνότητα.

Στάδιο 3°: Διαχείριση πληροφοριακού κινδύνου ή επικινδυνότητας (risk management)

Βήμα 1: Προσδιορισμός προτεινόμενων αντιμέτρων: Η CRAMM προτείνει με αυτόματο τρόπο τα αντίμετρα, σύμφωνα με τα αποτελέσματα της ανάλυσης επικινδυνότητας. Ένα αντίμετρο μπορεί να είναι είτε *Εγκατεστημένο* (installed) είτε *Προς υλοποίηση* (to be installed) ή *Υπό υλοποίηση* (implementing recommendation) ή *Προτεινόμενο για υλοποίηση* (implemented recommendation) ή τέλος *Εφαρμοζόμενο* (already covered)

Βήμα 2: Σχέδιο ασφάλειας πληροφοριακών και επικοινωνιακών συστημάτων: περιλαμβάνει το Σχέδιο Πολιτικής Ασφάλειας, τα Μέτρα Ασφάλειας και τη Στρατηγική για την εφαρμογή του Σχεδίου Ασφάλειας.

3.1.3 Μεθοδολογία FRAP

Η διαδικασία Facilitated Risk Assessment Process (FRAP) είναι δημιουργία του Thomas Peltier. Βασίζεται στην εφαρμογή τεχνικών διαχείρισης κινδύνου, με ένα εξαιρετικά αποδοτικό τρόπο. Η FRAP χρησιμοποιεί επίσημες ποιοτικές μεθοδολογίες ανάλυσης κινδύνου χρησιμοποιώντας Ανάλυση Αδυναμιών , Ανάλυση Επιπτώσεων των Κινδύνων, Ανάλυση των Απειλών και Ερωτηματολόγια. Επιπλέον, η FRAP δίνει έμφαση στον προκαταρκτικό έλεγχο των συστημάτων και την εκτέλεση μόνο επίσημων αξιολογήσεων του κινδύνου σχετικά με τα συστήματα, όταν συντρέχουν λόγοι. Τέλος, ο κίνδυνος FRAP συνδέει τον κίνδυνο με την επίπτωση χρησιμοποιώντας την Ανάλυση Επιχειρησιακών επιπτώσεων, ως βάση για τον προσδιορισμό των επιπτώσεων.

Η μέθοδος FRAP σχεδιάστηκε ως μια αποδοτική και πειθαρχημένη διαδικασία για την διασφάλιση ότι οι κίνδυνοι στην λειτουργία ενός οργανισμού που σχετίζονται με τα πληροφοριακά συστήματα αναγνωρίζονται και καταγράφονται. Η διαδικασία ορίζει την ανάλυση ενός συστήματος ή εφαρμογής κάθε φορά.

Συνέρχεται μια ομάδα ατόμων που περιλαμβάνει μέλη από την διοίκηση που είναι εξοικειωμένα με τις πληροφοριακές ανάγκες του οργανισμού καθώς και από το τεχνικό προσωπικό που έχουν λεπτομερή γνώση του συστήματος που εξετάζεται, των ευπαθειών του και των αντίμετρων που υπάρχουν για να τις αντιμετωπίσουν. Οι συσκέψεις της ομάδας, που ακολουθούν συγκεκριμένο πρόγραμμα, υποβοηθούνται από ένα άτομο που είναι υπεύθυνο για τον συντονισμό της διαδικασίας, την διασφάλιση της σωστής επικοινωνίας μεταξύ των μελών της ομάδας και την τήρηση του προγράμματος. Το άτομο αυτό ονομάζεται «οργανωτής» του FRAP. Κατά την διάρκεια της σύσκεψης η ομάδα ανταλλάζει ιδέες για την αναγνώριση των ενδεχόμενων απειλών, ευπαθειών και των επακόλουθων αντίκτυπων στην ακεραιότητα, εμπιστευτικότητα και διαθεσιμότητα των δεδομένων. Έπειτα, η ομάδα αναλύει τις συνέπειες των αντίκτυπων αυτών στην λειτουργία του οργανισμού και κατατάσσει τους κινδύνους με βάση προτεραιότητας. Δεν προσπαθεί να ψάξει ή να καθορίσει συγκεκριμένους αριθμούς για την πιθανότητα των απειλών ή το ποσό των απωλειών, εκτός και αν αυτά τα δεδομένα υπάρχουν ήδη. Αντιθέτως, βασίζεται στην γνώση και την εμπειρία των μελών της καθώς και στη γενική 0γνώση που προκύπτει για τις απειλές και ευπάθειες από την διεθνή βιβλιογραφία, τον τύπο, το Internet κτλ.

Μετά την αναγνώριση και κατηγοριοποίηση των κινδύνων, η ομάδα επιλέγει τα αντίμετρα που θα μπορούσαν να υλοποιηθούν για την αντιμετώπιση τους, εστιάζοντας κυρίως σε αυτά που έχουν τον καλύτερο λόγο κόστους / απόδοσης. Σαν σημείο εκκίνησης έχει μια λίστα από 26 γενικά αντίμετρα που έχουν σχεδιαστεί για να αντιμετωπίζουν διάφορους τύπους κινδύνων.

Κατά την διάρκεια της ανάλυσης μπορεί να συμφωνηθεί η προσθήκη νέων αντίμετρων στην λίστα. Η τελική απόφαση για το ποια αντίμετρα χρειάζονται ανήκει στην διοίκηση του οργανισμού, που λαμβάνει υπ'όψιν τη φύση των πληροφοριών, την σημασία τους στην λειτουργία του οργανισμού και το κόστος των αντιμέτρων. Τα συμπεράσματα της ομάδας για τους κινδύνους που υφίστανται, την προτεραιότητα τους και τα αντίμετρα που χρειάζονται

καταγράφονται και στέλνονται στον υπεύθυνο του project (project lead) και στον διευθυντή του συγκεκριμένου τμήματος του οργανισμού για την επεξεργασία τους και την κατάρτιση του σχεδίου δράσης (action plan). Σε αυτό το σημείο ένας ειδικός για θέματα ασφαλείας μπορεί να βοηθήσει τον διευθυντή να προσδιορίσει ποια αντίμετρα προσφέρουν καλό λόγο κόστους/απόδοσης και ικανοποιούν της ανάγκες του οργανισμού. Όταν κάθε κίνδυνος έχει αντιμετωπιστεί ή αποδεχθεί, υπογράφεται το ολοκληρωμένο κείμενο της ανάλυσης κινδύνων και η διαδικασία τελειώνει.

Η διαδικασία FRAP μπορεί να χωριστεί σε τέσσερα μέρη:

1. Την αρχική σύσκεψη, η οποία διαρκεί περίπου μια ώρα και περιλαμβάνει τον διευθυντή, τον υπεύθυνο του project και τον οργανωτή του FRAP.

2. Την κυρίως σύσκεψη, η οποία διαρκεί περίπου τέσσερις ώρες και στην οποία συμμετέχουν 7-15 άτομα, αν και έχουν γίνει με επιτυχία συσκέψεις από 4 μέχρι και 50 άτομα.

3. Η ανάλυση FRAP και δημιουργία της αναφοράς (report), η οποία διαρκεί συνήθως 4-6 μέρες και ολοκληρώνεται από τον «οργανωτή» του FRAP και τον γραμματέα.

4. Η τελική σύσκεψη που διαρκεί περίπου μια ώρα και συμμετέχουν τα ίδια άτομα με την αρχική σύσκεψη.

3.1.4 Μεθοδολογία Magerit

Η Magerit είναι μια ανοικτή μεθοδολογία για την Ανάλυση και τη Διαχείριση κινδύνου, που αναπτύχθηκε από το ισπανικό Υπουργείο Δημόσιας Διοίκησης, προσφέρεται ως πλαίσιο και οδηγός για τη Δημόσια Διοίκηση. Δεδομένης της ανοιχτή φύση του, χρησιμοποιείται επίσης κι εκτός της Διοίκησης. Η Magerit v1 δημοσιεύθηκε το 1997 και η v2 δημοσιεύτηκε το 2005. Διατίθεται ανοιχτά στα ισπανικά και τα αγγλικά.

Ο σκοπός της Magerit είναι άμεσα συνδεδεμένος με τη γενικευμένη χρήση των ηλεκτρονικών, της πληροφορικής και της τηλεματικής των μέσων ενημέρωσης, οι οποίες φέρνουν προφανή οφέλη για το κοινό, αλλά που υπόκεινται επίσης σε ορισμένους κινδύνους που πρέπει να περιοριστούν στο ελάχιστο με αντίμετρα ασφάλειας που παράγουν εμπιστοσύνη στη χρήση αυτών των μέσων.

Η μεθοδολογία αυτή παρουσιάζει ιδιαίτερο ενδιαφέρον για όσους εργάζονται με μηχανοκίνητες πληροφορίες και τα συστήματα του υπολογιστή που τις χειρίζονται. Εάν αυτές οι πληροφορίες, ή τις υπηρεσίες που παρέχονται χάρη σε αυτή, είναι άξια, η μεθοδολογία αυτή θα τους επιτρέψει να γνωρίζουν πόσο αυτή η τιμή είναι σε κίνδυνο και θα τους βοηθήσει για να το προστατεύσουν.

Η Magerit επιδιώκει την επίτευξη των ακόλουθων στόχων:

- <u>Άμεσοι στόχοι:</u>

1. Να ενημερώνει τους υπεύθυνους των συστήματα πληροφοριών για την ύπαρξη των κινδύνων και την ανάγκη για τη θεραπεία τους στην ώρα τους.

2. Να προσφέρει μια συστηματική μέθοδο για την ανάλυση των κινδύνων αυτών.

3. Να βοηθάει στην περιγραφή και τον σχεδιασμό των κατάλληλων μέτρων για την τήρηση των κινδύνων στο πλαίσιο του ελέγχου.

- <u>Έμμεσοι στόχοι:</u>

4. Να προετοιμάζει την οργάνωση για τις διαδικασίες αξιολόγησης, ελέγχου, πιστοποίησης ή διαπίστευσης, που έχουν σημασία σε κάθε περίπτωση.

Αποσκοπεί επίσης στην επίτευξη ομοιομορφίας στις εκθέσεις που περιέχουν τις διαπιστώσεις και τα συμπεράσματα από την ανάλυση κινδύνου και τη διαχείριση του έργου:

Εκτίμηση μοντέλου: Περιγραφή της αξίας των κεφαλαίων της οργάνωσης καθώς και των εξαρτήσεων μεταξύ των διαφόρων κεφαλαίων.

Χάρτης Κινδύνων: Ο λογαριασμός των απειλών στους οποίους εκτίθενται τα κεφάλαια.

Διασφάλιση της αξιολόγησης: Η αξιολόγηση της αποτελεσματικότητας των υφιστάμενων διασφαλίσεων σε σχέση με τον κίνδυνο που αντιμετωπίζουν.

Κατάσταση Κινδύνου: Η κατάταξη των κεφαλαίων από τον υπολειπόμενο κίνδυνο τους. Δηλαδή, από το τι θα μπορούσε να συμβεί, αφού ληφθούν υπόψη οι διασφαλίσεις.

Έκθεση Ελλείψεων: Έλλειψη ή αδυναμία των εγγυήσεων που φαίνεται σκόπιμο να μειώσουν τους κινδύνους του συστήματος.

Σχέδιο Ασφαλείας: Ομάδα των προγραμμάτων ασφάλειας που θέτουν σε δράση τις αποφάσεις διαχείρισης του κινδύνου.

Οι φάσεις Εκτίμησης Κινδύνου της μεθόδου είναι οι ακόλουθες:

Αναγνώριση κινδύνου: Κεφάλαια: ταυτοποίηση, ταξινόμηση και αξία κεφαλαίων εξαρτήσεις μεταξύ των κεφαλαίων. Απειλές: Η σχέση ταύτισης με τα κεφάλαια και η αξιολόγηση των αδυναμιών. Διασφαλίσεις: εντοπισμός και αξιολόγηση, εργαλείο στήριξης.

Ανάλυση κινδύνου: Συσσώρευση και απόκλιση επιπτώσεων και κινδύνων, εργαλείο στήριξης.

Αξιολόγηση κινδύνου: Από τους τεχνικούς κινδύνους σε επιχειρηματικούς κινδύνους.

Οι Φάσεις Διαχείρισης Κινδύνου της μεθόδου είναι:

Αξιολόγηση κινδύνου

Μεταχείριση κινδύνου: Υποστήριξη των σεναρίων: φάσεις, σχέδια ασφάλειας, μακροπρόθεσμοι στόχοι

Αποδοχή Κινδύνου: δείκτες ασφαλείας

Γνωστοποίηση κινδύνου: Ορισμός των εκθέσεων που περιέχουν τις διαπιστώσεις και τα συμπεράσματα από την ανάλυση κινδύνου και τη διαχείριση του έργου: υπόδειγμα αξίας, χάρτης κινδύνου, διασφάλιση της αξιολόγησης, κατάσταση κινδύνου, έκθεση ελλείψεων και σχέδιο ασφαλείας. Σχετικό λογισμικό (EAR / Pilar) παράγει ευρεία ποικιλία των παραδοτέων σε τυποποιημένες και προσαρμόσιμες μορφές, κειμένου και γραφικών.

Υπάρχουν δύο μεγάλα εργασίες που πρέπει να διενεργούνται: α) Ανάλυση Κινδύνου και β) Αξιολόγηση Κινδύνου

α) Ανάλυση Κινδύνου

Στη φάση αυτή καθορίζεται τι έχει η οργάνωση και εκτιμάται τι μπορεί να συμβεί. Τα στοιχεία που χρησιμοποιούνται είναι τα εξής:

1. Περιουσιακά στοιχεία, τα οποία είναι τα στοιχεία του πληροφοριακού συστήματος (ή συνδέονται στενά με αυτό) που δίνουν αξία στον οργανισμό.

2. Απειλές, οι οποίες είναι τα πράγματα που μπορούν να συμβούν με τα περιουσιακά στοιχεία, προκαλώντας βλάβη στον οργανισμό.

3. Αντίμετρα, τα οποία αποτελούν στοιχεία της άμυνας ανεπτυγμένα, έτσι ώστε αυτές οι απειλές να μη προκαλούν τόση ζημιά.

Τα στοιχεία αυτά επιτρέπουν την εκτίμηση του αντίκτυπου, εννοώντας τι μπορεί να συμβεί, και του κινδύνου, δηλαδή τι θα συμβεί κατά πάσα πιθανότητα. Μέσω της ανάλυσης του κινδύνου τα στοιχεία αναλύονται μεθοδικά για να καταλήξουμε σε συμπεράσματα με μια βάση.

Η ανάλυση κινδύνου είναι μια μεθοδική προσέγγιση για τον προσδιορισμό του κινδύνου, ακολουθώντας συγκεκριμένα βήματα:

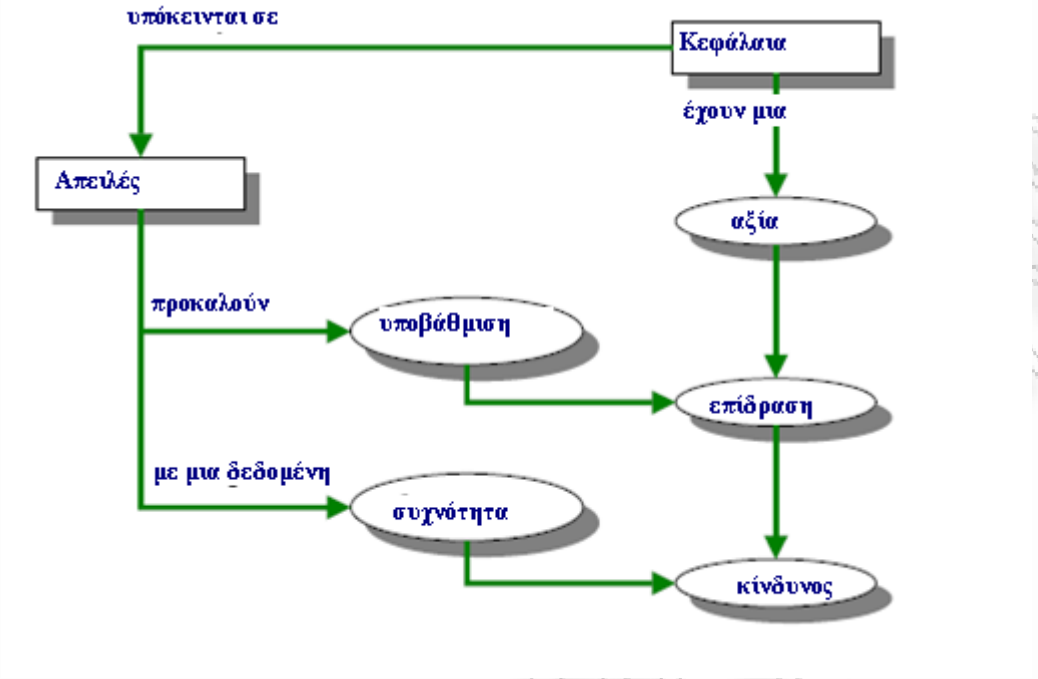
- Προσδιορίζονται τα περιουσιακά στοιχεία που αφορούν την οργάνωση, οι μεταξύ τους σχέσεις και η αξία τους. Τα κεφάλαια είναι οι πόροι του πληροφοριακού συστήματος ή σχετίζονται με αυτό, που είναι αναγκαίοι για τον οργανισμό για να λειτουργήσει σωστά και να επιτευχθούν οι στόχοι που προτείνονται από τη διαχείρισή του. Το βασικό περιουσιακό στοιχείο είναι οι πληροφορίες που διαχειρίζεται το σύστημα, δηλαδή τα

δεδομένα. Δεν είναι όλα τα περιουσιακά στοιχεία του ίδιου τύπου. Οι απειλές και τα αντίμετρ διαφέρουν ανάλογα με το είδος των κεφαλαίων.

- Καθορίζονται οι απειλές στις οποίες είναι εκτεθειμένα τα περιουσιακά αυτά στοιχεία. Οι απειλές είναι "πράγματα που συμβαίνουν." Από όλα τα πράγματα που θα μπορούσαν να συμβούν, εκείνες που παρουσιάζουν ενδιαφέρον είναι εκείνες που θα μπορούσαν να συμβούν στα κεφάλαια ενός οργανισμού και να προκαλέσουν βλάβη. Δεν είναι όλες οι απειλές που επηρεάζουν όλα τα περιουσιακά στοιχεία, αλλά υπάρχει κάποια σχέση μεταξύ του τύπου του περιουσιακού στοιχείου και του τι μπορεί να συμβεί σε αυτό.
- Προσδιορίζονται τα διαθέσιμα αντίμετρα και πόσο αποτελεσματικά είναι έναντι του κινδύνου. Διασφαλίσεις ή αντίμετρα είναι οι διαδικασίες ή οι τεχνολογικοί μηχανισμοί που μειώνουν τον κίνδυνο. Υπάρχουν απειλές που μπορεί να αφαιρεθούν απλώς από τον κατάλληλο οργανισμό, άλλες απαιτούν τεχνικά μέσα (προγράμματα ή εξοπλισμό), ενώ άλλες χρειάζονται φυσική ασφάλεια. Τέλος, υπάρχει η πολιτική προσωπικού.
- Εκτιμάται το αντίκτυπο, που ορίζεται ως η ζημία που προκύπτει σε κάποιο περιουσιακό στοιχείο από την εμφάνιση μιας απειλής. Αντίκτυπο είναι η μέτρηση της ζημίας που προκλήθηκε σε περιουσιακό στοιχείο που προκύπτει από την εμφάνιση μιας απειλής. Με τη γνώση της αξίας των περιουσιακών στοιχείων (σε διάφορες διαστάσεις), καθώς και την υποβάθμιση που προκαλείται από τις απειλές, τις επιπτώσεις τους στο σύστημα, οι επιπτώσεις μπορούν να βρεθούν απευθείας. Η μόνη εξέταση που απαιτείται αφορά τις εξαρτήσεις μεταξύ των κεφαλαίων. Συχνά, η αξία του πληροφόριακού συστήματος επικεντρώνεται στις υπηρεσίες που παρέχει και τα δεδομένα που χειρίζεται, ενώ οι απειλές συνήθως εμφανίζονται στα μέσα ενημέρωσης.
- Εκτιμάται ο κίνδυνος, ο οποίος ορίζεται ως η σταθμισμένη επίπτωση στο ρυθμό εμφάνισης (ή την προσδοκία της εμφάνισης) της απειλής. Κίνδυνος είναι η μέτρηση της πιθανής βλάβης στο σύστημα. Γνωρίζοντας τις επιπτώσεις των απειλών για τα περιουσιακά στοιχεία, ο κίνδυνος μπορεί να προέρχεται απευθείας, απλά λαμβάνοντας υπόψη τη συχνότητα εμφάνισης. Ο κίνδυνος αυξάνεται με την επίδραση και με τη συχνότητα. Ο κίνδυνος υπολογίζεται ως εξής:

Κίνδυνος = Αντίκτυπο × Συχνότητα

Αυτή είναι μια πραγματική αξία, μεγαλύτερη από το μηδέν. Ένα όριο "r0" βρίσκεται κάτω από το οποίο ο κίνδυνος είναι «αμελητέα», δηλαδή: r0 = v0.



Σχήμα 1:Εκτίμηση του κινδύνου

β) Διαχείριση Κινδύνου

Στη φάση αυτή επιτρέπεται σε μια πλήρη και συνετή άμυνα να οργανωθεί, έτσι ώστε τίποτα κακό να μη συμβεί και την ίδια στιγμή γίνονται προετοιμασίες για την αντιμετώπιση καταστάσεων έκτακτης ανάγκης, την επιβίωση από περιστατικά και τη διατήρηση της λειτουργίας υπό τις καλύτερες προϋποθέσεις. Επειδή τίποτα δεν είναι τέλειο, λέγεται ότι ο κίνδυνος έχει μειωθεί σε ένα υπολειπόμενο επίπεδο, στο οποίο η διαχείριση μπορεί να ζήσει.

Τα βήματα που ακολουθούντα εδώ είναι τα ακόλουθα:

- Ερμηνεύονται οι τιμές των επιπτώσεων και των κινδύνων. Ο αντίκτυπος και ο υπολειπόμενος κίνδυνος είναι μια μέτρηση της παρούσας κατάστασης, μεταξύ της δυνητικής ανασφάλειας (χωρίς καμία προστασία) και των κατάλληλων μέτρν που θα μειώσουν τις επιπτώσεις και τους κινδύνους στις ελάχιστες τιμές. Επομένως, είναι μια μέτρηση των ελλείψεων.
- Επιλέγονται τα αντίμετρα. Κατ 'αρχήν, οι απειλές πρέπει να καταπολεμηθούν, και ενώ η εναλλακτική λύση δεν μπορεί να δικαιολογηθεί. Είναι αναγκαίο να προγραμματιστεί η ομάδα των κατάλληλων μέτρων για την πρόληψη τόσο των επιπτώσεων όσο και του κινδύνου, είτε με τη μείωση της υποβάθμισης του περιουσιακού στοιχείου (ελαχιστοποίηση της ζημιάς), ή με τη μείωση της συχνότητας της απειλής (ελαχιστοποίηση των δυνατοτήτων του).

Η Magerit v2 έχει δομηθεί σε τρία βιβλία:

Βιβλίο I: Μεθοδολογία. Περιγράφει τα αρχικά βήματα και τις βασικές εργασίες για την πραγματοποίηση ενός έργου για την ανάλυση και διαχείριση των κινδύνων. Περιλαμβάνει την επίσημη περιγραφή του έργου, την εφαρμογή για την ανάπτυξη πληροφοριακών συστημάτων και παρέχει έναν μεγάλο αριθμό πρακτικών ενδείξεων, καθώς και τα θεωρητικά θεμέλια , μαζί με κάποιες άλλες συμπληρωματικές πληροφορίες.

Βιβλίο II: Κατάλογος των στοιχείων. Παρέχει πρότυπα στοιχεία και κριτήρια για τα πληροφοριακά συστήματα και τη μοντελοποίησης των κινδύνων: τις κατηγορίες των κεφαλαίων, τις διαστάσεις αποτίμησης, τα κριτήρια αξιολόγησης, τις τυπικές απειλές, και τις εγγυήσεις για να θεωρηθούν. Περιγράφει επίσης τις εκθέσεις που περιέχουν τις διαπιστώσεις και τα συμπεράσματα (πρότυπο αξίας, χάρτης κινδύνου, αξιολόγησης εγγυήσεων, κατάσταση των

κινδύνων, έκθεση ελλείψεων και σχέδιο ασφαλείας), συμβάλλοντας έτσι στην επίτευξη ομοιομορφίας.

Βιβλίο III: Πρακτικές τεχνικές. Περιγράφει τις τεχνικές που χρησιμοποιούνται συχνά για να πραγματοποιηθεί η ανάλυση των κινδύνων και η διαχείριση έργων όπως: πινακοειδής και αλγοριθμική ανάλυση, δέντρα απειλών, ανάλυση κόστους-οφέλους, διαγράμματα ροής δεδομένων, διαγράμματα διαδικασίας, γραφικές τεχνικές, το σχεδιασμό του έργου, συνεδρίες εργασίας (συνεντεύξεις, συναντήσεις, παρουσιάσεις) , και την ανάλυση Delphi. Η εφαρμογή της μεθοδολογίας μπορεί να υποστηριχθεί από το Pilar λογισμικό / EAR, το οποίο εκμεταλλεύεται και αυξάνει τις δυνατότητες και την αποτελεσματικότητά της (το λογισμικό Pilar περιορίζεται στην ισπανική δημόσια διοίκηση ενώ το EAR είναι ένα εμπορικό προϊόν).

3.1.5 Μεθοδολογία IT-Grundschutz (BSI)

Η μεθοδολογία IT-Grundschutz είναι μια BSI μεθοδολογία για την αποτελεσματική διαχείριση της ασφάλειας των πληροφοριών που μπορεί να προσαρμοστεί εύκολα στην κατάσταση μιας συγκεκριμένης οργάνωσης. Ένα σύστημα διαχείρισης για την ασφάλεια των πληροφοριών (ISMS) είναι η προγραμματισμένη και οργανωμένη πορεία των μέτρων που λαμβάνονται για να επιτευχθεί και να διατηρηθεί το κατάλληλο επίπεδο ασφάλειας των πληροφοριών. Για το λόγο αυτό, η προτεινόμενη εφαρμογή για την IT-Grundschutz παρουσιάζεται σαφώς για κάθε μία φάση που περιγράφεται στο πρότυπο BSI 100-1.

Η IT-Grundschutz αποτελεί ένα πρότυπο για τη δημιουργία και διατήρηση ενός κατάλληλου επιπέδου προστασίας για όλες τις πληροφορίες σε έναν οργανισμό. Η μέθοδος αυτή, που εισήχθη από την BSI το 1994 και τελειοποιήθηκε από τότε, προσφέρει τόσο μια μεθοδολογία για τη δημιουργία ενός συστήματος διαχείρισης της ασφάλειας των πληροφοριών όσο και μια συνολική βάση για την αξιολόγηση των κινδύνων, την παρακολούθηση του υπάρχοντος επιπέδου ασφάλειας, καθώς και την εφαρμογή της κατάλληλης προστασίας των πληροφοριών.

Ένας από τους σημαντικότερους στόχους της IT-Grundschutz είναι να μειωθεί το κόστος της διαδικασίας ασφαλείας των πληροφοριών προσφέροντας την επαναχρησιμοποίηση γνωστών διαδικασιών για τη βελτίωση της ασφάλειας των πληροφοριών. Με τον τρόπο αυτό, η Κατάλογοι της IT-Grundschutz περιέχουν τυπικούς κινδύνους και διασφαλίσεις για τις τυπικές επιχειρησιακές διαδικασίες ασφάλειας και τα συστήματα IT που μπορούν να χρησιμοποιηθούν σε μια εταιρεία.

Απευθύνεται κυρίως σε εκείνους που είναι υπεύθυνοι για την ασφάλεια, σε αξιωματικούς ασφαλείας, και γενικότερα σε κάθε ενδιαφερόμενο ο οποίος είναι εξοικειωμένος με τη διαχείριση της ασφάλεια πληροφοριών. Η Μεθοδολογία IT-Grundschutz απευθύνεται σε οργανισμούς όλων των τύπων και μεγεθών που απαιτούν μια οικονομικώς αποδοτική και στοχοθετημένη μέθοδο για τη δημιουργία και την εφαρμογή του κατάλληλου επιπέδου ασφαλείας.

Η μεθοδολογία αυτή παρέχει ένα ολοκληρωμένο πλαίσιο για μια ISMS και πρέπει μόνο να προσαρμοστεί στις συνθήκες ενός οργανισμού, ώστε να μπορεί να δημιουργηθεί ένα κατάλληλο σύστημα διαχείρισης της ασφάλεια των πληροφοριών.

Η IT-Grundschutz μεθοδολογία παρέχει ενίσχυση στη δημιουργία και τη διατήρηση της διαδικασίας ασφαλείας πληροφοριών σε έναν οργανισμό αποκαλύπτοντας μονοπάτια και μεθόδους για τη γενική πορεία δράσης, αλλά και για λύσεις σε ειδικά προβλήματα.

Για να επιτευχθεί το κατάλληλο επίπεδο ασφάλειας, μια συστηματική προσέγγιση είναι απαραίτητη για το σχεδιασμό της διαδικασίας ασφάλειας. Η διαδικασία της ασφάλειας αποτελείται από τις ακόλουθες φάσεις στο πλαίσιο της IT-Grundschutz:

1. ***Κίνηση της διαδικασίας ασφάλειας***: Η διοίκηση πρέπει να κινήσει, να ελέγξει και να παρακολουθήσει τη διαδικασίας της ασφάλειας. Για να επιτευχθεί αυτό, απαιτούνται βασικές στρατηγικές δηλώσεις σχετικά με την ασφάλεια των πληροφοριών, καθώς και οργανωτικό πλαίσιο.

- ***Αποδοχή της ευθύνης από τη διοίκηση:*** Η διαχείριση είναι ενημερωμένη σχετικά με τους πιθανούς κινδύνους και τις συνέπειες της ανεπαρκούς ασφάλειας των πληροφοριών και αναλαμβάνει πλήρως την ευθύνη για την ασφάλεια των πληροφοριών. Η διαχείριση είναι αυτή που κινεί τη διαδικασία ασφάλειας των πληροφοριών στο πλαίσιο του οργανισμού.
- ***Σχεδιασμός και προγραμματισμός της διαδικασίας ασφάλειας:*** Διορίζονται πρόσωπα επαφής για όλες τις επιχειρηματικές διαδικασίες και τις εξειδικευμένες εργασίες, εκτελείται μια πρόχειρη εκτίμησης της αξίας των πληροφοριών, των επιχειρηματικών διαδικασιών, καθώς και των εξειδικευμένων καθηκόντων, προσδιορίζονται οι γενικές απαιτήσεις, εκτιμάται η σημασία των επιχειρηματικών διαδικασιών, των εξειδικευμένων στόχων, καθώς και των πληροφοριών, καθορίζονται οι γενικοί στόχοι της ασφάλειας των πληροφοριών και επιτυγχάνεται η συμφωνία της διοίκησης.
- ***Δημιουργία της πολιτικής για την ασφάλεια των πληροφοριών:*** Αποκτάται ένα αίτημα από τη διοίκηση για την ανάπτυξη της πολιτικής της ασφάλειας, διευκρινίζεται το πεδίο εφαρμογής, στη συνέχεια καλείται μια ομάδα ανάπτυξης για την πολιτική ασφαλείας και οργανώνεται η έγκριση από τη διαχείριση για την πολιτική ασφάλειας. Μετά, ανακοινώνεται η πολιτική ασφάλειας, ελέγχεται και ενημερώνεται τακτικά εάν είναι απαραίτητο.
- ***Δημιουργία μιας κατάλληλης οργανωτικής δομής για τη διαχείριση της ασφάλειας πληροφοριών:*** Καθορίζονται οι ρόλοι για το σχεδιασμό της διαδικασίας της ασφάλειας των πληροφοριών, ανατίθενται τα καθήκοντα και οι περιοχές των ρόλων στους αρμόδιους και καθορίζονται οι ανθρώπινοι πόροι που απαιτούνται για τους ρόλους αυτούς. Επίσης, τεκμηριώνεται η οργάνωση ασφάλειας πληροφοριών και ενσωματώνεται η διαχείριση της ασφάλειας των πληροφοριών σε επίπεδο διεργασιών και διαδικασιών μιας οργάνωσης.
- ***Παροχή οικονομικών πόρων, του προσωπικού και του απαραίτητου χρόνου:*** Εξετάζονται οι παράγοντες της καταλληλότητας και της σχέσης κόστους-αποτελεσματικότητας κατά τη διαδικασία ασφάλισης και επιβεβαιώνεται ότι υπάρχει μια ισορροπία μεταξύ των οργανωτικών και τεχνικών ασφάλειας των πληροφοριών. Ακόμα, ζητούνται κατάλληλοι πόροι για πράξεις ΤΠ, τη διαχείριση της ασφάλειας των πληροφοριών, καθώς και την παρακολούθηση της ασφάλειας των πληροφοριών. Αν χρειαστεί, χρησιμοποιούνται εξωτερικοί πόροι.
- ***Ένταξη όλων των εργαζομένων στη διαδικασία της ασφάλειας:*** Εργαζόμενοι και επιτροπές εργαζομένων ή του εποπτικού συμβουλίου συμμετέχουν στον προγραμματισμό και τον σχεδιασμό των δικλείδων ασφαλείας και των κανόνων σε πρώιμο στάδιο. Όλοι οι εργαζόμενοι εξασκούνται στις σχετικές πτυχές της ασφάλειας των πληροφοριών και εγείρουν την ευαισθητοποίηση τους τακτικά. Ο σκοπός της διασφάλισης της ασφάλειας εξηγείται σε όλους τους εργαζόμενους, ορίζεται ένα άτομο επαφής για θέματα ασφαλείας και οι εργαζομένους ενημερώνονται για το τι είναι υπεύθυνο αυτό το πρόσωπο. Διευκρινίζονται και ανακοινώνονται η πορεία αναφοράς και η κλιμάκωση των συμβάντων ασφαλείας. Τέλος, εξασφαλίζεται ότι οι απαιτούμενες εγγυήσεις ασφάλειας ακολουθούνται όταν ένας εργαζόμενος αποχωρήσει ή διακοπούν θέσεις εργασίας.

2. ***<u>Δημιουργία ενός σχεδίου ασφάλειας</u>***: Καθορίζονται το περιεχόμενο του σχεδίου ασφαλείας, οι κρίσιμες επιχειρηματικές διαδικασίες, οι εξειδικευμένοι στόχοι, ή τα τμήματα ενός οργανισμού που θα περιλαμβάνονται στο σχέδιο. Καθορίζονται σαφώς τα όρια του πεδίου εφαρμογής και περιγράφονται οι διεπαφές στους εξωτερικούς συνεργάτες

   - ***Καθορισμός του στόχου:*** Πριν από τη δημιουργία ενός σχεδίου ασφάλειας, στους τομείς της οργάνωσης στην οποία θα ισχύει, πρέπει να καθορίζεται το πεδίο εφαρμογής της έννοιας της ασφάλειας. Το πεδίο εφαρμογής μπορεί να είναι ίδιο με το πεδίο εφαρμογής της πολιτικής για την ασφάλεια των πληροφοριών, αλλά θα είχε επίσης νόημα να αναπτυχθούν σχέδια ασφαλείας για μικρότερες περιοχές.

- ***Ανάλυση της δομής:*** Η ανάλυση της δομής χρησιμοποιείται για τη διεξαγωγή μιας προκαταρκτικής έρευνας για τις πληροφορίες που απαιτούνται για τις επιπλέον διαδικασίες κατά τη δημιουργία ενός σχεδίου ασφάλειας, σύμφωνα με IT-Grundschutz. Σε αυτή την περίπτωση, αυτό σημαίνει την τεκμηρίωση των στοιχείων (πληροφορίες, εφαρμογές, συστήματα πληροφορικής, τα δωμάτια, τα δίκτυα επικοινωνίας) που απαιτούνται για την άσκηση των επιχειρηματικών διαδικασιών ή εξειδικευμένων εργασιών που καθορίζονται να είναι στο πεδίο εφαρμογής.
- ***Προσδιορισμός των απαιτήσεων για την προστασία:*** Προσδιορίζονται οι κατηγορίες των απαιτήσεων προστασίας: Εξετάζονται τα τυπικά σενάρια βλάβης για τον καθορισμό των κατηγοριών των απαιτήσεων για την προστασία. Ορίζονται οι "κανονική", "υψηλή " και "πολύ υψηλή" κατηγορίες απαιτήσεων προστασίας, ή προσαρμόζονται ανάλογα με την οργάνωση. Ο κίνδυνος μπορεί να υπολογίζεται από τον πολλαπλασιασμό της έκτασης βλάβης με την πιθανότητα εμφάνισης. Στον παρακάτω πίνακα φαίνεται η σύγκριση των κατηγοριών ζημίας και των κατηγοριών απαιτήσεων για την προστασία.

Κατηγορίες Ζημίας		**Κατηγορίες Απαιτήσεων Προστασίας**	
Κατηγορία	**Επεξήγηση**	**Κατηγορία**	**Επεξήγηση**
"ΧΑΜΗΛΗ"	Η αποτυχία έχει μια μικρή, μόλις αξιοπρόσεχτη επίδραση.		
"ΜΕΤΡΙΑ"	Η αποτυχία έχει αξιοσημείωτες επιπτώσεις.	**"ΜΕΤΡΙΑ"**	Τα αποτελέσματα της ζημίας είναι περιορισμένες και διαχειρίσιμες.
"ΥΨΗΛΗ"	Η αποτυχία έχει σοβαρές επιπτώσεις.	**"ΥΨΗΛΗ"**	Τα αποτελέσματα της ζημίας μπορεί να είναι σημαντικό.
"ΠΟΛΎ ΥΨΗΛΗ"	Η αποτυχία ή η βλάβη οδηγεί σε αποτελέσματα που απειλούν την ύπαρξη της οργάνωσης.	**"ΠΟΛΎ ΥΨΗΛΗ"**	Τα αποτελέσματα της ζημίας μπορεί να φτάσει σε καταστροφικά επίπεδα που απειλεί την ύπαρξη της οργάνωσης.

Πίνακας 7: Σύγκριση των κατηγοριών ζημίας και των κατηγοριών απαιτήσεων για την προστασία

- ***Επιλογή και προσαρμογή των μέτρων διασφάλισης***
- ***Βασικός έλεγχος ασφαλείας:*** Γίνεται η οργανωτική προετοιμασία για το βασικό έλεγχο ασφαλείας, εκτελείται ο στόχος, ουσιαστικά γίνεται σύγκριση με την πραγματική κατάσταση και τέλος τεκμηριώνονται τα αποτελέσματα.
- ***Συμπληρωματική ανάλυση ασφαλείας:*** Γίνεται προσέγγιση της μεθοδολογίας IT-Grundschutz σε δύο στάδια: Στο πρώτο στάδιο, καθορίζονται οι απαιτήσεις για την προστασία του αντικειμένου στον τομέα της πληροφορικής. Στο δεύτερο στάδιο εξετάζονται ποιοι άλλοι κίνδυνοι σχετίζονται με τον τομέα της πληροφορικής και πρέπει να ληφθούν υπόψη. Επίσης, γίνεται συμπληρωματική ανάλυση ασφαλείας.

3. ***Εφαρμογή του σχεδίου ασφάλειας***: Ένα ικανοποιητικό επίπεδο ασφάλειας μπορεί να επιτευχθεί μόνο εάν οι υπάρχουσες αδυναμίες καθορίζονται κατά την ανάλυση της ασφάλειας, αν το στάτους κβο είναι εγγεγραμμένο στην έννοια της ασφάλειας, αν οι αναγκαίες διασφαλίσεις έχουν προσδιοριστεί και, πάνω απ 'όλα, αν οι διασφαλίσεις αυτές, έχουν επίσης, πλήρως υλοποιηθεί.

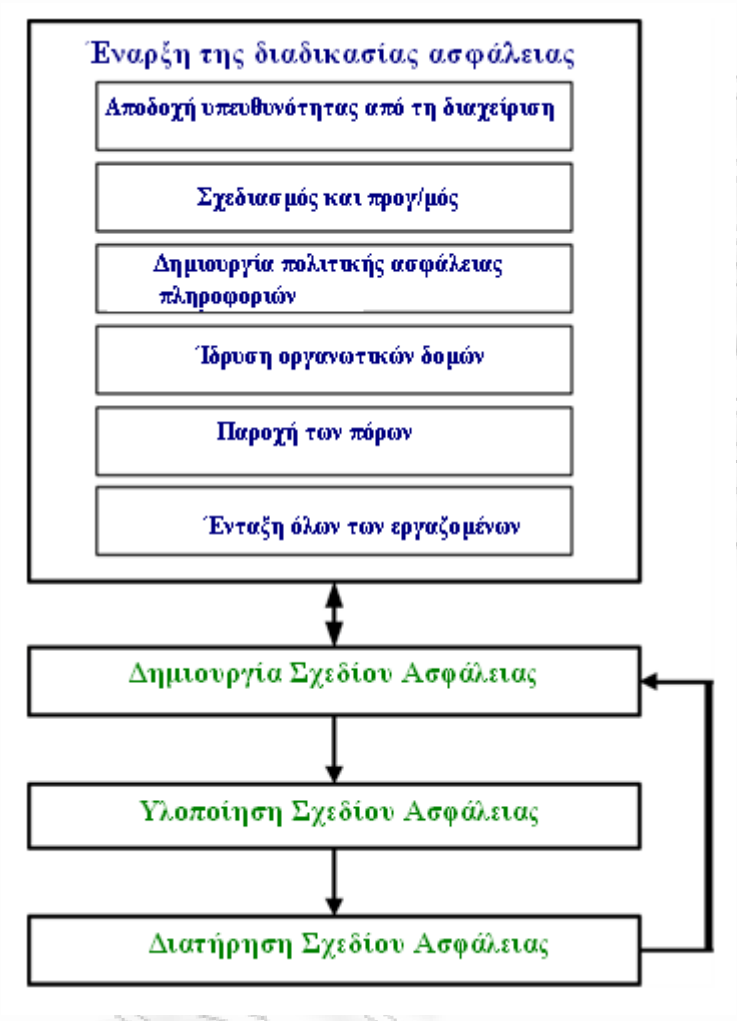
   - ***Επισκόπηση των αποτελεσμάτων της εξέτασης:*** Οι εγγυήσεις που λείπουν ή έχουν εν μέρει υλοποιηθεί θα πρέπει να αξιολογηθούν σε μια συνολική ιδέα. Οι αναλύσεις κινδύνου μπορούν να χρησιμοποιηθούν για τον εντοπισμό τυχόν πρόσθετων

εγγυήσεων που πρέπει να υλοποιηθούν. Αυτές θα πρέπει να τεκμηριώνεται με τη μορφή ενός πίνακα. Οι συμπληρωματικές αυτές εγγυήσεις θα πρέπει να ανατίθενται στα αντικείμενα-στόχους που εξετάστηκαν κατά τη μοντελοποίηση και οι αντίστοιχες IT-Grundschutz ενότητες σύμφωνα με τον τομέα τους.

- ***Εδραίωση της διασφάλισης:*** Πρώτα εδραιώνονται οι εγγυήσεις ασφάλειας που πρέπει ακόμα να υλοποιηθούν. Αν εκτελούνται πρόσθετες αναλύσεις κινδύνου, τότε πρόσθετες εγγυήσεις ασφάλειας μπορούν να προσδιοριστούν, οι οποίες συμπληρώνουν ή ακόμη αντικαθιστούν τις διασφαλίσεις των Κατάλογων IT-Grundschutz. Σε αυτήν την περίπτωση, θα πρέπει να εξεταστεί ποια ή ποιες IT-Grundschutz εγγυήσεις δε πρέπει να εφαρμοστούν, δεδομένου ότι θα αντικατασταθούν από τις εγγυήσεις ασφάλειας υψηλότερης ποιότητας.
- ***Εκτίμηση των απαιτούμενων εξόδων και προσωπικού:*** Καθορίζεται το κόστος της επένδυσης και το μέγεθος του προσωπικού που απαιτείται για την υλοποίηση κάθε διασφάλισης που αναφέρεται στην εφαρμογή.
- ***Καθορισμός της σειράς εφαρμογής των εγγυήσεων:*** Εάν ο υφιστάμενος προϋπολογισμός ή οι πόροι του προσωπικού δεν επαρκούν για να υλοποιηθούν οι εγγυήσεις που λείπουν, τότε πρέπει να καθορίζεται η σειρά με την οποία οι εγγυήσεις αυτές θα τεθούν σε εφαρμογή.
- ***Καθορισμός των καθηκόντων και των ευθυνών:*** Μετά τον καθορισμό της σειράς εφαρμογής των εγγυήσεων, πρέπει να διευκρινιστεί ποιος θα υλοποιήσει ποια διασφάλιση και μέχρι πότε πρέπει να εφαρμοστούν.
- ***Διασφαλίσεις που συνοδεύουν την υλοποίηση:*** Είναι εξαιρετικά σημαντικό να σχεδιάσει και να προγραμματιστεί η εφαρμογή των πρόσθετων εγγυήσεων που θα συνοδεύουν την εφαρμογή μιας συγκεκριμένης διασφάλισης.

4. ***Διατήρηση της ασφάλειας των πληροφοριών κατά τη διάρκεια ενεργών εργασιών και εφαρμογή μιας διαδικασίας συνεχούς βελτίωσης***: Ο στόχος της διαχείρισης της ασφάλειας είναι να επιτευχθεί το επιθυμητό επίπεδο ασφάλειας, να διατηρηθεί αυτό το επίπεδο μακροπρόθεσμα, και να βελτιωθεί. Για το λόγο αυτό, η καταλληλότητα, η αποτελεσματικότητα, και η αποδοτικότητα της διαδικασίας της ασφάλειας και των οργανωτικών δομών για την ασφάλεια των πληροφοριών πρέπει να ελέγχονται τακτικά. Πρέπει επίσης να εξεταστεί το αν οι εγγυήσεις στο σχέδιο ασφάλειας είναι πρακτικές και έχουν εφαρμοστεί σωστά.

   - ***Έλεγχος της διαδικασίας ασφάλειας των πληροφοριών σε όλα τα επίπεδα***: Ελέγχονται οι μέθοδοι για τον έλεγχο της διαδικασίας ασφάλειας των πληροφοριών, η εφαρμογή των μέτρων διασφάλισης της ασφάλειας και η καταλληλότητα της στρατηγικής ασφάλειας των πληροφοριών. Γίνεται ενσωμάτωση των αποτελεσμάτων στη διαδικασία της ασφάλειας των πληροφοριών.
   - **Ροή των πληροφοριών κατά τη διαδικασία της ασφάλειας των πληροφοριών**: Γίνονται αναφορές προς τη διαχείριση και τεκμηριώνεται το πλαίσιο της διαδικασίας της ασφάλειας των πληροφοριών.



Σχήμα 2: Ροή των πληροφοριών κατά τη διαδικασία της ασφάλειας των πληροφοριών

3.2 Εργαλεία που αποτελούν από μόνα τους μια μεθοδολογία για Πληροφοριακά συστήματα

Τα παρακάτω εργαλεία για τη διαχείριση των κινδύνων στα πληροφοριακά συστήματα αποτελούν τα ίδια μεθοδολογίες από μόνα τους:

3.2.1 Μεθοδολογία/ Εργαλείο OCTAVE

Το Software Engineering Institute (SEI) στο Carnegie Mellon University αναπτύξει τη διαδικασία Operationally Critical, Threat, Asset and Vulnerability Evaluation (OCTAVE). Ο κύριος στόχος στην ανάπτυξη της OCTAVE είναι να βοηθήσει τους οργανισμούς να βελτιώσουν την ικανότητά τους να διαχειρίζονται και να προστατεύουν τον εαυτό τους από κινδύνους για την ασφάλεια των πληροφοριών. Η OCTAVE είναι βασισμένη στο εργαστήριο και στο εργαλείο. Αυτό σημαίνει ότι αντί να συμπεριλαμβάνεται εκτεταμένη εμπειρογνωμοσύνη ασφάλειας σε ένα εργαλείο, οι συμμετέχοντες στην αξιολόγηση του κινδύνου πρέπει να κατανοήσουν τους κινδύνους και τις συνιστώσες του. Το εργαστηριακή προσέγγιση ενστερνίζεται την αρχή ότι ο οργανισμός θα καταλάβει τον κίνδυνο καλύτερα από ότι ένα εργαλείο και ότι οι αποφάσεις θα λαμβάνονται από τον οργανισμό και όχι από ένα εργαλείο. Υπάρχουν τρεις φάσεις των εργαστηρίων:

Στην **1η Φάση** συλλέγονται γνώσεις σχετικά με σημαντικά κεφάλαια, τις απειλές και την προστασία των στρατηγικών από τα ανώτερα διοικητικά στελέχη. Η 1η φάση αποτελείται από τις ακόλουθες διαδικασίες:

- Διαδικασία 1: Εντοπισμός των Γνώσεων της Ανώτερης Διαχείρισης
- Διαδικασία 2: (πολλαπλός) Προσδιορισμός των Γνώσεων της Διαχείρισης στον Επιχειρησιακό Χώρο
- Διαδικασία 3: (πολλαπλός) Προσδιορισμός των Γνώσεων του Προσωπικού
- Διαδικασία 4: Δημιουργία του Προφίλ των Απειλών

Στη **2η Φάση** συλλέγεται η γνώση των διαχειριστών στον επιχειρησιακό τομέα. Η Φάση 2 αποτελείται από τις ακόλουθες διεργασίες:

- Διαδικασία 5: Να επισημανθούν τα βασικά συστατικά
- Διαδικασία 6: Αξιολόγηση επιλεγμένων συστατικών

Στην **3η Φάση** συγκεντρώνεται η γνώση από το προσωπικό. Η Φάση 3 αποτελείται από τις ακόλουθες διαδικασίες:

- Διαδικασία 7: Διεξαγωγή Ανάλυση Κινδύνου
- Διαδικασία 8: Ανάπτυξη Στρατηγικής Προστασίας (εργαστήριο Α: ανάπτυξη στρατηγικής) (εργαστήριο Β: επισκόπηση, αναθεώρηση, έγκριση στρατηγικής)

Οι δραστηριότητες αυτές παράγουν μια όψη του κινδύνου που λαμβάνει υπόψη απόψεις από ολόκληρο τον οργανισμό, ελαχιστοποιώντας παράλληλα τον χρόνο των μεμονωμένων συμμετεχόντων. Οι έξοδοι της διαδικασίας OCTAVE είναι:

- Στρατηγική Προστασίας
- Σχέδιο μετριασμού
- Κατάλογος Ενέργεια

Η προσέγγιση OCTAVE (Operationally Critical, Threat, Asset and Vulnerability Evaluation) ορίζει μια στρατηγική αξιολόγησης και τεχνική σχεδιασμού για την ασφάλεια με βάση τον κίνδυνο. Η OCTAVE είναι μια αυτο-κατευθυνόμενη προσέγγιση, πράγμα που σημαίνει ότι οι άνθρωποι από μια οργάνωση αναλαμβάνουν την ευθύνη για τον καθορισμό στρατηγικής για την ασφάλεια του οργανισμού. Η OCTAVE-S είναι μια παραλλαγή της προσέγγισης προσαρμοσμένη στα περιορισμένα μέσα και τους μοναδικούς περιορισμούς που κατά κανόνα βρίσκονται σε μικρούς οργανισμούς (λιγότερο από 100 άτομα). Η OCTAVE-S οδηγείται από μια μικρή, διεπιστημονική ομάδα (τριών έως πέντε ατόμων) του προσωπικού ενός οργανισμού η οποία συγκεντρώνει και αναλύει τα στοιχεία, παράγει μια στρατηγική προστασίας και μετριασμού των σχεδίων με βάση το μοναδικό λειτουργικό κίνδυνο ασφαλείας του οργανισμού. Για την αποτελεσματική διεξαγωγή της OCTAVE-S, η ομάδα πρέπει να έχει ευρεία γνώση των δραστηριοτήτων της οργάνωσης και των διαδικασιών ασφαλείας, ώστε να είναι σε θέση να διεξάγει όλες τις δραστηριότητες από μόνη της.

Επίπεδο αναφοράς του προϊόντος: Δημόσιοι / κυβερνητικοί οργανισμοί όπως το Carnegie Mellon University (USA) και CERT (Computer Emergency Response Team). Ο καταλληλότερος τύπο οργανισμών στους οποίους αποσκοπεί το προϊόν αυτό είναι SME. Το είδος των χρηστών στο οποίο στοχεύει είναι Προσωπικό Διαχείρισης και Λειτουργικό προσωπικό**.**

Τέλος, η μέθοδος αυτή παρέχει διασυνδέσεις με άλλες οργανωτικές διαδικασίες όπως η Διασφάλιση Πληροφοριών.

3.2.2 Μεθοδολογία/ Εργαλείο EBIOS

Η EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité - Έκφραση των Αναγκών και Προσδιορισμός των Στόχων Ασφαλείας) μας επιτρέπει να εκτιμήσουμε και να

αντιμετωπίσουμε τους κινδύνους. Προβλέπει, επίσης, όλα τα στοιχεία που είναι απαραίτητα για την επικοινωνία εντός του οργανισμού και έναντι των αναληφθεισών εταίρων της, καθώς και την επικύρωση του αντίμετρου. Πρόκειται συνεπώς για μια πλήρη διαχείριση των κινδύνων.

Σε γενικές γραμμές η EBIOS διαχειρίζεται τους κινδύνους με τα εξής βήματα:

- Ίδρυση του πλαισίου
- Αξιολόγηση των κινδύνων
- Διαχείριση των κινδύνων
- Επικύρωση του αντίμετρου
- Επικοινωνία και διαβούλευση σχετικά με τους κινδύνους
- Παρακολούθηση και επανεξέταση των κινδύνων

Η EBIOS είναι μια εργαλειοθήκη για ποικίλες χρήσεις ανάλογα με το θέμα που θα μελετηθεί. Μπορεί να χρησιμοποιηθεί για τη διαχείριση του κινδύνου σε μια βιομηχανία, έναν οργανισμό, ένα υποσύνολο ή μια διεργασία των τελευταίων, ένα σύστημα πληροφοριών, ένα σύστημα ηλεκτρονικού υπολογιστή, ένα σύστημα διασύνδεσης, μια εφαρμογή, ένα προϊόν ασφάλειας, ή ακόμη και ένα συστατικό του προϊόντος. Υποστηρίζει ποικιλία εργαλείων και στυλ, σύμφωνα με τα αναμενόμενα αποτελέσματα και το βάθος της διακυμαίνεται ανάλογα με τον κύκλο ζωής του αντικειμένου μελέτης. Μπορεί να υπάρξει παραλλαγή του πλαισίου ανά τομέα. Μια εξέταση της στρατηγικής που θα εφαρμοστεί είναι απαραίτητη.

Η αποτελεσματική και αξιόπιστη λήψη αποφάσεων Το εργαλείο EBIOS με τα κατάλληλα δικαιολογητικά μπορεί να είναι κατάλληλο για τη διαπραγμάτευση και τη διαιτησία κατά τη λήψη αποφάσεων. Είναι ένα εργαλείο εκπαίδευσης όλων των εμπλεκομένων φορέων του έργου και είναι συμβατό με τα διεθνή πρότυπα. Είναι ευέλικτο στη χρήση πολλαπλών παραδοτέων, είναι γρήγορο και επαναχρησιμοποιήσιμο εργαλείο. Η δομημένη προσέγγιση της μεθόδου EBIOS επιτρέπει τον προσδιορισμό και τον συνδυασμό των στοιχείων του κινδύνου. Αυτή η μέθοδος κατασκευής εξασφαλίζει την πληρότητα της ανάλυσης κινδύνου. Η EBIOS έχει πλούσιες βάσεις γνώσης που προσαρμόζονται σε ένα ελεύθερο και δωρεάν λογισμικό εκπαίδευσης για την ποιότητα στον δημόσιο και ιδιωτικό τομέα και για τα διάφορα υλικά επικοινωνίας. Τέλος, η μέθοδος και το εργαλείο EBIOS χρησιμοποιούνται ευρέως στον δημόσιο και τον ιδιωτικό τομέα σε Γαλλία και εξωτερικό.

Πιο αναλυτικά, η προσέγγιση της μεθόδου χωρίζεται στις παρακάτω ενότητες:

- **Στάδιο 1 - Μελέτη του Πλαισίου**
  - Βήμα 1 - Καθορισμός του πεδίου εφαρμογής της διαχείρισης:
    - Πλαισίωση της ανάλυσης κινδύνου
    - Περιγραφή του γενικού πλαισίου
    - Καθορισμός του πεδίου εφαρμογής της μελέτης
    - Προσδιορισμός των παραμέτρων προς εξέταση
    - Εντοπισμός των πηγών των απειλών
  - Βήμα 2 - Προετοιμασία μετρήσεων
    - Καθορισμός των απαιτήσεων ασφαλείας και ανάπτυξη τις κλίμακες των αναγκών
    - Ανάπτυξη μιας κλίμακας των επιπέδων δριμύτητας
    - Ανάπτυξη μιας κλίμακας των επιπέδων της πιθανότητας
    - Καθορισμός των κριτηρίων διαχείρισης των κινδύνων
  - Βήμα 3 - Προσδιορισμός των περιουσιακών στοιχείων
    - Εντοπισμός των κρίσιμων στοιχείων του ενεργητικού, των σχέσεων τους και των θεματοφυλάκων τους
    - Προσδιορισμός των κατόχων των ακινήτων, των σχέσεων τους και των ιδιοκτητών τους
    - Προσδιορισμός των σχέσεων μεταξύ των βασικών αγαθών και των κρίσιμων στοιχείων του ενεργητικού
    - Εντοπισμός υφιστάμενων μέτρων ασφαλείας

- **Στάδιο 2 – Μελέτη των επίφοβων εκδηλώσεων**
  - Βήμα 1 - Εκτίμηση των επίφοβων γεγονότων
    - Σάρωση όλων επίφοβων γεγονότων
    - Αξιολόγηση κάθε επίφοβης περίπτωσης

- **Στάδιο 3 – Μελέτη των απειλητικών σεναρίων**
  - Βήμα 1 - Αξιολόγηση των απειλητικών σεναρίων

- **Στάδιο 4 - Μελέτη των κινδύνων**
  - Βήμα 1 - Αξιολόγηση των κινδύνων
  - Βήμα 2 - Προσδιορισμός των στόχων ασφάλειας
    - Επιλέγεται το αντίμετρο των επιλεγμένων κινδύνων
    - Αναλύονται οι κινδύνους που εξακολουθούν να υπάρχουν

- **Στάδιο 5 - Ανασκόπηση της Ασφάλειας**
  - Βήμα 1 - Επισημοποίηση των μέτρων ασφαλείας προς εφαρμογή
    - Καθορίζονται τα μέτρα ασφαλείας
    - Αναλύονται οι κινδύνους που εξακολουθούν να υπάρχουν
    - Πλήρης δήλωση της εφαρμογής
  - Βήμα 2 - Εφαρμογή των μέτρων ασφαλείας
    - Ανάπτυξη σχεδίου δράσης και παρακολούθηση της εφαρμογή τους
    - Αναλύονται οι κινδύνους που εξακολουθούν να υπάρχουν
    - Χορηγείται η σχετική έγκριση ασφάλειας

3.2.3 Μεθοδολογία/ Εργαλείο COBRA

Το εργαλείο λογισμικού Cobra δίνει τη δυνατότητα αξιολόγησης των κινδύνων ασφαλείας που πρέπει να αναληφθεί από τους ίδιους τους οργανισμούς. Αξιολογεί τη σχετική σημασία όλων των απειλών και των τρωτών σημείων, και δημιουργεί τις κατάλληλες λύσεις και προτάσεις. Συνδέει αυτόματα τους κινδύνους που προσδιορίζονται με τις πιθανές συνέπειες για την επιχειρηματική μονάδα. Εναλλακτικά, μια ιδιαίτερη περιοχή ή θέμα μπορεί να εξετασθεί «μεμονωμένα», χωρίς καμία ένωση των επιπτώσεων. Το COBRA είναι εξοπλισμένο με τέσσερις διακριτές βάσεις γνώσης που μπορεί να προσαρμοστούν περαιτέρω χρησιμοποιώντας το στοιχείο Διευθυντής Module.

Τα στάδια Αξιολόγησης του κινδύνου είναι τα εξής:

- Αναγνώριση κινδύνου: Εντοπισμός απειλών του συστήματος, αδυναμιών και εκθέσεων. Μετράται ο βαθμός του πραγματικού κινδύνου για κάθε περιοχή ή πτυχή του συστήματος, και απευθείας συνδέεται με αυτόν το πιθανό αντίκτυπο των επιχειρήσεων.
- Ανάλυση κινδύνου
- Αξιολόγηση κινδύνου: Εντοπισμός απειλών του συστήματος, των τρωτών σημείων και εκθέσεων.

Τα στάδια Διαχείρισης του κινδύνου είναι τα εξής:

- Αξιολόγηση του κινδύνου
- Διαχείριση κινδύνου: Προσφέρονται λεπτομερείς λύσεις και προτάσεις για τη μείωση των κινδύνων.
- Γνωστοποίηση των κινδύνων: Παροχή επιχειρήσεων, καθώς και τεχνικών κι εκθέσεων.

3.3 Σύγκριση και Αξιολόγηση των παραπάνω μεθόδων

Στους παρακάτω πίνακες φαίνονται τα χαρακτηριστικά των πιο σημαντικών μεθοδολογιών/ εργαλείων που αναφέρθηκαν και αναλύθηκαν προηγουμένως.

Μεθοδολογία	Γενικές Πληροφορίες	Επίπεδο Αναφοράς	Αξιολόγηση και Διαχείριση Επικινδυνότητας	Πρότυπα ΠΣ
Cramm	CRAMM = CCTA Risk Analysis and Management Method Όνομα Προμηθευτή : Insight Consulting Χώρα Προέλευσης : Ηνωμένο Βασίλειο	Δημόσια/κυβερνητική οργάνωση: British CCTA (Central Communication and Telecommunication Agency)	• Προσδιορισμός και αποτίμηση αγαθών (identification and valuation of assets). • Ανάλυση πληροφορικού κινδύνου ή επικινδυνότητας (risk analysis). • Διαχείριση πληροφορικού κινδύνου ή επικινδυνότητας (risk management).	ISO/IEC 17799
Ebios	EBIOS = Expression des Besoins et Identification des Objectifs de Sécurité Όνομα Προμηθευτή : DCSSI (Direction Centrale de la Sécurité des Systémes d'Information, Premier Ministre) Χώρα Προέλευσης : Γαλλία	Οργάνωση ιδιωτικού τομέα/ένωση&Δημόσια/κυβερνητική οργάνωση: Club EBIOS, συγκέντρωση περίπου 60 επιχειρήσεων, των γαλλικών υπουργείων, καθώς και ανεξάρτητων εμπειρογνωμόνων	• Ίδρυση του πλαισίου • Αξιολόγηση των κινδύνων • Διαχείριση των κινδύνων • Επικύρωση του αντίμετρου • Επικοινωνία και διαβούλευση σχετικά με τους κινδύνους • Παρακολούθηση και επανεξέταση των κινδύνων	- ISO/IEC 27001 - ISO/IEC 15408 - ISO/IEC 17799 - ISO/IEC 13335 - ISO/IEC 21827
Magerit	Όνομα Προμηθευτή : Ministerio de Administraciones Publicas (Spanish Ministry for Public Administrations) Χώρα Προέλευσης :	Κυβερνητική οργάνωση: Ministerio de Administraciones Publicas (Ισπανικό Υπουργείο για τη Δημόσια Διοίκηση)	• Εκτίμηση μοντέλου • Χάρτης Κινδύνων • Διασφάλιση της αξιολόγησης • Κατάσταση Κινδύνου • Έκθεση Ελλείψεων • Σχέδιο Ασφαλείας	- ISO/IEC 27001/2005 - ISO/IEC 15408/2005 - ISO/IEC 17799/2005 - ISO/IEC 13335/2004

	Ισπανία			
Octave	OCTAVE v2.0, OCTAVE-S v1.0 Όνομα Προμηθευτή : Carnegie Mellon University, SEI (Software Engineering Institute) Χώρα Προέλευσης : Η.Π.Α.	Δημόσια/κυβερνητική οργάνωση: Carnegie Mellon University (USA), CERT (Computer Emergency Response Team)	• 1η Φάση: συλλέγονται γνώσεις σχετικά με σημαντικά κεφάλαια, τις απειλές και την προστασία των στρατηγικών από τα ανώτερα διοικητικά στελέχη • 2η Φάση: συλλέγεται η γνώση των διαχειριστών στον επιχειρησιακό τομέα • 3η Φάση: συγκεντρώνεται η γνώση από το προσωπικό	
NIST	Risk Management Guide for Information Technology systems Όνομα Προμηθευτή : National Institute for Standards and Technology (NIST) Χώρα Προέλευσης : Η.Π.Α.	Εθνικός οργανισμός τυποποίησης: NIST (Η.Π.Α)	• Βήμα1: Χαρακτηρισμός Συστήματος • Βήμα2: Εντοπισμός Απειλής • Βήμα 3: Προσδιορισμός Αδυναμιών • Βήμα 4: Ανάλυση Ελέγχου • Βήμα 5: Προσδιορισμός Πιθανοτήτων • Βήμα 6: Ανάλυση των επιπτώσεων • Βήμα 7: Προσδιορισμός Κινδύνων • Βήμα 8: Συστάσεις Ελέγχου • Βήμα 9: Τεκμηρίωση Αποτελεσμάτων	
IT-Grundschutz	IT-Grundschutz (IT Baseline Protection Manual) Όνομα Προμηθευτή : Federal Office for Information Security (BSI) Χώρα Προέλευσης : Γερμανία	Εθνικός οργανισμός τυποποίησης: BSI (Γερμανία)	• Κίνηση της διαδικασίας ασφάλειας • Δημιουργία ενός σχεδίου ασφάλειας • Εφαρμογή του σχεδίου ασφάλειας • Διατήρηση της ασφάλειας των πληροφοριών κατά τη διάρκεια ενεργών εργασιών και εφαρμογή μιας διαδικασίας συνεχούς βελτίωσης	- ISO/IEC 17799 - ISO/IEC 27001

Μεθοδολογία	Πρότυπα ΠΣ	Εργαλείο

Cramm	ISO/IEC 17799	**Εμπορικά εργαλεία:** **CRAMM expert CRAMM express**
Ebios	- ISO/IEC 27001 - ISO/IEC 15408 - ISO/IEC 17799 - ISO/IEC 13335 - ISO/IEC 21827	**Μη εμπορικό εργαλείο δωρεάν: EBIOS**
Magerit	- ISO/IEC 27001/2005 - ISO/IEC 15408/2005 - ISO/IEC 17799/2005 - ISO/IEC 13335/2004	**Μη εμπορικό εργαλείο: PILAR** **Εμπορικό εργαλείο:** **EAR**
Octave		**Εμπορικά εργαλεία:** **Αυτοματοποιημένο εργαλείο Octave**
NIST		
IT-Grundschutz	- ISO/IEC 17799 - ISO/IEC 27001	**Μη εμπορικό εργαλείο: GSTOOL ,** δωρεάν για τις δημόσιες αρχές **Εμπορικά εργαλειά:** **BSI – GSTOOL** **HiSolutions AG HiScout SME** **INFODAS GmbH - SAVe** **inovationtec - IGSDoku** **Kronsoft e.K. - Secu-Max** **Swiss Infosec AG - Baseline-Tool** **WCK - PC-Checkheft**

Πίνακας 8: Σύγκριση βασικών μεθοδολογιών διαχείρισης επικυνδυνότητας

4 Αξιολόγηση Επικινδυνότητας και Διαχείριση Κινδύνων σε έργα (projects) σε πληροφοριακά συστήματα

Έργο είναι μια χρονικά περιορισμένη προσπάθεια για τη δημιουργία ενός μοναδικού προϊόντος ή μιας μοναδικής υπηρεσίας, ενώ, λειτουργία είναι μια χρονικά συνεχής και επαναλαμβανόμενη προσπάθεια . Στη σημερινή εποχή, στους οργανισμούς, αναπτύσσεται όλο και περισσότερο η εργοκεντρική αντίληψη διοίκησης, δηλαδή «**Η Διοίκηση μέσω έργων (Management by project)»,** που βασίζεται στην υποκατάσταση λειτουργιών από έργα.

Ανάλυση και Διαχείριση Κινδύνων Έργου είναι μια διαδικασία που επιτρέπει την ανάλυση και διαχείριση των κινδύνων που συνδέονται με ένα έργο. Αν διενεργηθεί σωστά θα αυξήσει την πιθανότητα επιτυχούς ολοκλήρωσης του έργου όσον αφορά το κόστος, το χρόνο και τις επιδόσεις που έχει ως στόχο.

Κίνδυνοι για τους οποίους υπάρχουν άφθονα στοιχεία μπορούν να αξιολογηθούν στατιστικά. Ωστόσο, δεν υπάρχει περίπτωση δύο έργα είναι τα ίδια. Συχνά τα πράγματα πάνε στραβά, για λόγους μοναδικούς σε ένα έργο ή βιομηχανία ή εργασιακό περιβάλλον. Η αντιμετώπιση κινδύνων σε έργα διαφέρει από καταστάσεις όπου υπάρχουν επαρκή στοιχεία για να υιοθετηθεί μια αναλογιστική προσέγγιση. Επειδή τα έργα αφορούν πάντα μια ισχυρά τεχνικό, μηχανικό, καινοτόμο ή στρατηγικό περιεχόμενο, έχει αποδειχθεί ότι μια συστηματική διαδικασία είναι προτιμότερη από μια διαισθητική προσέγγιση.

4.1 Ανάλυση κινδύνου

. Αυτό το στάδιο της διαδικασίας γενικά χωρίζεται σε δύο επιμέρους στάδια: την *Ποιοτική* ανάλυση που εστιάζει στον εντοπισμό και την υποκειμενική εκτίμηση των κινδύνων και την *Ποσοτική* ανάλυση που εστιάζει σε μια αντικειμενική αξιολόγηση των κινδύνων.

- ***Ποιοτική Ανάλυση***

Ποιοτική ανάλυση επιτρέπει να προσδιοριστούν οι βασικές πηγές ή οι παράγοντες των κινδύνων. Αυτό μπορεί να είναι γίνει, για παράδειγμα, με τη βοήθεια καταλόγων ελέγχου, συνεντεύξεις ή brainstorming συνεδρίες. Αυτό είναι συνήθως συνδέεται με κάποια μορφή αξιολόγησης η οποία θα μπορούσε να είναι η περιγραφή του κάθε κινδύνου και των επιπτώσεων του ή μια υποκειμενική επισήμανση κάθε κίνδυνου (π.χ. υψηλός / χαμηλός), όσον αφορά τόσο τον αντίκτυπό του και την πιθανότητα εμφάνισης του. Ένας βασικός στόχος είναι ο προσδιορισμός των βασικών κινδύνων, ίσως μεταξύ πέντε ή δέκα, για κάθε έργο (ή μέρος του έργου όταν πρόκειται για μεγάλα έργα), οι οποίοι στη συνέχεια θα αναλυθούν και θα διαχειριστούν με περισσότερες λεπτομέρειες.

- ***Ποσοτική Ανάλυση***

Η ποσοτική ανάλυση περιλαμβάνει συνήθως πιο εξελιγμένες τεχνικές, συνήθως απαιτούν λογισμικό ηλεκτρονικών υπολογιστών. Για μερικούς αυτό είναι το πιο τυπική πτυχή της όλης διαδικασίας που απαιτείται:

- Μέτρηση της αβεβαιότητας ως προς το κόστος και το χρόνο
- Πιθανολογικός συνδυασμός των μεμονωμένων αβεβαιοτήτων.

Τέτοιες τεχνικές μπορούν να εφαρμοστούν με ποικίλα επίπεδα προσπάθειας που κυμαίνονται από μέτρια ως πιο εκτενή. Συνιστάται οι νέοι χρήστες να αρχίσουν σιγά-σιγά, ίσως ακόμα και αγνοώντας αυτή την επιμέρους φάση, μέχρι να αναπτυχθεί ένα κλίμα αποδοχής για την ανάλυση και τη διαχείριση των κινδύνων του έργου μέσα στην οργάνωση.

Μια πρώτη ποσοτική ανάλυση είναι απαραίτητη. Αυτό φέρνει σημαντικά οφέλη από άποψη κατανόηση του έργου και των προβλήματά του ανεξάρτητα από το αν διεξάγεται ποσοτική ανάλυση ή όχι. Χρησιμεύσει επίσης για να υπογραμμίζονται οι δυνατότητες για «κλείσιμο» του κινδύνου, δηλαδή η ανάπτυξη ενός ειδικού σχεδίου για την αντιμετώπιση ενός συγκεκριμένου θέματος του κινδύνου.

Η εμπειρία έχει δείξει ότι η ποιοτική ανάλυση συνήθως οδηγεί σε μια αρχικό, αν και απλό, επίπεδο ποσοτικής ανάλυσης. Εάν, για οποιοδήποτε λόγο – όπως χρόνο ή πίεση των πόρων ή περιορισμούς κόστους - είναι αδύνατο να διεξαχθούν και η ποιοτική αλλά και η ποσοτική ανάλυση, τότε είναι η ποιοτική ανάλυση που θα πρέπει να παραμείνει.

4.2 Διαχείριση κινδύνου

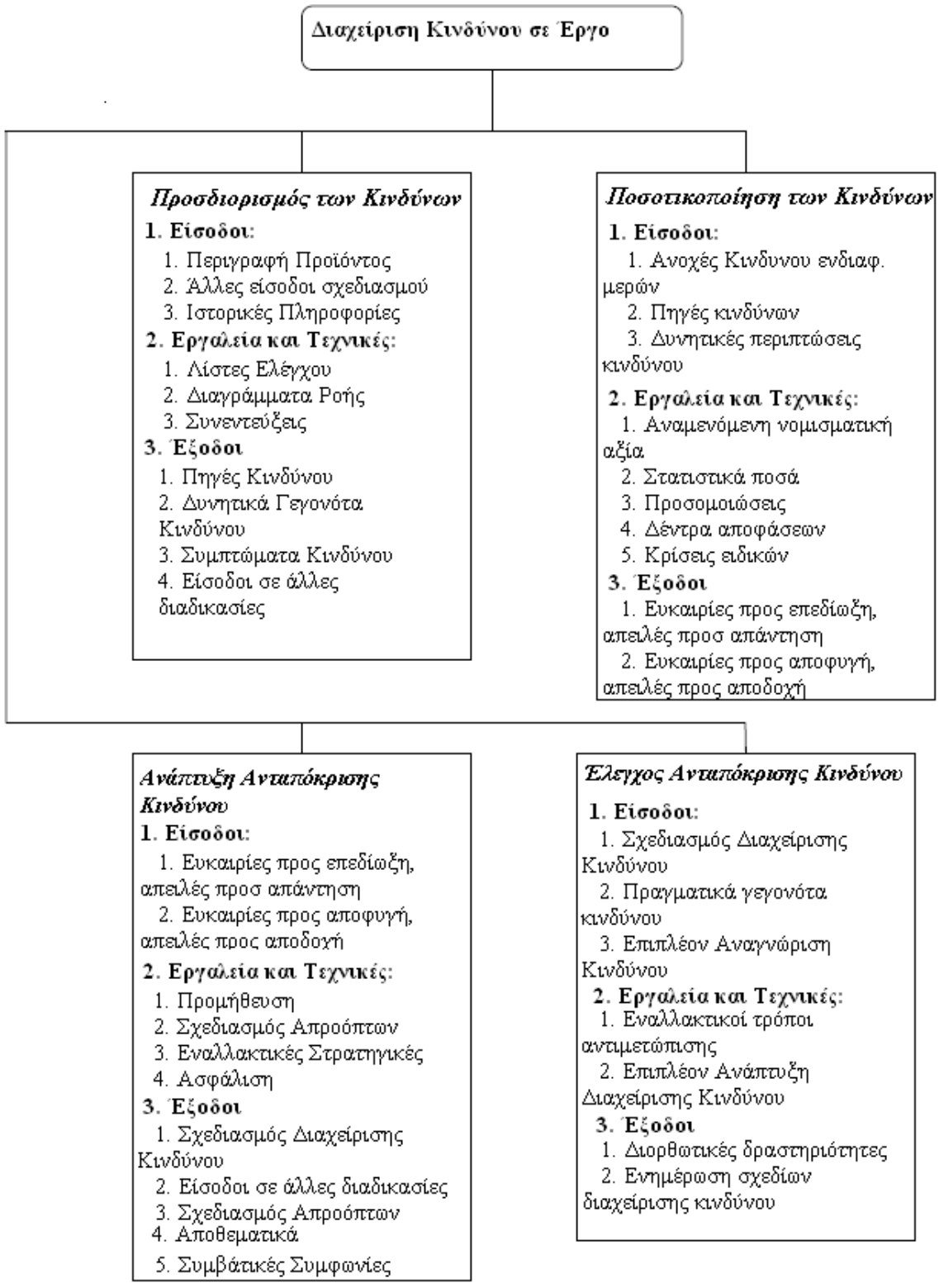
Αυτό το στάδιο της διαδικασίας περιλαμβάνει την διατύπωση των απαντήσεων διαχείρισης για τους κυριότερους κινδύνους. Η διαχείριση κινδύνων μπορεί να αρχίσει κατά τη φάση της ποιοτικής ανάλυσης καθώς η ανάγκη για ανταπόκριση στους κινδύνους μπορεί να είναι επείγουσα και η λύση αρκετά προφανής. Η επανάληψη μεταξύ της ανάλυσης και της διαχείρισης του κινδύνου είναι πιθανή. Η διαχείριση κινδύνων μπορεί να περιλαμβάνει:

- Τον εντοπισμό προληπτικών μέτρων για την αποφυγή κινδύνου ή τη μείωση της επίδρασής του
- Τη θέσπιση σχεδίων έκτακτης ανάγκης για την αντιμετώπιση κινδύνων, εάν χρειαστεί
- Νέες έρευνες για τη μείωση των αβεβαιότητας μέσω καλύτερης πληροφόρησης
- Την εξέταση της μεταβίβασης κινδύνων στους ασφαλιστές
- Την εξέταση της κατανομής των κινδύνων στις συμβάσεις
- Τον καθορισμό προοπτικών στις εκτιμήσεις κόστους, «σωσίβιο» στα προγράμματα και τα όρια ανοχής ή «απόδοση χώρου» στο προδιαγραφές απόδοσης

Οι βασικά στάδια της διαχείρισης κινδύνου ενός έργου είναι οι ακόλουθες:

- ***Προσδιορισμός των κινδύνων:*** Το στάδιο αυτό περιλαμβάνει την επισήμανση των κινδύνων που μπορεί να επηρεάσουν ένα έργο. Η αναγνώριση κινδύνου πρέπει να διεξάγεται σε τακτά χρονικά διαστήματα καθ 'όλη τη διάρκεια ζωής του έργου. Εδώ πρέπει να λαμβάνονται υπόψη εσωτερικοί και εξωτερικοί παράγοντες. Οι εσωτερικοί παράγοντες ενέχουν κινδύνους τους οποίους μπορεί να διαχειριστεί η ομάδα η οποία χειρίζεται το έργο (π.χ. η ανάθεση του έργου, το πάγωμα των αδειών, η κατανομή του προϋπολογισμού). Οι εξωτερικοί παράγοντες ενέχουν κινδύνους για τους οποίους δεν έχει λόγο το προσωπικό του έργου (π.χ. οι οικονομικές διακυμάνσεις, η πολιτική αναδιάρθρωσης ή φυσικές καταστροφές).
- ***Ποσοτικοποίηση του κινδύνου:*** Ποσοτικοποίηση είναι η εκτίμηση των κινδύνων και πώς συνδέονται με διαφορετικούς κινδύνους και επικοινωνούν μεταξύ τους, προκειμένου να προσδιοριστεί η δραστηριότητα που απαιτείται για τα διαφορετικά περιστατικά κινδύνου. Εδώ περιλαμβάνονται αρκετές διαφορετικές πτυχές:
    - Πολύπλοκοι υπολογισμοί μπορεί να οδηγήσουν σε μη ακρίβεια και συνέπεια.
    - Καλές προοπτικές για έναν παράγοντα μπορεί να είναι κακές για έναν άλλο.
    - Η εμφάνιση του κινδύνου μπορεί να προκαλέσει «φαινόμενο χιονοστιβάδας».
    - Πιθανότητα και τρόπους για να εκμεταλλευτούν την ευκαιρία επικοινωνίας με απροσδόκητους τρόπους.
- ***Ανάπτυξη Απόκρισης Κίνδυνος:*** περιλαμβάνει προληπτικά μέτρα ενάντια στις απειλές. Αυτά τα μέτρα εμπίπτουν σε μία από τις παρακάτω τέσσερις κατηγορίες:
    - Αποφυγή - κατάργηση ενός ιδιαίτερου κινδύνου. Αυτό συμβαίνει με την κατάργηση της ρίζας του προβλήματος.
    - Μείωση - μειώνεται το κόστος εμφάνισης ενός κινδύνου, με τον περιορισμό της πιθανότητας αυτού του περιστατικό.
    - Αποδοχή - για να απορροφηθούν οι συνέπειες

- ***Έλεγχος Απόκρισης Κινδύνου:*** Για την αντιμετώπιση περιστατικών κινδύνου κατά τη διάρκεια ζωής του έργου, υπάρχει ανάγκη για ελέγχου απόκρισης του κινδύνου ο οποίος περιλαμβάνει την εκτέλεση του σχεδίου διαχείρισης των κινδύνων.



Σχήμα 3: Επισκόπηση Διαχείρισης Κινδύνου ενός Έργου

5 Μεθοδολογίες και εργαλεία Ανάλυσης και διαχείρισης επικινδυνότητας για έργα (projects) σε πληροφοριακά συστήματα

Η χρήση σύγχρονων μεθοδολογιών διαχείρισης έργων κατά την υλοποίηση έργων πληροφορικής και ειδικότερα έργων Ηλεκτρονικής Διακυβέρνησης (eGovernment), κερδίζει διαρκώς έδαφος στο υφιστάμενο, δυναμικά μεταβαλλόμενο, επιχειρησιακό περιβάλλον. Οι απαιτήσεις σε αποτελεσματικές και αποδοτικές μεθοδολογίες και εργαλεία διαχείρισης έργων Ηλεκτρονικής Διακυβέρνησης είναι συνεχώς αυξανόμενες.

Οι μεθοδολογίες (Project Management Body of Knowledge, Projects IN Controlled Environments, Goal Driven Project Management, RiskNaV, NRisk) θα εξετασθούν όσον αφορά την εφαρμογή τους σε έργα πληροφορικής και ειδικότερα σε έργα Ηλεκτρονικής Διακυβέρνησης (eGovernment). Στο Πρακτικό Μέρος παρακάτω, θα παρουσιασθεί μελέτη εφαρμογής (Case Study) της μεθοδολογίας NRisk για κάποιο έργο υλοποίησης λογισμικού τηλεπικοινωνιών σταθερής τηλεφωνίας.

5.1 Μεθοδολογία PRINCE

Η μεθοδολογία PRINCE2 (**PR**ojects **IN C**ontrolled **E**nvironments) είναι μια δομημένη μέθοδος διαχείρισης του έργου που εγκρίθηκε από την κυβέρνηση του Ηνωμένου Βασιλείου ως το πρότυπο διαχείρισης έργων για τα δημόσια έργα. Η μεθοδολογία αυτή περιλαμβάνει τη διαχείριση, τον έλεγχο και την οργάνωση ενός σχεδίου. Η PRINCE2 είναι ένα de facto πρότυπο που χρησιμοποιείται ευρέως από τη βρετανική κυβέρνηση. Είναι ευρέως αναγνωρισμένη και χρησιμοποιείται στον ιδιωτικό τομέα, τόσο στη Βρετανία όσο και διεθνώς.

Η PRINCE δημιουργήθηκε το 1989 από την CCTA (the Central Computer and Telecommunications Agency), δεδομένου ότι μετονομάστηκε το OGC (the Office of Government Commerce). Βασίστηκε αρχικά στην PROMPT, μια μέθοδο διαχείρισης έργου που δημιουργήθηκε από την Simpact Systems Ltd το 1975. Όταν η PRINCE ξεκίνησε το 1989, ουσιαστικά αντικατέστησε την PROMPT στο πλαίσιο των έργων κυβέρνησης. Η PRINCE παραμένει στο δημόσιο τομέα και τα πνευματικά δικαιώματα διατηρούνται από την κυβέρνηση. Είναι ένα κατοχυρωμένο εμπορικό σήμα του OGC. Η PRINCE2 δημοσιεύθηκε το 1996, έχει συμβάλει στην κοινοπραξία των περίπου 150 ευρωπαϊκών οργανώσεων.

Τα βασικά χαρακτηριστικά του PRINCE2 είναι οι εξής:

- Η εστίασή της στην δικαίωση των επιχειρήσεων
- Μια καθορισμένη δομή οργάνωσης για την ομάδα διαχείρισης του έργου
- Η προσέγγιση σχεδιασμού με βάση τα προϊόντα
- Η έμφαση στη διαίρεση του έργου σε στάδια διαχείρισης και ελέγχου
- Η ευελιξία της που εφαρμόζεται σε επίπεδο κατάλληλο για το έργο.

Η PRINCE2 είναι μια διαδικασία με γνώμονα την μέθοδο διαχείρισης του έργου, η οποία έρχεται σε αντίθεση με τις αντιδραστικές / προσαρμοστικές μεθόδους, όπως scrum. Η PRINCE2 2009 ορίζει 40 ξεχωριστές δραστηριότητες και τις οργανώνει σε επτά διαδικασίες:

- **Αρχικοποίηση του έργου**

Σε αυτή τη διαδικασία ορίζεται η ομάδα που θα ασχοληθεί με το έργο και ετοιμάζεται μια περίληψη του έργου (όπου θα περιγράφεται, σε γενικές γραμμές, τι προσπαθεί να επιτύχει το έργο και την αιτία που η εκάστοτε επιχείρηση ξεκινά αυτό το έργο). Επιπλέον, αποφασίζεται η γενική προσέγγιση που πρέπει να ληφθεί και προγραμματίζεται η επόμενη φάση του έργου.

Μόλις ολοκληρωθεί αυτή η διαδικασία, το διοικητικό συμβούλιο του έργου καλείται να εξουσιοδοτήσει το επόμενο στάδιο, δηλαδή την έναρξη του έργου.

Οι βασικές δραστηριότητες σε αυτή τη φάση είναι οι εξής: ο διορισμός ενός διευθυντή και διαχειριστή του έργου, ο σχεδιασμός και ο διορισμός μιας ομάδας διαχείρισης του έργου, η προετοιμασία ενός σύντομου σχεδίου, ο προσδιορισμός της προσέγγιση του έργου και ο σχεδιασμός του επόμενου σταδίου (έναρξη).

- **Έναρξη του έργου**

Η διαδικασία αυτή βασίζεται στο έργο της διαδικασίας αρχικοποίησης, και η σύντομη περίληψη του έργου διευρύνεται προκειμένου να σχηματιστεί μια *Επιχειρήσιακή Υπόθεση*. Η προσέγγιση που ακολουθείται για την εξασφάλιση της ποιότητας του έργου συμφωνεί με τη συνολική προσέγγιση για τον έλεγχο του ίδιου του έργου (έλεγχοι του έργου). Δημιουργούνται επίσης τα αρχεία του έργου των σχεδίων ως ένα συνολικό σχέδιο για το έργο. Ένα σχέδιο για την επόμενη φάση του έργου επίσης δημιουργείται. Οι πληροφορίες που προκύπτουν μπορούν να τεθούν ενώπιον του τμήματος του έργου για να εγκρίνει το ίδιο το έργο.

Οι βασικές δραστηριότητες που περιλαμβάνονται εδώ είναι: ο σχεδιασμός της ποιότητας, ο σχεδιασμός ενός έργου, η διύλισης του επιχειρηματικού ενδιαφέροντος και των κινδύνων, η δημιουργία των ελέγχων για το έργο, η δημιουργία αρχείων του έργου και η συγγραφή ενός εγγράφου έναρξης του έργου.

- **Διεύθυνση του έργου**

Αυτή η διαδικασία υπαγορεύει στο Διοικητικό Συμβούλιο του Έργου (η οποία αποτελείται από τέτοιους ρόλους, όπως ο διευθύνων χορηγός ή ο χορηγός του έργου) τον τρόπο που θα πρέπει να ελέγχουν το σύνολο του σχεδίου. Επίσης, υπαγορεύεται ο τρόπος που το διοικητικό συμβούλιο του έργου θα πρέπει να εγκρίνει ένα σχέδιο, συμπεριλαμβανομένου και οποιουδήποτε σχέδιο του σταδίου, το οποίο αντικαθιστά ένα υπάρχον σχέδιο σταδίου λόγω ολίσθηση ή άλλων απρόβλεπτων καταστάσεων. Επίσης καλύπτεται ο τρόπος με τον οποίο το διοικητικό συμβούλιο μπορεί να δώσει ad-hoc κατεύθυνση για ένα έργο και τον τρόπο με τον οποίο ένα έργο πρέπει να κλείσει.

Οι βασικές δραστηριότητες που λαμβάνουν χώρα σε αυτή τη φάση είναι: έγκριση της έναρξη, έγκριση ενός έργου, έγκριση ενός σχεδίου σταδίου ή όχι, η ad-hoc κατεύθυνση και η επιβεβαίωση του κλεισίματος του έργου.

- **Έλεγχος ενός σταδίου**

Η PRINCE2 υποδηλώνει ότι τα έργα θα πρέπει να αναλύονται σε στάδια και αυτές οι επιμέρους διεργασίες υπαγορεύουν πώς θα πρέπει να ελέγχεται το κάθε στάδιο. Βασικά, περιλαμβάνει τον τρόπος με τον οποίο έχουν εγκριθεί και ληφθεί τα πακέτα εργασίας. Επίσης καθορίζει τον τρόπο με τον οποίο η πρόοδος πρέπει να παρακολουθείται και πώς τα κυριότερα σημεία της προόδου θα πρέπει να αναφέρονται στο διοικητικό συμβούλιο του έργου. Προτείνεται ένα μέσο για τη συγκέντρωση και την αξιολόγηση των παραμέτρων του έργου, σε συνδυασμό με τον τρόπο με τον οποίο πρέπει να ληφθούν διορθωτικά μέτρα. Καθορίζει επίσης τον τρόπο με τον οποίο ορισμένα θέματα του έργου θα πρέπει να κλιμακωθούν στο διοικητικό συμβούλιο του έργου.

Οι βασικές δραστηριότητες που περιλαμβάνονται είναι οι εξής: η έγκριση των πακέτων εργασίας, η αξιολόγηση της προόδου, η λήψη και η εξέταση των ζητημάτων του έργου, η αναθεώρηση της κατάστασης του σταδίου, τα σημαντικά σημεία των αναφορών, η λήψη διορθωτικών μέτρων, η κλιμάκωση των θεμάτων του έργου και η λήψη μιας ολοκληρωμένης δέσμης εργασιών.

- **Διαχείριση των ορίων του σταδίου**

Η διαδικασία ελέγχου ενός σταδίου υπαγορεύει τι πρέπει να γίνει μέσα σε ένα στάδιο, Η διαδικασία διαχείρισης των ορίων του σταδίου υπαγορεύει τι πρέπει να γίνει προς το τέλος ενός σταδίου. Είναι προφανές ότι το επόμενο στάδιο θα πρέπει να προγραμματιστεί και το συνολικό σχέδιο του έργου, η καταγραφή του κινδύνου και η τροποποίηση της επιχειρηματική υπόθεσης τροποποιούνται όπως απαιτείται. Η διαδικασία καλύπτει επίσης το τι πρέπει να γίνει για ένα

στάδιο που έχει ξεπεράσει τα επίπεδα ανοχής του. Τέλος, η διαδικασία υπαγορεύει πως θα πρέπει να αναφερθεί το τέλος του σταδίου.

Οι βασικές δραστηριότητες σε αυτή τη φάση είναι: ο σχεδιασμός μιας φάσης, η ενημέρωση ενός σχέδιο του έργου, η ενημέρωση ενός επιχειρηματικού σχεδίου, η καταγραφή του κινδύνου, η αναφορά του τελικού σταδίου και η παραγωγή ενός σχεδίου εξαίρεσης.

- **Διεύθυνση παράδοσης των προϊόντων**

Η Διεύθυνση παράδοσης των προϊόντων έχει σκοπό τον έλεγχο της σχέσης μεταξύ του Υπεύθυνου Συντονιστή και του Υπεύθυνου της (των) Ομάδας(ων) με την τοποθέτηση τυπικών προϋποθέσεων όσον αφορά την αποδοχή, την εκτέλεση και την παροχή εργασιών του έργου. Οι στόχοι της διαχειριστικής διαδικασίας παράδοσης των προϊόντων είναι:

- Να εξασφαλιστεί ότι οι εργασίες για τα προϊόντα που διατίθενται για την ομάδα έχουν εγκριθεί και συμφωνηθεί,
- Ο(ι) διαχειριστής (ές) των ομάδων, τα μέλη της ομάδας και οι προμηθευτές είναι σαφείς ως προς το τι πρέπει να παράγεται και ποια είναι η αναμενόμενη προσπάθεια, το κόστος και τα χρονοδιαγράμματα,
- Τα προγραμματισμένα προϊόντα παραδίδονται στα πλαίσια των προσδοκιών και εντός της ανοχής,
- Παρέχονται στο διαχειριστή του έργου ακριβείς πληροφορίες για την πρόοδο σε μια συμφωνημένη συχνότητα για να εξασφαλίσει ότι οι προσδοκίες ελέγχονται.

Οι βασικές δραστηριότητες είναι οι εξής: Αποδοχή ενός πακέτου εργασίας, εκτέλεση ενός πακέτου εργασίας και η παράδοση του.

- **Περάτωση του έργου**

Εδώ περιλαμβάνονται τα πράγματα που θα πρέπει να γίνουν στο τέλος του έργου. Το έργο θα πρέπει να είναι επίσημα «ελεύθερο» (και οι πόρους θα απελευθερωθούν για την κατανομή σε άλλες δραστηριότητες), οι ακόλουθες πράξεις πρέπει να εντοπίζονται και το ίδιο το έργο να αξιολογηθεί επισήμως.

Οι βασικές δραστηριότητες εδώ είναι: ο παροπλισμός ενός έργου, ο εντοπισμός των παρεπόμενων αγωγών και η αναθεώρηση της αξιολόγησης του έργου.

5.2 Μεθοδολογία GDPM

Η μεθοδολογία ***Goal Directed Project Management (GDPM)*** εισήχθη τη δεκαετία του 1980 από μια ομάδα συμβούλων διαχείρισης έργου (Kristoffer B. Grude, Erling Andersen και Tor Haug). Η GDPM έχει περάσει από πολλές εξελίξεις από την έναρξή της και η *Fast Forward Project Management LLP* αναγνωρίζει τη δύναμη και την αξία μιας «ευθείας προς τα εμπρός» και πραγματιστικής προσέγγισης της διαχείρισης ενός έργου που όχι μόνο βελτιώνει την αποτελεσματικότητα, αλλά επίσης αυξάνει την πιθανότητα επιτυχίας του έργου μέσω της χρήσης λίγων απλών τεχνικών και προτύπων.

Πρόκειται για μια ήπια και μη γραφειοκρατική προσέγγιση, η οποία διασπά την πολυπλοκότητα της διαχείρισης ενός έργου με τη χρήση απλών, πρακτικών τεχνικών οι οποίες είναι εύκολα κατανοητές από τους ανθρώπους, ανεξάρτητα από το αν είναι έμπειροι στη διαχείριση έργων ή όχι. Η GDPM μπορεί να χρησιμοποιηθεί, είτε ως αυτόνομη προσέγγιση ή σε συνδυασμό, με άλλες μεθόδους, όπως η PRINCE2, η APM, η PMI κλπ.

Η GDPM, όπως υποδηλώνει το όνομά της (***Goal Directed Project Management = Στόχος Απευθυνόμενος στη Διαχείριση Έργου)*** επικεντρώνεται στον τελικό στόχο του έργου και στο τι αποτελέσματα θα πρέπει να επιτευχθεί καθώς το έργο κινείται «προς τα εμπρός» μέσα από μια σειρά επιτευγμάτων που βασίζεται στα ορόσημα και δεν επικεντρώνεται στις λεπτομέρειες των δραστηριοτήτων για το πώς θα επιτευχθεί. Τα προκύπτοντα σχέδια για τα ορόσημα είναι συνήθως απλούστερα. Συχνά ένα σχέδιο σε μια σελίδα, το καθιστά ιδανικό

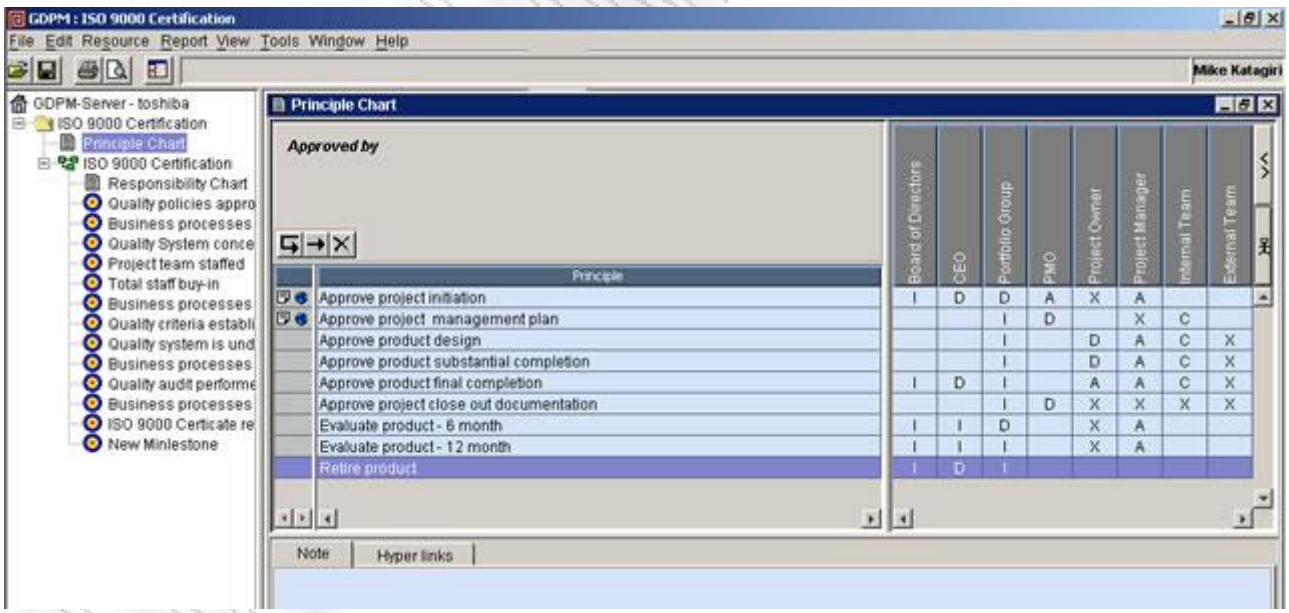
εργαλείο επικοινωνίας και ελέγχου και επειδή η εστίαση είναι σε αυτό που χρειάζεται, τα ορόσημα είναι πιο ανθεκτικά στις αλλαγές.

Η GDPM ενθαρρύνει την ενεργό χορηγία και τη συμμετοχή των ενδιαφερομένων να αποσαφηνιστεί το πεδίο εφαρμογής του σχεδίου, τα όρια, τους SMART (**S**pecific, **M**easurable, **A**chievable, **R**elevant and **T**imed = Ειδικούς, Μετρήσιμους, Εφικτούς, Σχετικούς και Χρονικά Προσδιορισμένους) στόχους και τα κριτήρια επιτυχίας. Ξεχωρίζει το σχεδιασμό του «τι» από το «πώς» και δίνει έμφαση στη συνεργατική συμμετοχή παρά στην επιβολή, για την ανάπτυξη του σχεδίου ορόσημο του έργου. Οι ρόλοι και αρμοδιότητες της ομάδας είναι σαφώς καθορισμένα χρησιμοποιώντας έναν πίνακα υπευθυνοτήτων και συμβάσεις των πόρων για να εστιάσουν την προσοχή των ατόμων στο έργο. Το μικρό και απλό σύνολο εγγράφων μεταφέρει όλες τις σχετικές πληροφορίες και καθιστά ευκολότερη τη διατήρηση του ελέγχου του έργου. Τέλος ένα πολυδιάστατο εργαλείο χρησιμοποιείται ως «συνείδηση» της ομάδας για να εξασφαλίσει ότι το έργο έχει συσταθεί και ελέγχεται αποτελεσματικά.

Η μεθοδολογία GDPM είναι μια ιδιαίτερα καλή προσέγγιση όταν χρησιμοποιείται για να προχωρήσει σε αλλαγή της επιχείρησης, χωρίς να χαλάσει λειτουργικά όρια και τη συμμετοχή ανθρώπων από όλους τους τομείς της οργάνωσης - πολλοί μπορεί να έχουν ελάχιστη ή να μην έχουν καθόλου εμπειρία διαχείρισης έργου. Είναι ήπια, μη γραφειοκρατική και εκφράζεται με απλούς όρους που χρησιμοποιούν μια γλώσσα που μπορεί να γίνει κατανοητή και να εγκριθεί τόσο από ανθρώπους που δεν είναι επαγγελματίες διαχειριστές έργων όσο και από αυτούς που έχουν ένα υπόβαθρο διαχείρισης έργου.

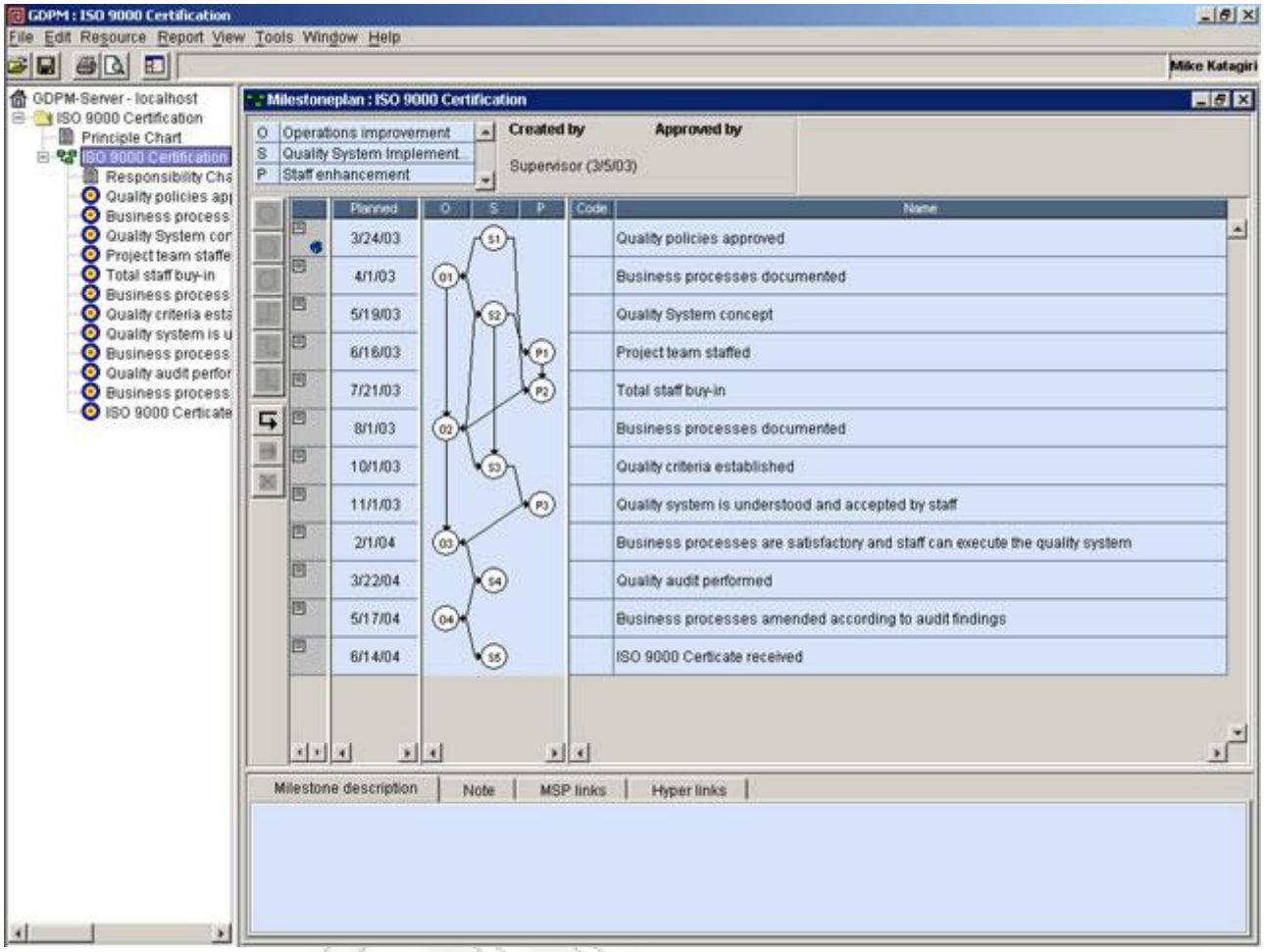
Το εργαλείο της μεθοδολογίας αυτής είναι το **Goal Director** και τα βήματα που ακολουθούνται μέσω αυτού είναι τα εξής:

1. **Καθορίζεται ο λόγος δημιουργίας του έργου *(Γιατί)***: Σε αυτό το επίπεδο, οι επιχειρηματικοί στόχοι συνδέονται σαφώς με τον σκοπό του έργου, τις αρχές και τις διαδικασίες για τη διαχείριση του έργου με σαφήνεια.



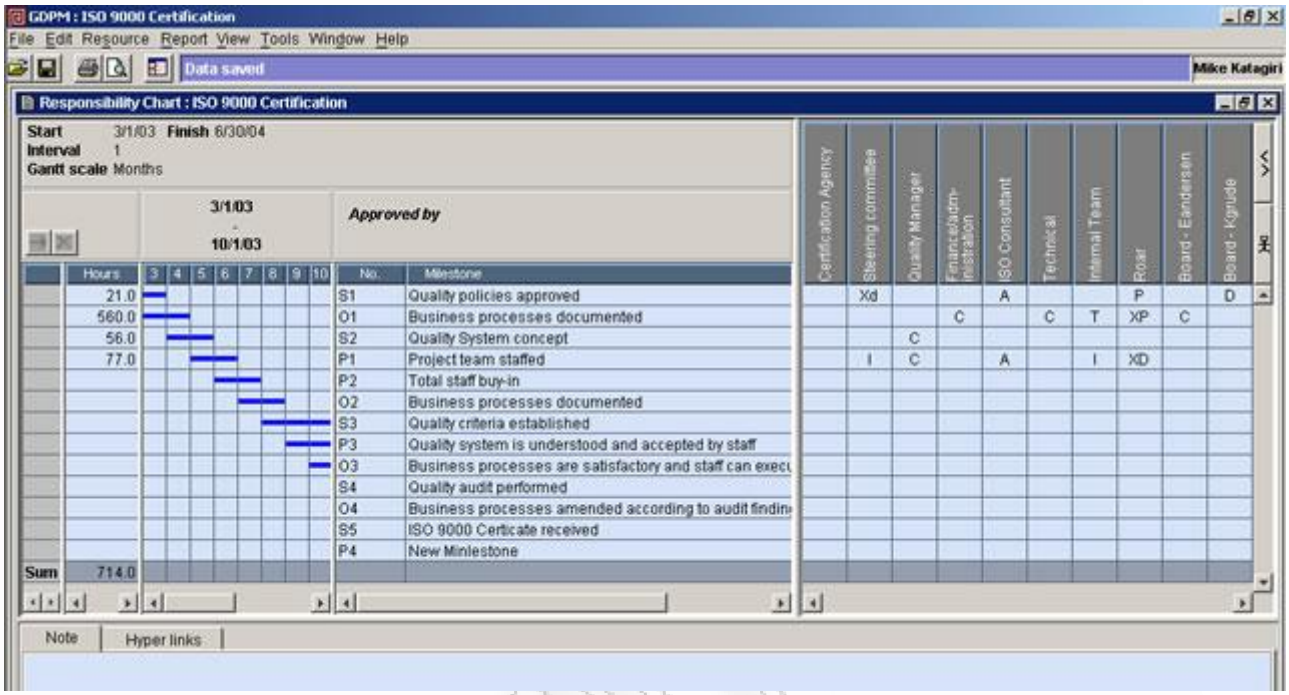
Εικόνα 1: Καθορισμός του λόγου δημιουργίας του έργου στο εργαλείο Goal Director

2. **Καθορίζονται τα Ορόσημα *(Τι)***: Το σχέδιο οροσήμων περιγράφει σαφώς τα απαιτούμενα αποτελέσματα σε μακροσκοπικό επίπεδο και παρέχει μια σταθερή εικόνα του συνόλου του έργου συμπεριλαμβανομένων των προθεσμιών.



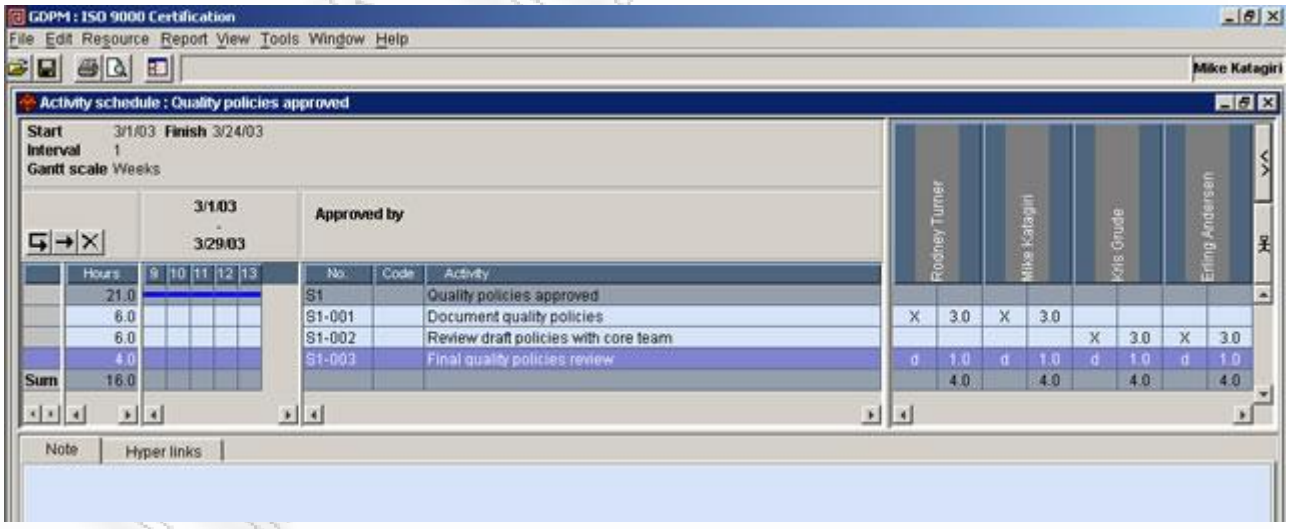
Εικόνα 2: Καθορισμός των οροσήμων στο εργαλείο Goal Director

3. **Καθορίζονται οι ευθύνες *(Ποιος)***: Ο προσδιορισμός των ρόλων που είναι αναγκαίοι για την εκτέλεση των εργασιών γίνεται απόλυτα σαφής. Έμφαση δίνεται, επίσης, σε σημαντικούς ρόλους για τους ανθρώπους μέσα και έξω από το έργο, όπως σε αυτούς που παίρνουν αποφάσεις, σε αυτούς που λαμβάνουν υπ' όψιν τις συμβουλές και σε εκείνους που ενημερώνουν.



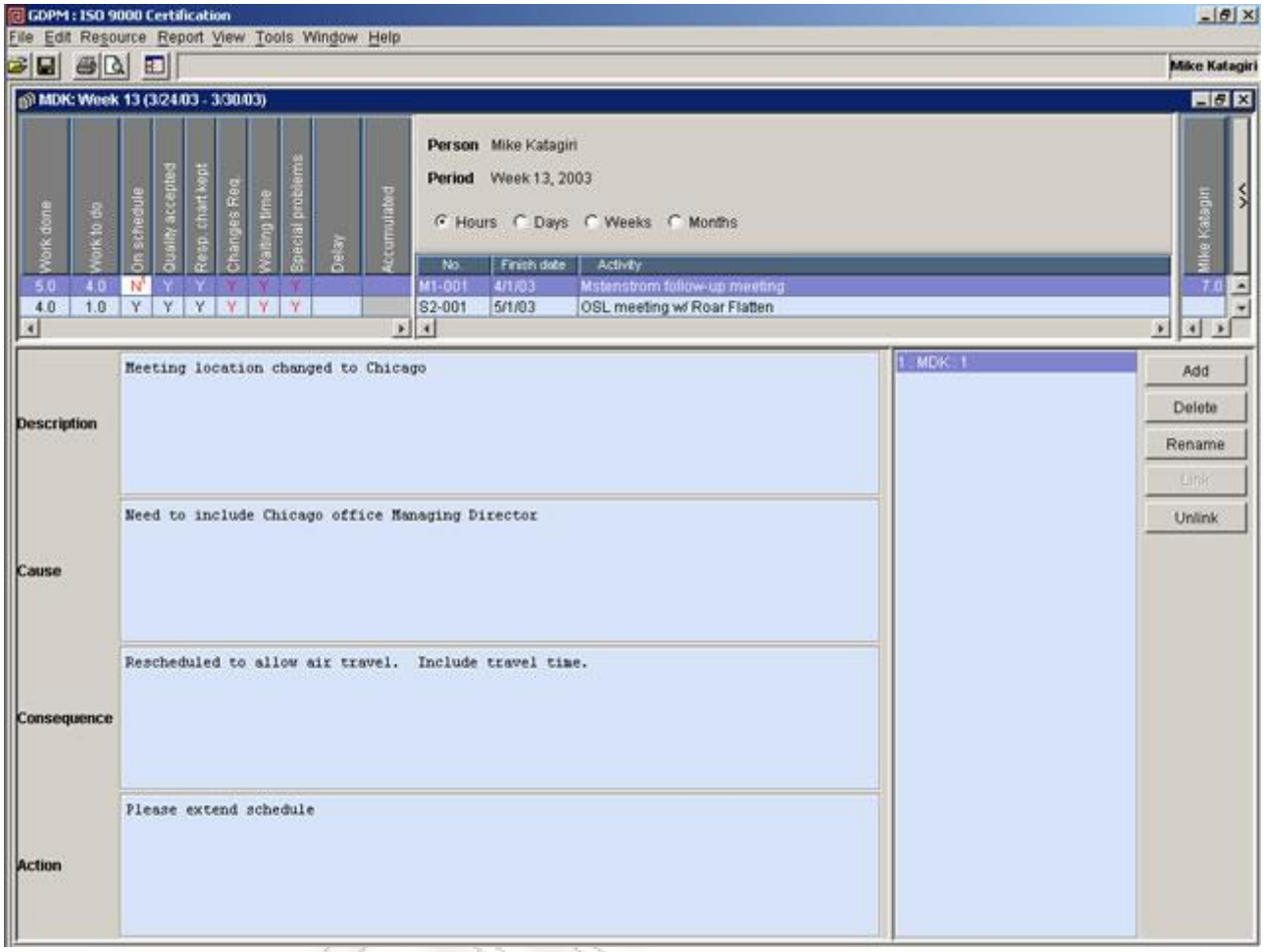
Εικόνα 3: Καθορισμός των ευθυνών στο εργαλείο Goal Director

4. **Καθορίζονται οι Δραστηριότητες *(Πώς και Πότε)***: Σε αυτό το επίπεδο, περιγράφεται η επιλογή συγκεκριμένων ανθρώπων για τους απαραίτητους ρόλους καθώς και η εκτίμηση της πραγματικής δουλειάς και του απαραίτητου χρόνου για να επιτευχθεί το κάθε ορόσημο. Όλη η απαραίτητη δουλειά για να επιτευχθούν τα ορόσημα ανατίθενται και ποσοτικοποιείται σαφώς.



Εικόνα 4: Καθορισμός των δραστηροτήτων στο έργο στο εργαλείο Goal Director

5. **Εκτέλεση Ελέγχου**: Τα φύλλα και οι εκθέσεις προόδου παρέχουν τα στοιχεία για την ανάλυση της διαχείρισης της προόδου των οροσήμων και τον προγραμματισμό των ομάδων για τις συνεργατικής δραστηριότητες που απαιτούνται για να παραμείνουν εστιασμένες στους στόχους τους.



Εικόνα 5: κτέλεση του έργου στο εργαλείο Goal Director

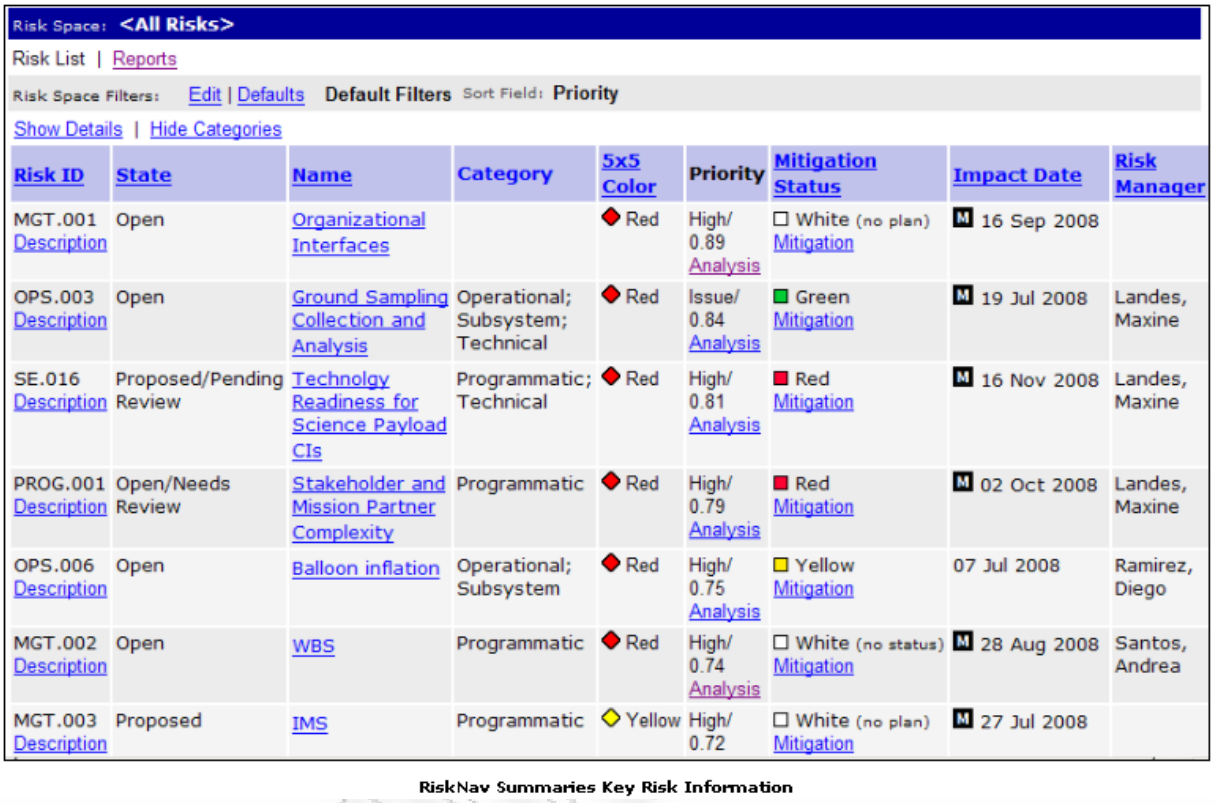
Το **Goal Director** βοηθά τις εταιρείες να επιτύχουν καλύτερα αποτελέσματα στα έργα τους με τη διευκόλυνση της ομαδικής εργασίας σε ένα σύνολο πολλών έργων και προγραμμάτων. Χορηγοί και ενδιαφερόμενα μέλη είναι σε θέση να διαχειριστούν σε υψηλό επίπεδο με τη μορφή των σχεδίων των οροσήμων. Τα μέλη της ομάδας είναι σε θέση να προγραμματίζουν και να ελέγχουν την εργασία τους με τη μορφή λεπτομερών σχεδίων δραστηριοτήτων. Οι ευθύνες γίνονται απόλυτα σαφείς και για τα δύο επίπεδα διαχείρισης. Το Goal Director μπορεί να εγκατασταθεί ως ενιαία αυτόνομη εφαρμογή ή ως πολλαπλοί πελάτες συνδεδεμένοι με ένα διακομιστή.

5.3 Μεθοδολογία RiskNav

Το RiskNav είναι ένα καλά δοκιμασμένο εργαλείο που αναπτύχθηκε από τη MITRE για να διευκολύνει τη διαδικασία του κινδύνου και να βοηθήσει τους υπεύθυνους προγραμμάτων στη διαχείριση το διάστημα του κινδύνου τους. Το RiskNav επιτρέπει να γίνει συλλογή, ανάλυση, ιεράρχηση, παρακολούθηση και απεικόνιση των πληροφοριών του κινδύνου με ένα συνεργατικό τρόπο. Αυτό το εργαλείο προσφέρει τρεις διαστάσεις της πληροφορίας γραφικά (προτεραιότητα κινδύνου, πιθανότητα, και μετριασμός/διαχείριση της κατάστασης).

Το RiskNav, αρχικά συντάχθηκε για λογαριασμό της κυβέρνησης των ΗΠΑ, έχει σχεδιαστεί για να συλλαμβάνει, να αναλύει, και να εμφανίζει τους κινδύνους σε ένα έργο ή σε ένα επίπεδο επιχειρήσεων. Το RiskNav αυτή τη στιγμή αναπτύσσεται σε ολόκληρη την κοινότητα των υπηρεσιών πληροφοριών, της ESC, FAA, Cencus και τους άλλους χορηγούς της MITRE. Το Γραφείο Μεταφοράς της Τεχνολογίας της Επιχείρησης MITRE έχει αδειοδοτήσει δύο εμπορικές εταιρείες για τη RiskNav τεχνολογία.

Το RiskNav παρουσιάζει το χώρο του κινδύνου και σε δύο μορφές:πίνακα και γραφική. Η μορφή πίνακα, όπως φαίνεται στην εικόνα παρακάτω, παρουσιάζει τις βασικές πληροφορίες για κάθε κίνδυνο και επιτρέπει στο χώρο του κινδύνου να φιλτράρεται και να διαλέγεται ώστε να επικεντρωθεί στις πιο σημαντικές τους κινδύνους.



Risk Space: <All Risks>

Risk List | Reports

Risk Space Filters: Edit | Defaults Default Filters Sort Field: Priority

Show Details | Hide Categories

Risk ID	State	Name	Category	5x5 Color	Priority	Mitigation Status	Impact Date	Risk Manager
MGT.001 Description	Open	Organizational Interfaces		Red	High/ 0.89 Analysis	White (no plan) Mitigation	16 Sep 2008	
OPS.003 Description	Open	Ground Sampling Collection and Analysis	Operational; Subsystem; Technical	Red	Issue/ 0.84 Analysis	Green Mitigation	19 Jul 2008	Landes, Maxine
SE.016 Description	Proposed/Pending Review	Technolgy Readiness for Science Payload CIs	Programmatic; Technical	Red	High/ 0.81 Analysis	Red Mitigation	16 Nov 2008	Landes, Maxine
PROG.001 Description	Open/Needs Review	Stakeholder and Mission Partner Complexity	Programmatic	Red	High/ 0.79 Analysis	Red Mitigation	02 Oct 2008	Landes, Maxine
OPS.006 Description	Open	Balloon inflation	Operational; Subsystem	Red	High/ 0.75 Analysis	Yellow Mitigation	07 Jul 2008	Ramirez, Diego
MGT.002 Description	Open	WBS	Programmatic	Red	High/ 0.74 Analysis	White (no status) Mitigation	28 Aug 2008	Santos, Andrea
MGT.003 Description	Proposed	IMS	Programmatic	Yellow	High/ 0.72	White (no plan) Mitigation	27 Jul 2008	

RiskNav Summaries Key Risk Information

Εικόνα 6: Οι βασικές πληροφορίες για κάθε κίνδυνο στο RiskNav

Το RiskNav χρησιμοποιεί ένα μοντέλο σταθμισμένου μέσου όρου που υπολογίζει μια συνολική βαθμολογία για κάθε προσδιορισμένο κίνδυνο. Η προτεραιότητα του κινδύνου είναι ο σταθμισμένος μέσος όρος του χρονικού πλαισίου (πόσο σύντομα ο κίνδυνος θα συμβεί), της πιθανότητας εμφάνισης, και των επιπτώσεων (κόστος, χρονοδιάγραμμα, τεχνική). Η βαθμολογία αυτή παρέχει μια φθίνουσα κρίσιμη σειρά κατάταξης των κινδύνων. Επισήμως, αυτό το μοντέλο βαθμολόγησης προέρχεται από την έννοια της γραμμικής χρησιμότητας, οπότε οι πιο σημαντικοί κίνδυνοι παίρνουν υψηλότερα νούμερα και τα κενά μεταξύ των αριθμών αντιστοιχούν στη σχετική δύναμη των διαφορών.

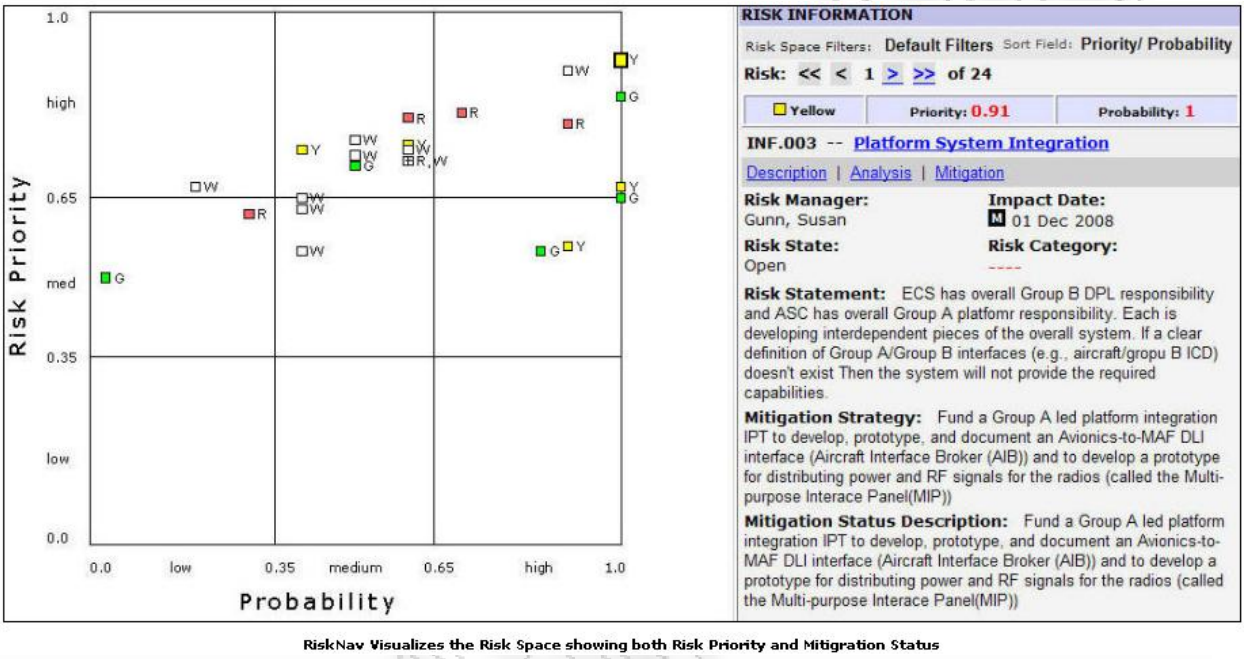
Risk Analysis Inputs		Computed Risk Scores	
Impact Date:	16 Sep 2008	Risk Timeframe:	Short-term/ 0.99
Probability:	High/ 0.90	Overall Risk Impact:	High/ 0.79
Cost Impact Rating:	High/ 0.83	Risk Consequence:	High/ 0.89
Schedule Impact Rating:	High/ 0.83	Risk Priority:	High/ 0.89
Technical Impact Rating:	High/ 0.65	Risk Ranking (Ranks "Open" risks with priority > 0)	
Compliance & Oversight Impact Rating:	High/ 0.83	Rank in Program:	1 of 17
		Rank in Organization:	1 of 4
		Rank in Project:	1 of 2

RiskNav uses a Scoring Model to prioritize Risks

Εικόνα 7: Συνολική βαθμολογία για κάθε προσδιορισμένο κίνδυνο στο RiskNav

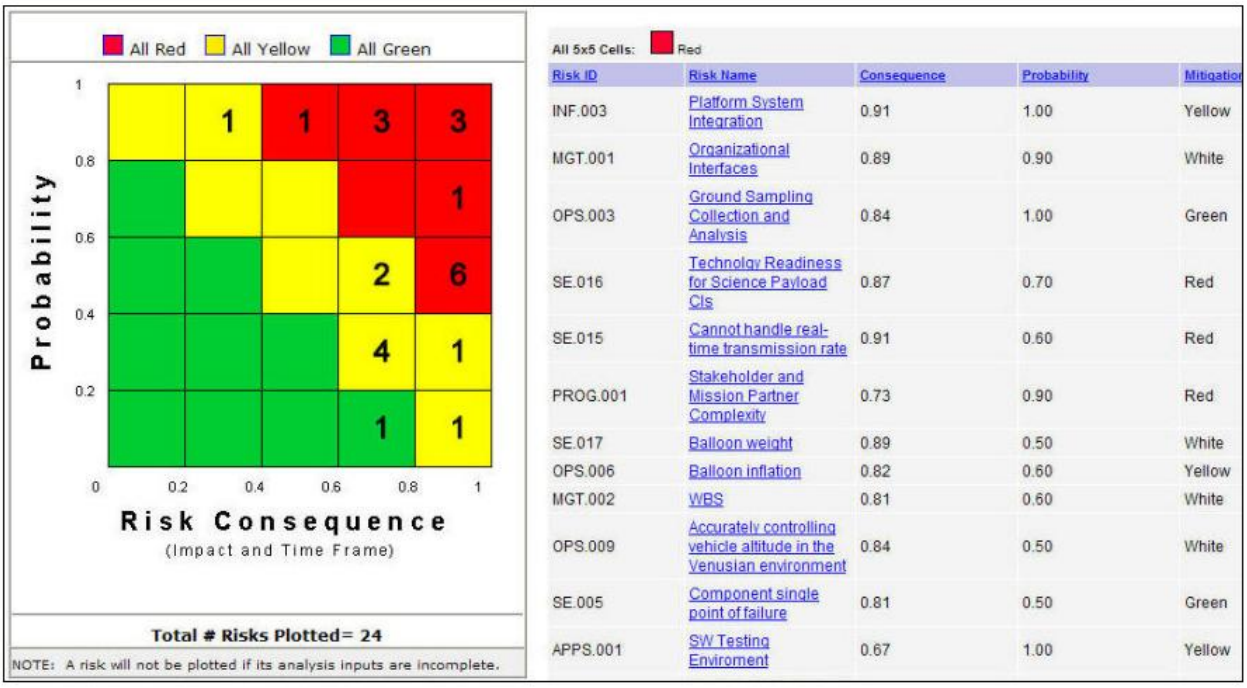
Σε γραφική μορφή, το RiskNav αντιπροσωπεύει τρεις βασικές πτυχές του κάθε κινδύνου στη διάσταση του κινδύνου: την προτεραιότητα του κινδύνου, την πιθανότητα, και το μετριασμό / διαχείριση της κατάστασης. Τα δεδομένα σημεία αντιπροσωπεύουν τους κινδύνους,

και το χρώμα ενός κουτιού υποδεικνύει την κατάσταση της δράσης μετριασμού (Άσπρο: κανένα σχέδιο, Κόκκινο: το σχέδιο δεν λειτουργεί, Κίτρινο: μπορεί να μη λειτουργεί, Πράσινο: κατά πάσα πιθανότητα είναι επιτυχές, Μπλε: ολοκληρώθηκε με επιτυχία, Μαύρο: οι δράσεις θα ξεκινήσουν σε μεταγενέστερο στάδιο). Τα δεδομένα σημεία μπορούν να επιλεγούν για να δείξουν αναλυτικές πληροφορίες για τον κίνδυνο σχετικά με την ανάλυση, ποιος ασχολείται με τις ενέργειες διαχείρισης, την κατάσταση, καθώς και άλλες πληροφορίες.



Εικόνα 8: Γραφική μορφή του RiskNav την προτεραιότητα του κινδύνου, την πιθανότητα, και το μετριασμό / διαχείριση της κατάστασης

Το RiskNav εμφανίζει επίσης ένα 5x5 διάγραμμα συχνότητας που δείχνει τον αριθμό των κινδύνων σε κάθε τετράγωνο ενός 5x5 πίνακα των πιθανοτήτων έναντι του εύρους των συνεπειών. Τα κόκκινα κουτιά περιέχουν υψηλής προτεραιότητας κινδύνους. Τα κίτρινα και πράσινα κουτιά περιέχουν μέσης και χαμηλής προτεραιότητας κινδύνους, αντίστοιχα. Το RiskNav ενσωματώνει μια δυνατότητα διαχείρισης που επιτρέπει στο εύρος της πιθανότητας και των συνεπειών του γραφήματος να προσαρμοστούν. Κάνοντας κλικ σε ένα κελί παρέχει μια λεπτομερή λίστα με τους κινδύνους σε αυτό το κελί. Το *All Red*, *All Yellow* και *All Green* εικονίδια στην κορυφή του γραφήματος μπορεί να χρησιμοποιηθούν στη λίστα των κινδύνων σε όλα τα κουτιά ενός συγκεκριμένου χρώματος.



Εικόνα 9: Πίνακας των πιθανοτήτων έναντι του εύρους των συνεπειών

5.4 Μέθοδος PBMOK με τη χρήση του εργαλείου NRISK

Η PMBOK είναι μια συλλογή διαδικασιών και γνώσης γενικά αποδεκτές ως βέλτιστες πρακτικές στη διαχείριση ενός έργου. Ως ένα διεθνώς αναγνωρισμένο πρότυπο (IEEE Std 1490-2003), παρέχει τις βασικές αρχές της διαχείρισης ενός έργου, ανεξάρτητα από τον τύπο του έργου είτε πρόκειται για κατασκευή, λογισμικό, κατασκευές, αυτοκινητοβιομηχανία κ.λπ.

Η PMBOK αναγνωρίζει 5 βασικές ομάδες της διαδικασίας και 9 γνωστικά πεδία που χαρακτηρίζουν σχεδόν όλα τα έργα. Οι βασικές έννοιες είναι εφαρμόσιμες σε έργα, προγράμματα και δράσεις. Οι πέντε βασικές ομάδες της διαδικασίας είναι τα εξής:

- Έναρξη
- Σχεδιασμός
- Εκτέλεση
- Παρακολούθηση και Έλεγχος
- Κλείσιμο

Οι διεργασίες επικαλύπτονται και αλληλεπιδρούν κατά τη διάρκεια ολόκληρου του έργου ή της φάσης. Οι διαδικασίες περιγράφονται στα πλαίσια των όρων:

- Είσοδοι (έγγραφα, προγραμματισμός, σχέδια, κλπ.)
- Εργαλεία και τεχνικές (μηχανισμοί που εφαρμόζονται στις εισροές)
- Έξοδοι (έγγραφα, προϊόντα, κλπ.)

Οι εννέα τομείς της γνώσης είναι οι εξής:

- Διαχείριση Ολοκλήρωση Έργου
- Διαχείριση Πεδίου Έργου
- Διαχείριση Χρόνου Έργου
- Διαχείριση Κόστος Έργου
- Διαχείριση Ποιότητας Έργου
- Διοίκηση Ανθρώπινου Δυναμικού Έργου
- Διαχείριση Επικοινωνιών Έργου
- Διαχείριση Κινδύνου Έργου

- Διαχείριση Προμηθειών Έργου

Μεγάλο μέρος της PMBOK είναι μοναδικό στη διαχείριση του έργου. Ορισμένες περιοχές επικαλύπτονται με άλλους κλάδους της διαχείρισης. Η γενική διαχείριση περιλαμβάνει επίσης τον σχεδιασμό, την οργάνωση, τη στελέχωση, την εκτέλεση και τον έλεγχο των εργασιών ενός οργανισμού. Οι οικονομικές προβλέψεις, η οργανωτική συμπεριφορά και οι τεχνικές σχεδιασμού είναι επίσης παρόμοια.

Το NRisk είναι ένα εργαλείο κλειστού κώδικα. Δεν είναι διαθέσιμο για άλλους εκτός της εταιρείας τηλεπικοινωνιών που έχει τα δικαιώματα. Έχει σκοπό την εξασφάλιση μόνιμης και ενημερωμένης διαφάνειας των ευκαιριών και των κινδύνων για προγράμματα (projects) κατά τη φάση της υλοποίησης, λαμβάνοντας επίσης υπόψη τις διατάξεις σχετικά με τον ισολογισμό και τους υπολογισμένους απρόβλεπτους κινδύνους σε παγκόσμιο επίπεδο.

Περιπτώσεις Χρήσης	Χρησιμοποιείται από/ για
STP, LRP, LE	Ελεγκτές Κινδύνου: η υποβολή περιοδικών εκθέσεων του κινδύνου, συνολικά επίπεδα
Project	Ομάδες ατόμων από τη μεριά του πελάτη για την Εκτέλεση Έργων (κάθε μήνα)
Sales Opportunity	Ομάδες Προσφοράς κατά τη διάρκεια της διαπραγμάτευσης και το στάδιο έγκρισης
Program	Ομάδες Προγράμματος στο κέντρο Έρευνας και Ανάπτυξης
Product	Διαχειριστές Προϊόντος για τα επίπεδα κινδύνων του προϊόντος μετά το P3 (ορόσημο της εταιρείας)
Case	Κάθε περίπτωση με έμφαση στη μη-οικονομική αξιολόγηση των κινδύνων
Other	Αξιολόγηση κινδύνων γενικού σκοπού, οικονομική αποτίμηση

Πίνακας 9*: Περιπτώσεις Χρήσης του NRisk*

Το NRisk είναι ένα αυτόνομο εργαλείο για τη διαχείριση του κινδύνου. Σε γενικές γραμμές εφαρμόζεται σε όλους τους τύπους εκτίμησης των κινδύνων. Κάνει τεκμηρίωση των ανεξάρτητων μεταξύ τους κινδύνων με πιθανότητα και κατηγορία των επιπτώσεων (RPN), καθώς και συναφείς δράσεις. Δημιουργεί διαγράμματα χαρτών κινδύνου για αυτόματη επιλογή των κινδύνων.

Τα τρέχοντα στοιχεία για τους κινδύνους αποθηκεύονται σε MS-Access βάση δεδομένων, για την αναθεώρηση της ανάπτυξης κινδύνου: 3 αξιολογήσεις αριθμού προτεραιότητας κινδύνου (RPN) ανά κίνδυνο (αρχικός, προηγούμενος, τρέχων). Έχει τη δυνατότητα εισαγωγής άλλων βάσεων δεδομένων και NRisk Excel προκατόχων για τη συλλογή των κινδύνων που προέρχονται από διαφορετικές πηγές σε μία βάση δεδομένων.

Το γραφικό περιβάλλον του χρήστη (GUI) του NRisk είναι εύκολο στη χρήση. Μπορεί να χρησιμοποιηθεί αυτόνομα (και σε απομακρυσμένες καταστάσεις). Χρησιμοποιείται σε όλες τις διαδικασίες σε επίπεδο διαχείρισης κινδύνων της εταιρείας: ομοιόμορφη ορολογία, μέτρα αξιολόγησης, κατηγορίες που επιτρέπουν τη συσσώρευση και την ενοποίηση. Τα τέσσερα βασικά βήματα είναι:

1. Επιλογή περίπτωση χρήσης, έργου
2. Περιγραφή του κινδύνου, των αντίκτυπων και των ενεργειών
3. Εισαγωγή, διαλογή, φιλτράρισμα, ομαδοποίηση των κινδύνων
4. Απεικόνιση και εξαγωγή αποτελεσμάτων

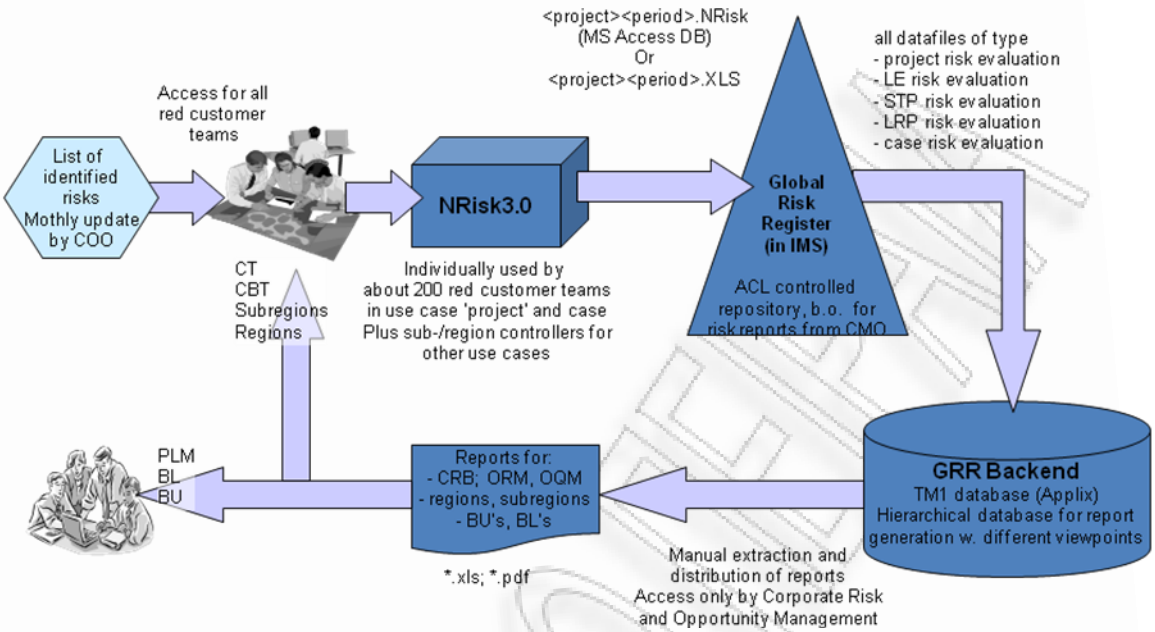
Το NRisk3 δουλεύει με τοπικές βάσεις δεδομένων. Η τοποθεσία μπορεί να είναι σε οποιονδήποτε φάκελο στον τοπικό υπολογιστή ή σε οποιοδήποτε ομαδικό εξυπηρετητή. Το πρόσφατα χρησιμοποιημένο μονοπάτι έχει μείνει στη μνήμη και προσφέρεται στην επόμενη

περιήγηση. Η βάση δεδομένων του NRisk3 είναι μια βάση δεδομένων ενός χρήστη, δηλαδή δεν επιτρέπεται η ταυτόχρονη πρόσβαση εγγραφής. Δεν υπάρχουν εσωτερικοί μηχανισμοί προστασίας της πρόσβασης. Το NRisk3 επιτρέπει μόνο πρόσβαση για ανάγνωση για την προστασία εγγραφής των βάσεων δεδομένων που έχουν ήδη προσπελαστεί. Θα μπορούσε να τρέξει αρκετές φορές παράλληλα στον ίδιο υπολογιστή με διαφορετικές βάσεις δεδομένων.

Το NRisk3.1 υποστηρίζει διάφορες περιπτώσεις χρήσης:

(i) Το NRisk σε ευρύ πλαίσιο περιοδικών διεργασιών της εταιρείας:

1. **Αξιολόγηση των κινδύνων ενός έργου.** Αυτό αναφέρεται στην υλοποίηση των έργων των πελατών. Χρησιμοποιούνται κοινές κατηγορίες, οι βάσεις δεδομένων του NRisk ελέγχονται σε κεντρικό αποθετήριο των συγκεντρωτικών εκθέσεων από διαφορετικές απόψεις. Γίνεται επίσης νομισματική εστίαση της αξιολόγησης των κινδύνων: σε βραχυπρόθεσμο (STP) και μακροπρόθεσμο (LE) χρονικό ορίζοντα.
2. **Αξιολόγηση των κινδύνων ενός προϊόντος.** Χρησιμοποιείται στις επιχειρηματικές μονάδες της εταιρείας για τους κινδύνους των προγραμμάτων και των προϊόντων. Οι κίνδυνοι για την επικοινωνία με τη Γενική Διεύθυνση Μάρκετινγκ μπορούν να εξαχθούν. Η ενδιάμεση μορφή επικοινωνίας με τη Γενική Διεύθυνση Μάρκετινγκ είναι εκτός του NRisk (Excel λίστα). Συνιστάται να χρησιμοποιούνται οι κατηγορίες κινδύνου του έργου ως παράμετροι για την ταξινόμηση. Γίνεται επίσης νομισματική εστίαση της αξιολόγησης των κινδύνων: σε (LT) και μακροπρόθεσμο (LE) χρονικό ορίζοντα.
3. **Τελευταία εκτίμηση αξιολόγησης των κινδύνων (LE)**. Χρησιμοποιείται κατά περιοχή, υποπεριοχή, επιχειρηματική μονάδα ή επίπεδο για την αναφορά του κινδύνου ως προσθήκη στην επιστολή διαχείρισης. Η νομισματική αξιολόγηση του κινδύνου επικεντρώνονται: σε μακροπρόθεσμο (LE) χρονικό ορίζοντα. (4 τρίμηνα)
4. **Βραχυπρόθεσμο σχέδιο (STP)** - ακριβώς όπως LE, αλλά με έμφαση στο σχέδιο για την περίοδο μισού έτους. Η νομισματική αξιολόγηση του κινδύνου εστιάζει: σε βραχυπρόθεσμο (STP) χρονικό ορίζοντα (6 μήνες).
5. **Σχέδιο μεγάλου εύρους (LRP).** Χρησιμοποιείται κατά περιοχή, υποπεριοχή, BU, η BL και ορισμένες κεντρικές λειτουργίες για την αναφορά των κινδύνων κατά το σχέδιο τριών ετών (LRP). Χρησιμοποιούνται κοινές κατηγορίες κινδύνου LRP. Γίνεται επίσης νομισματική εστίαση της αξιολόγησης των κινδύνων: σε μεγάλου εύρους **(**LRP) χρονικό ορίζοντα (3 έτη).
6. **Αξιολόγηση των κινδύνων ενός προγράμματος**. Χρησιμοποιείται κυρίως σε προγράμματα Γενικής Διεύθυνσης (COO) με έμφαση σε δράσεις και τις μη δημοσιονομικές επιπτώσεις. Τροφοδοτεί την αξιολόγηση κινδύνου των προϊόντων.



Σχήμα 4: **Αξιολόγηση των κινδύνων ενός προγράμματος**

(ii) Το NRisk εκτός κλίμακας περιοδικών διεργασιών της εταιρείας:

Υπάρχουν τρεις περιπτώσεις χρήσης, όπου το NRisk χρησιμοποιείται σε διεργασίες που καθορίζονται από γεγονότα, ή ακόμη και από διαδικασίες ανεξάρτητα από την εταιρεία. Οι βάσεις δεδομένων του NRisk θα πρέπει να αρχειοθετούνται στο πλαίσιο αυτών των διαδικασιών, αλλά δεν υπάρχει κεντρική συγκέντρωση, αξιολόγηση ή υποβολή των εκθέσεων.

1. **Ευκαιρίες Πωλήσεις:** Κατά το στάδιο προσφοράς και κατά τη διάρκεια της διαδικασίας έγκρισης του έργου, οι εκτιμήσεις κινδύνου με βάση το NRisk είναι υποχρεωτικές για όλα τα Α, Β, Γ έργα και όλα τα έργα με τον όγκο πωλήσεών μεγαλύτερο των 2εκ.ευρώ. Η βάση δεδομένων NRisk θα πρέπει να ελέγχει σε SWF μαζί με τα δικαιολογητικά για την έγκριση. Μετά την θετική απόφαση αξιολόγησης του κινδύνου θα χρησιμοποιηθεί ως αρχική αξιολόγηση κινδύνων για την τακτική διαχείριση του κινδύνου του έργου στο CT / επίπεδο έργων .
2. **Περίπτωση υπό μελέτη:** Η αξιολόγηση του κινδύνου, κατά τον καθορισμό / τη φάση διαπραγμάτευσης μιας περίπτωσης υπό μελέτη (όχι επιχειρηματική περίπτωση ή τις ευκαιρία πώλησης), για όσο διάστημα μη οικονομική αξιολόγηση της υπόθεσης και των ενσωματωμένων κινδύνων είναι στο επίκεντρο. Το NRisk χρησιμοποιείται αυτόνομα σε αυτή την περίπτωση χρήσης (μη συνυπολογισμός των κινδύνων για τις πιθανές περιπτώσεις).
3. **Άλλα:** Νομισματική αξιολόγηση του κινδύνου για τις περιπτώσεις επιχειρήσεων (προϊόν, επενδύσεις, κλπ), καθώς και άλλες ειδικές διαδικασίες και καταστάσεις (π.χ.: χώρα / αξιολόγηση του κινδύνου περιοχής, των δικαιωμάτων πνευματικής ιδιοκτησίας των κινδύνων κλπ). Μη υποχρεωτικά πεδία πέραν της «ύπαρξης», των «επικύνδυνων γεγονότων» και του «εναντίον», η επιλογή παραμέτρων ή χρήση των συγκεκριμένων κατηγοριών κινδύνου είναι για λογαριασμό του αρμόδιου διαχειριστή κινδύνου.

5.5 Σύγκριση και Αξιολόγηση των παραπάνω μεθόδων

Το εργαλείο NRisk αυτό έχει τα εξής προτερήματα:

- Για την εταιρεία:
  - Απόδοση (σε σχέση με τη συντήρηση εργαλείων, κατάρτισης, κλπ)

- Διαλειτουργική αναζήτηση της αιτίας του κινδύνου
- Δομημένη προσέγγιση από τη βάση προς τα πάνω, με αποτέλεσμα την επίτευξη της αύξησης της εμπιστοσύνης των ενδιαφερομένων

o Για τις διάφορες Επιχειρηματικές Μονάδες / Γραμμές της εταιρείας:

- Απλοποιημένη συνάθροιση
- Προσδιορισμός των κινδύνων διασποράς σε SR
- Απλοποιημένη δημιουργία της επιστολής διαχείρισης
- Ο κίνδυνος παρουσιάζεται στην ίδια δομημένη μορφή με σκοπό την αποφυγή παρεξηγήσεων και ερωτήσεων

o Για τον πελάτη:

- Κοινή πλατφόρμα για όλες τις λειτουργίες
- Δε χρειάζεται προσπάθεια για τη δημιουργία και τη συντήρηση των ιδίων εργαλείων / προτύπων
- Διαφάνεια της κατάστασης των κινδύνων και της θέσης δράση στην πορεία των τακτικών πελατών
- Η πλατφόρμα για τις κλιμακώσεις είναι σε γνωστή μορφή και περιλαμβάνει γεγονότα εκτός της υπεύθυνης περιοχής

Επίσης:

o **Υποστηρίζει τις βασικές / εξειδικευμένες ανάγκες των χρηστών και την αυτόματη δημιουργία βασικού χάρτη κινδύνου:**

- Το περιεχόμενο της βασικής κατάστασης λειτουργίας είναι παρόμοιο με την Βασική Ανάλυση Κινδύνου (KRA - Key Risk Analysis, πρώην Βασική Λίστα Κινδύνου).
- Σε προηγμένη κατάσταση λειτουργίας τα χαρακτηριστικά του περιεχομένου και συναφή είναι παρόμοια με τη Risk Log, αλλά αναπτύσσονται περαιτέρω.
- Ο χρήστης μπορεί να σώσει και να φορτώσει τις δικές του λειτουργίες (π.χ. σειρά των στηλών).
- Αυτόματη δημιουργία χάρτη κινδύνου σύμφωνα με τους χρήστες επιλογή των στοιχείων που θα συμπεριληφθούν

o **Πλεονεκτήματα για τα άτομα που ενσωματώνουν και αναφέρουν τις πληροφορίες κινδύνου**:

- Είναι εύκολο εργαλείο ανταλλαγής.
- Το NRisk αρχείο εισαγωγής / εξαγωγής - αυτόματος έλεγχος μεταξύ των νέων δεδομένων και ενημερώσεων των δεδομένων.
- Εκπαίδευση και μάθηση – αυτόματη αποθήκευση των βασικών στατιστικών στοιχείων και δεδομένων του ιστορικού.
- Παρουσιάσεις - όλα τα δεδομένα, εικόνες ή όψεις της οθόνης μπορούν να αντιγραφούν σε PPT εφαρμογή κλπ. Αποτελεσματικότητα στην ενημέρωση των πληροφοριών του κινδύνου μεταξύ Ν χρηστών.

o Ατομική αναγνώριση για κάθε δημιουργημένο κίνδυνο και σχετικών δράσεων που δίνονται από το εργαλείο, π.χ. αυτόματος διαχωρισμός μεταξύ των νέων / επίκαιρων πληροφοριών σε περιπτώσεις εισαγωγής.

- Υποστηρίζει την αποθήκευση και την κατανομή του κινδύνου ειδικά συνημμένα
- Ελαχιστοποιήστε χειρωνακτική εργασία σε σύγκριση με εναλλακτικά εργαλεία

6 Συμπεράσματα – Επίλογος –Μέλλον

Η διαχείριση καταστάσεων επικινδυνότητας απαιτεί χρήσιμη και επεξεργασμένη πληροφορία σε κρίσιμο χρόνο, εμπειρία και συντονισμό. Κατάλληλα τεχνολογικά εργαλεία μπορούν να προσφέρουν την απαιτούμενη πληροφορία σε πραγματικό χρόνο, να διαθέσουν επεξεργασμένη και αποθηκευμένη γνώση καθώς και αιτιολογημένες προτάσεις για την υποστήριξη σωστών αποφάσεων την κατάλληλη στιγμή.

Η διαχείριση επικινδυνότητας αποτελεί αδιαμφισβήτητα ένα πολύ σημαντικό κομμάτι οποιουδήποτε έργου λογισμικού και είναι ιδιαίτερα κρίσιμη για μεγάλα έργα, για έργα που χαρακτηρίζονται από υψηλή αβεβαιότητα ή για έργα των οποίων μια πιθανή δυσλειτουργία θα μπορούσε να προκαλέσει μη αναστρέψιμες καταστροφές.

Χωρίς αμφιβολία λοιπόν η εφαρμογή συστημάτων διαχείρισης γνώσης και υποστήριξης λήψης αποφάσεων, αποτελεί βαρόμετρο στην επιτυχία σχεδιασμού προετοιμασίας και διοίκησης μιας καταστάσεως επικινδυνότητας. Τεχνολογίες υπάρχουν ήδη αρκετές και αποτελεσματικές. Όμως στην πράξη παρατηρείται ολική ή μερική απουσία εργαλείων σχεδιασμού που μπορεί να διαθέτει μια αναπτυσσόμενη κυρίως κοινωνία, στην προσπάθειά της να οργανωθεί απέναντι στον κίνδυνο. Αυτό ίσως να οφείλεται πρωτίστως στην δυσκολία προμήθειας τέτοιου εξοπλισμού για κοστολογικούς καθαρά λόγους ή ακόμα στην έλλειψη κατάλληλου τεχνολογικού υπόβαθρου που παρατηρείται σε εμπλεκόμενους οργανισμούς ή υπηρεσίες.

Αυτό όμως που πρέπει να γίνει κατανοητό είναι ότι ακόμα και αν έχουν αντιμετωπιστεί κατάλληλα οι κίνδυνοι στις προηγούμενες φάσεις, δεν υπάρχει ποτέ πιθανότητα να εκτελεστεί ένας τόσο εξαντλητικός έλεγχος ο οποίος να μπορέσει να διασφαλίσει ότι όλα θα λειτουργήσουν κατά το προσδοκώμενο και ότι τίποτα δεν θα μπορέσει να προκαλέσει μια αποτυχία του λογισμικού. Χρειάζεται σε κάθε περίπτωση είναι να εκτιμάται κατάλληλα ποια είναι η προσφορά των τεχνολογιών αυτών σε ένα τόσο κρίσιμο τομέα μιας κοινωνίας, όπου η οργανωτική αποδοτικότητα και η εκπλήρωση των προκαθορισμένων στόχων για την ικανοποίηση της κοινωνικής ασφάλειας και της προόδου, στηρίζεται σε τόσο μεγάλο βαθμό στην συλλογική δημιουργία, την διάχυση και χρήση της υπάρχουσας εμπειρίας και γνώσης.

Μελλοντική Έρευνα

Η παρούσα εργασία, αποδεικνύοντας το γεγονός ότι πάντα υπάρχει ένα ποσοστό επικινδυνότητας που απομένει μετά την ολοκλήρωση του ελέγχου του λογισμικού, παρέχει μια καλή βάση πάνω στην οποία μπορεί να στηριχθεί περαιτέρω έρευνα του πεδίου που προκύπτει από τη συσχέτιση των εννοιών της διαχείρισης επικινδυνότητας λογισμικού και του ελέγχου που διεξάγεται σε αυτό.

Πιο συγκεκριμένα, λαμβάνοντας κανείς τους παράγοντες που επηρεάζουν το ποσοστό της εναπομείνασας επικινδυνότητας θα μπορούσε να κάνει μια προσπάθεια ποσοτικοποίησης τους και ανεύρεσης κατάλληλων μετρικών, ώστε να δοθεί τελικά η δυνατότητα υπολογισμού αυτού του ποσοστού μέσω μαθηματικού τύπου, ο οποίος θα είναι σύμφωνος με τη σχέση που έχει ήδη παρουσιασθεί. Επίσης, θα μπορούσε να πραγματοποιηθεί μοντελλοποίηση της επικινδυνότητας του λογισμικού σε σχέση πάντα με τον έλεγχο.

Τέλος, αυτό που είναι σημαντικό να επιτευχθεί είναι ένας κατάλληλος ποιοτικός, αλλά κυρίως ποσοτικός συνδυασμός της επικινδυνότητας του λογισμικού με τα διάφορα κριτήρια ποιότητας που το χαρακτηρίζουν, όπως είναι για παράδειγμα η αξιοπιστία ή η ασφάλεια, ώστε να παρέχεται στον ενδιαφερόμενο μια πληρέστερη και ακριβέστερη εικόνα του.

7 Πρακτικό Μέρος

7.1 Εισαγωγή

Η μελέτη περίπτωσης που παρουσιάζεται σε αυτήν την ενότητα αφορά μία εταιρεία τηλεπικοινωνιών. Η εταιρεία αυτή προσφέρει στην αγορά υπηρεσίες έρευνας και ανάπτυξης λογισμικού για τηλεπικοινωνίες. Σε πρώτη φάση, αναπτύσσει λογισμικό και μετά το ελέγχει μέσω προγραμμάτων προσομοίωσης του συστήματος.

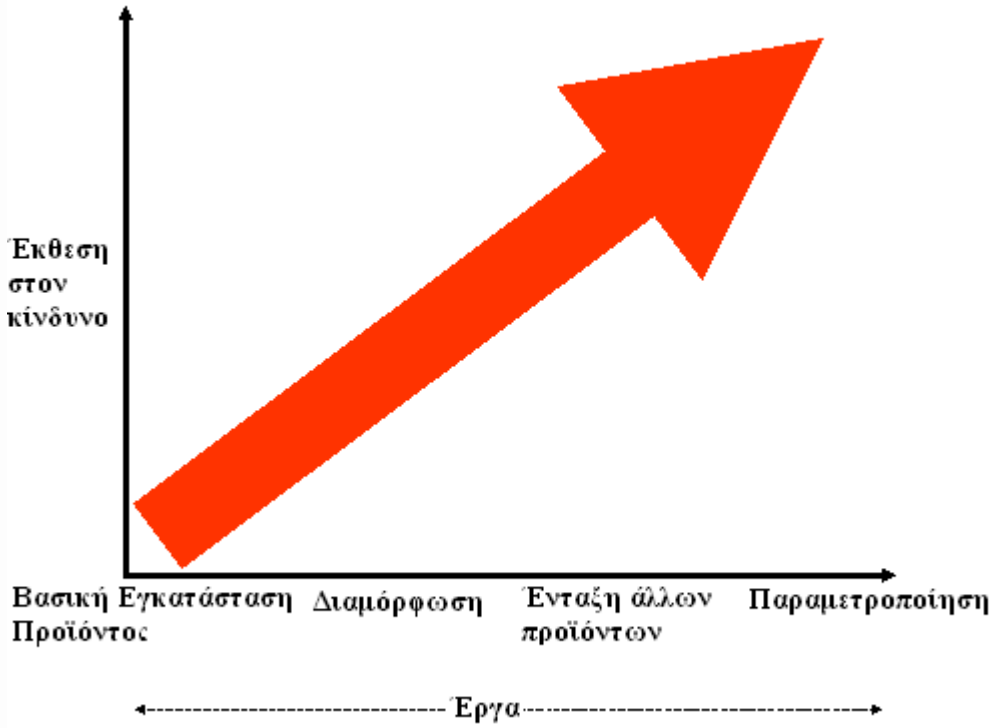
Η εταιρεία δρα ως «ανάδοχη» των εκάστοτε έργων που της ανατίθενται από διάφορους παρόχουν τηλεφωνίας. Ο ρόλος της είναι κρίσιμος για την επιτυχή λειτουργία του λογισμικού και η ανάλυση και διαχείριση επικινδυνότητας, έχει στόχο την προδιαγραφή των απαιτήσεων ασφάλειας και την επιλογή συγκεκριμένων μέτρων προστασίας για τη διασφάλιση του έργου.

Το τμήμα πληροφορικής ανά έργο είναι σχετικά ολιγάριθμο (8-18 άτομα). Τα μεσαία και ανώτερα διοικητικά στελέχη της εταιρείας παρουσιάζονται να έχουν ευνοϊκή προδιάθεση και διάθεση συνεργασίας, έχοντας και οι ίδιοι κάποιες γνώσεις στον τομέα πληροφορικής. Οι βασικές αρχές της ανάλυσης επικινδυνότητας και οι σημαντικοί όροι, όπως επικινδυνότητα, απειλή, ευπάθεια, επίπτωση και αντίμετρο είναι ξεκάθαροι σε όλη την ομάδα διαχείρισης του έργου.

Για την ανάπτυξη του λογισμικού χρησιμοποιήθηκαν οι γλώσσες προγραμματισμού Assembly και C++, για την προσωμοίωση του συστήματος του πελάτη και τον έλεγχο του λογισμικού χρησιμοποήθηκε το κατάλληλο υλικό (υπολογιστές, switches κλπ) και λογισμικό (REMO, NetManager,PEGASUS κλπ). Και για την ανάλυση, διαχείριση και παρακολούθηση των κινδύνων χρησιμοποιήθηκε το εργαλείο NRisk, το οποίο έχει αναπτυχθεί από άτομα της ίδιας της εταιρείας.

Το NRisk, όπως αναφέρθηκε και παραπάνω, είναι ένα εργαλείο-μεθοδολογία κλειστού κώδικα. Δεν είναι διαθέσιμο για άλλους εκτός της εταιρείας. Έχει σκοπό την εξασφάλιση μόνιμης και ενημερωμένης διαφάνειας των ευκαιριών και των κινδύνων για προγράμματα (projects) κατά τη φάση της υλοποίησης, λαμβάνοντας επίσης υπόψη τις διατάξεις σχετικά με τον ισολογισμό και τους υπολογισμένους απρόβλεπτους κινδύνους σε παγκόσμιο επίπεδο.

Για την ελαχιστοποίηση των αρνητικών επιπτώσεων των κινδύνων ή την πιθανότητα αυτοί πραγματικά να συμβούν, θα πρέπει να εντοπιστούν, να αναλυθούν και να διαχειριστούν οι κίνδυνοι επαγγελματικά για να εξασφαλιστεί ότι τα έργα θα παραδοθούν στα όρια του προϋπολογισμού, στην ώρα τους και απολύτως σύμφωνα με τις προδιαγραφές. Όπως και να συμβάλει στην ικανοποίηση των πελατών είναι επίσης κρίσιμος παράγοντας που επιτρέπει ΝΡΟ να λειτουργούν επικερδώς.



Σχήμα 5:Πολυπλοκότητα έναντι Έκθεσης στον κίνδυνο

Η συστηματική διαχείριση των κινδύνων επιτρέπει τη στοχευμένη και βασισμένη σε πραγματικά γεγονότα λήψη αποφάσεων και, την καλύτερη αξιολόγηση της ανάληψης κινδύνων, καθώς επίσης βοηθά τη συγκρισιμότητα των διαφόρων εναλλακτικών αποφάσεων των επιχειρηματικών προοπτικών.

7.2 Διαδικασία Διαχείρισης Κινδύνου μέσω του εργαλείου/μεθοδολογίας του NRisk

Η γενική διαδικασία διαχείρισης των κινδύνων που χρησιμοποιείται στα έργα που αναλαμβάνει η εταιρεία, βασίζεται στην PMBOK ® Guide. Πρόκειται για μια κυκλική διαδικασία που περιλαμβάνει τα ακόλουθα κύρια στάδια:

- Σχεδιασμός Διαχείρισης κινδύνου(ων)
- Αναγνώριση κινδύνου(ων)
- Ανάλυση κινδύνου(ων)
- Σχεδιασμός αντίδρασης κινδύνου(ων)
- Παρακολούθηση και Έλεγχος κινδύνου(ων)

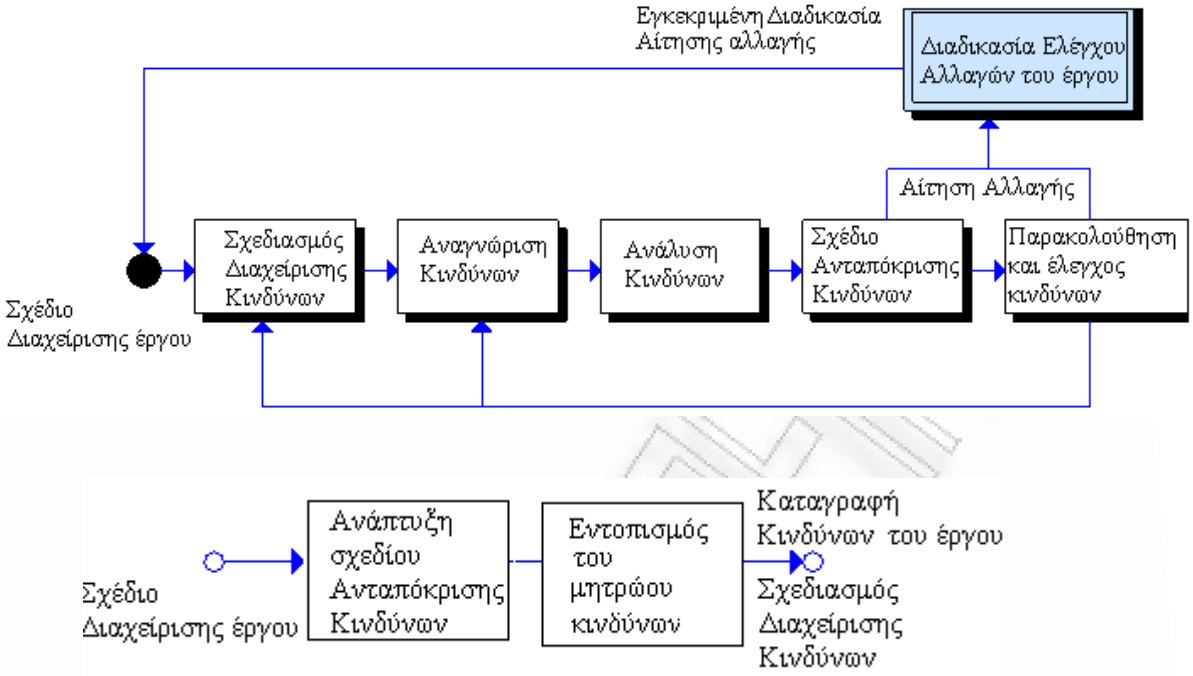
Σχήμα 6:Διαδικασία Διαχείρισης Κινδύνου της εταιρείας

Μετά το σχεδιασμό της διαχείρισης του κινδύνου που έχει πραγματοποιηθεί η διαδικασία εισέρχεται σε μια κυκλική λειτουργία ξεκινώντας με τον εντοπισμό του κινδύνου. Ο κύκλος συνεχίζεται μέχρι την παρακολούθηση και τον έλεγχο των κινδύνων μετά τα οποία η διαδικασία μπορεί να συνεχιστεί είτε με την ταυτοποίηση κινδύνων ή άμεσα με την ανάλυση κινδύνου, ανάλογα με την κατάσταση του έργου.

Στην ουσία, η διαχείριση του κινδύνου είναι μια διαδικασία που εφαρμόζεται σε όλο τον κύκλο ζωής του έργου. Ο οδηγός για αυτό είναι το γεγονός ότι κατά τη διάρκεια εκτέλεσης του έργου σε πολλοί απρόβλεπτοι παράγοντες μπορούν να επηρεάσουν την πρόοδο του έργου. Ως εκ τούτου, η διαχείριση του κινδύνου θα πρέπει να εφαρμόζεται και να αναθεωρείται / ενημερώνεται σε εβδομαδιαία βάση μέχρι την ολοκλήρωση του έργου.

7.2.1 Σχεδιασμός Διαχείρισης κινδύνου(ων)

Σχεδιασμός της διαχείρισης των κινδύνων είναι η διαδικασία ανάπτυξης μιας προσέγγισης και ενός σχεδίου για τις δραστηριότητες διαχείρισης κινδύνου σε ένα έργο.



Σχήματα 7+8: Σχεδιασμός Διαχείρισης Κινδύνου ενός έργου

Η έξοδος από αυτό το βήμα της διαδικασίας είναι ένα έγγραφο Διαχείρισης Κινδύνου. Το έγγραφο αυτό περιγράφει πως ο προσδιορισμού του κινδύνου, η ποιοτική και ποσοτική ανάλυση του, ο σχεδιασμός αντίδρασης του, η παρακολούθηση και ο έλεγχος του κινδύνου θα είναι δομημένα και θα εκτελούνται κατά τη διάρκεια του κύκλου ζωής του έργου. Δεν εξετάζει τις απαντήσεις σε μεμονωμένους κινδύνους, αυτό καλύπτεται από την έγγραφο σχεδίου απάντησης των κινδύνων. Το έγγραφο Διαχείρισης Κινδύνου περιλαμβάνει τα ακόλουθα:

• **Μεθοδολογία:** καθορίζει τους προσανατολισμούς, τα εργαλεία και τις πηγές δεδομένων που μπορούν να χρησιμοποιηθούν για την εκτέλεση της διαχείρισης του κινδύνου σε ένα συγκεκριμένο έργο.

• **Ρόλοι και Ευθύνες:** ορίζει το προβάδισμα, τη στήριξη και τα μέλη της ομάδας διαχείρισης του κινδύνου για κάθε τύπο δράσης του εγγράφου διαχείρισης κινδύνου.

• **Προϋπολογισμός:** ορίζει τον προϋπολογισμό για τη διαχείριση των κινδύνων για το έργο.

• **Χρόνος:** καθορίζει πόσο συχνά θα πραγματοποιούνται οι διαδικασίες διαχείρισης του κινδύνου καθ 'όλη τη διάρκεια ζωής του έργου.

• **Βαθμολόγηση και Ερμηνεία:** οι κατάλληλες μέθοδοι βαθμολόγησης και ερμηνείας για το χρονοδιάγραμμα της ποιοτικής και ποσοτικής ανάλυσης των κινδύνων που διεξάγονται. Οι μέθοδοι και η βαθμολόγηση πρέπει να καθορίζονται εκ των προτέρων για να εξασφαλιστεί η συνοχή.

• **Όρια:** τα βασικά κριτήρια για τους κινδύνους που θα ακολουθηθούν, από ποιον και με ποιο τρόπο. Αξίζει να σημειωθεί και συμπεριληφθεί γιατί ο ιδιοκτήτης του έργου, οι πελάτες και τα άλλα ενδιαφερόμενα μέρη έχουν διαφορετικά επίπεδα στο κατώφλι του κινδύνου.

• **Μορφή έκθεσης:** περιγράφει το περιεχόμενο και τη μορφή του σχεδίου απάντησης κινδύνου. Το τμήμα αυτό καθορίζει επίσης τον τρόπο που τα αποτελέσματα των διαδικασιών διαχείρισης κινδύνων θα πρέπει να τεκμηριώνονται, να αναλύονται και να κοινοποιούνται στην ομάδα του έργου και των εσωτερικών / εξωτερικών φορέων.

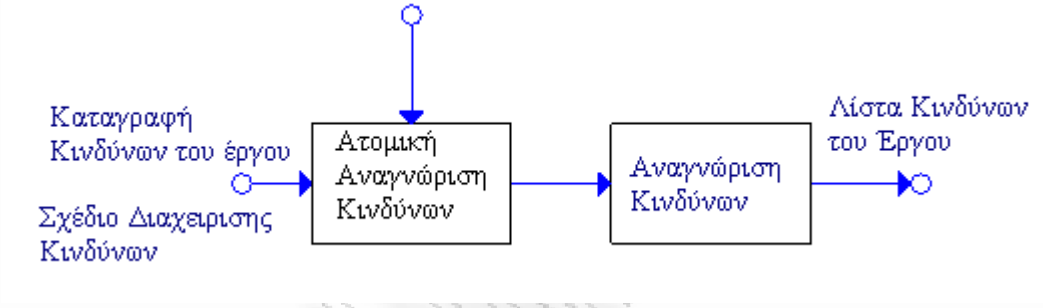
• **Παρακολούθηση:** τεκμηριώνει τον τρόπο με τον οποίο όλες οι πτυχές των δραστηριοτήτων του κινδύνου θα πρέπει να καταγράφονται.

Τυπικά, ο Υπεύθυνος Συντονιστής εκτελεί τον σχεδιασμό Διαχείρισης Κινδύνων μαζί με τα βασικά μέλη της ομάδας έργου. Τα αποτελέσματα, με τη μορφή του εγγράφου, κοινοποιούνται σε όλους τους ενδιαφερομένους. Στη συνέχεια, θα διαμορφωθεί ένα αρχείο καταγραφής του κινδύνου σύμφωνα με τα αποτελέσματα του σχεδιασμού διαχείρισης του.

7.2.2 Αναγνώριση κινδύνου(ων)

Αναγνώριση κινδύνου είναι η διαδικασία που προσδιορίζει και καθορίζει τους κινδύνους που είναι το πιο πιθανό να αποτρέψουν το έργο από την επίτευξη των στόχων του. Η αναγνώριση κινδύνου περιλαμβάνει την τεκμηρίωση των χαρακτηριστικών των εντοπισθέντων κινδύνων. Η έξοδος από τον εντοπισμό του κινδύνου είναι μια λίστα με τους κινδύνους του έργου.

Αναγνώριση του κινδύνου είναι μια επαναληπτική διαδικασία που θα πρέπει να γίνεται σε συνεχή βάση κατά τη διάρκεια του έργου. Η διαδικασία αναγνώρισης θα πρέπει να καλύπτει όλα τα είδη των κινδύνων. Οι κίνδυνοι που είναι πέραν των δυνάμεων της εξουσίας της ομάδας έργου κοινοποιούνται στους ενδιαφερόμενους για περαιτέρω ανάλυση.



Σχήμα 9: Αναγνώριση Κινδύνου

Τεχνικές για τον εντοπισμό του κινδύνου

Υπάρχουν διάφορες τεχνικές που χρησιμοποιούνται για τον εντοπισμό του κινδύνου:

• Αναθεώρηση των εγγράφων του έργου (δομημένη επανεξέταση π.χ. του χρονοδιάγραμμάτος του έργου, των προδιαγραφών, των απαιτήσεων κ.λπ.)

• Τεχνικές συλλογής πληροφοριών:

  ο Σύσκεψη για ανταλλαγή ιδεών

  ο Συνεντεύξεις

  ο Ανάλυση SWOT

• Κατάλογοι ελέγχου

• Ανάλυση των υποθέσεων του έργου

• Τεχνικές δημιουργίας διαγραμμάτων:

  ο Διαγράμματα αιτίας-αποτελέσματος

  ο Διαγράμματα ροής της διαδικασίας ή όλου του συστήματος

Η ομάδα του προγράμματος είναι ελεύθερη να επιλέξει όποια τεχνική θέλη. Η πιο σημαντική πτυχή είναι να κρατήσει μια δομημένη προσέγγιση και ειλικρίνεια για την αναγνώριση νέων, πρώην αγνώστων κινδύνων.

Οι λίστες ελέγχου του κινδύνου είναι επίσης πολύ χρήσιμες για τον έλεγχο των εντοπισθέντων κινδύνων. Ωστόσο, οι λίστες ελέγχου θα πρέπει να χρησιμοποιούνται με φειδώ καθώς έχουν το μειονέκτημα να αντανακλούν μόνο την παλιά γνώση των κινδύνων που έχει συσσωρευτεί στον οργανισμό και μπορεί να εμποδίσει την ομάδα του έργου από το να είναι δημιουργική στον προσδιορισμό νέων και πρώην αγνώστων κινδύνων.

Η διαδικασία της ταυτοποίησης του κινδύνου θα μπορούσε επίσης να γίνεται από τους αρχικά εντοπισμένους τομείς της αβεβαιότητας στο έργο, και τους στόχους του έργου, όπως προσδιορίζονται στο Σχέδιο Διαχείρισης του Έργου. Είναι ευκολότερο να εντοπίζονται οι κίνδυνοι (που εμφανίζονται στα πεδία της αβεβαιότητας), που είτε άμεσα είτε έμμεσα (μέσω άλλων κινδύνων) επηρεάζουν τους στόχους του έργου.

Κατά τον προσδιορισμό των κινδύνων, είναι εξαιρετικά σημαντικό να γίνει διάκριση μεταξύ των κινδύνων και θεμάτων. Οι κίνδυνοι είναι πάντα αβέβαια γεγονότα, υπό την έννοια ότι μπορεί να συμβούν ή να μην συμβούν. Το μεγαλύτερο λάθος είναι να αντιμετωπίζονται συγκεκριμένες εκδηλώσεις (π.χ. θέματα), όπως οι κίνδυνοι, διότι σε αυτή την περίπτωση:

• Η συνολική εικόνα των κινδύνων του έργου θα είναι μεροληπτική και η κατάταξη των πραγματικών κινδύνων θα μειωθεί

• Οι προσπάθειες απόκρισης του κινδύνου θα επικεντρωθεί σε προβλήματα (γιατί αυτά θα κατατάσσονται υψηλότερα), το οποίο δεν μπορεί να προληφθεί

• Η αναποτελεσματικότητα των απαντήσεων των κινδύνων θα δημιουργήσει μεγάλη απογοήτευση μεταξύ της ομάδας του σχεδίου.

Ο προσδιορισμός των κινδύνων είναι ευκολότερος αν εκτός από το πραγματικό γεγονός του κινδύνου εντοπίζονταν και τα αίτια του κινδύνου και των επιπτώσεων.

7.2.3 Ανάλυση κινδύνου(ων)

Η ανάλυση κινδύνου είναι η διαδικασία αξιολόγησης των επιπτώσεων και της πιθανότητας προσδιορισμού των κινδύνων, της προτεραιότητας τους σύμφωνα με την σοβαρότητα των επιπτώσεών τους για τους στόχους του έργου, την αξιολόγηση του συνολικού επιπέδου των κινδύνων του έργου και την πιθανότητα επίτευξης των στόχων όσον αφορά το κόστος και το χρόνο του έργου καθώς και τη σκοπιμότητα των διαφόρων σεναρίων έργου.

Η ανάλυση κινδύνου είναι χωρισμένη σε δύο μεγάλα στάδια:

• ***Ποιοτική ανάλυση κινδύνου***

Η ποιοτική ανάλυση κινδύνου είναι η διαδικασία αξιολόγησης των επιπτώσεων και των πιθανοτήτων κινδύνων που εντοπίζονται σε μια ποιοτική βάση, δηλαδή χωρίς τη χρήση αριθμητικών μεθόδων. Οι κίνδυνοι έχουν επίσης πάρει προτεραιότητα ανάλογα με το βαθμό σοβαρότητας των δυνητικών επιπτώσεων των στόχων του έργου.

Η ποιοτική ανάλυση είναι μια γρήγορη και πρόχειρη μέθοδος που παρέχει την αρχική κατανόηση της σοβαρότητας του κινδύνου. Επιτρέπει, ωστόσο, τη συνέχιση της διαδικασίας διαχείρισης των κινδύνων με τη μετάβαση στον σχεδιασμό της αντίδρασης του κινδύνου, χωρίς να χάνει χρόνο σε πολύ πιο λεπτομερή και χρονοβόρα ποσοτική ανάλυση.

Το αποτέλεσμα αυτής της διαδικασίας είναι μια λίστα προτεραιότητων των κινδύνων. Επίσης, σε αυτό το στάδιο επιλέγονται οι κίνδυνοι που πρέπει να ληφθούν για περαιτέρω ποσοτική ανάλυση.

• ***Ποσοτική ανάλυση κινδύνου***

Ποσοτική ανάλυση κινδύνου εμβαθύνει περαιτέρω την ανάλυση των επιμέρους κινδύνων μέσω της αξιολόγησης των αριθμητικών επιπτώσεών στους στόχους του έργου, δηλαδή ως προς το χρόνο και τον αντίκτυπο του κόστους. Η ποσοτική ανάλυση μπορεί επίσης να παρέχει τα ακόλουθα αποτελέσματα:

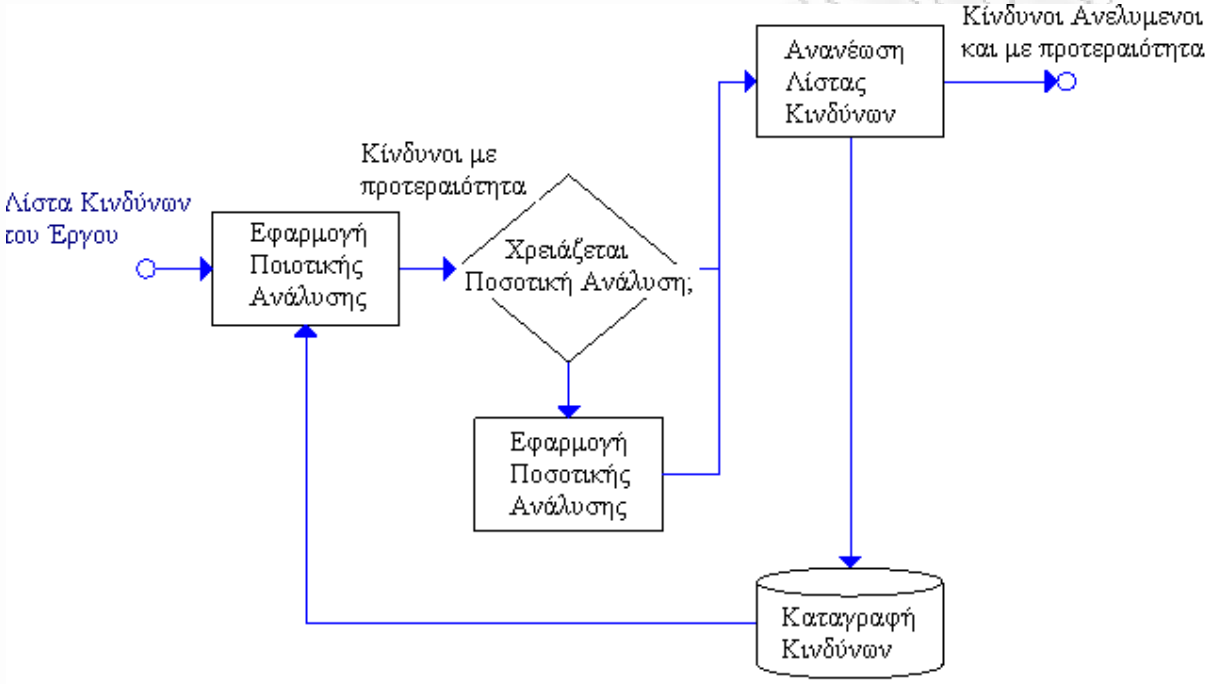
• Πιθανοτικό πρόγραμμα ανάλυσης κινδύνου έργου (με τη μέθοδο Monte Carlo)

• Πιθανότητα επίτευξης των στόχων ως προς το χρόνο και το κόστος του έργου

• Συνολικό επίπεδο των κινδύνων του έργου

• Ρεαλιστικοί στόχοι για το κόστος και το χρόνο

Η ποσοτική ανάλυση θα μπορούσε μερικές φορές να παραλείφθεί μέσω της διαδικασίας σχεδιασμού της αντίδρασης του κινδύνου, αμέσως μετά την ποιοτική ανάλυση. Το πεδίο εφαρμογής και το επίπεδο λεπτομέρειας της ποσοτικής ανάλυσης μπορούν επίσης να διαφέρουν πολύ. Σε ορισμένες περιπτώσεις είναι αρκετό να γίνουν μόνο αριθμητικές εκτιμήσεις των επιπτώσεων των επιμέρους κινδύνων είναι στη διακριτική ευχέρεια του Υπεύθυνου Συντονιστή.



Σχήμα 10: Ανάλυση Κινδύνου

7.2.4 Σχεδιασμός αντίδρασης κινδύνου(ων)

Ο σχεδιασμός αντίδρασης κίνδυνου είναι η διαδικασία ανάπτυξης εναλλακτικών προτάσεων και καθορισμού των δράσεων για την αντιμετώπιση των κινδύνων του έργου που στην πραγματικότητα καταλήγουν να συμβαίνουν. Αυτή η διαδικασία εξασφαλίζει ότι οι κίνδυνοι αντιμετωπίζονται ορθά και οι ευθύνες για τις συμφώνημένες απαντήσεις αποδίδονται στα σχετικσή μέλη της ομάδας.

Η στρατηγική ανταπόκρισης των κίνδυνων ορίζεται πριν από τον προγραμματισμό των δράσεων επέμβασης των κινδύνων. Υπάρχουν τέσσερις στρατηγικές αντιμετώπισης κινδύνων που είναι διαθέσιμες:

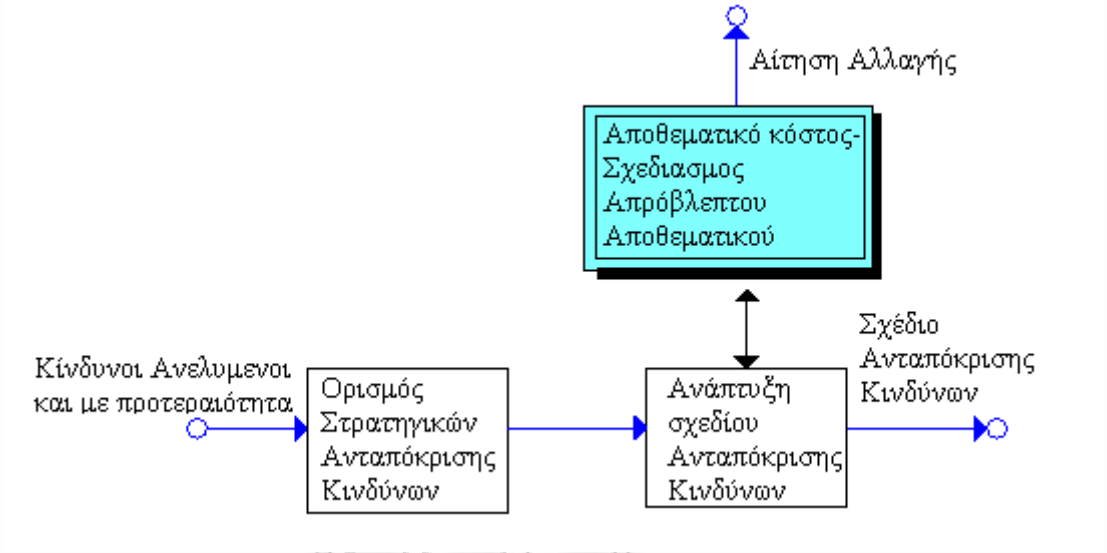
1. Αποφυγή: Στόχος είναι η εξάλειψη ενός κινδύνου, συνήθως η εξάλειψη της αιτίας του κινδύνου. Η δυνατότητα αποφυγής ορισμένων από τους κινδύνους είναι σχετικά καλή κατά τη διάρκεια του δραστηριότητων πριν τις πωλήσεις, όταν υπάρχει ακόμη δυνατότητα να επιλεχθούν διαφορετικές προσεγγίσεις και να επιρρεαστούν οι συμβατικοί όροι και οι δεσμεύσεις. Μετά την υπογραφή της σύμβασης με τις δυνατότητες αποφυγής των κινδύνων είναι πολύ χαμηλότερο, επειδή η κατανομή της πλειοψηφίας των κινδύνων που έχουν γίνει από τη σύμβαση.

2. Μετριασμός: Ο στόχος είναι η μείωση της πιθανότητας και / ή των συνεπειών του κινδύνου σε ένα αποδεκτό επίπεδο. Οι πρωταρχικές προσπάθειες πρέπει να είναι για τη μείωση της πιθανότητας επηρεάζοντας τις διασυνδέσεις των εκδήλωσεων του κινδύνου με την αιτία που προκαλεί κίνδυνο.

3. Μεταβίβαση: Η μεταφορά του κινδύνου έχει ως στόχο να στρέψει τις συνέπειες του κινδύνου σε ένα άλλο μέρος (π.χ. πελάτης ή υπεργολάβος) μαζί με την κυριότητα της απάντησης. Αξίζει

να σημειωθεί ότι η μεταβίβαση του κινδύνου μεταφέρει μόνο την ευθύνη για τη διαχείριση του κινδύνου αυτού. Δεν εξαλείφει τον κίνδυνο.

4. Αποδοχή: Η επιλογή αυτή χρησιμοποιείται όταν η ομάδα του έργου αποφασίσει να μην λάβει δράσεις αντιμετώπισης των κινδύνων ή δεν μπορεί να εντοπίσει οποιαδήποτε άλλη κατάλληλη στρατηγική απάντησης. Η ομάδα του έργου θα πρέπει να προετοιμαστεί στη συνέχεια να δει και να αποδεχθεί τις συνέπειες του κινδύνου που θα πρέπει πραγματικά να συμβούν (παθητική αποδοχή). Η ομάδα του προγράμματος μπορεί επίσης να αναπτύξει ένα σχέδιο έκτακτης ανάγκης που θα εφαρμοστεί όταν ο κίνδυνος συμβεί (ενεργός αποδοχή). Σε περίπτωση ασήμαντου κινδύνου αυτό μπορεί να είναι η πιο οικονομικά αποδοτική επιλογή. Ωστόσο, η αποδοχή των «υψηλών» κινδύνων δεν πρέπει να είναι μια επιλογή κάτω από οποιεσδήποτε συνθήκες.



Σχήμα 11: Σχεδιασμός Ανταπόκρισης Κινδύνου

Η έξοδος από το σχεδιασμό της αντίδρασης του κινδύνου έχει ως εξής:

• Σχέδιο αντιμετώπισης του κινδύνου

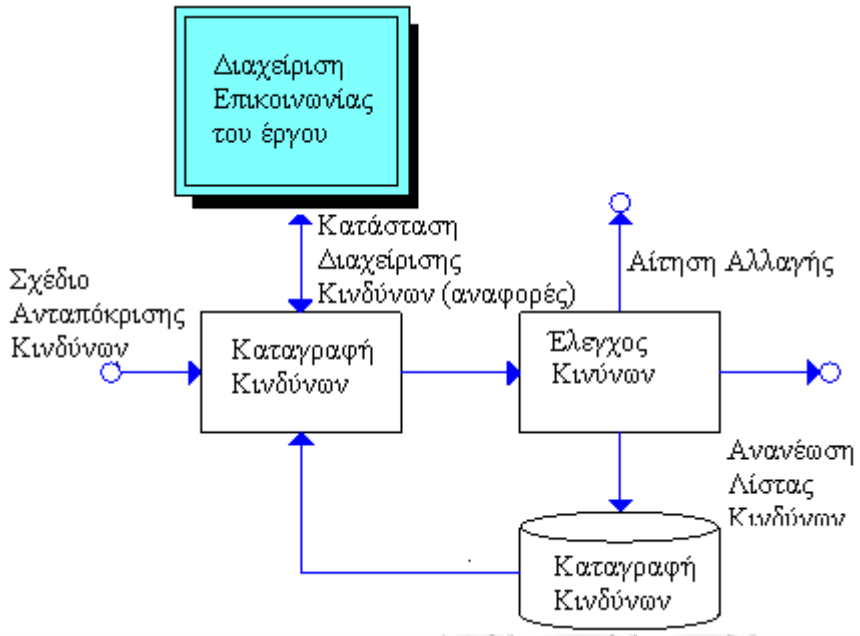
• Σχέδιο έκτακτης ανάγκης και αποθεματικό για απρόβλεπτα

• Συμβατικές συμφωνίες οι οποίες αντικατοπτρίζουν τις αποφάσεις για τη μεταφορά ορισμένων κινδύνων

7.2.5 Παρακολούθηση και Έλεγχος κινδύνου(ων)

Ένα κατάλληλο επίσημο όργανο για την παρακολούθηση και τον έλεγχο των κινδύνων σε ένα έργο είναι η εβδομαδιαία σύσκεψη για την κατάσταση έργου. Δεν είναι επιθυμητό να επανεξετάζεται το καθεστώς του κινδύνου λιγότερο συχνά.

Οι κίνδυνοι πρέπει, ωστόσο, συνεχώς (ως πρακτική ημέρα με την ημέρα) να παρακολουθούνται και να ελέγχονται από τους ιδιοκτήτες της εκάστοτε κατηγορίας κινδύνου και να λαμβάνονται τα απαραίτητα μέτρα χωρίς καθυστέρηση. Ο σκοπός της ύπαρξης ενός επισήμου φόρουμ για την παρακολούθηση και τον έλεγχο των κινδύνων είναι η ανταλλαγή πληροφοριών σχετικά με τον κίνδυνο με όλη την ομάδα και τα άλλα ενδιαφερόμενα μέρη, η τελευταία έκθεση της κατάστασης του κινδύνου, και η κλιμάκωση των κινδύνων ή η λήψη αποφάσεων σε σχέση με τους κινδύνους.



Σχήμα 12: Απεικόνιση και Έλεγχος Κινδύνου

Ο στόχος της παρακολούθησης των κινδύνων είναι να ελέγχονται τα ακόλουθα:

• Η υλοποίηση δράσεων για την ανταπόκριση του κινδύνου (τόσο για την ολοκλήρωση όσο και την κατάσταση των εν εξελίξει δράσεων)

• Η ισχύ της υποθέσεις σχετικά με το περιβάλλον του έργου

• Το κύρος και τις αλλαγές στις συμβατικές δεσμεύσεις και τους στόχους του σχεδίου

• Είναι απαραίτητη η διενέργεια πρόσθετου εντοπισμού των κινδύνων και / ή ανάλυση. Σε ορισμένες περιπτώσεις μπορεί να είναι ακόμη αναγκαία και η επανεξέταση του Σχεδίου Διαχείρισης Κινδύνου.

• Αν έχουν υλοποιηθεί όλοι οι κίνδυνοι ή αν έχουν αποφευχθεί.

• Αν έχουν ενεργοποίηθεί ενέργειες έκτακτης ανάγκης από πραγματοποιημένους κινδύνους (αποτελεσματικά).

Ο έλεγχος των κινδύνων συνεπάγεται τη διαχείριση της εφαρμογής των δράσεων επέμβασης κινδύνου ή την ανάληψη διορθωτικών ενεργειών για την απόκριση κινδύνου. Μπορεί να περιλαμβάνει επίσης την έναρξη των ενεργειών έκτακτης ανάγκης, ή τον ανασχεδιασμό του έργου.

7.3 Εφαρμογή ανάλυσης και διαχείρισης επικυνδυνότητας σε εταιρεία τηλεπικοινωνιών μέσω του εργαλείου NRisk

Η εγκατάσταση είναι πολύ απλή, μέσω μιας εφαρμογής και οι ενημερώσεις εγκαθίστανται αυτόματα. Αφορά τα πληροφοριακά έργα που αναλαμβάνει η συγκεκριμένη εταιρεία με σκοπό τον σχεδιασμό και τη διαχείριση των όποιων κινδύνων στην έναρξη αλλά και κατά τη διάρκεια του έργου.

Για να χρησιμοποιηθεί το NRisk πρέπει να συμπληρωθούν κάποιες παράμετροι και πρακτικές:

- *Γενικές Πληροφορίες:* Ορισμός του πεδίου εφαρμογής και εστίαση στις πληροφορίες. Εν μέρει σύνδεση και με άλλες σελίδες.
- *Χρησιμοποιούμενες κατηγορίες κινδύνου στο πλαίσιο της ομάδας:* Γενικές κατηγορίες κινδύνου που πρέπει να χρησιμοποιούνται.

- *Παρακολούθηση Κινδύνου & Ιδιοκτήτες Κινδύνου*: συμφωνηθέντες πρακτικές ελέγχου και καθορισμένες ιδιοκτησίες κίνδυνο πάνω και μέσα στην ομάδα.
- *Σταθερές Παράμετροι Αξιολόγηση Κινδύνου & Καθορισμένοι κύριοι επιχειρηματικοί στόχοι που πρέπει να προστατευθούν:* Επιβεβαίωση της κοινής κατανόησης των μέτρων
- *Κύριες στρατηγικές ελέγχου κινδύνων:* Οι κύριες στρατηγικές προς επιλογή
- *Ορισμός Κατάστασης για τις δράσεις*: εν συντομία ορίζεται η κατάσταση (σταθεροί ορισμοί προς επιλογή).

RM SET UP for NI | Case / project: 0 | Customer: 0 | Version 1.0

General Information — Print RM Mandate

Business Group		Case /project	
Management Team		System/Technology	
Customer		(Duration)	

Risk Monitoring Practices, Risk Categories, Risk Owners

Team risk monitoring frequency	
Date of last review:	

Risk Rating Parameters & Team Key Business Goals to be protected

RISK RATING MATRIX						
		Risk Rate = (p x i)				
(Near Certainty)	0.9	0,90	1,80	**2,70**	**3,60**	**4,50**
(Highly Likely)	0.7	0,70	1,40	2,10	**2,80**	**3,50**
(Likely)	0.5	0,50	1,00	1,50	2,00	**2,50**
(Unlikely)	0.3	0,30	0,60	0,90	1,20	1,50
(Remote)	0.1	0,10	0,20	0,30	0,40	0,50
Probability (p) / **Impact (i)**		1 (Very Low)	2 (Low)	3 (Moderate)	4 (High)	5 (Very High)

Risk Magnitudes - definitions by risk rate

HIGH	(p x i) more than	2,1	
MEDIUM	(p x i) between	0,9	2,1
LOW	(p x i) less than	0,9	

Proposed practices by Risk Magnitude

Risk Magnitude	Team indications	Proposed best practices to consider.
HIGH	Most likely unacceptable or not feasible to accept.	Perform adequate analysis. Define risk control plan. Escalate decisions if defined to do so. Put risk for monthly monitoring, report to adequate managers / management forums.
MEDIUM	Might be normal business risk taking - but risk rewards versus feasibility of controlling actions to be considered.	Define risk control plan. Escalate decisions if defined to do so. Put risk for regular monitoring, report to adequate managers / management forums.
LOW	Minimum disruption	Minimum oversight (1-2 times a year) needed to ensure risk remains low. But if defined - escalate the decision's).

Main Risk Control Strategies

Accept	We consider that the existing processes and procedures are enough.
Mitigate	It is feasible to lower the probability or/and limit the possible impact instead of solving the problems later on.
Avoid	It is necessary or feasible to avoid the risk (changes in way of doing the business).
Transfer	We smooth the possible effect by transferring the risk - and we consider the current processes & practices are enough as control.

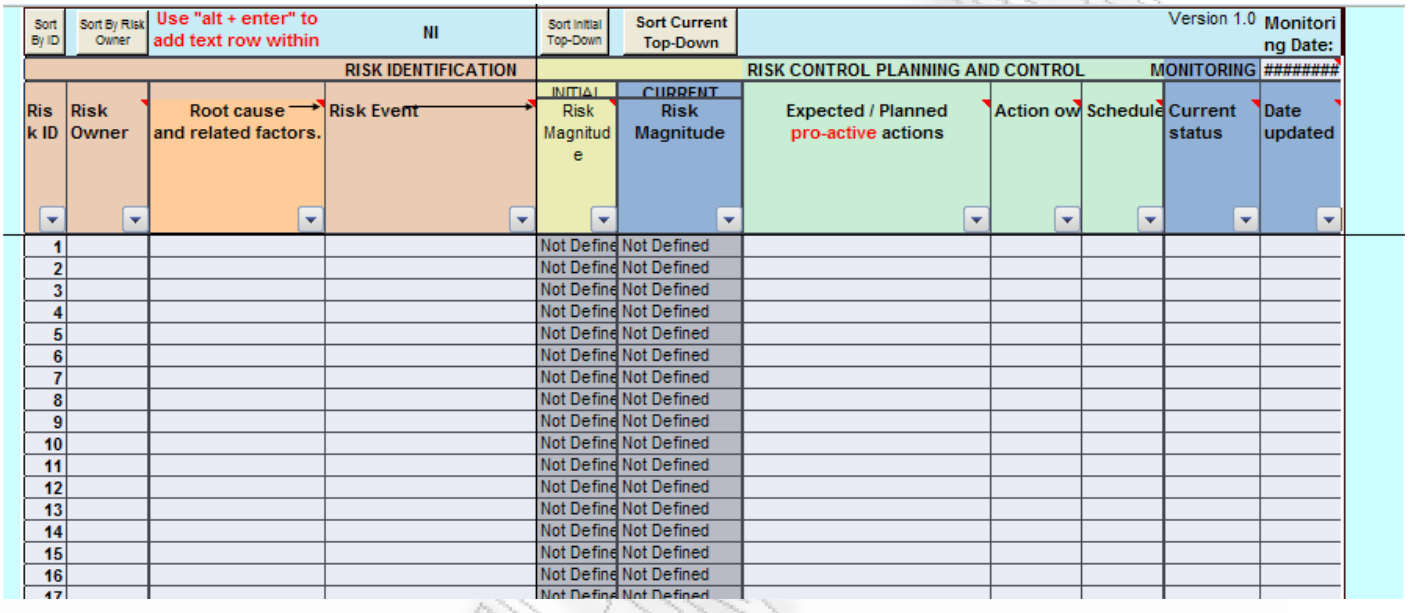
Status definitions for actions

Not started	Actions not agreed or started
Proceeding	Implementation of agreed actions proceeding as planned.
Behind the plan	Implementation delays.
Actions implemented	Actions implemented as planned.
Continuous	Actions in place are continuous - consider if the monitoring can be also closed or is team follow up still needed.
Closed	The risk is materialized or avoided.

Εικόνα 10:Βασικά Πεδία/Εντολές Κινδύνου στο NRisk

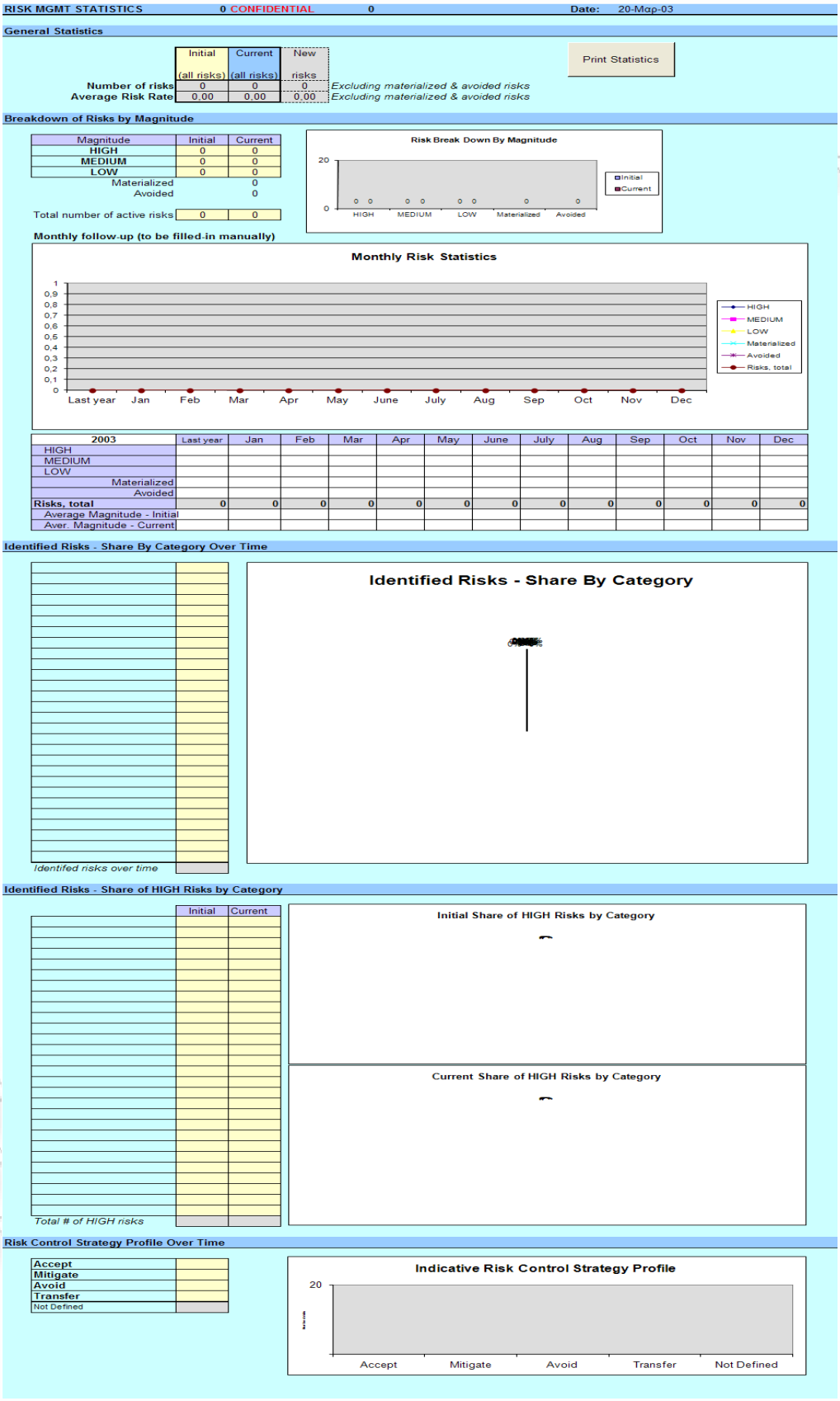
Στο πρακτικό αυτό κομμάτι της εργασίας θα δούμε τι γίνεται στα παραπάνω βήματα χρήσης του εργαλείου σε ένα πραγματικό έργο ανάπτυξης, προσομοίωσηςκαι παράδοσης λογισμικού για τηλεπικοινωνιακό πάροχο. Το ζητούμενο είναι να υπολογιστούν οι κίνδυνοι και πως αυτοί μπορούν να αντιμετωπιστούν έγκαιρα πριν την περάτωση του έργου ή αν αυτό δεν είναι εφικτό τι συνέπειες θα υπάρξουν στο έργο.

Παρακάτω, φαίνονται αναλυτικά τα βήματα χρήσης του NRisk από την έναρξη του εργαλείου ως και τον τέλος του έργου.



Sort By ID	Sort By Risk Owner	Use "alt + enter" to add text row within	NI	Sort Initial Top-Down	Sort Current Top-Down					Version 1.0	Monitoring Date:
RISK IDENTIFICATION				RISK CONTROL PLANNING AND CONTROL						MONITORING	########
Risk ID	Risk Owner	Root cause and related factors.	Risk Event	INITIAL Risk Magnitude	CURRENT Risk Magnitude	Expected / Planned pro-active actions	Action ow	Schedule	Current status	Date updated	
1				Not Define	Not Defined						
2				Not Define	Not Defined						
3				Not Define	Not Defined						
4				Not Define	Not Defined						
5				Not Define	Not Defined						
6				Not Define	Not Defined						
7				Not Define	Not Defined						
8				Not Define	Not Defined						
9				Not Define	Not Defined						
10				Not Define	Not Defined						
11				Not Define	Not Defined						
12				Not Define	Not Defined						
13				Not Define	Not Defined						
14				Not Define	Not Defined						
15				Not Define	Not Defined						
16				Not Define	Not Defined						
17				Not Define	Not Defined						

Εικόνα 11: Διαχείριση Κινδύνου στο NRisk

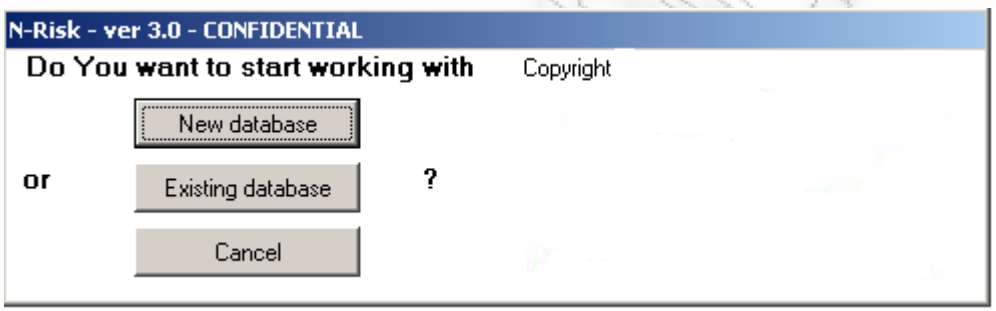


Εικόνα 12: Στατιστικά στο NRisk

7.3.1 Πρώτη Αξιολόγηση

1. Έναρξη Nrisk

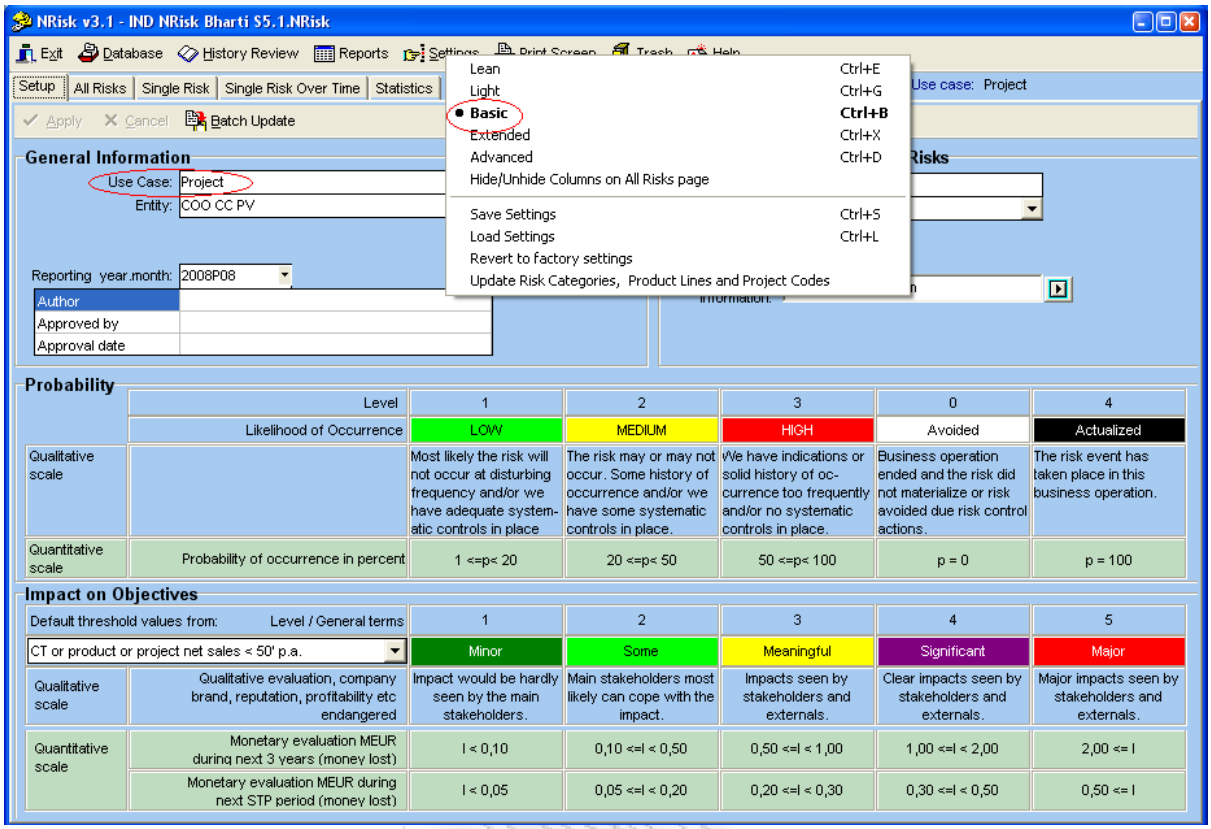
2. Δημιουργία βάσης δεδομένων, που ονομάζεται: xxx.NRisk. Μετά ανοίγει η οθόνη ρυθμίσεων του NRisk, όπου ουσιατικά δημιουργείται η βάση δεδομένων.



Οι γενικές πληροφορίες για τη βάση δεδομένων είναι μοναδικές. Δεν τηρούνται σε περίπτωση ενιαίου κινδύνου. Οι τιμές των προεπιλεγμένων πληροφοριών θα κληρονομηθούν αυτόματα σε όλους τους κινδύνους που δημιουργούνται μέσα στη βάση δεδομένων, και είναι έγκλειστες ως στοιχεία αναφοράς, επίσης, για την εξαγωγή των πληροφοριών του κινδύνου.

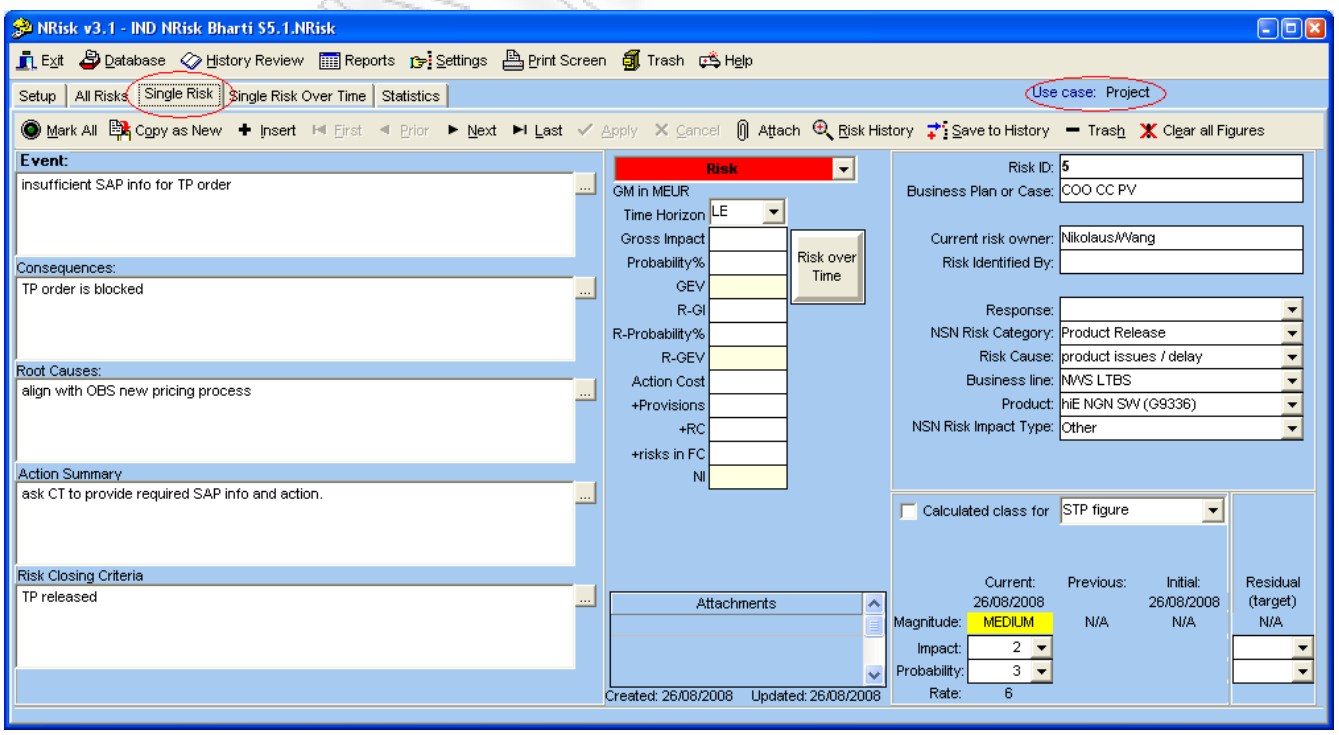
Σε περίπτωση που η βάση δεδομένων υπάρχει ήδη, επιλέγουμε τη θέση και το όνομα του αρχείου.

3. Επιλέγουμε τη *Βασική* ***(Basic)*** λειτουργία συνιστάται για αρχάριους χρήστες, η πιο Ελαφριά ***(Light)*** λειτουργία για τις Πωλήσεις.

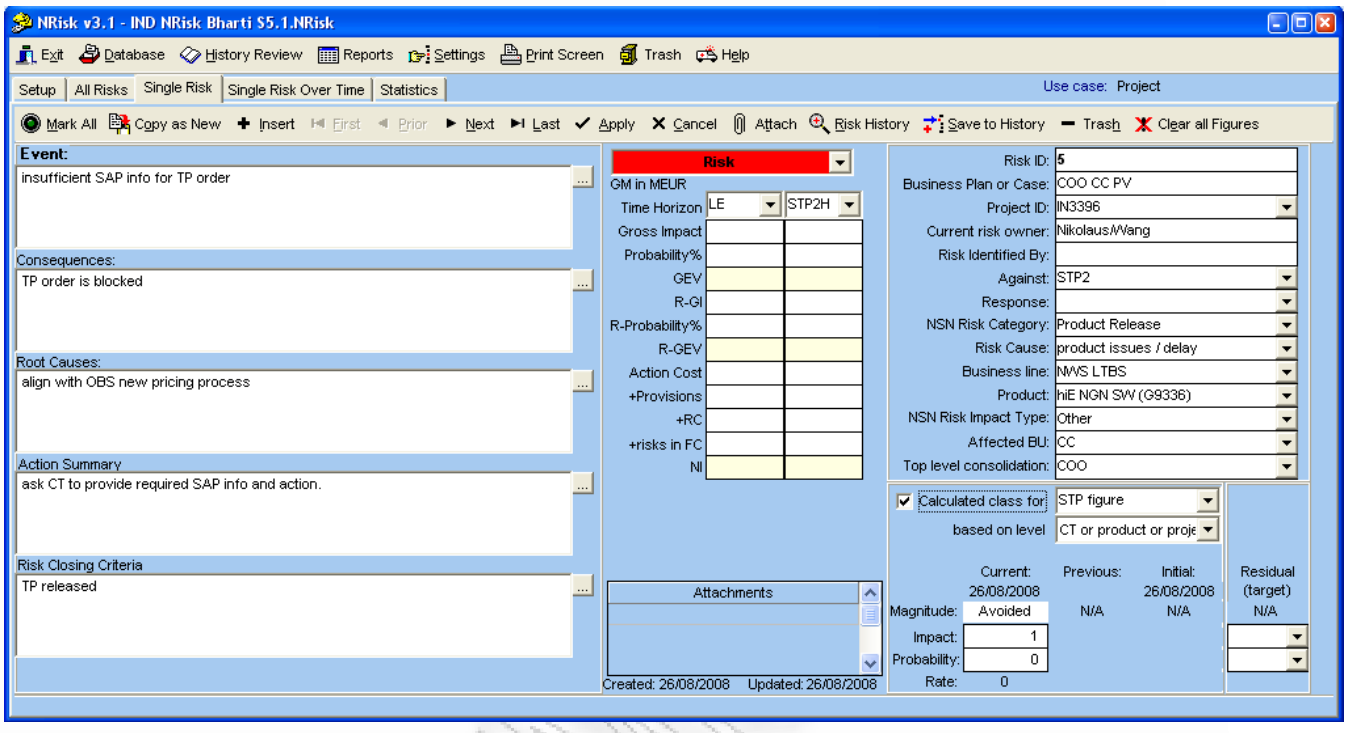


Εικόνα 13: Επιλογή λειτουργίας χρήστη

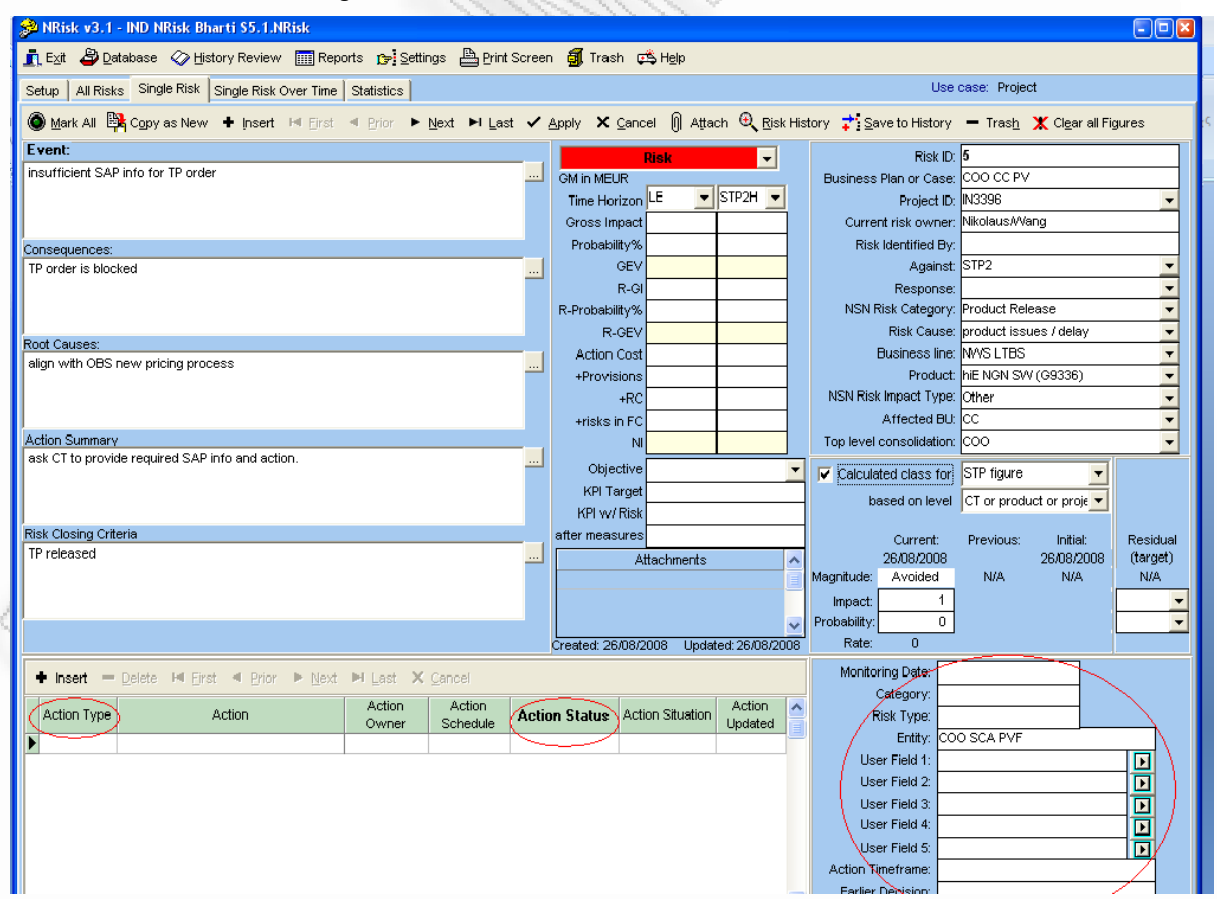
Ο Προχωρημένος ***(Advanced)*** τρόπος λειτουργίας συνιστάται για έμπειρους χρήστες. Η Εκτεταμένη ***(Extended)*** λειτουργία χρησιμοποιείται σε περιπτώσεις όπως για παράδειγμα η περίπτωση χρήσης Πρόγραμμα (use case Program), όπου οι στόχοι του κινδύνου είναι προκαταρκτικά μη χρηματοπιστωτικές.



Εικόνα 14: Light mode – Single Risk view

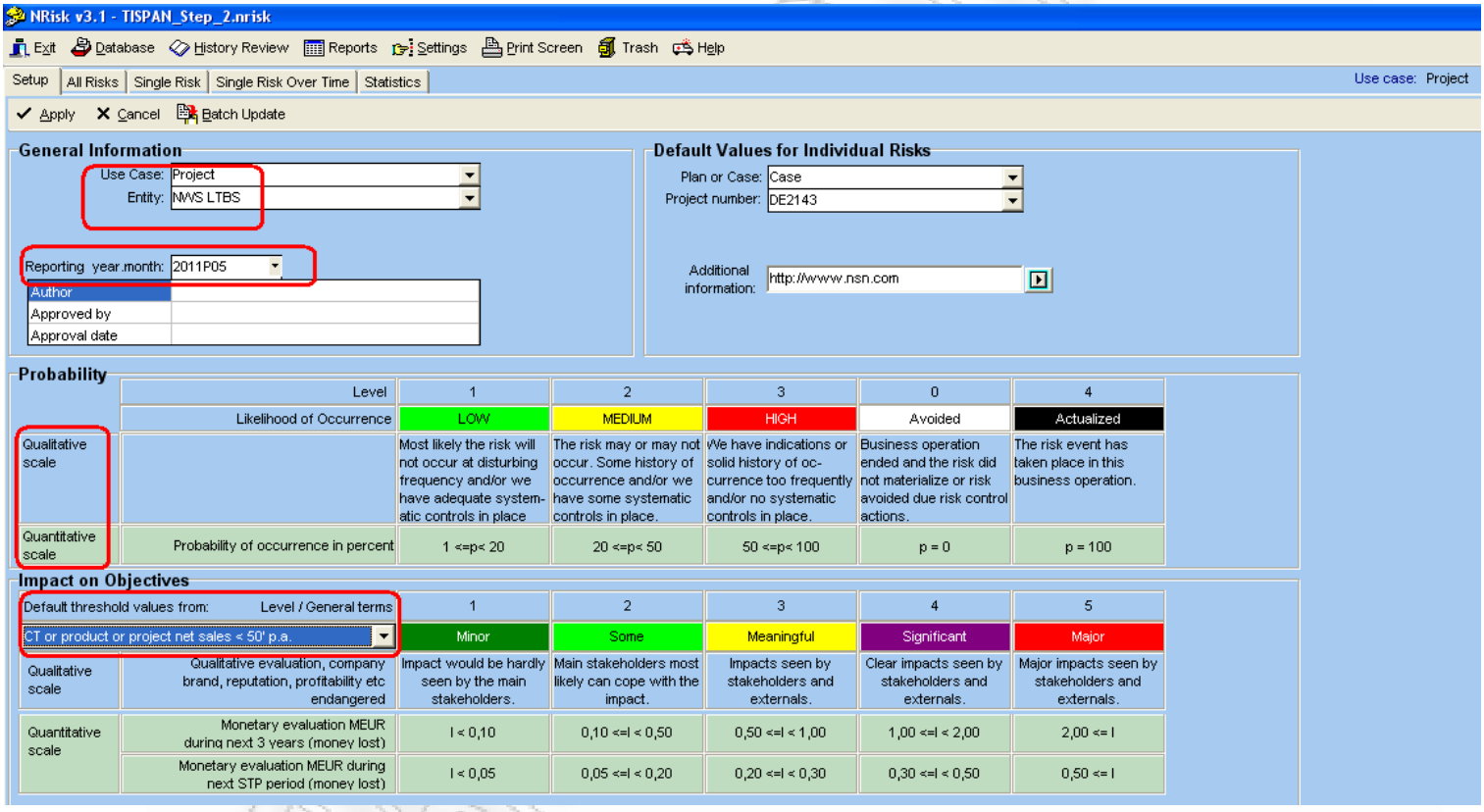


Εικόνα 15: Basic mode – Single Risk view



Εικόνα 16: Advanced mode – Single Risk view

4. Επιλέγουμε Περίπτωση Χρήσης ***(Use Case "Project")***
5. Επιλέγουμε Περίοδο Αναφοράς ***(Reporting Period)*** (από προεπιλογή, είναι ο τρέχων μήνας)
6. Επιλέγουμε το φορέα μας ***(Entity)***(από το μενού: μέχρι το επίπεδο 3)
7. Επιλέγουμε το έργο μας ***(Project)*** με τον PRS αριθμό (πληκτρολογούμε τον κωδικό χώρας και μεταβαίνουμε στο έργο)
8. Πληκτρολογούμε το σχέδιο ή υπόθεση ***(Plan or Case)***: το όνομα της ομάδας του πελάτη ή το όνομα της υπηρεσία του οργανισμού ή το έργο
9. Επιλέγουμε Επίπεδο ***(Level)***
10. Πατάμε Εφαρμογή ***(Apply)***



Εικόνα 17: Αρχικό παράθυρο στησίματος

7.3.2 Δεσμευτικές συμβάσεις για την αξιολόγηση των κινδύνων

Τα *Υποχρεωτικά* για την αξιολόγηση των κινδύνων του έργου είναι τα εξής:

- Επιλογή της κατηγορίας κινδύνου του έργου ***(project risk category)*** και του είδους των επιπτώσεων των κινδύνων του έργου ***(project risk impact type)***.
- Μακρυπρόθεσμες (LE) και βραχυπρόθεσμες (STP) *Ποσοτικές* τιμές ***(Quantitative values)***: Περιθώρια / επιπτώσεις του κόστους και πιθανότητες.
- Χρονικές σειρές στις ποσοτικές τιμές του κινδύνου μέχρι χρονικό ορίζοντα LRP.
- Ταυτότητα του κινδύνου *(Risk ID)*, Γεγονότα Κινδύνου *(Risk Event)*.

Όλες οι οικονομικές αξίες είναι εγγεγραμμένες σε εκατομμύρια ευρώ. Σε περίπτωση ενιαίας προβολής του κινδύνου: επιπτώσεις περιθώριο.
Κίνδυνος: αύξησης του κόστους = περιθώριο δυσλειτουργίας = αρνητικό πρόσημο

Ευκαιρία: βελτίωση του περιθωρίου κέρδους: θετικό πρόσημο

Προβλέψεις: και ήδη αναγνωρισμένοι κινδύνους: θετικό πρόσημο

Προβλεπόμενες ευκαιρίες (που κατέχει ήδη στις προβλέψεις): αρνητικό πρόσημο

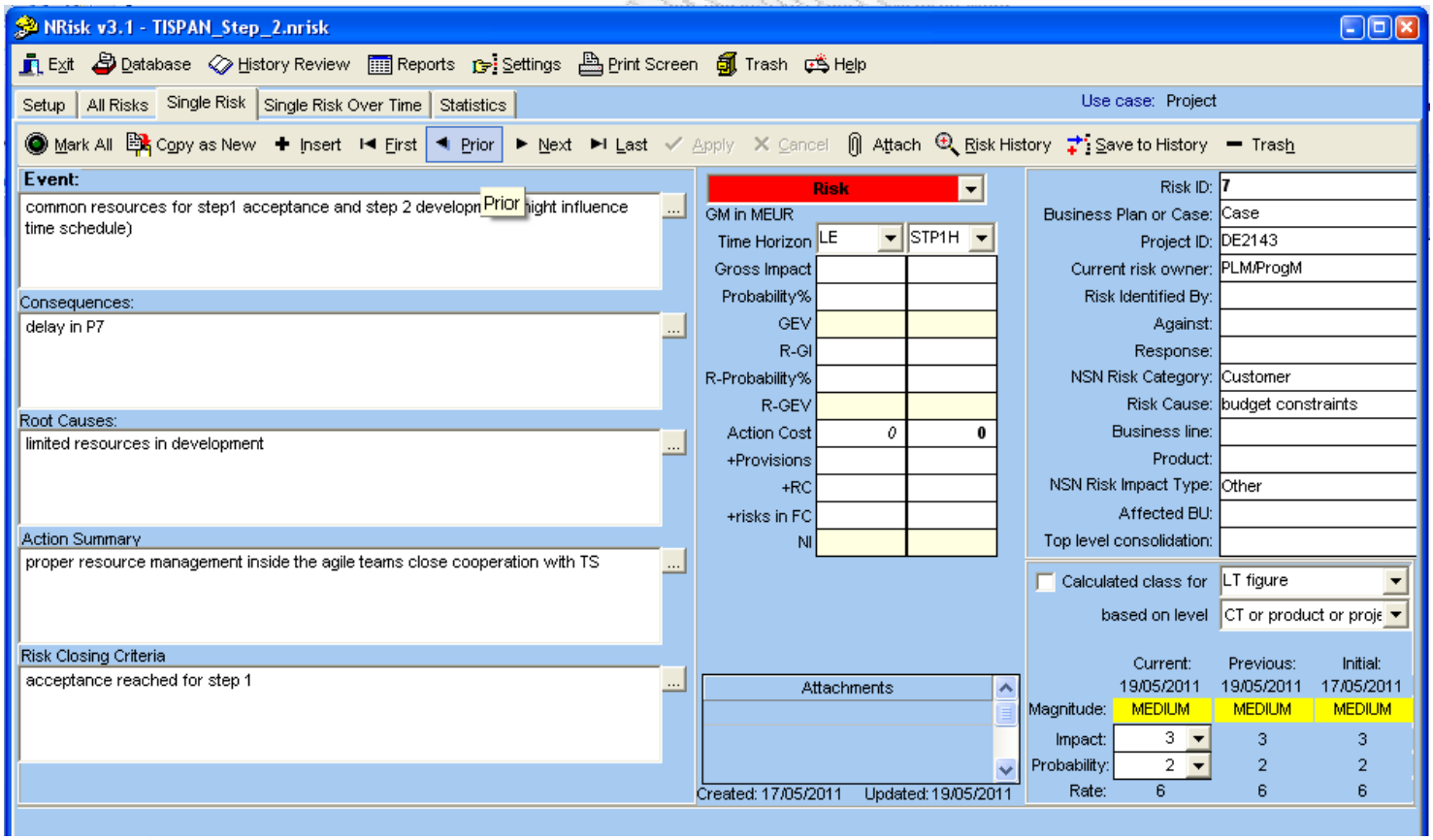
Κόστος Δράσης: αρνητικό πρόσημο

Για ειδικές κατηγορίες κινδύνων έργου, περισσότερες πληροφορίες είναι υποχρεωτικές για την εδραίωση της ανάδρασης:

- Για κινδύνους αποδέσμευσης του προϊόντος: επιλέγουμε από τη λίστα το προϊόν και την αιτία του κινδύνου.
- Για κινδύνους παράδοσης του προϊόντος: επιλέγουμε από τη λίστα το προϊόν και την αιτία του κινδύνου.
- Για κινδύνους εφαρμογής: επιλέγουμε από τη λίστα την αιτία του κινδύνου.

7.3.3 Εισαγωγή των κινδύνων και οι σχετικές δράσεις

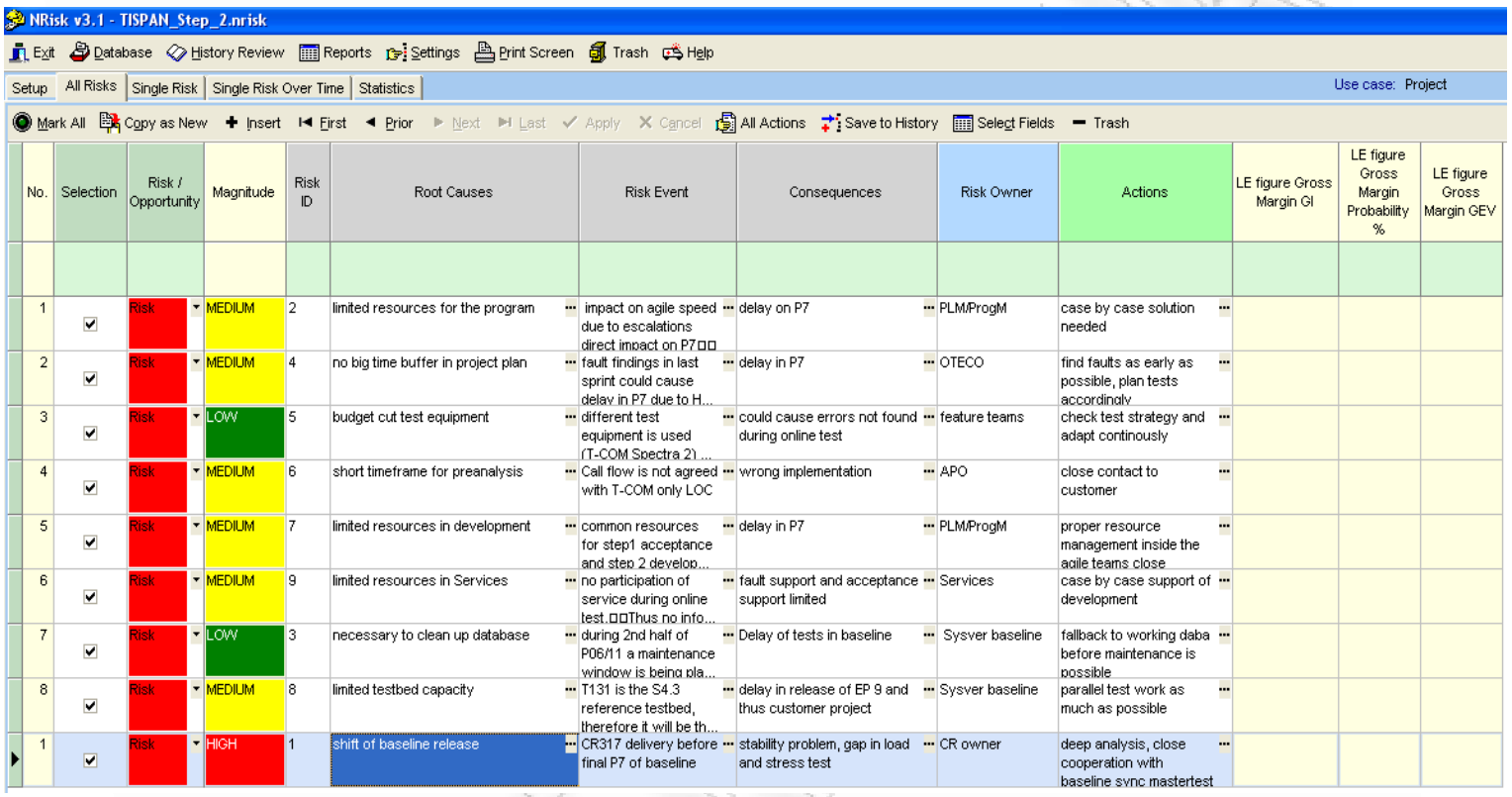
Η είσοδος των κινδύνων μπορεί να γίνει είτε με "ενιαίο κίνδυνο" ή στο "Κατά Παντός Κινδύνου" άποψη. Συνιστάται η χρήση "ενιαίο κίνδυνο» άποψη για την εισαγωγή των κινδύνων, και η χρήση "Κατά Παντός Κινδύνου" για το φιλτράρισμα και τη διαλογή.



Εικόνα 18: Εισαγωγή κινδύνου

Η διαγραφή των κινδύνων είναι επίσης δυνατή και από τις δύο απόψεις. Ορισμένα πεδία δεδομένων των οποίων η ανάγνωση / εγγραφή είναι δυνατά στην προβολή "ενιαίου κινδύνου" ενώ στην "Κατά Παντός Κινδύνου" άποψη είναι δυνατή μόνο ανάγνωση.

Σε κάθε πιθανό κίνδυνο δίνεται μια ταυτότητα, καθορίζεται το επίπεδο της επικυνδυνότητας, οι συνέπειες, ο ιδιοκτήτης του κινδύνου και τα αντίμετρα.



No.	Selection	Risk / Opportunity	Magnitude	Risk ID	Root Causes	Risk Event	Consequences	Risk Owner	Actions	LE figure Gross Margin GI	LE figure Gross Margin Probability %	LE figure Gross Margin GEV
1	☑	Risk	MEDIUM	2	limited resources for the program	impact on agile speed due to escalations direct impact on P7□□	delay on P7	PLM/ProgM	case by case solution needed			
2	☑	Risk	MEDIUM	4	no big time buffer in project plan	fault findings in last sprint could cause delay in P7 due to H...	delay in P7	OTECO	find faults as early as possible, plan tests accordingly			
3	☑	Risk	LOW	5	budget cut test equipment	different test equipment is used (T-COM Spectra 2) ...	could cause errors not found during online test	feature teams	check test strategy and adapt continously			
4	☑	Risk	MEDIUM	6	short timeframe for preanalysis	Call flow is not agreed with T-COM only LOC	wrong implementation	APO	close contact to customer			
5	☑	Risk	MEDIUM	7	limited resources in development	common resources for step1 acceptance and step 2 develop...	delay in P7	PLM/ProgM	proper resource management inside the agile teams close			
6	☑	Risk	MEDIUM	9	limited resources in Services	no participation of service during online test.□□Thus no info...	fault support and acceptance support limited	Services	case by case support of development			
7	☑	Risk	LOW	3	necessary to clean up database	during 2nd half of P06/11 a maintenance window is being pla...	Delay of tests in baseline	Sysver baseline	fallback to working daba before maintenance is possible			
8	☑	Risk	MEDIUM	8	limited testbed capacity	T131 is the S4.3 reference testbed, therefore it will be th...	delay in release of EP 9 and thus customer project	Sysver baseline	parallel test work as much as possible			
1	☑	Risk	HIGH	1	shift of baseline release	CR317 delivery before final P7 of baseline	stability problem, gap in load and stress test	CR owner	deep analysis, close cooperation with baseline sync mastertest			

Εικόνα 19:Προβολή όλων των κινδύνων με τα αντίμετρα, συνέπειες κ.λ.π.

Συνήθως, οι κίνδυνοι αφορούν τα εξής πεδία:

- Διαθεσιμότητα υλικού
- Διατήριση χρονικών πλαισίων
- Κόστος υλοποίησης
- Λάθη που προκύπτουν από τον έλεγχο του λογισμικού

Οι συνέπειες αφορούν συνήθως:

- Την ποιότητα του λογισμικού
- Την ημερομηνία παράδοσής του
- Την τήρηση του συμβολαίου και των απαιτήσεων του πελάτη (ποινές)
- Πιθανή ακύρωση του έργου

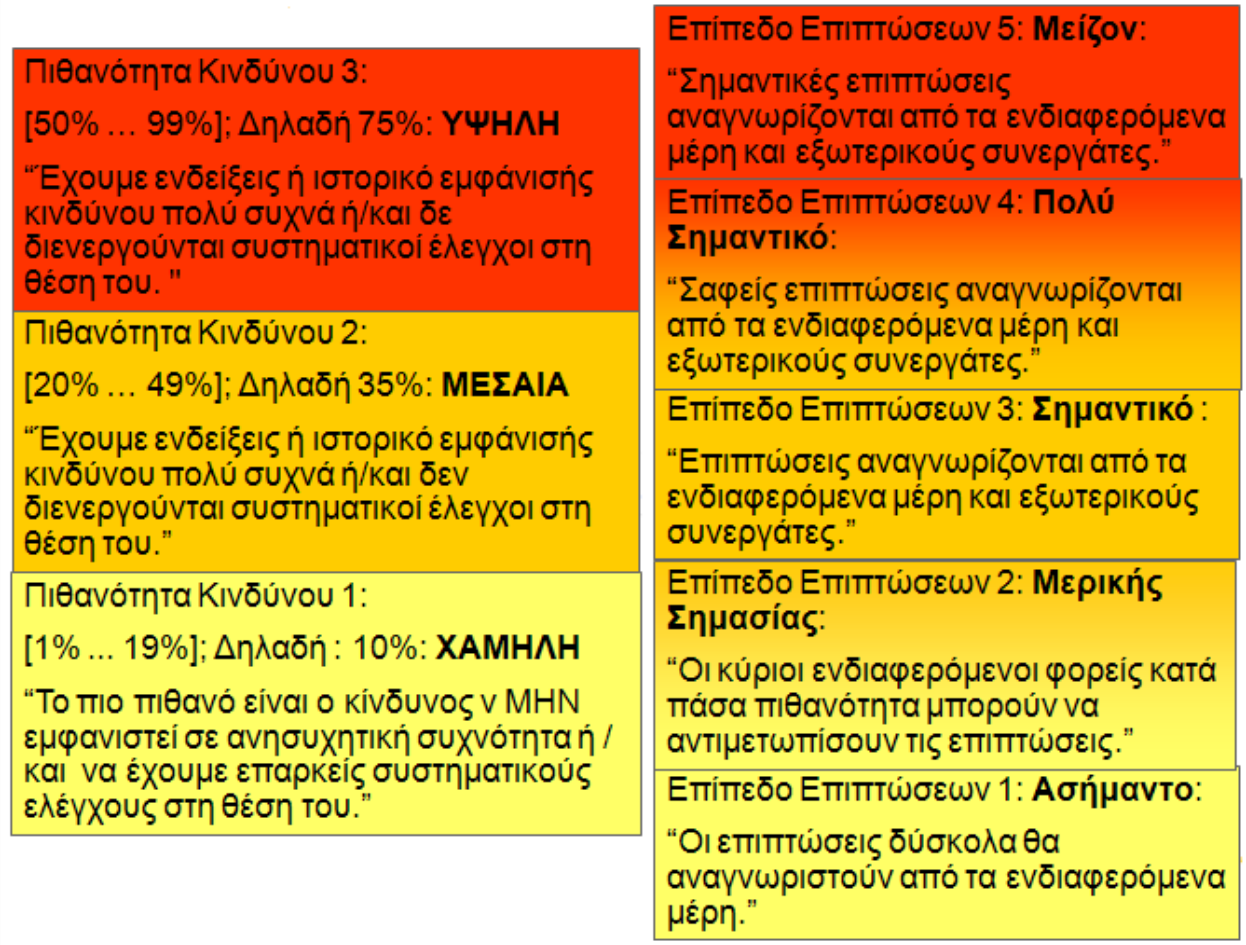
Και τα αντίμετρα που προκύπτουν είναι:

- Παράταση έργου
- Αύξηση του προσωπικού
- Αύξηση κόστους (επιπλέον εξοπλισμός, υπερωρίες κλπ)

7.3.4 Ποιοτική και Ποσοτική Ανάλυση Κινδύνου

Η ποιοτική ανάλυση ορίζει τον κίνδυνο από υποκειμενική ή ποιοτική άποψη. Προσδιορίζονται οι τιμές των πιθανοτήτων και των επιπτώσεων. Τα αποτελέσματα των ποιοτικών εκτιμήσεων των κινδύνων ορίζουν την πιθανότητα κινδύνου ως «Υψηλή», «Μέτρια»,

«Χαμηλή». Στο παρακατω σχήμα φαίνονται τα επίπεδο των επιπτώσεων και των πιθανοτήτων και η περιγραφή τους.



Σχήμα 13: Επίπεδα επιπτώσεων και πιθανοτήτων κινδύνων – Ποιοτική Ανάλυση

Για την ποσοτική αξιολόγηση του κινδύνου, η πιθανότητα εμφάνισης του κινδύνου και η μέγιστο ρεαλιστικό αντίκτυπο εκφράζονται σε επίπεδο αριθμών.

- Οι πιθανότητες εμφανίζονται σε ποσοστό μεταξύ 1% και 99%.
- Οι τιμές που εκφράζουν τις επιπτώσεις σε εκατομύρια €.

Τα ακόλουθα χρηματοπιστωτικά μέσα υπόκεινται σε αξιολόγηση του κινδύνου:

- Όγκος πωλήσεων (εδώ περιλαμβάνονται οι μεταβολές όγκου μεταξύ των περιόδων προγραμματισμού, που εμφανίζονται ως κίνδυνοι της μείωσης της περιόδου και ως ευκαιρία στην αυξημένη περίοδος)
- Μικτό Περιθώριο (για την ανάλυση κινδύνων του έργου είναι οι πιο πρόσφατες εκτιμήσεις)
- Οι δαπάνες πέρα από το ακαθάριστο περιθώριο
- Ταμειακές ροές

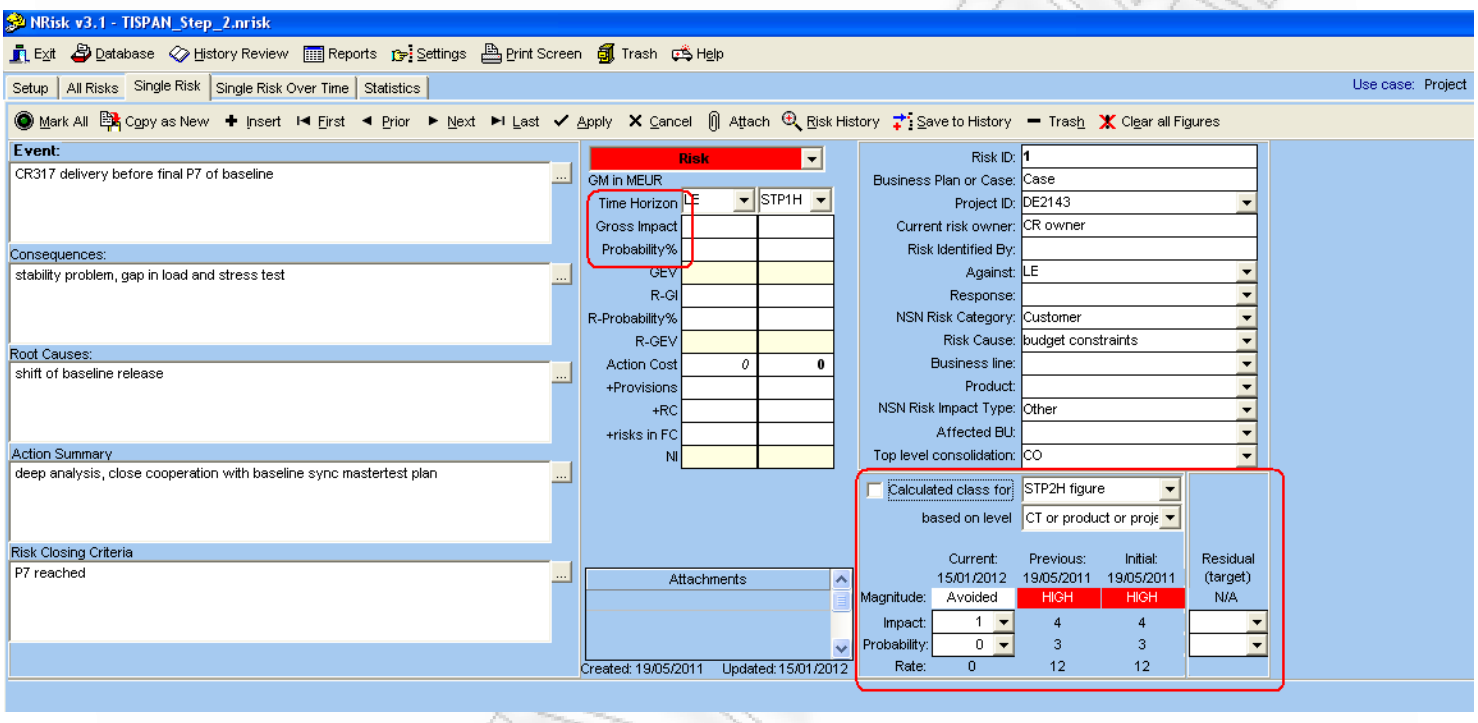
Η ποσοτική εκτίμηση των κινδύνων δείχνει τους κινδύνους σε σχέση με το χρονικό ορίζοντα της εμφάνισης των δυνητικών κινδύνων (κίνδυνοι έκθεσης, π.χ. από τη χρηματοδότηση), ή της αναμενόμενης υλοποίησης (κίνδυνοι για το είδος συναλλαγής, π.χ. αύξηση του κινδύνου κόστους), αντίστοιχα.

Για τις προβλέψεις, το χρονοδιάγραμμα της απαιτούμενης οικονομικής διαχείρισης μπορεί να είναι εξίσου σημαντικό με την πιθανή ημερομηνία της εμφάνισης του κινδύνου.

Ο ορισμός της ποσοτικής εκτίμησης του κινδύνου θα μπορούσε να εκφραστεί με τον τύπο:

Συνολικές Επιπτώσεις (€) x Πιθανότητες (%) = Ολικό Αναμενόμενο Κόστος (€)

Το NRisk δίνει την δυνατότητα ενεργοποίησης του αυτόματου υπολογισμού. Έτσι, η καταχώρηση στις τάξεις του αντίκτυπου και των πιθανοτήτων γίνεται αυτόματα σύμφωνα με την επιλεγμένη κλίμακα ορίου και του χρονοδιαγράμματος. Ο κίνδυνος έχει πάντα αρνητικό πρόσημο ενώ η πιθανότητα πάντα θετικό.



Εικόνα 20: Ποσοτική εκτίμηση κινδύνου στο NRisk

Υπάρχει επίσης η δυνατότητα χρονοσειράς των τιμών της ποσοτικής ανάλυσης. Αφού επιλεγεί ο πρώτα το έτος για την προβολή της έκθεσης ανάπτυξης του κινδύνου κατά την πάροδο του χρόνου. Αφού συμπληρωθούν το πεδίο των επιπτώσεων σε εκατομμύρια ευρώ και το ποσοστό της πιθανότητας για όλο τον χρονικό ορίζοντα, σωρεύονται οι τιμές έκθεσης πριν από μέτρα (GI, P) και μετά από τα μέτρα (R-GI, RP), καθώς και τα οικονομικά στοιχεία διακίνησης και το κόστος των δράσεων.

7.3.5 Ταξινόμηση και φιλτράρισμα των κινδύνων

Το εργαλείο δίνει τη δυνατότητα ταξινόμησης και φιλτραρίσματος των κινδύνων τα οποία όμως δεν αποθηκεύονται αυτόματα μετά την έξοδο από τη βάση δεδομένων. Το φιλτράρισμα είναι ένας χρήσιμος τρόπος για την επιλογή ορισμένων κινδύνων, σύμφωνα με ορισμένα κριτήρια καθ' όλη την προβολή του κινδύνου και το παράθυρο παρακολούθησης. Μερικά φίλτρα είναι τα εξής:

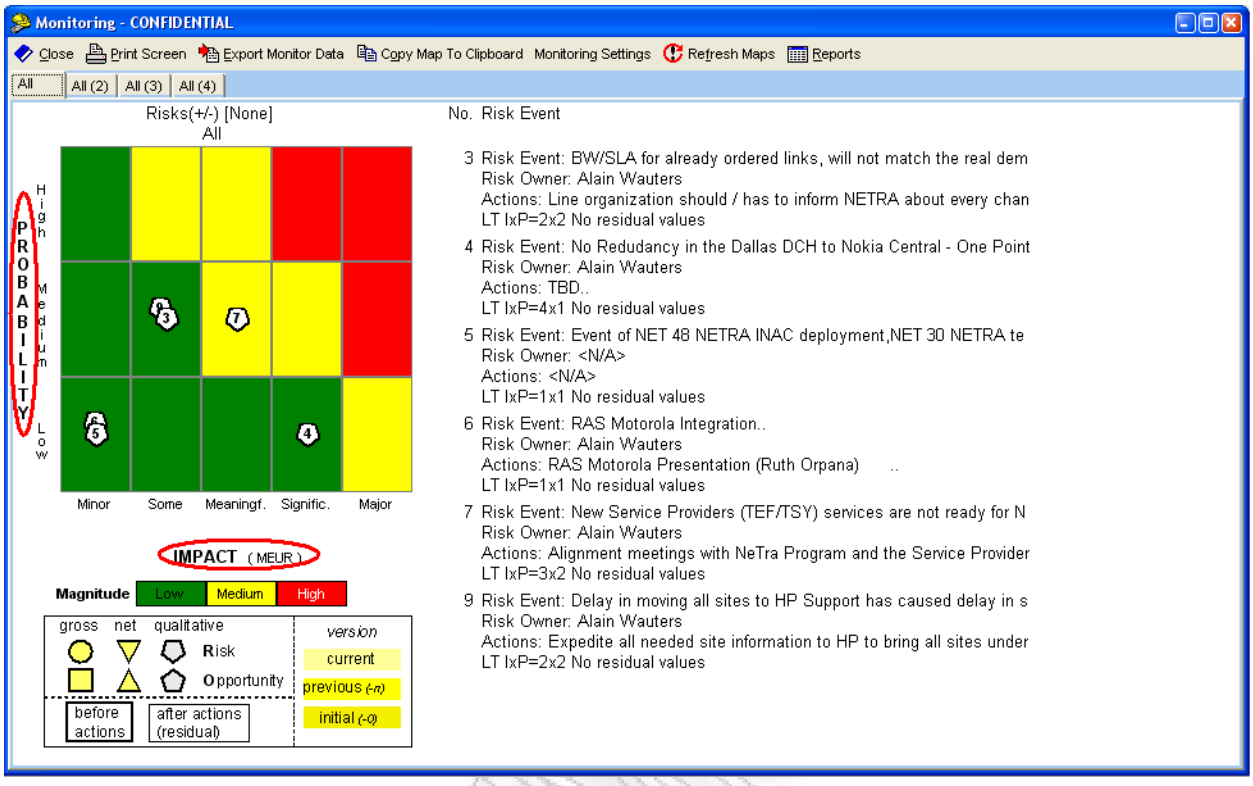
<3
>3
!=2 <>2
x OR *y*
x AND *y*
Abc
Ab
*Ab
Ab*
IPT

Για κάθε είδος προϊόντος συναφών κινδύνων, το NRisk φέρει το όνομα του προϊόντος ως κριτήριο κατάταξης προσανατολισμένο στην αιτία που προκλήθηκε. Τα προϊόντα έχουν ήδη εκχωρηθεί προηγουμένως στην γραμμή των επιχειρήσεων τους για την ταξινόμηση και το φιλτράρισμα. Τα προϊόντα είναι ταξινομημένο κατά επιχειρηματική μονάδα και επιχειρηματική γραμμή.

7.3.6 Παράθυρο Παρακολούθησης

Με το NRisk μπορουμε να παρακολουθούμε τους κινδύνους σε γραφική μορφή. Αφού, λοιπόν, επιλέξουμε ποιους κινδύνους θέλουμε να παρακολουθούμε μπορούμε να επιλέξουμε οποιονδήποτε συνδυασμό: στοιχεία κινδύνου - χρονικούς ορίζοντες, εκδόσεις, επιλογή απόκρυψης εκδόσεων και στοιχείων για την προβολή. Οι επιλογές εμφάνισης είναι οι εξής:

- στοιχεία κειμένου συμπεριλαμβανομένου αριθμητικών στοιχείων
- συνεχής ή με τάξεις κινδύνου εμφάνισης
- συμβολική επικάλυψη απόστασης (για τη συνεχή εμφάνιση)
- επιλογή σελιδοποίησης
- συνδυασμένοι / χωριστοί χάρτες
- κλίμακα επιπτώσεων (σύμφωνα με τις προεπιλογές επιπέδου της εταιρείας)
- μορφοποίηση κειμένου (αλλαγές γραμμής ...)



Εικόνα 21: Παράθυρο παρακολούθησης των κινδύνων

Ο χάρτης των κινδύνων μπορεί να εμφανίζεται ξεχωριστά για τις ευκαιρίες του κινδύνου ή σε συνδυασμό. Τα στοιχεία κινδύνου απεικονίζονται ως εξής:

Μικτός Κίνδυνος	●
Μικτή Ευκαιρία	■
Καθαρός Κίνδυνος	▼
Καθαρή Ευκαιρία	▲
Χειροποίητος Κίνδυνος	⬟
Χειροποίητη Ευκαιρία	⬟

Πίνακας 9: Απεικόνιση στοιχείων κινδύνου

Το NRisk3.1 υποστηρίζει τη δημιουργία ειδικών εκθέσεων με τη χρήση του Excel με αυτόματη αντιγραφή του riskmap.

7.4 Αποτελέσματα και συμπεράσματα

Η εταιρεία έχει δεσμευτεί για την συστηματική αντιμετώπιση των κινδύνων. Συνεπώς, χρειάζεται ένα καλό εργαλείο που να υποστηρίζει την ισχυρή σύνδεση με τη διαδικασία διαχείρισης κινδύνων της εταιρείας, να είναι εύκολο στη χρήση, γραφικό και να κάνει εύκολη την εισαγωγή, την εξαγωγή και την παρακολούθηση των αλλαγών.

Το Nrisk είναι ένα εργαλείο για όλα τα είδη των εκτιμήσεων κινδύνου. Διατίθεται για πολλαπλά σενάρια χρήσης και παρέχει την ευκαιρία ελέγχου των έργων των πελατών κατά τη φάση της υλοποίησης. Είναι ένα λειτουργικό εργαλείο στο σύνολο του κύκλου διαχείρισης των κινδύνων του έργου.

Τα αποτελέσματα ανάλυσης και διαχείρισης των κινδύνων με τη βοήθεια του εργαλείου Nrisk είναι η συλλογή, η εκτίμηση και η συνεχής παρακολούθηση των κινδύνων που εμφανίζονται καθ' όλη τη διάρκεια διεξαγωγής ενός έργου ανάπτυξης, ελέγχου και παράδοσης του λογισμικού.

Πιο συγκεκριμένα, τα αποτελέσματα είναι τα εξής:

- Εξασφαλίζεται η κερδοφορία μέσω της διαχείρισης των κινδύνων και την αξιοποίηση ευκαιριών.
- Προσδιορίζονται οι παράγοντες που είναι πιθανό να επηρεάσουν τους στόχους του οργανισμού
- Ποσοτικοποιούνται οι πιθανές επιπτώσεις του κάθε παράγοντα και αξιολογείται το όφελος από τη χρήση κατάλληλων πόρων και την ιεράρχηση αντιμέτρων
- Παρέχεται μια βάση για τους μη ελεγχόμενη κινδύνους
- Εκτελείται διαχείριση κινδύνων σε επίπεδο προϊόντος σε όλο τον κύκλο ζωής του προϊόντος
- Αναλύονται οι στόχοι και αξιολογούνται οι επιπτώσεις της μη επίτευξης των στόχων
- Προετοιμάζονται προτάσεις για να αποφασιστούν οι δράσεις μετριασμού

Ενώ υπάρχουν πολλοί παράγοντες για την αποτυχία ενός σχεδίου, δεν υπάρχει μόνο μία λύση. Ο παράγοντας που πλησιάζει περισσότερο είναι ο σχεδιασμός. Πολλά έργα αποτυγχάνουν επειδή οι ομάδες βλέπουν το σχέδιο του έργου ως ένα στατικό έγγραφο αντί ενός δυναμικού πλαισίου για την επίτευξη μιας σειράς στόχων.

Για να δούμε τα προβλήματα πριν αυτά συμβούν, θα πρέπει να υπάρχει πολύ προληπτική ανάλυση και ανάπτυξη σχέσεων. Αυτό απαιτεί πολύ χρόνο και έξοδα, έτσι συχνά ο προγραμματισμός κόβεται στο στάδιο προ-πωλήσεων. Ένα ισχυρή επιχειρηματική περίπτωση, ένα σχέδιο διαχείριση έργου και τον καταστατικό κινδύνου θα εκθέσει δυνατά και αδύνατα σημεία του έργου. Έτσι, οι διαχειριστές του έργου μπορούν να προσδιορίσουν ποιοι κίνδυνοι μπορούν να αποφευχθούν, ποιοι να μετριαστούν και ποιοι να γίνουν αποδεκτοί.

Η αποφυγή του κινδύνου είναι ιδιαίτερα ευνοϊκή, δεδομένου ότι επιτρέπει στον διαχειριστή του προγράμματος να μείνει με την τεχνική αναφορά και το χρονοδιάγραμμα. Αυτό συμβάλλει άμεσα στην ικανοποίηση του πελάτη δεδομένου ότι ο υπεύθυνος έργου δεν ασχολείται πάντα σε κατάσταση κρίσης, που οδηγεί σε μεγαλύτερη πιθανότητα να επιτευχθούν τα ορόσημα και οι στόχοι του έργου.

Μελλοντική Επέκταση

Η ανάγκη ύπαρξης συγκεκριμένου πλαισίου μέσα στο οποίο γίνεται η χρήση του δικτύου ενός οργανισμού έχει προβλεφθεί, όπως μαρτυρά η ύπαρξη μιας πληθώρας προϊόντων λογισμικού που διατίθενται στο εμπόριο. Τα εργαλεία αυτά εστιάζουν στους δύο βασικούς τομείς της ανάλυσης ρίσκου και της αποτίμησης των κινδύνων, συμβάλλοντας αποτελεσματικά στην δημιουργία μιας πολιτικής ασφάλειας που θα είναι πλήρης, αλλά κυρίως «προσωποποιημένη» σε κάθε δίκτυο.

Η κατανομή των ρόλων είναι ένα κομμάτι στο οποίο μπορεί να υπάρξει πλούσιο πεδίο για μελλοντική επέκταση. Οργανισμοί και επιχειρήσεις έχουν υποστεί καταστροφικά λάθη εξαιτίας λανθασμένων επιλογών στο κρίσιμο αυτό ζήτημα. Εκτός από τα παραπάνω, στο μέλλον, θα μπορούσε κάποιος να εργαστεί πάνω στην βελτίωση της παρουσίασης των γραπτών αναφορών. Είναι σημαντικό, ο διαχειριστής, να μελετάει μία αναφορά η οποία να είναι οπτικά ελκυστική και να τον βοηθάει στο να επικεντρωθεί στα καίρια σημεία της, να έχει όσο δυνατόν καλύτερες και κατατοπιστικές προτάσεις. Κάτι τέτοιο θα μπορούσε, ως ένα βαθμό, να επιτευχθεί πιθανώς με την προσθήκη στατιστικών γραφημάτων σε ορισμένα σημεία.

Είναι επίσης γεγονός ότι στις διάφορες εταιρίες αυτό που έχει σημασία στο τέλος της ημέρας είναι το κόστος. Θα μπορούσαν λοιπόν στο πρόγραμμα να προστεθούν κάποιες ερωτήσεις, μέσα από τις οποίες στην τελική αναφορά θα προκύπτει κάποιο συμπέρασμα για το οικονομικό κόστος που θα υπάρξει από μια ενδεχόμενη παραβίαση ασφάλειας. Αυτό είναι ένα επιχείρημα που πείθει τους περισσότερους διοικητικούς στην λήψη των αναγκαίων μέτρων.

Τέλος, η προσθήκη νέων κατηγοριών και ερωτήσεων ή τροποποίηση αυτών που υπάρχουν ήδη, προκειμένου να επιτευχθεί καλύτερη συλλογή δεδομένων για το διαχειριζόμενο πληροφοριακό σύστημα, λόγω του ότι υπάρχει πάντα το ενδεχόμενο να εμφανιστούν νέες και καλύτερες τεχνολογίες, θα ήταν ένα καλό πεδίο για μελλοντική βελτίωση.

8 Βιβλιογραφικές Πηγές

1. **Steve, Elky**. "*An Introduction to Information System Risk Management".* May 31, 2006
2. **Gary Stoneburner, Alice Goguen1, and Alexis Feringa. "***Risk Management Guide for Information Technology System".* July 2002
3. **Christopher Alberts, Audrey Dorofee, James Stevens, and Carol Woody. "***OCTAVE®-, Implementation Guide v1".* January 2005
4. *"BSI-Standard 100-3: Risk analysis based on IT-Grundschut".* 2008
5. *"EBIOS-1-GuideMethodologique"*. Paris, 2010
6. **Francisco López Crespo, Miguel Angel Amutio Gómez, Javier Candau, and José Antonio Mañas. "***MAGERIT – version 2, Methodology for Information Systems Risk Analysis and Managemen"t.* Madrid, 20 June 2006
7. **SIEMENS**. *"The Logic behind CRAMM's Assessment of Measures of Risk and Determination of Appropriate Countermeasure".* October 2005
8. http://rm-inv.enisa.europa.eu/rm_ra_methods.html
9. http://www.iso27001security.com/html/27001.htm, *"ISO/IEC 27001:2005 Information technology -- Security techniques -- Specification for an Information Security Management System"*
10. **Catriona Norris – UMIST, Professor John Perry - The University of Birmingham, Peter Simon - CPS Project Management. "***PROJECT RISK ANALYSIS AND MANAGEMENT".* March1992, republished January 2000
11. **Mohamed Noordin Yusuff**. "*CONTEMPORARY APPROACHES TO PROJECT RISK MANAGEMENT: ASSESSMENT & RECOMMENDATIONS"*
12. http://c4pe.com/gdpm_systems/gd.html
13. http://en.wikipedia.org/wiki
14. http://www.ffwdpm.com/why-use-gdpm.html
15. **Σωκράτης Κ. Κάτσικας,** *"Ανάλυση, Αποτίμηση και Διαχείριση Επικινδυνότητας Πληροφοριακών Συστημάτων".*
16. Νόμος 2474/1999, Προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα.
17. Ασφάλεια πληροφοριακών συστημάτων και δικτύων, **Γ. Πάγκαλος, Ι. Μαυρίδης**, κεφάλαιο 2 «Πολιτικές και Μοντέλα Ασφάλειας ΠΣ»