ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ
ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ
ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ
ΥΠΟΛΟΓΙΣΤΩΝ

ΠΑΝΕΠΙΣΤΗΜΙΟ
ΠΕΙΡΑΙΩΣ
ΤΜΗΜΑ ΒΙΟΜΗΧΑΝΙΚΗΣ
ΔΙΟΙΚΗΣΗΣ ΚΑΙ
ΤΕΧΝΟΛΟΓΙΑΣ

ΔΙΕΠΙΣΤΗΜΟΝΙΚΟ – ΔΙΑΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ «ΤΕΧΝΟ-ΟΙΚΟΝΟΜΙΚΑ
ΣΥΣΤΗΜΑΤΑ»

Ολοκληρωμένη Μεθοδολογία Διαχείρισης Κινδύνου Έργων και Υπηρεσιών Πληροφορικής

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Ηλιάνα Π. Αυγερίκου-Σαμωνά

Επιβλέπων : Γεώργιος Ματσόπουλος

Επίκουρος Καθηγητής Ε.Μ.Π.

Αθήνα, Ιούνιος 2014

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΤΜΗΜΑ ΒΙΟΜΗΧΑΝΙΚΗΣ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ

ΔΙΕΠΙΣΤΗΜΟΝΙΚΟ – ΔΙΑΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ «ΤΕΧΝΟ-ΟΙΚΟΝΟΜΙΚΑ ΣΥΣΤΗΜΑΤΑ»

Ολοκληρωμένη Μεθοδολογία Διαχείρισης Κινδύνου Έργων και Υπηρεσιών Πληροφορικής

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Ηλιάνα Π. Αυγερίκου-Σαμωνά

Επιβλέπων : Γεώργιος Ματσόπουλος
Επίκουρος Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 3η Ιουνίου 2014.

.....	.....	.....
Γ. Ματσόπουλος	Σ. Παπαβασιλείου	Α. Παναγόπουλος
Επίκουρος Καθηγητής Ε.Μ.Π.	Αναπληρωτής Καθηγητής Ε.Μ.Π.	Επίκουρος Καθηγητής Ε.Μ.Π.

Αθήνα, Ιούνιος 2014

.....

Ηλιάνα Π. Αυγερίκου-Σαμωνά

Απόφοιτη Τμήματος Πληροφορικής του Πανεπιστημίου Πειραιά.

Περίληψη

Το ερευνητικό πεδίο της παρούσας διπλωματικής εργασίας αφορά στη διαχείριση κινδύνου έργων και υπηρεσιών πληροφορικής. Συγκεκριμένα, αναπτύσσεται ένα ολοκληρωμένο και συνεκτικό μοντέλο διαχείρισης κινδύνου, το οποίο ενσωματώνει σε μια ενιαία μεθοδολογία τις πρακτικές διαχείρισης κινδύνου στη μηχανογράφηση ενός οργανισμού, με τις υπάρχουσες επιχειρησιακές πρακτικές.

Το προτεινόμενο μοντέλο βασίζεται στη μέθοδο RiskIT, η οποία παρέχει ένα πλήρες εννοιολογικό πλαίσιο για τη διαχείριση των κινδύνων χρησιμοποιώντας μια προσέγγιση στόχου/προσδοκίας από τους ενδιαφερόμενους και τους κινδύνους που απειλούν τους στόχους. Παρά το γεγονός αυτό, η RiskIT έχει ορισμένα κενά, τα οποία μπορεί να περιορίσουν την αποτελεσματική εφαρμογή της σε μεγάλους οργανισμούς. Για την επίλυση αυτών των προβλημάτων, προτείνουμε την ενσωμάτωση τριών επιπλέον μεθοδολογιών που θα έχουν βοηθητικό χαρακτήρα. Οι δευτερεύουσες αυτές μεθοδολογίες είναι το πρότυπο ISO 31000, η βιβλιοθήκη υποδομής ITIL και το πλαίσιο M_o_R. Η συνεργασία τους ορίζει τις γενικές αρχές και κατευθυντήριες γραμμές για την αποτελεσματική διαχείριση του κινδύνου, παράγει τα απαιτούμενα KRI, και στη συνέχεια τα παρέχει σαν ερεθίσματα στη RiskIT για την επιλογή των κατάλληλων στρατηγικών αντιδράσεων και τον έλεγχο της διαδικασίας.

Η αποτελεσματικότητα και αξιοπιστία της προτεινόμενης μεθοδολογίας διαχείρισης κινδύνου παρουσιάζεται μέσα από τη εφαρμογή της στη μηχανογράφηση ενός μεγάλου Τραπεζικού Ιδρύματος.

Λέξεις Κλειδιά: κίνδυνος, διαχείριση κινδύνου, έργα λογισμικού, μηχανογράφηση, RiskIT, ISO 31000, ITIL, M_o_R, KRI.

Abstract

The research scope of this thesis refers to the risk management of software projects and IT services. Specifically, a comprehensive and coherent risk management model is developed, which incorporates in a single methodology, risk management practices of an organization's IT Division in combination with existing business practices.

The proposed model is based on the RiskIT method, which provides a comprehensive conceptual framework for risk management using a goal/expectation approach of stakeholders and the threats of these goals. However, RiskIT has some gaps that may limit its effective implementation in large organizations. To solve this problem, we propose the inclusion of three additional auxiliary methodologies. These secondary methodologies are the standard ISO 31000, the Infrastructure Library ITIL and M_o_R framework. Their collaboration provides the general principles and guidelines for effective risk management, produces the required KRI's, and then provides them as stimuli in RiskIT for the selection of appropriate response strategies and process control.

The effectiveness and reliability of the proposed risk management methodology is illustrated through the case study of its implementation in the IT Division of a large Bank Institute.

Keywords: risk, risk management, software projects, IT Division, RiskIT, ISO 31000, ITIL, M_o_R, KRI.

Ευχαριστίες

Αρχικά θα ήθελα να ευχαριστήσω τον Καθηγητή μου κ. Γεώργιο Ματσόπουλο, για την εμπιστοσύνη που μου έδειξε δίνοντας μου τη δυνατότητα να εκπονήσω τη διπλωματική μου εργασία στον επιστημονικό τομέα που επιθυμούσα, αλλά και για τη βοήθεια και την καθοδήγηση που μου παρείχε.

Επίσης, θα ήθελα να ευχαριστήσω θερμά την οικογένειά μου για την ηθική συμπαράσταση όχι μόνο κατά τη διάρκεια της εκπόνησης της διπλωματικής μου εργασίας, αλλά και καθ' όλη τη διάρκεια των σπουδών μου.

Περιεχόμενα

Περίληψη 5

Abstract 6

Ευχαριστίες 7

Ακρωνύμια 10

Λίστα Εικόνων 11

Λίστα Πινάκων 11

1. Εισαγωγή 13

1.1 Σκοπός Διπλωματικής Εργασίας 14

1.2 Διάρθρωση Διπλωματικής Εργασίας 14

2. Διαχείριση Κινδύνου 16

2.1 Γενικά 16

2.2 Ο Κίνδυνος στα Τραπεζικά Ιδρύματα 20

2.2.1 Η Μηχανογράφηση των Τραπεζικών Ιδρυμάτων 20

2.2.2 Πλαίσιο Διαχείρισης Λειτουργικού Κινδύνου 22

2.2.3 Περιγραφή Προβλημάτων στη Μηχανογράφηση 23

2.3 Συμπεράσματα 25

3. Προτεινόμενο Μοντέλο 26

3.1 Βασικές αρχές 26

3.1.1 Πολιτική Διαχείρισης Κινδύνου 27

3.1.2 Επανεξέταση στόχου 28

3.1.3 Αναγνώριση Κινδύνου 29

3.1.4 Ανάλυση Κινδύνου 30

3.1.5 Προγραμματισμός Διαχείρισης Κινδύνου 31

3.1.6 Έλεγχος Κινδύνου 32

3.1.7 Παρακολούθηση Κινδύνων 33

3.2 Μεθοδολογίες 34

3.2.1 ISO 31000 34

3.2.2 ITIL 36

3.2.3 M_o_R 38

3.3 Εννοιολογικός χάρτης μοντέλου 39
3.4 Συμπεράσματα 42
4. Case Study 43
4.1 Περιγραφή 43
4.2 Αναγνώριση Κινδύνων 44
4.3 Ανάλυση Κινδύνων 46
4.3 Προγραμματισμός Διαχείρισης Κινδύνων 50
4.4 Έλεγχος Κινδύνων 51
4.5 Παρακολούθηση Κινδύνων 61
4.6 Φύλλα Κινδύνου 61
4.7 Αποτελέσματα 64
5. Συμπεράσματα και μελλοντικές επεκτάσεις 65
5.1 Συμπεράσματα 65
5.2 Μελλοντικές Επεκτάσεις 66
5.2.1 QIP 66
5.2.2 COBIT και Val IT 68
5.2.3 Κατασκευή λογισμικού Διαχείρισης Κινδύνου 70
Αναφορές 72
Βιβλιογραφία 73

Ακρωνύμια

IRGC	International Risk Governance Council
CSF	Critical Success Factor
KPI	Key Performance Indicators
KRI	Key Risk Indicators
IT	Information Technology
RCSA	Risk & Control Self Assessment
ISO	International Organization for Standardization
ITIL	IT Infrastructure Library
M_o_R	Management of Risk
OGC	Office of Government Commerce (United Kingdom)
QIP	Quality Improvement Paradigm
PMI	Project Management Institute
IRM	Institute of Risk Management
ISACA	Information Systems Audit and Control Association

Λίστα Εικόνων

Εικόνα 1: Η μέθοδος RiskIT 27
Εικόνα 2: Οι δραστηριότητες της Ανάλυσης Κινδύνου 31
Εικόνα 3: Το πλαίσιο διαχείρισης κινδύνων κατά το ISO 31000 35
Εικόνα 4: Ο κύκλος ζωής της βιβλιοθήκης ITIL 37
Εικόνα 5: Το πλαίσιο M_o_R 38
Εικόνα 6: Ο Εννοιολογικός χάρτης του Προτεινόμενου Μοντέλου 41
Εικόνα 7: Ιεραρχία του κινδύνου 51
Εικόνα 8: Ο κύκλος και οι λειτουργίες της QIP 67
Εικόνα 9: Οι δραστηριότητες της QIP και της RiskIT 68
Εικόνα 10: Αλληλεπίδραση της RiskIT με τα πλαίσια COBIT και Val IT. 69
Εικόνα 11: Η απεικόνιση των διαδικασιών της ITIL σε υψηλό επίπεδο 70

Λίστα Πινάκων

Πίνακας 1: Μεθοδολογίες Διαχείρισης Κινδύνου 18
Πίνακας 2: Διαφορές ανάμεσα σε KPI και KRI 19
Πίνακας 3: Η διαδικασία της Πολιτικής Διαχείρισης Κινδύνου 28
Πίνακας 4: Η διαδικασία της Επανεξέτασης στόχου 29
Πίνακας 5: Η διαδικασία της Αναγνώρισης Κινδύνου 30
Πίνακας 6: Η διαδικασία της Ανάλυσης Κινδύνου 30
Πίνακας 7: Η διαδικασία του Προγραμματισμού Ελέγχου Κινδύνου 32
Πίνακας 8: Η διαδικασία του Ελέγχου Κινδύνου 32
Πίνακας 9: Η διαδικασία της Παρακολούθησης Κινδύνων 33
Πίνακας 10: Ταξινόμηση των Κινδύνων 46
Πίνακας 11: Κατάταξη των Κινδύνων 47
Πίνακας 12: Πιθανότητα Εμφάνισης των Κινδύνων 48
Πίνακας 13: Πιθανότητα Συνεπειών-Επιπτώσεων 48
Πίνακας 14: Έκθεση των Κινδύνων 49

Πίνακας 15: Σχέδια Αντιμετώπισης Κινδύνων.....50
Πίνακας 16: KRI, Στρατηγική Απάντηση για τον κίνδυνο 1 52
Πίνακας 17: KRI, Στρατηγική Απάντηση για τον κίνδυνο 2 53
Πίνακας 18: KRI, Στρατηγική Απάντηση για τον κίνδυνο 3 54
Πίνακας 19: KRI, Στρατηγική Απάντηση για τον κίνδυνο 4 55
Πίνακας 20: KRI, Στρατηγική Απάντηση για τον κίνδυνο 5 55
Πίνακας 21: KRI, Στρατηγική Απάντηση για τον κίνδυνο 6 56
Πίνακας 22: KRI, Στρατηγική Απάντηση για τον κίνδυνο 7 57
Πίνακας 23: KRI, Στρατηγική Απάντηση για τον κίνδυνο 8 58
Πίνακας 24: KRI, Στρατηγική Απάντηση για τον κίνδυνο 9 60
Πίνακας 25: KRI, Στρατηγική Απάντηση για τον κίνδυνο 10 60
Πίνακας 26: Φύλλο Κινδύνου #1 62
Πίνακας 27: Φύλλο Κινδύνου #2 63

1. Εισαγωγή

Η Διαχείριση Κινδύνου έγινε αναγκαία στα τέλη της δεκαετίας του ’90 λόγω των μεγάλων και πολύπλοκων έργων που αναπτύχθηκαν διεθνώς. Παρά τη ραγδαία εξέλιξή της τα τελευταία χρόνια, η Διαχείριση Κινδύνου αποτελούσε μέχρι πολύ πρόσφατα μια επιπλέον διαδικασία στην περιοχή της Διαχείρισης Έργων και Προγραμμάτων. Τελευταία, έχει ξεκινήσει η αναθεώρηση αυτής της πρακτικής και η πλήρης ενσωμάτωσή της, όχι μόνο στις διαδικασίες του οργανισμού αλλά και σε όλη τη διάρκεια ανάπτυξης και εκτέλεσης ενός έργου.

Ο κύκλος ζωής ενός έργου αποτελείται από τέσσερις φάσεις. Στη φάση της αρχικοποίησης γίνεται η σύλληψη της ιδέας και ορίζεται ο σκοπός και οι επιχειρηματικοί κίνδυνοι του έργου. Η αναγνώριση των κινδύνων αποτελεί το πρώτο και ένα από τα πιο κρίσιμα στάδια της Διαχείρισης Κινδύνων, καθώς, αφορά στον εντοπισμό και καταγραφή όλων των κινδύνων που είναι πιθανό να επηρεάσουν τους στόχους ενός έργου. Στη φάση του σχεδιασμού, αφού έχει σχεδόν αποφασιστεί ότι το έργο θα υλοποιηθεί, καθορίζονται οι κύριοι στόχοι και γίνεται ανάλυση των κινδύνων που ορίστηκαν στην προηγούμενη φάση, για να καθορισθεί το μέγεθος της συνέπειάς τους στο έργο. Επιπλέον, προσδιορίζονται οι μέθοδοι αντιμετώπισης αυτών των κινδύνων. Στην τρίτη φάση, αυτή της εκτέλεσης και του ελέγχου, αρχίζει να εκτελείται το έργο ανάλογα με το χρονοδιάγραμμα που έχει οριστεί από τον οργανισμό/επιχείρηση. Οι κίνδυνοι που έχουν καταγραφεί και αναλυθεί στις προηγούμενες φάσεις ποσοτικοποιούνται και παρακολουθούνται. Παράλληλα, συνεχίζεται η αναζήτηση νέων κινδύνων που μπορεί να προκύψουν κατά τη διάρκεια της εκτέλεσης του έργου. Στην τελευταία φάση του κύκλου ζωής του έργου, γίνεται η παράδοση των τελικών προϊόντων ή υπηρεσιών στον πελάτη και ελέγχεται κατά πόσο η ομάδα ανάπτυξης και υποστήριξης ανταποκρίθηκε στις απαιτήσεις και πέτυχε τους αρχικούς στόχους.

Με βάση την παραπάνω ανάλυση, γίνεται αντιληπτό ότι για να είναι αποτελεσματική η Διαχείριση Κινδύνου, πρέπει να ενσωματώνεται στον κύκλο ζωής του έργου και να εναρμονίζεται με την επίτευξη των στόχων του οργανισμού και τις διαδικασίες του προσωπικού σε όλα τα επίπεδα.

1.1 Σκοπός Διπλωματικής Εργασίας

Σκοπός της παρούσας διπλωματικής εργασίας είναι η παρουσίαση μιας ολοκληρωμένης μεθοδολογίας ανάλυσης και διαχείρισης κινδύνου, εστιασμένη σε έργα υπηρεσιών πληροφορικής.

Οι γνωστές μεθοδολογίες διαχείρισης κινδύνων καταγράφουν απλώς τους κινδύνους που εμφανίζονται στα έργα πληροφορικής, χωρίς να εξετάζουν σε βάθος τις αιτίες που συμβάλλουν στην εμφάνιση αυτών, και δεν προτείνουν στοχευμένες δράσεις για την αντιμετώπιση τους. Η απουσία μιας συγκροτημένης, επίσημης και ολοκληρωμένης μεθοδολογίας διαχείρισης κινδύνου αποδεικνύεται καθημερινά στην πράξη, με τις συνεχείς αστοχίες, αποτυχίες και τα προβλήματα των προγραμμάτων μεγάλης κλίμακας τόσο σε διεθνές, όσο και σε τοπικό επίπεδο.

Αυτή η έρευνα προσπαθεί να εντοπίσει και να κατανοήσει τους παράγοντες που συμβάλλουν στον κίνδυνο των έργων λογισμικού και να προσδιορίσει τη διαδικασία ελέγχου των κινδύνων αυτών. Επιπλέον, με βάση την ανάλυση που πραγματοποιείται, καθίσταται σαφής η αναγκαιότητα δημιουργίας μιας ολοκληρωμένης μεθοδολογίας διαχείρισης κινδύνων έργων και προγραμμάτων, η οποία θα απαντά με ενιαίο τρόπο στο πρόβλημα της διαχείρισης των κινδύνων συνολικά ενός προγράμματος, αλλά και στο πρόβλημα της διαχείρισης κινδύνων των επιμέρους έργων.

1.2 Διάρθρωση Διπλωματικής Εργασίας

Η συγκεκριμένη έρευνα αποτελείται από **5** κεφάλαια, τα οποία περιγράφονται στη συνέχεια.

Κεφάλαιο 1: Εισαγωγή

Αποτελεί το παρόν κεφάλαιο, στο οποίο παρουσιάζεται το πρόβλημα και στηρίζεται η ανάγκη ανάπτυξης μιας ολοκληρωμένης μεθοδολογίας διαχείρισης κινδύνων έργων και προγραμμάτων. Επίσης, αναλύεται πλήρως το αντικείμενο και ο στόχος της έρευνας.

Κεφάλαιο 2: Διαχείριση Κινδύνου

Στο κεφάλαιο αυτό επιχειρείται η αποσαφήνιση κάποιων κρίσιμων εννοιών και διεξάγεται μια σύντομη ιστορική αναδρομή στις μεθοδολογίες διαχείρισης κινδύνου

που έχουν αναπτυχθεί κατά καιρούς. Επιπλέον, παρουσιάζονται οι κίνδυνοι στη μηχανογράφηση των τραπεζικών ιδρυμάτων και το πλαίσιο διαχείρισης του λειτουργικού κινδύνου.

Κεφάλαιο 3: Προτεινόμενο Μοντέλο

Στο κεφάλαιο αυτό περιγράφεται αναλυτικά το προτεινόμενο μοντέλο ανάλυσης και διαχείρισης κινδύνου, συμπεριλαμβανομένων των βασικών αρχών και μεθοδολογιών που χρησιμοποιεί.

Κεφάλαιο 4: Case Study

Στο κεφάλαιο αυτό παρουσιάζεται η πιλοτική εφαρμογή της προτεινόμενης μεθοδολογίας για την αναγνώριση και διαχείριση κινδύνων με πραγματικά δεδομένα, στη μηχανογράφηση ενός μεγάλου τραπεζικού ιδρύματος.

Κεφάλαιο 5: Συμπεράσματα και Μελλοντικές Επεκτάσεις

Στο τελευταίο κεφάλαιο αναφέρονται τα συμπεράσματα που απορρέουν από την παρούσα εργασία, καθώς και οι μελλοντικές επεκτάσεις της έρευνας που πραγματοποιήθηκε.

2. Διαχείριση Κινδύνου

Σε αυτή την ενότητα αναλύονται οι έννοιες του κινδύνου και της διαχείρισης κινδύνου και περιγράφονται συνοπτικά κάποιες γνωστές μεθοδολογίες αντιμετώπισης του. Επιπλέον, παρουσιάζονται οι κίνδυνοι στη μηχανογράφηση των Τραπεζικών Ιδρυμάτων και το πλαίσιο διαχείρισης του λειτουργικού κινδύνου μιας τράπεζας.

2.1 Γενικά

Ο κίνδυνος είναι παρών σε κάθε πτυχή της ζωής. Ο όρος **κίνδυνος (risk)** αποκτά διαφορετικό νόημα και διάσταση σε διαφορετικούς ανθρώπους, καθώς η έννοια του ποικίλλει ανάλογα με την οπτική, τις εμπειρίες και τη νοοτροπία. Ο ακριβής ορισμός του κινδύνου στα πλαίσια έργων, έχει απασχολήσει αρκετά τη διεθνή βιβλιογραφία. Συνήθως, ορίζεται ως «ένα αβέβαιο γεγονός ή κατάσταση, που σε περίπτωση που προκύψει, έχει θετική ή αρνητική συνέπεια σε κάποιο στόχο του έργου» [1].

Εκτός όμως από τις διαφορετικές ερμηνείες όσον αφορά τον κίνδυνο, άλλη μία σημαντική διάσταση απόψεων παρατηρείται και ως προς το είδος των κινδύνων που θεωρούν ότι αντιμετωπίζουν τα στελέχη του κάθε επιπέδου. Συγκεκριμένα, τα στελέχη των αρχών διαχείρισης δίνουν μεγαλύτερη έμφαση στους κινδύνους διαχείρισης. Αντίθετα, τα στελέχη των αναδόχων βάζουν υψηλότερα στις προτεραιότητές τους τεχνικούς και οικονομικούς κινδύνους, ενώ τέλος τα στελέχη των φορέων υλοποίησης θεωρούν πιο σημαντικούς τους τεχνικούς κινδύνους καθώς και τους κινδύνους σχεδιασμού. Γενικά, οι κίνδυνοι χωρίζονται βάσει δύο παραμέτρων, της φύσης και της προέλευσής τους.

Α. Φύση κινδύνων

Με βάση τη φύση τους διακρίνονται σε ευκαιρίες και απειλές και σε περίπτωση εμφάνισης τους επιφέρουν θετικές ή αρνητικές συνέπειες αντίστοιχα για το έργο.

Β. Προέλευση κινδύνων

Όσον αφορά την προέλευση οι κίνδυνοι μπορεί να είναι εσωτερικοί ή εξωτερικοί.

- Εσωτερικοί είναι οι κίνδυνοι που η πιθανότητα εμφάνισής τους επηρεάζεται από τις ενέργειες του οργανισμού και διακρίνονται σε τεχνολογικούς, οργανωτικούς και απρόβλεπτους.

- Ενώ εξωτερικοί είναι οι κίνδυνοι που η ομάδα του έργου δεν μπορεί να προβεί σε καμία ενέργεια για να επηρεάσει την πιθανότητα εμφάνισης τους ή τις συνέπειες τους και διακρίνονται σε προβλέψιμους και απρόβλεπτους.

Ως **Διαχείριση Κινδύνων (Risk Management)** ενός έργου, ορίζεται «το σύνολο των διαδικασιών αναγνώρισης, ανάλυσης, ανταπόκρισης και παρακολούθησης κινδύνων κατά τη διάρκεια της ζωής ενός έργου με στόχο την επίτευξη των αρχικών του στόχων» [1]. Η Διαχείριση Κινδύνων θεωρείται βασική παράμετρος για την επιτυχή ολοκλήρωση μεγάλων και πολύπλοκων έργων, καθώς επηρεάζει θέματα όπως το χρονοδιάγραμμα, τον προϋπολογισμό και την ικανοποίηση των πελατών.

Κατά καιρούς έχουν προταθεί πολλές μεθοδολογίες Διαχείρισης Κινδύνου. Μερικές από αυτές παρουσιάζονται συνοπτικά στον παρακάτω πίνακα.

Μεθοδολογία	Βήματα Διαχείρισης Κινδύνου
Project Management Institute (PMI 2004) "A Guide to the project Management Body of Knowledge"	• Σχεδιασμός • Αναγνώριση κινδύνων • Ποιοτική ανάλυση κινδύνων • Ποσοτική ανάλυση κινδύνων • Σχεδιασμός ενεργειών μείωσης του κινδύνου • Έλεγχος και παρακολούθηση
Klein και Cork (1998) "An approach to technical risk assessment"	• Αναγνώριση • Ανάλυση • Έλεγχος • Τεκμηρίωση - Αναφορά
Chapman και Ward (1999) "Project Risk Management Processes, Techniques and Insights"	• Καθορισμός • Στρατηγική προσέγγιση • Αναγνώριση κινδύνων • Δόμηση πληροφορίας • Αρμοδιότητες - πεδία ευθύνης • Υπολογισμός αβεβαιότητας • Σημαντικότητα κινδύνων • Παρακολούθηση • Έλεγχος
Carter et al (2001) "Introducing Riskman Methodology"	• Βασικό (ανάλυση με ποιοτικούς όρους) • Ενδιάμεσο (πρόχειρη ποσοτικοποίηση) • Λεπτομέρειες (πλήρης ποσοτικοποίηση)
Fairley (1994)	• Αναγνώριση • Ανάλυση

"Risk management Software projects"	• Περιορισμός κινδύνων • Παρακολούθηση • Σχεδιασμός εναλλακτικών σχεδίων ανάγκης • Διαχείριση κρίσης • Έξοδος από την κρίση
Boehm (1991) "Software Risk Management"	• Ανάλυση κινδύνου (αναγνώριση, ανάλυση, ιεράρχηση) • Διαχείριση κινδύνου (σχεδιασμός ενεργειών διαχείρισης κινδύνου, αποφάσεις διαχείρισης, παρακολούθηση και διορθωτικές ενέργειες)
Software Engineering Institute (1992) "The SEI Approach for Technical Risks"	• Αναγνώριση • Ανάλυση • Διαχείριση • Έλεγχος • Παρακολούθηση
IRGC (2005) "White paper on Risk Governance"	• Προ-αξιολόγηση • Αποτίμηση • Εκτίμηση ανεκτικότητας απέναντι στον κίνδυνο • Διαχείριση κινδύνου • Επικοινωνία
Institute of Civil Engineers and the Faculty and Institute of Actuaries (1998) "Risk Analysis and Management for Projects (RAMP)"	• Εκκίνηση • Ανασκόπηση • Διαχείριση κινδύνων • Κλείσιμο

Πίνακας 1: Μεθοδολογίες Διαχείρισης Κινδύνου

Παρατηρείται πως παρά τη διαφοροποίηση των σταδίων και τη διαφορετική ονομασία υπάρχουν πολλά κοινά σημεία, όσον αφορά στα βήματα που περιλαμβάνονται. Η γενική μεθοδολογία Διαχείρισης Κινδύνων έργων, που χρησιμοποιείται από όλες τις ολοκληρωμένες μεθόδους που εφαρμόζονται διεθνώς, αποτελείται από τέσσερα βασικά στάδια: τον εντοπισμό, την ανάλυση, την αντιμετώπιση και τέλος την παρακολούθηση των κινδύνων του έργου.

Παρακάτω παρατίθενται κάποιες βασικές έννοιες στα πλαίσια αναφοράς της διαχείρισης κινδύνου [2, 3]:

- **Κρίσιμοι Παράγοντες Επιτυχίας (Critical Success Factors - CSF)** είναι τα στοιχεία και οι βασικοί τομείς δραστηριότητας που απαιτούνται για τη διασφάλιση της επιτυχίας μιας επιχείρησης ή ενός οργανισμού.

- **Βασικοί Δείκτες απόδοσης (Key Performance Indicators - KPI)** Αποτυπώνουν τους κρίσιμους παράγοντες επιτυχίας σε έναν οργανισμό και διαμορφώνονται ανάλογα με τις επιχειρηματικές δραστηριότητες του οργανισμού αλλά και τις ανάγκες των ενδιαφερόμενων μελών.

- **Βασικοί Δείκτες Αποτελεσμάτων (Key Risk Indicators - KRI)** Παρέχουν πληροφόρηση τόσο στους ενδιαφερόμενους του εξωτερικού περιβάλλοντος, για τη σταθερότητα και την κερδοφορία της επιχείρησης, όσο και στη διοίκηση δημιουργώντας μια βάση πάνω στην οποία θα στηρίξουν τις αποφάσεις τους.

Στον επόμενο πίνακα φαίνονται οι κύριες διαφορές τον Βασικών Δεικτών:

KPIs	KRIs
Αποκλειστικά μη οικονομικοί δείκτες	Οικονομικοί και μη οικονομικοί δείκτες (π.χ. ποσοστό ικανοποίησης πελατών, απόδοση κεφαλαίου).
Συχνή μέτρηση (π.χ. 24/7, ημερήσια, εβδομαδιαία).	Μέτρηση μηνιαία ή τριμηνιαία.
Ιδανικοί για την υποβολή εκθέσεων στο διευθύνοντα σύμβουλο (CEO) και στην ομάδα του management.	Ιδανικοί για την παρουσίαση της εξελικτικής πορείας στο συμβούλιο.
Το προσωπικό κατανοεί τόσο τους δείκτες όσο και τις διορθωτικές κινήσεις που πρέπει να γίνουν.	Δεν παρέχουν πληροφορίες για τις περιοχές που χρειάζονται βελτίωση με αποτέλεσμα να μην μπορούν να αξιοποιηθούν από το προσωπικό.
Η ευθύνη αποδίδεται ατομικά αλλά και σε ολόκληρη την ομάδα	Υπεύθυνος για αυτά είναι αποκλειστικά ο διευθύνων σύμβουλος (CEO).
Έχουν θετική επιρροή απέναντι σε όλα τα άλλα μέτρα απόδοσης	Είναι αποτέλεσμα πολλών δραστηριοτήτων η διαχείριση των οποίων γίνεται μέσα από μια ποικιλία μέτρων απόδοσης
Συνήθως παρουσιάζονται με τη χρήση ενδοδικτύου, οπότε η ενημέρωση μπορεί να γίνει ακόμη και με ένα τηλεφώνημα.	Συνήθως παρουσιάζονται με ένα γράφημα τάσης, που καλύπτει τη δραστηριότητα τουλάχιστον των τελευταίων 15 μηνών.

Πίνακας 2: Διαφορές ανάμεσα σε KPI και KRI

2.2 Ο Κίνδυνος στα Τραπεζικά Ιδρύματα

Τα Τραπεζικά Ιδρύματα καλούνται να αντιμετωπίσουν τον κίνδυνο αγοράς, τον πιστωτικό κίνδυνο, τον κίνδυνο κεφαλαιακής ανάλυσης, τον λειτουργικό κίνδυνο και τον κίνδυνο ρευστότητας. Ο κυριότερος από αυτούς θεωρείται ο Λειτουργικός Κίνδυνος (Operational Risk), αφού έχει διαπιστωθεί ότι οι περισσότερες από τις περιπτώσεις εμφάνισης μεγάλων ζημιών, οφείλονται σε κάποια πηγή λειτουργικού κινδύνου η οποία δεν έχει αντιμετωπιστεί σωστά.

Ο λειτουργικός κίνδυνος σχετίζεται με τις καθημερινές τραπεζικές εργασίες και εμπεριέχει ελλιπείς ή ανεπιτυχείς διαδικασίες εσωτερικού ελέγχου, δυσλειτουργίες των κανόνων της παρακολούθησης κινδύνων, ανεπαρκή διαχωρισμό καθηκόντων και ανεπαρκή πληροφοριακά συστήματα [4]. Συνοψίζοντας, ο κίνδυνος αυτός αναφέρεται σε ανθρώπους, διαδικασίες, τεχνική υποστήριξη και συστήματα.

Εμείς θα ασχοληθούμε περισσότερο με τον τεχνολογικό κίνδυνο, ο οποίος αποτελεί ένα σημαντικό είδος λειτουργικού κινδύνου. Ο τεχνολογικός κίνδυνος αναφέρεται στην πιθανότητα βλάβης ή ανεπάρκειας των πληροφοριακών συστημάτων και είναι ενσωματωμένος σε κάθε δραστηριότητα της μηχανογράφησης μιας τράπεζας.

2.2.1 Η Μηχανογράφηση των Τραπεζικών Ιδρυμάτων

Στα τραπεζικά ιδρύματα είναι απαραίτητη η χρήση μιας καλά οργανωμένης μηχανογράφησης (IT Division) με αξιόπιστα μηχανογραφικά προγράμματα και σύγχρονους ηλεκτρονικούς υπολογιστές. Τα συστήματα αυτά είναι προηγμένης τεχνολογίας, διαθέτουν πολλές βάσεις δεδομένων για την επεξεργασία μεγάλου όγκου στοιχείων, είναι υψηλού κινδύνου δεδομένου ότι επικοινωνούν με το κεντρικό σύστημα με πολλά interfaces, καθώς και υψηλού κόστους επειδή είναι περίπλοκα.

Ένα σωστά μηχανογραφημένο περιβάλλον πρέπει να περιέχει τα παρακάτω στοιχεία:

- **Υλικό (Hardware):** Το Hardware αποτελείται από ένα σύνολο μηχανημάτων και συσκευών (κεντρικές μονάδες ηλεκτρονικών υπολογιστών, servers, routers κ.λπ.).

- **Λογισμικό (Software)**: Περιλαμβάνει τα προγράμματα των πληροφοριακών συστημάτων που χρησιμοποιούνται για την εκτέλεση γενικών λειτουργιών, καθώς και τα προγράμματα εφαρμογών για την επεξεργασία στοιχείων.

- **Τεκμηρίωση (Documentation):** Περιλαμβάνει την επαρκή περιγραφή του συστήματος, των προγραμμάτων, των εσωτερικών διαδικασιών και των ελέγχων.

- **Στοιχεία (Data):** Αφορά τα δεδομένα και τις σχετικές πληροφορίες που έχουν εισαχθεί, επεξεργαστεί και παραχθεί από το σύστημα.

- **Προσωπικό:** Τα άτομα που σχεδιάζουν, διαχειρίζονται και ελέγχουν το σύστημα.

- **Δραστηριότητες ελέγχου (Control Activities):** Είναι οι πολιτικές και οι διαδικασίες που διασφαλίζουν ότι πραγματοποιούνται ενέργειες για την αντιμετώπιση των κινδύνων στο σύνολο των λειτουργιών του οργανισμού.

- **Παρακολούθηση (Monitoring):** Η παρακολούθηση των συστημάτων είναι η πιο σημαντική λειτουργία ενός συστήματος διαχείρισης. Περιλαμβάνει τη συλλογή και ανάλυση της δικτυακά μεταδιδόμενης κίνησης, την ανάλυση των επιδόσεων συγκεκριμένων εφαρμογών, την αξιολόγηση της απόδοσης των συστημάτων ελέγχου και την ανίχνευση απειλών ασφαλείας.

Θέματα όπως η απώλεια και η αλλοίωση στοιχείων, η προβληματική λειτουργία ή η διακοπή της λειτουργίας του εξοπλισμού και η ακαταλληλότητα του λογισμικού, μπορεί να επιφέρουν οικονομικές απώλειες, δυσφήμηση ή να προκαλέσουν ακόμα και διακοπή της λειτουργίας του Τραπεζικού Ιδρύματος.
Για την αποτροπή τέτοιον σφαλμάτων η κάθε τράπεζα οφείλει να σχεδιάζει ένα πλήρες και αποτελεσματικό σύστημα Εσωτερικού Ελέγχου, που θα εξασφαλίζει την ασφαλή οργάνωση και λειτουργία των μηχανογραφημένων συστημάτων.

2.2.2 Πλαίσιο Διαχείρισης Λειτουργικού Κινδύνου

Οι αρχές διαχείρισης κινδύνων ενός Τραπεζικού Ομίλου διαμορφώνονται από την Επιτροπή Διαχείρισης Κινδύνων του Διοικητικού Συμβουλίου. Συγκεκριμένα, συστήνεται μια Μονάδα Λειτουργικού Κινδύνου σε κάθε παράρτημα της μηχανογράφησης η οποία είναι αρμόδια για την εφαρμογή της επιχειρησιακής στρατηγικής και του πλαισίου διαχείρισης λειτουργικών κινδύνων.

Αξιοποιώντας τις διατάξεις της οδηγίας 2006/48/ΕΚ, ο Όμιλος χρησιμοποιεί την τυποποιημένη προσέγγιση για να αντιμετωπίσει τον λειτουργικό κίνδυνο και εφαρμόζει κάποιες διαδικασίες οι οποίες εστιάζονται στον εντοπισμό του κινδύνου, τον έλεγχο, τη διαχείριση, την αξιολόγηση, τους μηχανισμούς μεταφοράς κινδύνου και την υποβολή εκθέσεων. Αυτές οι διαδικασίες υποστηρίζονται και εφαρμόζονται από τις παρακάτω μεθόδους [4]:

- **Αυτοαξιολόγηση Λειτουργικών Κινδύνων & Ελέγχων (Risk & Control Self Assessment - RCSA) -** είναι μια τεχνική με κύριο στόχο τον εντοπισμό, την αξιολόγηση και τελικά, τον περιορισμό του λειτουργικού κινδύνου. Η RCSA διεξάγεται κάθε χρόνο, εάν όμως εντοπιστούν σημαντικές αλλαγές, μπορεί να γίνει και πιο συχνά.
- **Δείκτες Λειτουργικού Κινδύνου (Key Risk Indicators - KRIs) -** Βασίζονται σε ιστορικά δεδομένα που σχετίζονται με συγκεκριμένες και μετρήσιμες δραστηριότητες και αναφέρουν την έκθεση σε λειτουργικό κίνδυνο. Οι δείκτες λειτουργικού κινδύνου είναι ποσοτικοί και εκφράζονται ως ποσοστό ή αναλογία.
- **Γεγονότα λειτουργικού κινδύνου**, εντοπίζονται και καταγράφονται με σκοπό την ενημέρωση μιας εσωτερικής βάσης δεδομένων και τη δημιουργία αναφορών. Ταξινομούνται ανάλογα με την αρμόδια μονάδα, την αιτία, την κατηγορία κινδύνου, τις επιπτώσεις, τις σχετικές επιχειρηματικές δραστηριότητες, κ.α.
- **Ανάλυση σεναρίων λειτουργικού κινδύνου (Scenario Analysis) -** Είναι η δομή εντός της οποίας καθορίζονται, τεκμηριώνονται και επιλέγονται τα σενάρια για ανάλυση και για μέτρηση.

2.2.3 Περιγραφή Προβλημάτων στη Μηχανογράφηση

Οι δύο τομείς της μηχανογράφησης στους οποίους ελλοχεύουν οι περισσότεροι κίνδυνοι είναι οι υπάρχουσες ή νέες εφαρμογές και η παρακολούθηση συστημάτων και εφαρμογών. Παρακάτω αναφέρουμε τα προβλήματα που παρατηρήθηκαν στη μηχανογράφηση ενός μεγάλου Τραπεζικού Ιδρύματος (για ευνόητους λόγους δεν θα αναφέρουμε το όνομα) μετά από συζήτηση με τους διαχειριστές και τους χρήστες του συστήματος.

Εφαρμογές (Applications)

- Λάθη προγραμματισμού. Μπορεί να προκαλέσουν δυσαρέσκεια στον πελάτη και περιλαμβάνουν τον κίνδυνο να μην είναι γνωστές οι απαιτήσεις, να μην είναι γνωστό το πλήρες αντικείμενο του έργου ή να μην υλοποιηθούν οι αρχικές υποθέσεις για το έργο.
- Μη τήρηση του χρονοδιαγράμματος: Έχει τη δυνατότητα να επηρεάσει το έργο πέρα από το ένα τρίτο της αρχικής εκτιμώμενης διάρκειας.
- Στον βωμό της «διάθεσης» της εφαρμογής το συντομότερο δυνατό στην παραγωγή (roll-out) της εκάστοτε υπηρεσίας-επιχείρησης, θυσιάζονται σημαντικοί παράγοντες ασφάλειας κατά την υλοποίηση πληροφοριακών συστημάτων (π.χ. disaster recovery, stress-penetration tests, user acceptance tests κ.λπ.).
- Ελλιπής ή καθόλου τεκμηρίωση (documentation) σχετική με την υποστήριξη των συστημάτων και των εφαρμογών σε περίπτωση προβλήματος. Αυτό έχει σαν αποτέλεσμα να υπάρχουν καθυστερήσεις επαναφοράς της πλήρους λειτουργικότητας από τις ομάδες υποστήριξης.
- Απουσία κοινής και ενιαίας πλατφόρμας και αρχιτεκτονικής κατά την υλοποίηση πληροφοριακών συστημάτων. Η «πολυφωνία» στις τεχνολογίες που εφαρμόζονται σε συνδυασμό με την ελλιπή κατάρτιση του προσωπικού στο μεγάλο πλήθος τεχνολογιών εν τέλει κοστίζει περισσότερο στην διαχείριση και υποστήριξη.

Παρακολούθηση Συστημάτων και Εφαρμογών (Monitoring)

- Έμφαση στο monitoring μεμονωμένων υποσυστημάτων με αποτέλεσμα την αδυναμία παρακολούθησης της εφαρμογής ως σύνολο παρεχόμενων υπηρεσιών.
- Πληθώρα monitoring εργαλείων που παρακολουθούν διαφορετικές πτυχές των ίδιων συστημάτων και μηχανισμών, με αποτέλεσμα την αδυναμία καταμέτρησης (με αξιοπιστία και ασφάλεια) της διαθεσιμότητας των εφαρμογών-υπηρεσιών.
- Λανθασμένη και υπερβολική παραμετροποίηση των μηχανισμών παρακολούθησης με αποτέλεσμα τον καταιγισμό μηνυμάτων alert (που συχνά οδηγεί στο αντίθετο από το προσδοκώμενο αποτέλεσμα).

2.3 Συμπεράσματα

Με βάση τα παραπάνω παρατηρούμε ότι η υπάρχουσα μεθοδολογία της τράπεζας δεν επαρκεί για να καλύψει όλες τις πτυχές του λειτουργικού και τεχνολογικού κινδύνου.

Για να είναι αποτελεσματική η διαχείριση των κινδύνων απαιτείται ένα κοινό πλαίσιο, που θα περιλαμβάνει τη διαχείριση των κινδύνων στις διαδικασίες του οργανισμού και στις δραστηριότητες του προσωπικού σε όλα τα επίπεδα. Αυτό, δεν συμβάλλει μόνο στην καλή διακυβέρνηση του Τραπεζικού Ιδρύματος, αλλά παρέχει και προστασία στους υπεύθυνους σε περίπτωση αρνητικών αποτελεσμάτων.

Η διαχείριση κινδύνων πρέπει να εφαρμόζεται όχι μόνο στην οργανωτική δομή της τράπεζας αλλά και κατά τη διάρκεια του κύκλου ζωής ενός έργου, ώστε να αποφεύγονται όσο το δυνατόν περισσότεροι κίνδυνοι.

Οι παράγοντες που θεωρούνται κρίσιμοι για τον αποτελεσματικό σχεδιασμό των μεθόδων αντιμετώπισης των κινδύνων είναι οι εξής:

- Επικοινωνία
- Σαφής καθορισμός ρόλων και ευθυνών
- Προσδιορισμός του κατάλληλου χρόνου για την αντιμετώπιση του κάθε κινδύνου
- Αναθεώρηση κόστους και χρονοδιαγράμματος έργου
- Καταγραφή αλληλεπιδράσεων κινδύνων - δράσεων αντιμετώπισης
- Εξασφάλιση των κατάλληλων δράσεων αντιμετώπισης των κινδύνων
- Καταγραφή τόσο των απειλών όσο και των ευκαιριών
- Ανάπτυξη στρατηγικής

3. Προτεινόμενο Μοντέλο

Σε αυτό το κεφάλαιο παρουσιάζεται το προτεινόμενο μοντέλο Ανάλυσης και Διαχείρισης Κινδύνου. Αρχικά αναλύονται οι βασικές αρχές και οι μεθοδολογίες που χρησιμοποιεί και στο τέλος περιγράφεται ο εννοιολογικός χάρτης του μοντέλου.

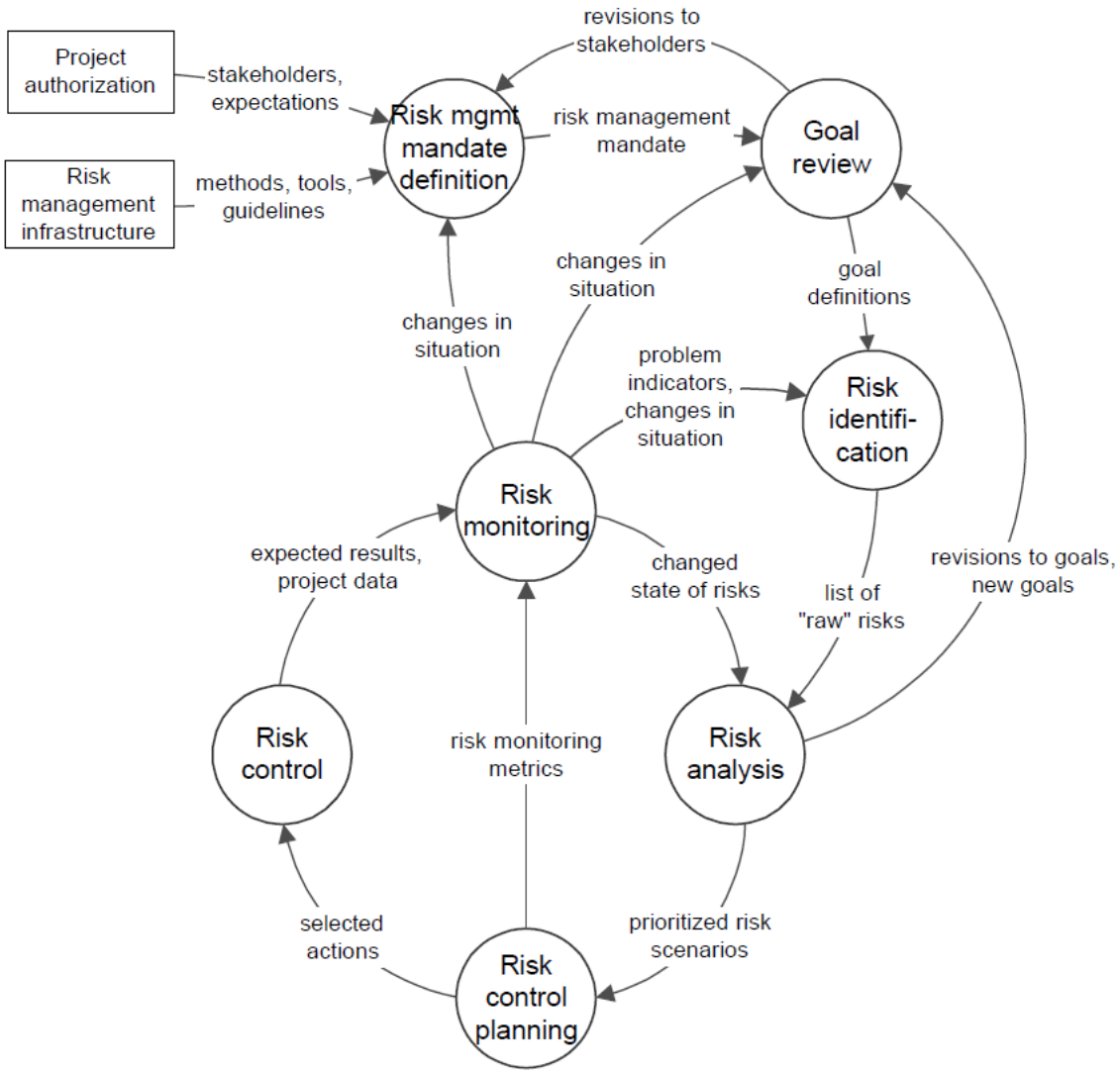
3.1 Βασικές αρχές

Μια αποτελεσματική διαχείριση κινδύνων βασίζεται σε ένα ολοκληρωμένο πλαίσιο, που εσωκλείει τη διαχείριση των κινδύνων σε όλες τις διαδικασίες του οργανισμού. Το πρωτεύον πλαίσιο διαχείρισης κινδύνου που επιλέχθηκε είναι η μέθοδος **RiskIT.** Η RiskIT παρέχει ένα σύνολο κατευθυντήριων αρχών για την αποτελεσματική διαχείριση του μηχανογραφικού κινδύνου [5]. Η μέθοδος RiskIT έχει αναπτυχθεί κυρίως για την υποστήριξη έργων λογισμικού και διαχείρισης των κινδύνων που μπορεί να παρουσιαστούν σε κάθε τομέα εφαρμογής, όπως ενσωματωμένα συστήματα, συστήματα συναλλαγών, τηλεπικοινωνιακές εφαρμογές, ηλεκτρονικό εμπόριο κ.α. Οι επιχειρήσεις που έχουν υιοθετήσει κάποιο πλαίσιο διακυβέρνησης μπορούν να χρησιμοποιήσουν ένα μοντέλο που βασίζεται στη RiskIT για να ενισχύσουν την υπάρχουσα διαχείριση κινδύνου.

Οι αρχές της RiskIT [5]:

- Συνδέεται πάντοτε με τους επιχειρηματικούς στόχους,
- Ευθυγραμμίζει τον IT κίνδυνο με την συνολική επιχειρησιακή διαχείριση κινδύνου,
- Ορίζει και επιβάλλει προσωπική ευθύνη για ειδικές κατηγορίες κινδύνων,
- Εξισορροπεί τα κόστη και τα οφέλη από την διαχείριση του IT κινδύνου,
- Είναι μια συνεχής διαδικασία και μέρος των καθημερινών δραστηριοτήτων.

Η μέθοδος RiskIT παρέχει ένα συστηματικό τρόπο για τον εντοπισμό, την ανάλυση, τον έλεγχο και τέλος την παρακολούθηση των κινδύνων που μπορούν να αποτελέσουν απειλή για τους στόχους του έργου. Τα βασικά βήματα της RiskIT φαίνονται στην Εικόνα 1 και στη συνέχεια της ενότητας αναλύονται διεξοδικά [1, 6].



Εικόνα 1: Η μέθοδος RiskIT

3.1.1 Πολιτική Διαχείρισης Κινδύνου

Η **Πολιτική Διαχείρισης Κινδύνου** (Risk Management Mandate Definition) καθορίζει τις στρατηγικές ενσωμάτωσης της διαδικασίας διαχείρισης κινδύνων στα συστήματα και στις διαδικασίες του οργανισμού, καθώς και το κατάλληλο επίπεδο των πόρων και υποδομών που είναι απαραίτητο για την αποτελεσματική διαχείριση των κινδύνων.

Στην πολιτική διαχείρισης κινδύνων προσδιορίζεται επίσης πόσο συχνά πρέπει να γίνεται η διαχείριση των κινδύνων και αποδίδονται ρόλοι και αρμοδιότητες στους υπαλλήλους. Αυτό περιλαμβάνει ανάθεση ευθύνης για ειδικές κατηγορίες κινδύνων και εφαρμογή στρατηγικών αντιμετώπισης και ελέγχου των κινδύνων.

Ο Διαχειριστής του έργου (Project Manager) και ο Κύριος του έργου (Project Owner) είναι οι κύριοι υπεύθυνοι για τη διαχείριση των κινδύνων σε όλο τον οργανισμό και για την εξασφάλιση της αποτελεσματικής εφαρμογής της πολιτικής διαχείρισης κινδύνων.

Σκοπός:	Ορίζεται ο σκοπός και η συχνότητα της διαχείρισης του κινδύνου.
Περιγραφή:	Καθορίζεται η ευθύνη, το πεδίο εφαρμογής, και το επίκεντρο του κινδύνου διαχείρισης ενός έργου.
Κριτήρια Εισόδου:	[ο σχεδιασμός του έργου έχει ξεκινήσει] Ή [τα ενδιαφερόμενα μέρη έχουν αλλάξει] Ή [το συνολικό επίπεδο κινδύνου του έργου έχει αλλάξει] Ή [η ανοχή κινδύνου των ενδιαφερομένων έχει αλλάξει]
Είσοδος:	Πληροφορίες που αφορούν το έργο: στόχοι, πόροι, χρονοδιάγραμμα, προϋπολογισμός. Η πολιτική διαχείρισης κινδύνων του οργανισμού και η πρακτική.
Έξοδος:	Εντολή διαχείρισης του κινδύνου
Μέθοδοι και εργαλεία:	(δεν έχουν οριστεί)
Ευθύνη:	Διαχειριστής του έργου
Πόροι:	Κύριος του έργου, Διαχειριστής του έργου
Κριτήρια Εξόδου:	Τεκμηριωμένη και εγκεκριμένη εντολή διαχείρισης κινδύνου.

Πίνακας 3: Η διαδικασία της Πολιτικής Διαχείρισης Κινδύνου

3.1.2 Επανεξέταση στόχου

Σκοπός της **Επανεξέτασης στόχου** (Goal review) είναι να κατανοηθούν και, εάν είναι απαραίτητο, να αναθεωρηθούν οι στόχοι του έργου, έτσι ώστε να αντικατοπτρίζουν τα συμφέροντα και τις συμφωνίες των ενδιαφερομένων μερών.

Στην επανεξέταση στόχου πρέπει να προσδιοριστούν και τα εμπλεκόμενα μέρη, δηλαδή τα άτομα που μπορεί να επηρεαστούν από κάποιες αποφάσεις σχετικά με τη διαχείριση κινδύνων, ή να επηρεάσουν αυτές τις αποφάσεις. Τα εμπλεκόμενα μέρη μπορεί να είναι είτε εσωτερικά του οργανισμού/επιχείρησης, είτε εξωτερικά και είναι τα παρακάτω:

- Εργαζόμενοι
- Κυβέρνηση
- Προμηθευτές
- Πελάτες
- Τελικοί χρήστες συστήματος
- Διοίκηση οργανισμού/επιχείρησης
- Χορηγοί

Σκοπός:	Σαφής ορισμός των στόχων του έργου. Αναγνώριση όλων των ενδιαφερόμενων φορέων.
Περιγραφή:	Οι υφιστάμενοι στόχοι επανεξετάζονται και βελτιώνονται και αν είναι απαραίτητο ορίζονται έμμεσοι στόχοι. Αναγνώριση της σημασίας των διαφόρων ενδιαφερόμενων φορέων και της συσχέτισής τους με τους στόχους του έργου.
Κριτήρια Εισόδου:	[ο σχεδιασμός του έργου έχει ξεκινήσει] Ή [ορίζονται νέοι στόχοι ή ενδιαφερόμενοι φορείς] Ή [προκύπτει μια αλλαγή στους στόχους ή τα ενδιαφερόμενα μέρη]
Είσοδος:	Πληροφορίες που αφορούν το έργο: στόχοι, πόροι, χρονοδιάγραμμα, προϋπολογισμός. Η πολιτική διαχείρισης κινδύνων του οργανισμού και η πρακτική.
Έξοδος:	Ορισμός στόχων
Μέθοδοι και εργαλεία:	Ομαδοποίηση συγγένειας (Affinity grouping)
Ευθύνη:	Διαχειριστής του έργου
Πόροι:	Κύριος του έργου, Εμπλεκόμενοι φορείς, προσωπικό του έργου.
Κριτήρια Εξόδου:	Οι Στόχοι τεκμηριώνονται γραπτώς και οι συμμετέχοντες συμφωνούν με αυτούς.

Πίνακας 4: Η διαδικασία της Επανεξέτασης στόχου

3.1.3 Αναγνώριση Κινδύνου

Η διαδικασία διαχείρισης κινδύνων ξεκινάει με την **Αναγνώριση των Κινδύνων** (Risk Identification). Στο στάδιο αυτό δημιουργείται ένας μεγάλος κατάλογος με όλους τους πιθανούς παράγοντες κινδύνου που θα μπορούσε να αντιμετωπίσει το υπό εξέταση έργο. Οι πρώτοι αυτοί «ακατέργαστοι» κίνδυνοι συνήθως κατανέμονται σε ομάδες για περαιτέρω επεξεργασία στο στάδιο της ανάλυσης κινδύνου.

Στη διαδικασία αναγνώρισης κινδύνων πρέπει να λάβουν μέρος όλα τα τμήματα του οργανισμού που εμπλέκονται στους κύριους τομείς του έργου. Η αναγνώριση των κινδύνων μπορεί να βασίζεται σε δομημένες συζητήσεις για την ανταλλαγή ιδεών, σε συνεντεύξεις, ερωτηματολόγια και στην ανάλυση ενός συνόλου σεναρίων και παραδοχών.

Σκοπός:	Εντοπισμός δυνητικών απειλών για το έργο.
Περιγραφή:	Προσδιορισμός των πιθανών απειλών του έργου με χρήση πολλαπλών προσεγγίσεων.
Κριτήρια Εισόδου:	[ο σχεδιασμός του έργου έχει ξεκινήσει] Ή [ορίζονται νέοι στόχοι ή ενδιαφερόμενοι φορείς] Ή [προκύπτει μια αλλαγή στους στόχους ή τα ενδιαφερόμενα μέρη] Ή [το χρονικό διάστημα που αναφέρεται στην εντολή διαχείρισης κινδύνου έχει παρέλθει] Ή [έχει προκύψει μια σημαντική αλλαγή στην κατάσταση του έργου

Είσοδος:	Πληροφορίες που αφορούν το έργο: στόχοι, πόροι, χρονοδιάγραμμα, προϋπολογισμός. Η πολιτική διαχείρισης κινδύνων του οργανισμού και η πρακτική. Λίστες ελέγχου του κινδύνου. Πληροφορίες από ανάλογες εκθέσεις έργων.
Έξοδος:	Κατάλογος «ακατέργαστων» κινδύνων.
Μέθοδοι και εργαλεία:	Συσκέψεις για την ανταλλαγή και ανάπτυξη ιδεών (Brainstorming) Ανάλυση Παραδοχών Συνεντεύξεις Ερωτηματολόγια
Ευθύνη:	Διαχειριστής του έργου.
Πόροι:	Προσωπικό του έργου, Μεσολαβητής διαχείρισης κινδύνου.
Κριτήρια Εξόδου:	[Η οριακή απόδοση της αναγνώρισης κινδύνου πλησιάζει στο μηδέν] Ή [ο χρόνος εντοπισμού του κινδύνου έχει εξαντληθεί]

Πίνακας 5: Η διαδικασία της Αναγνώρισης Κινδύνου

3.1.4 Ανάλυση Κινδύνου

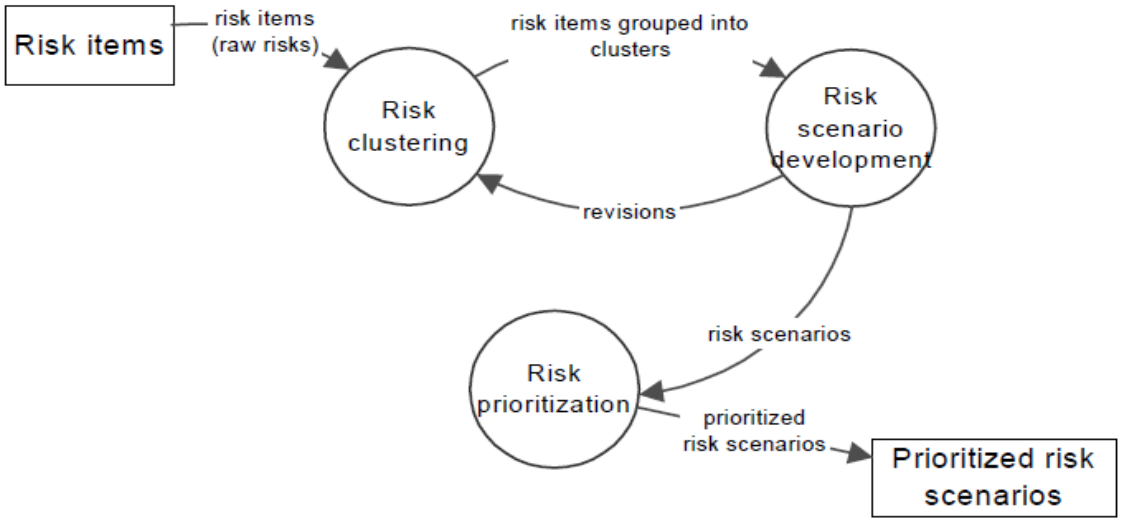
Η μέθοδος της **Ανάλυσης Κινδύνου** (Risk Analysis) εφαρμόζεται στους κινδύνους που έχουν εντοπισθεί στο προηγούμενο στάδιο (στάδιο αναγνώρισης). Η διαδικασία της ανάλυσης των κινδύνων ομαδοποιεί, αξιολογεί και ιεραρχεί ξεχωριστά τα χαρακτηριστικά των αναγνωρισμένων κινδύνων, παρέχοντας στη διαχείριση του έργου τα χαρακτηριστικά εκείνων που επηρεάζουν περισσότερο (θετικά ή αρνητικά) τους σκοπούς του έργου. Όσοι κίνδυνοι αξιολογηθούν ως υψηλής προτεραιότητας, είναι και αυτοί που θα λάβουν τη σημαντικότερη προσοχή στο στάδιο ελέγχου.

Σκοπός:	Κατανόηση και ιεράρχηση κινδύνων.
Περιγραφή:	Ανάλυση των κινδύνων και αξιολόγηση των επιπτώσεων τους έτσι ώστε να καθοριστούν οι πιο σημαντικοί από αυτούς.
Κριτήρια Εισόδου:	Εντοπισμός νέων δυνητικών κινδύνων
Είσοδος:	Λίστα κινδύνων
Έξοδος:	Μια λίστα προτεραιότητας των σεναρίων κινδύνου.
Μέθοδοι και εργαλεία:	Γράφος Ανάλυσης κινδύνων. Εργαλεία λήψης αποφάσεων. Τεχνικές κατάταξης.
Ευθύνη:	Διαχειριστής του έργου.
Πόροι:	Επιλεγμένο προσωπικό, Μεσολαβητής διαχείρισης κινδύνου.
Κριτήρια Εξόδου:	Οι συμμετέχοντες συμφωνούν με την προτεραιότητα των σημαντικότερων κινδύνων.

Πίνακας 6: Η διαδικασία της Ανάλυσης Κινδύνου

Οι τρεις κύριες δραστηριότητες που μπορούν να εντοπιστούν κατά τη διαδικασία ανάλυσης κινδύνου είναι:

- ομαδοποίηση των κινδύνων (Risk clustering)
- ανάπτυξη σεναρίων κινδύνου (Risk scenario development)
- ιεράρχηση των κινδύνων (Risk prioritization)



Εικόνα 2: Οι δραστηριότητες της Ανάλυσης Κινδύνου

3.1.5 Προγραμματισμός Διαχείρισης Κινδύνου

Ο στόχος του **Προγραμματισμού Διαχείρισης Κινδύνου** (Risk Control Planning) είναι να καθορίσει ποιες δραστηριότητες ελέγχου είναι αναγκαίο να ληφθούν. Τα κύρια ζητήματα στον προγραμματισμό διαχείρισης των κινδύνων είναι ο εντοπισμός των κινδύνων που εγκυμονούν τις μεγαλύτερες απειλές και η επιλογή των κατάλληλων στρατηγικών απόκρισης και δράσης για κάθε κίνδυνο ξεχωριστά. Στο τέλος αυτού του σταδίου ετοιμάζεται ένα ενοποιημένο σχέδιο διαχείρισης. Οι μέθοδοι αντιμετώπισης των απειλών είναι [5]:

- **Αποφυγή** (avoidance) - επιδιώκει να εξαλείψει την αβεβαιότητα
- **Μεταφορά** (transfer) - επιδιώκει να μεταβιβάσει την κυριότητα ή/και την ευθύνη σε τρίτους

- **Μείωση/μετριασμός** (mitigation) - επιδιώκει να μειώσει το μέγεθος της έκθεσης στον κίνδυνο κάτω από ένα αποδεκτό όριο
- **Αποδοχή** (acceptance) - αναγνωρίζει τους κινδύνους και επινοεί μεθόδους για τον έλεγχο και την παρακολούθηση τους

Σκοπός:	Επιλογή αποδοτικών δράσεων ελέγχου κινδύνου.
Περιγραφή:	Ορισμός δράσεων ελέγχου για τα πιο σημαντικά σενάρια κινδύνου.
Κριτήρια Εισόδου:	Αναγνώριση σημαντικών σεναρίων κινδύνου.
Είσοδος:	Μερική ιεράρχηση σεναρίων κινδύνου.
Έξοδος:	Επιλεγμένες δράσεις ελέγχου κινδύνου. Μετρήσεις παρακολούθησης κινδύνων.
Μέθοδοι και εργαλεία:	Αποφυγή, μεταφορά, μετριασμός και αποδοχή Μητρώο Διαχείρισης Κινδύνου (Risk Management Register)
Ευθύνη:	Διαχειριστής του έργου
Πόροι:	Επιλεγμένο προσωπικό, Μεσολαβητής διαχείρισης κινδύνου.
Κριτήρια Εξόδου:	Όλα τα επιλεγμένα σενάρια κινδύνου έχουν αντιμετωπιστεί.

Πίνακας 7: Η διαδικασία του Προγραμματισμού Ελέγχου Κινδύνου

3.1.6 Έλεγχος Κινδύνου

Στο στάδιο του **Ελέγχου Κινδύνου** (Risk Control) εφαρμόζονται οι εναλλακτικές δράσεις διαχείρισης κινδύνου. Επιπλέον, επιβεβαιώνεται ότι η εφαρμογή του προγραμματισμού της διαχείρισης κινδύνου έχει συντονιστεί και είναι σε αρμονία με τις δραστηριότητες διαχείρισης του προγράμματος.

Σκοπός:	Εφαρμογή δράσεων ελέγχου κινδύνου.
Περιγραφή:	Εφαρμογή των δράσεων ελέγχου κινδύνου που ορίστηκαν κατά τη διαδικασία του προγραμματισμού διαχείρισης κινδύνου.
Κριτήρια Εισόδου:	Μια δράση ελέγχου κινδύνου έχει επιλεγεί για εφαρμογή.
Είσοδος:	Επιλεγμένες δράσεις ελέγχου κινδύνου.
Έξοδος:	Εφαρμογή δράσεων ελέγχου κινδύνου. Αναφορές πιθανών προβλημάτων κατά την εφαρμογή.
Μέθοδοι και εργαλεία:	(δεν έχουν οριστεί)
Ευθύνη:	Διαχειριστής έργου
Πόροι:	Προσωπικό του έργου, εξωτερικές πηγές
Κριτήρια Εξόδου:	Επιλεγμένες δράσεις που έχουν υλοποιηθεί.

Πίνακας 8: Η διαδικασία του Ελέγχου Κινδύνου

3.1.7 Παρακολούθηση Κινδύνων

Στη φάση της **Παρακολούθησης Κινδύνων** (Risk Monitoring) η ομάδα διαχείρισης κινδύνων πρέπει να παρακολουθεί τους κινδύνους που έχει προσδιορίσει, αναλύσει και αξιολογήσει ώστε να δει ποιοι παράγοντες κινδύνου εμφανίστηκαν τελικά και πότε, καθώς και αν κάποιος κίνδυνος έχει αλλάξει μορφή. Ολόκληρη η διαδικασία επαναλαμβάνεται σε τακτά χρονικά διαστήματα ώστε να εντοπισθούν νέοι κίνδυνοι που ενδεχομένως έχουν προκύψει. Τέλος, με βάση όλα τα παραπάνω στοιχεία παρακολουθείται και η ανάγκη αναθεώρησης του Σχεδίου Διαχείρισης Κινδύνου.

Σκοπός:	Παρακολούθηση του έργου και της κατάστασης του κινδύνου.
Περιγραφή:	Διαρκής παρακολούθηση των μετρήσεων των κινδύνων και των πιθανών αλλαγών στην κατάσταση του έργου.
Κριτήρια Εισόδου:	Η υλοποίηση του έργου έχει ξεκινήσει. Η διαδικασία μπορεί να θεσπιστεί σε προκαθορισμένες συχνότητες.
Είσοδος:	Μετρήσεις παρακολούθησης των κινδύνων. Εντολή διαχείρισης του κινδύνου. Προκαθορισμένοι στόχοι. Γράφος Ανάλυσης κινδύνων.
Έξοδος:	Αναφορές κατάστασης (status reports).
Μέθοδοι και εργαλεία:	Πρόγραμμα μέτρησης ή μια βάση δεδομένων.
Ευθύνη:	Διαχειριστής έργου
Πόροι:	Προσωπικό του έργου
Κριτήρια Εξόδου:	Το έργο έχει ολοκληρωθεί ή τερματιστεί

Πίνακας 9: Η διαδικασία της Παρακολούθησης Κινδύνων

3.2 Μεθοδολογίες

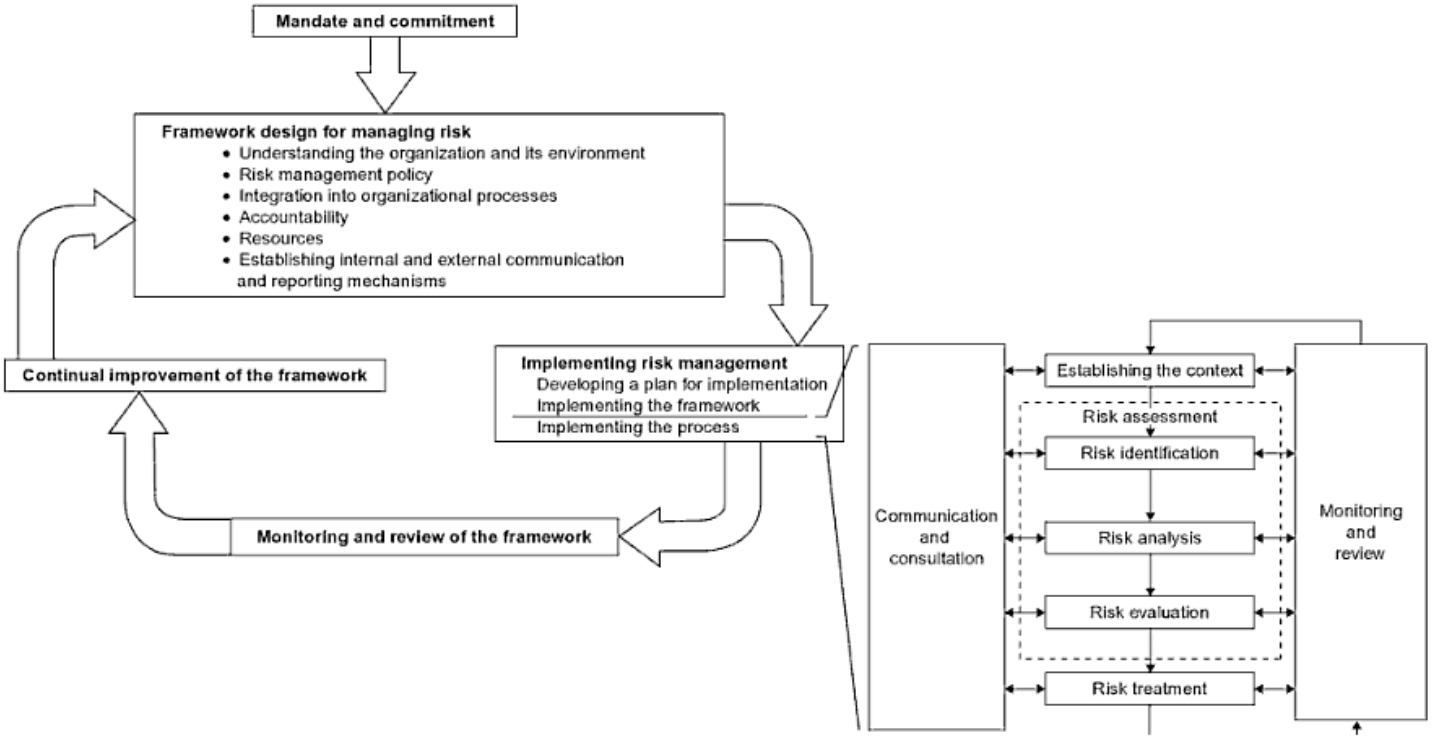
Η μέθοδος RiskIT αποτελεί τον βασικό κορμό του μοντέλου αλλά υποστηρίζεται από τρεις επιπλέον μεθοδολογίες διαχείρισης κινδύνου, οι οποίες αναλύονται στη συνέχεια.

3.2.1 ISO 31000

Το πρότυπο **ISO 31000:2009** αναπτύχθηκε από τον Διεθνή Οργανισμό Τυποποίησης (International Organization for Standardization - ISO) με σκοπό να παρέχει τις γενικές αρχές και κατευθυντήριες γραμμές για την αποτελεσματική διαχείριση του κινδύνου. Απευθύνεται σε εταιρείες κάθε επαγγελματικής δραστηριότητας, δημόσιου ή ιδιωτικού τομέα, που επιθυμούν να αναγνωρίσουν το κίνδυνο σε πρώιμο στάδιο.
Κατά το ISO 31000 η διαχείριση κινδύνου πρέπει να υπακούει στις ακόλουθες αρχές [7]:

- Δημιουργία αξίας
- Να είναι αναπόσπαστο μέρος των επιχειρησιακών διαδικασιών και όχι μια αυτόνομη δραστηριότητα
- Να είναι μέρος της διαδικασίας λήψης αποφάσεων
- Να είναι συστηματική και δομημένη
- Να βασίζεται στις βέλτιστες διαθέσιμες πληροφορίες (εμπειρία, παρακολούθηση, προβλέψεις και κρίση των εμπειρογνωμόνων)
- Η διαχείριση του κινδύνου θα πρέπει να ευθυγραμμιστεί με τις εξωτερικές και εσωτερικές δραστηριότητες του οργανισμού
- Θα πρέπει να λαμβάνει υπόψη τον ανθρώπινο παράγοντα
- Να είναι έγκυρη και να συμπεριλαμβάνει όλα τα ενδιαφερόμενα μέρη
- Να είναι δυναμική, επαναληπτική και να ανταποκρίνεται στις αλλαγές

Η παρακάτω εικόνα παρουσιάζει το πλαίσιο εντός του οποίου ένας οργανισμός μπορεί να ανιχνεύσει και να μετρήσει τον κίνδυνο και τη διαδικασία με την οποία μπορεί να το κάνει αυτό [7].



Εικόνα 3: Το πλαίσιο διαχείρισης κινδύνων κατά το ISO 31000

Σύμφωνα με το παραπάνω πλαίσιο η διαχείριση κινδύνου περιλαμβάνει τα εξής βήματα [7]:

Σχεδιασμός πλαισίου διαχείρισης κινδύνων

Βήμα 1: Κατανόηση του οργανισμού και του περιβάλλοντός του

Βήμα 2: Ορισμός της πολιτικής διαχείρισης κινδύνων

Βήμα 3: Ενσωμάτωση στις επιχειρησιακές διαδικασίες

Βήμα 4: Ορισμός ευθύνης

Βήμα 5: Προσδιορισμός Πόρων

Βήμα 6: Καθιέρωση εσωτερικής επικοινωνίας και μηχανισμών αναφοράς

Βήμα 7: Καθιέρωση εξωτερικής επικοινωνία και μηχανισμών αναφοράς.

Εφαρμογή διαχείρισης του κινδύνου

Βήμα 8: Ανάπτυξη ενός σχεδίου δράσης για την εφαρμογή

Βήμα 9: Εφαρμογή του πλαισίου για τη διαχείριση του κινδύνου

Βήμα 10: Εφαρμογή της διαδικασίας

Βήμα 10.1: Επικοινωνία

Βήμα 10.2: Καθιέρωση του πλαισίου

Βήμα 10.3: Ανάπτυξη κριτηρίων κινδύνου

Βήμα 10.4: Εκτίμηση κινδύνου

Βήμα 10.5: Προετοιμασία και εφαρμογή

Βήμα 10.6: Καταγραφή της διαδικασίας διαχείρισης κινδύνων

Βήμα 10.7: Παρακολούθηση και επανεξέταση

Βήμα 11: Παρακολούθηση και αναθεώρηση του πλαισίου

Βήμα 12: Συνεχής βελτίωση του πλαισίου

3.2.2 ITIL

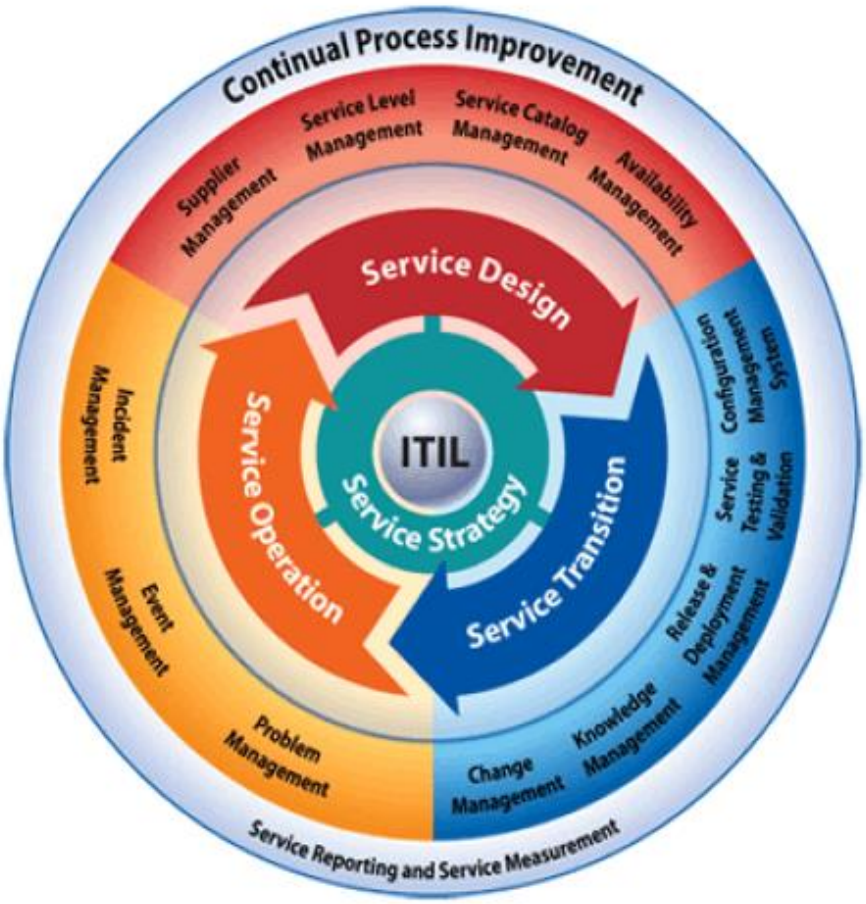
Η βιβλιοθήκη υποδομής τεχνολογίας πληροφοριών (Information Technology Infrastructure Library - ITIL) είναι ένα σύνολο βέλτιστων πρακτικών και οδηγιών που καθορίζουν μια ολοκληρωμένη διαδικασία, βασισμένη στην προσέγγιση για τη διαχείριση υπηρεσιών πληροφοριακής τεχνολογίας. Η ITIL μπορεί να προσαρμοστεί και να εφαρμοστεί σχεδόν σε κάθε τύπο περιβάλλοντος τεχνολογιών πληροφορίας (IT) συμπεριλαμβανομένου και του λειτουργικού περιβάλλοντος cloud. Η ITIL επιδιώκει να εξασφαλίσει ότι λαμβάνονται αποτελεσματικά μέτρα ασφάλειας πληροφοριών σε στρατηγικό, τακτικό, και λειτουργικό επίπεδο.

Η ITIL περιλαμβάνει τις εξής υπηρεσίες [8]:

- **Στρατηγική Ανάπτυξης Υπηρεσιών** (Service Strategy): ορίζει ποιοι είναι οι χρήστες της πληροφορικής, ποιες υπηρεσίες απαιτούνται για την κάλυψη των αναγκών των πελατών και τις δυνατότητες της πληροφορικής και των πόρων που απαιτούνται για την ανάπτυξη μιας ισχυρής οργάνωσης.
- **Σχεδιασμός Υπηρεσιών** (Service Design): εξασφαλίζει ότι οι νέες υπηρεσίες και οι αλλαγές στις υπάρχουσες υπηρεσίες έχουν σχεδιαστεί αποτελεσματικά προκειμένου να ανταποκριθούν στις προσδοκίες των πελατών.
- **Μετάβαση Υπηρεσιών** (Service Transition): γενική δραστηριότητα ή διεργασία που είναι υπεύθυνη για την παρακολούθηση και την παροχή πληροφόρησης. Αυτή η φάση εξασφαλίζει στους πελάτες ότι πέτυχαν τους στόχους τους.
- **Λειτουργία Υπηρεσιών** (Service Operation): η λειτουργία αυτή είναι υπεύθυνη για τη διαχείριση μιας εφαρμογής σε ολόκληρη τη διάρκεια του

κύκλου ζωής της. Αυτό περιλαμβάνει διαταραχές διαχείρισης συμβάντων, τον καθορισμό της πρωταρχικής αιτίας των προβλημάτων και την ανίχνευση των τάσεων που σχετίζονται με επαναλαμβανόμενα ζητήματα.

– **Συνεχής Βελτίωση Υπηρεσιών** (Continual Service Improvement): περιλαμβάνει τον μηχανισμό δημιουργίας ενός πίνακα με βασικούς δείκτες απόδοσης (KPIs) για τη μέτρηση και τη βελτίωση των επιπέδων παροχής υπηρεσιών, την αποδοτικότητα και την αποτελεσματικότητα των διαδικασιών που χρησιμοποιούνται στη συνολική διαχείριση των υπηρεσιών.

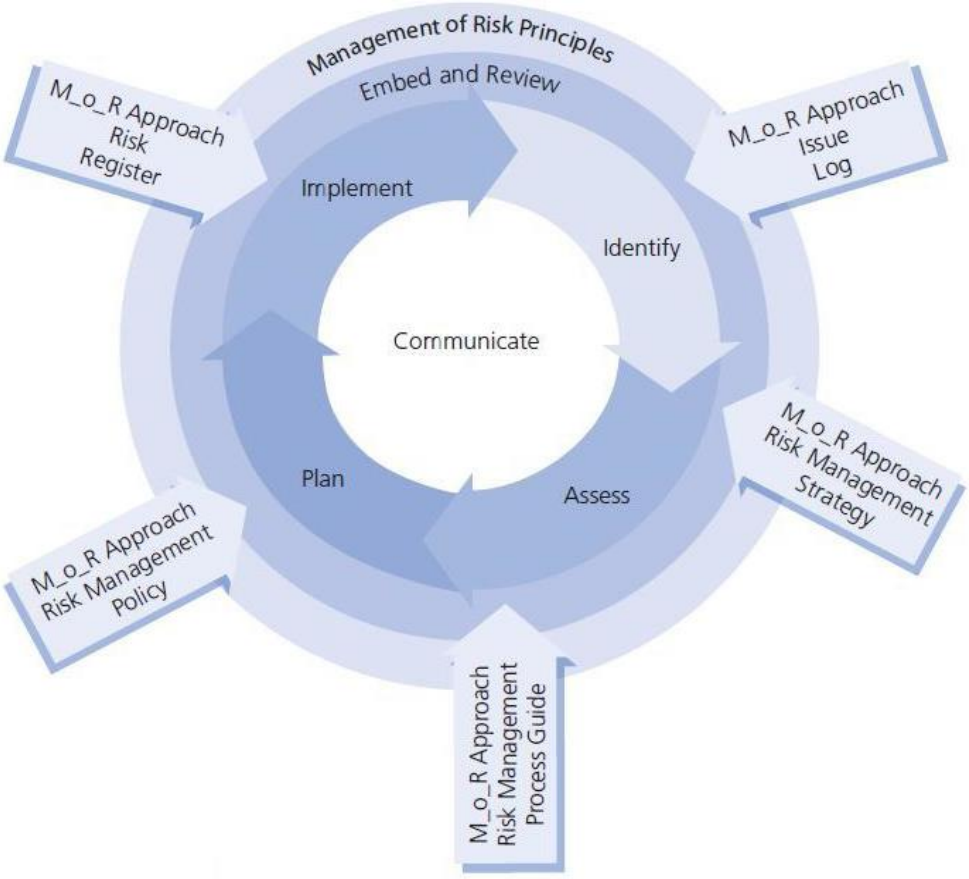


Εικόνα 4: Ο κύκλος ζωής της βιβλιοθήκης ITIL

3.2.3 M_o_R

Το πλαίσιο Διαχείρισης Κινδύνου **M_o_R** (Management of Risk) προτάθηκε από τον οργανισμό OGC και βασίζεται σε τέσσερις έννοιες [9]:

- **Αρχές** (Principles): απαραίτητες για την ορθή ανάπτυξη ενός συστήματος διαχείρισης κινδύνου. Βασίζονται στις αρχές της εταιρικής διακυβέρνησης και στις κατευθυντήριες γραμμές του ISO 31000 [10]
- **Προσέγγιση** (Approach): προσαρμογή των αρχών ώστε να ταιριάζουν στον εκάστοτε οργανισμό
- **Διαδικασίες** (Processes): περιγράφουν τις εισροές, τις εκροές καθώς και τις δραστηριότητες που εμπλέκονται, διασφαλίζοντας ότι ο κίνδυνος εντοπίζεται, αξιολογείται και ελέγχεται
- **Ενσωμάτωση και αναθεώρηση** (Embedding and Reviewing): διασφαλίσει ότι οι αρχές, η προσέγγιση και οι διαδικασίες εφαρμόζονται με συνέπεια από όλο τον οργανισμό και ότι η εφαρμογή τους υπόκειται σε συνεχή βελτίωση.



Εικόνα 5: Το πλαίσιο M_o_R

Για το M_o_R ο κίνδυνος δεν αποτελεί μόνο «απειλή» αλλά και «ευκαιρία». Με αυτόν τον ορισμό ο κίνδυνος μπορεί να διαχωριστεί σε ανεπιθύμητο ρίσκο (down-side risk), το οποίο αναφέρεται στην εμφάνιση σημαντικών απειλών ή ανεπιθύμητων συνεπειών, και σε επιθυμητό ρίσκο (up-side risk), το οποίο αναφέρεται στην εμφάνιση σημαντικών ευκαιριών ή επιθυμητών συνεπειών στους στόχους του έργου.

3.3 Εννοιολογικός χάρτης μοντέλου

Στις προηγούμενες ενότητες παρουσιάσαμε τέσσερις διαφορετικές μεθοδολογίες διαχείρισης κινδύνου. Αυτές οι μεθοδολογίες μοιράζονται τις ίδιες βασικές αρχές και είναι συνδεδεμένες μεταξύ τους. Παρόλο που παρουσιάζονται η κάθε μία χωριστά, στην πράξη εφαρμόζονται συνδυαστικά και πολλές φορές κυκλικά.

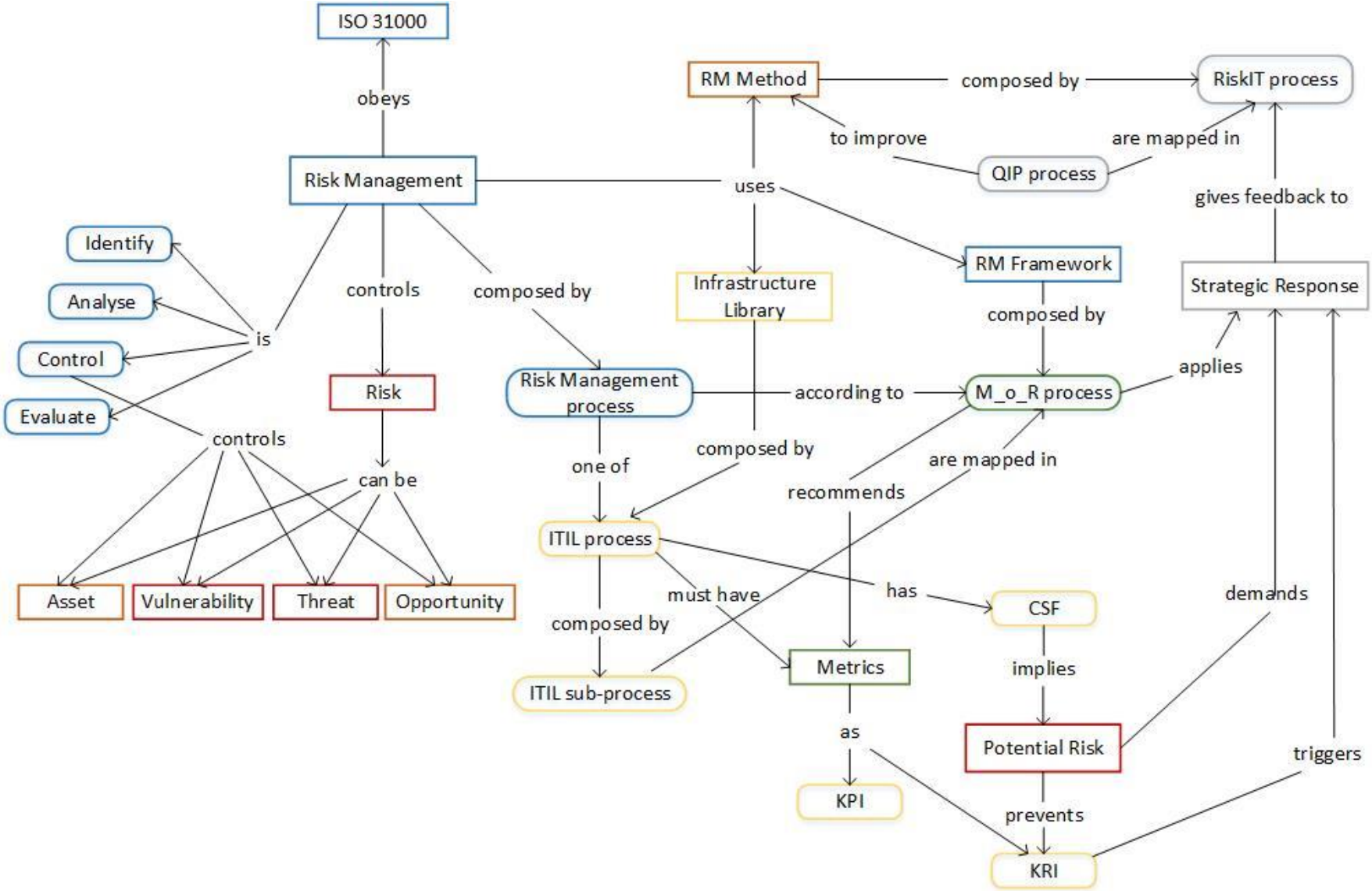
Οι δικές μας παρατηρήσεις για τα πλεονεκτήματα και τα μειονεκτήματα αυτών των μεθοδολογιών είναι:

- Το πρότυπο **ISO 31000** είναι ουσιαστικά ένας χρήσιμος πίνακας οδηγιών διαχείρισης κινδύνου. Εκφράζει κάποιες γενικές κατευθυντήριες γραμμές, αλλά σε καμία περίπτωση δεν μπορεί να θεωρηθεί ως ένα ολοκληρωμένο πλαίσιο διαχείρισης κινδύνου.
- Η **ITIL** είναι ένα σύνολο υπηρεσιών διαχείρισης κινδύνου, αρκετά αναλυτικό, αλλά παράλληλα στατικό (υστερεί στη μεθοδολογία υλοποίησης). Το βασικό της πλεονέκτημα είναι η ευχέρεια στην εξαγωγή των CSF, KPI's και KRI's που χρειάζεται ένα μοντέλο.
- Το **M_o_R** είναι ένα βασικό πλαίσιο διαχείρισης κινδύνου με περιορισμένο σύνολο λειτουργιών. Το βασικό του πλεονέκτημα είναι ότι μπορεί να συνδυάσει τις λειτουργίες του, με αυτές της ITIL σε επίπεδο απεικόνισης για την εξαγωγή των CSF, KPI's και KRI's.
- Η **RiskIT** είναι η πλέον ολοκληρωμένη μέθοδος διαχείρισης κινδύνου. Ακολουθεί τις διαδικασίες διαχείρισης έργου, εφαρμόζεται με αλγοριθμική διαδικασία και μπορεί να αποτελέσει την βάση για την δημιουργία ενός λογισμικού διαχείρισης κινδύνου. Το βασικό της μειονέκτημα είναι η δυσχέρεια στην εξαγωγή των CSF, KPI's και KRI's, τα οποία δημιουργούνται από κάποια άλλη μεθοδολογία.

Τώρα θα περιγράψουμε το προτεινόμενο μοντέλο Ανάλυσης και Διαχείρισης Κινδύνου για να απλοποιήσουμε και να αποσαφηνίσουμε την διαχείριση κινδύνου σε έναν οργανισμό, προτείνοντας ορισμένα νέα στοιχεία διαχείρισης κινδύνου. Τα κύρια στοιχεία του είναι:

- Η εναρμόνιση του μοντέλου με τις αρχές του ISO 31000,
- Η υλοποίηση των υπηρεσιών διαχείρισης κινδύνου σε επίπεδο διαχείρισης έργου,
- Η ταυτόχρονη χρήση και συνεργασία τεσσάρων πλαισίων διαχείρισης κινδύνου,
- Η μεθοδική και αποτελεσματική εξαγωγή των CSF, KPI's και KRI's που απαιτούνται,
- Η συστηματική βελτιστοποίηση των παρεχόμενων υπηρεσιών του μοντέλου

Στην επόμενη εικόνα (Εικόνα 6) παρουσιάζεται ο Εννοιολογικός χάρτης του Προτεινόμενου Μοντέλου.



Εικόνα 6: Ο Εννοιολογικός χάρτης του Προτεινόμενου Μοντέλου

3.4 Συμπεράσματα

Για να συνοψίσουμε, το παραπάνω μοντέλο συνδυάζει τέσσερα πλαίσια διαχείρισης κινδύνου, τα οποία εργάζονται παράλληλα. Το πρωτεύον πλαίσιο είναι το RiskIT το οποίο υλοποιεί τις διαδικασίες διαχείρισης κινδύνου σε επίπεδο διαχείρισης έργου (έχει συγκεκριμένα βήματα, τα οποία ενώ εκτελούνται έχουν λειτουργία ανάδρασης με όλα τα προηγούμενα). Η ITIL και το M_o_R είναι τα δευτερεύοντα πλαίσια και συνεργάζονται με τον ακόλουθο τρόπο: Οι διαδικασίες της ITIL ενισχύονται με στοιχεία διαχείρισης κινδύνου από το M_o_R. Εκτός από την εισαγωγή αυτών των νέων στοιχείων, όλες οι διαδικασίες της ITIL περικλείονται στις αρχές και τις προσεγγίσεις του M_o_R, όπως επιβάλλει το πλαίσιο ISO 31000 [10]. Η συνεργασία της ITIL με το M_o_R παράγει τα απαιτούμενα CSF, KPI's και KRI's, και στην συνέχεια τα παρέχει σαν ερεθίσματα στη RiskIT για την ολοκλήρωση της διαδικασίας. Τέλος, η συστηματική βελτιστοποίηση της διαχείρισης κινδύνου επιτυγχάνεται με την ενσωμάτωση των διαδικασιών της μεθοδολογίας QIP (Quality Improvement Paradigm, αναλύεται στο κεφάλαιο 5) στη μέθοδο RiskIT.

4. Case Study

Σε αυτή την ενότητα παρουσιάζεται μία μελέτη περίπτωσης (case study) για την Αναγνώριση και Διαχείριση Κινδύνων στη μηχανογράφηση ενός μεγάλου Τραπεζικού Ιδρύματος.

4.1 Περιγραφή

Η μελέτη περίπτωσης θα πραγματοποιηθεί στην διεύθυνση Ανάπτυξης και Διαχείρισης Εφαρμογών, και στην Διεύθυνση Παραγωγής και Λειτουργιών. Θα πρέπει να σημειωθεί ότι πρόκειται για μηχανογράφηση που απασχολεί γύρω στα 600 άτομα, με πολύπλοκη δομή, αλλά και με μεγάλο εύρος παροχής υπηρεσιών. Οι διευθύνσεις που προαναφέραμε αποτελούνται από πολλά τμήματα με τα οποία θα πρέπει να συνεργασθούμε για την υλοποίηση της μελέτης. Στη συγκεκριμένη μηχανογράφηση εφαρμόζονται κάποιες τυποποιημένες μεθοδολογίες αντιμετώπισης κινδύνων και προβλημάτων. Με βάση τις εμπειρίες που αποκτήσαμε κατά τη διάρκεια της συνεργασίας μας με αυτή, αλλά και τις παρατηρήσεις του προσωπικού για τα προβλήματα και τις ελλείψεις που αναφέραμε στην δεύτερη ενότητα, υπάρχουν αρκετά σημεία στα οποία χρειάζεται βελτίωση η διαχείριση κινδύνων. Μία από τις βασικές ελλείψεις είναι η πλήρης απουσία φύλλων καταγραφής κινδύνων.

Οι στόχοι αυτής της μελέτης είναι:

- ο προσδιορισμός των κινδύνων που εμπλέκονται σε ένα έργο λογισμικού,
- η ιεράρχηση τους κατά σειρά σπουδαιότητας και συχνότητα εμφάνισης και
- ο προσδιορισμός των δραστηριοτήτων που απαιτούνται από τους διαχειριστές του έργου για τον έλεγχο των κινδύνων που έχουν εντοπιστεί.

Για την υλοποίηση της μελέτης θα βασισθούμε στο μοντέλο που περιγράψαμε στην προηγούμενη ενότητα με την εξής λογική: Θα ακολουθήσουμε αναλυτικά τα βήματα της μεθόδου RiskIT, η οποία είναι ο κορμός του μοντέλου, πλαισιωμένα με την απαραίτητη ποιοτική και ποσοτική ανάλυση, αλλά σε αντίθεση με την κλασσική εφαρμογή της μεθόδου, η βιβλιοθήκη ITIL θα έχει βοηθητικό χαρακτήρα. Θα αντλήσουμε τα απαραίτητα KRIs τα οποία σχετίζονται με κινδύνους λογισμικού από την ITIL και θα τα επαυξήσουμε με βάση τα στοιχεία που θα προκύψουν κατά την διάρκεια της μελέτης. Αυτό γιατί δείκτες όπως KPIs, KRIs και παράγοντες όπως CSF έχουν νόημα μόνο όταν υπάρχει και εφαρμόζεται μία δομημένη μεθοδολογία

αντιμετώπισης κινδύνου σε έναν οργανισμό και θέλουμε να την βελτιώσουμε. Τέλος, η ανάλυση των κινδύνων, τα KRIs, οι έλεγχοι και οι ενέργειες που θα προτείνουμε θα αναδείξουν τις ελλείψεις διαχείρισης κινδύνου στον οργανισμό, με απώτερο σκοπό την βελτίωση της υπάρχουσας πολιτικής.

4.2 Αναγνώριση Κινδύνων

Στη φάση της αναγνώρισης πρέπει να εντοπιστούν οι πιθανοί κίνδυνοι χρησιμοποιώντας κάποια/κάποιες από τις μεθόδους εντοπισμού (συνεντεύξεις, ερωτηματολόγια, ομαδική παραγωγή ιδεών, κατάλογοι κινδύνων κ.α.) και να ταξινομηθούν σε διάφορες κατηγορίες πριν δοθούν για αξιολόγηση.

Οι μελέτες του Boehm (1991) και άλλων ερευνητών δείχνουν ότι τα περισσότερα σχέδια αποτυγχάνουν στη διοίκηση, όχι τεχνολογικά. Οι 10 κύριες πηγές κινδύνου για τα έργα λογισμικού κατά τον Boehm είναι [11]:

1. Ελλείψεις προσωπικού

2. Μη ρεαλιστικά χρονοδιαγράμματα και προϋπολογισμός

3. Ανάπτυξη λανθασμένων λειτουργιών στο λογισμικό

4. Λάθος ανάπτυξη στο περιβάλλον επικοινωνίας των χρηστών

5. Φαινόμενο επιχρύσωσης

6. Συνεχείς αλλαγές στις απαιτήσεις

7. Ελλείψεις σε παρεχόμενα τμήματα του έργου από εξωτερικούς συνεργάτες

8. Ελλείψεις σε παρεχόμενες εργασίες από εξωτερικούς συνεργάτες

9. Ελλείψεις υλοποίησης του έργου σε πραγματικό χρόνο

10. Εξάντληση των δυνατοτήτων του υπολογιστικού συστήματος

Στους παραπάνω κινδύνους προσθέτουμε μερικούς ακόμα που έχουν αναγνωριστεί από πολλούς ερευνητές και εμφανίζονται συχνά σε έργα λογισμικού:

11. Ασαφείς/παρερμηνευμένοι στόχοι και σκοπός του έργου

12. Αδιαφορία/αδυναμίες της ανώτερης διοίκησης στην υλοποίηση του έργου

13. Αποτυχία της Διοίκησης στη συμμετοχή των χρηστών στο έργο

14. Ανεπαρκείς γνώσεις και δεξιότητες

15. Ελλείψεις στην αποτελεσματική μεθοδολογία διαχείρισης του έργου

16.Υπεργολαβία (εξωτερικοί συνεργάτες)

17. Εσφαλμένη χρήση των διαθέσιμων πόρων και της απόδοσής του συστήματος

18. Προβλήματα από την εισαγωγή νέας τεχνολογίας.

19. Αδυναμία διαχείρισης προβλημάτων/συμβάντων

20. Έλλειψη εφεδρικού σχεδίου απρόσκοπτης λειτουργίας του συστήματος.

Μετά τον προσδιορισμό τους, οι πιθανοί κίνδυνοι ταξινομούνται στις διάφορες κατηγορίες όπως φαίνεται στον επόμενο πίνακα.

Κατηγορίες Κινδύνων	**Κίνδυνοι σε έργα λογισμικού**
Τεχνολογικοί	• Ανάπτυξη λανθασμένων λειτουργιών στο λογισμικό • Λάθος ανάπτυξη στο περιβάλλον επικοινωνίας των χρηστών • Φαινόμενο επιχρύσωσης • Προβλήματα από την εισαγωγή νέας τεχνολογίας • Εξάντληση των δυνατοτήτων του υπολογιστικού συστήματος
Λειτουργικοί-Οργανωτικοί	• Αδυναμία διαχείρισης προβλημάτων/συμβάντων • Ελλείψεις υλοποίησης του έργου σε πραγματικό χρόνο • Αποτυχία της Διοίκησης στη συμμετοχή των χρηστών στο έργο
Στρατηγικοί	• Αδιαφορία/αδυναμίες της ανώτερης διοίκησης στην υλοποίηση του έργου • Ελλείψεις στην αποτελεσματική μεθοδολογία διαχείρισης του έργου • Έλλειψη εφεδρικού σχεδίου απρόσκοπτης λειτουργίας του συστήματος.
Εξωτερικοί	• Συνεχείς αλλαγές στις απαιτήσεις • Ελλείψεις σε παρεχόμενα τμήματα του έργου από εξωτερικούς συνεργάτες • Ελλείψεις σε παρεχόμενες εργασίες από εξωτερικούς συνεργάτες • Ασαφείς/παρερμηνευμένοι στόχοι και σκοπός του

	έργου • Υπεργολαβία (εξωτερικοί συνεργάτες)
Ανθρώπινοι	• Ελλείψεις προσωπικού • Ανεπαρκής γνώσεις και δεξιότητες
Εκτίμησης	• Μη ρεαλιστικά χρονοδιαγράμματα και προϋπολογισμός • Εσφαλμένη χρήση των διαθέσιμων πόρων και της απόδοσής του συστήματος

Πίνακας 10: Ταξινόμηση των Κινδύνων

4.3 Ανάλυση Κινδύνων

Αφού εντοπίστηκαν οι κίνδυνοι που ενδέχεται να προκύψουν, πρέπει να αξιολογηθούν και να διαπιστωθεί το επίπεδο της συνολικής έκθεσης του έργου σε κάθε έναν από αυτούς.

Η ανάλυση των κινδύνων θα γίνει με τη βοήθεια ενός ερωτηματολόγιου που αποτελείται από 20 σύνολα ερωτήσεων, κάθε ένα εκ των οποίων αντιστοιχεί σε έναν υπό μελέτη κίνδυνο. Αρχικά οι χρήστες καλούνται να ιεραρχήσουν τους κινδύνους ανάλογα με τη σπουδαιότητά τους και στη συνέχεια να απαντήσουν σε μια σειρά ερωτήσεων, επιλέγοντας μια από τις προτεινόμενες απαντήσεις. Με βάση τις επιλογές των χρηστών, θα εξάγουμε την πιθανότητα εμφάνισης κάθε κινδύνου καθώς και την επίπτωση του.

Ο πίνακας 11 δείχνει την κατάταξη κάθε παράγοντα κινδύνου (για λόγους ευκολίας επιλέξαμε τους 10 πρώτους για περαιτέρω ανάλυση).

Κίνδυνος	Κατάταξη
11.Ασαφείς/παρερμηνευμένοι στόχοι και σκοπός του έργου	1
2.Μη ρεαλιστικά χρονοδιαγράμματα και προϋπολογισμός	2
3.Ανάπτυξη λανθασμένων λειτουργιών στο λογισμικό	3
6.Συνεχείς αλλαγές στις απαιτήσεις	4
13.Αποτυχία της Διοίκησης στη συμμετοχή των χρηστών στο έργο	5
1.Ελλείψεις προσωπικού	6
15.Ελλείψεις στην αποτελεσματική μεθοδολογία διαχείρισης του έργου	7

20.Έλλειψη εφεδρικού σχεδίου απρόσκοπτης λειτουργίας του συστήματος	8
19.Αδυναμία διαχείρισης προβλημάτων/συμβάντων	9
4.Λάθος ανάπτυξη στο περιβάλλον επικοινωνίας των χρηστών	10

Πίνακας 11: Κατάταξη των Κινδύνων

Εξαιτίας της υποκειμενικότητας που περιέχει η παραπάνω κατάταξη, κρίνεται απαραίτητη η δημιουργία δύο πινάκων που θα ταξινομούν τους κινδύνους αρχικά με βάση την πιθανότητα εμφάνισής τους και στη συνέχεια βάσει των επιπτώσεων που μπορεί να επιφέρουν στους στόχους του έργου. Για τον υπολογισμό της πιθανότητας εμφάνισης ενός κινδύνου χρησιμοποιήσαμε την κλίμακα του Ινστιτούτου Διαχείρισης Έργων (Project Management Institute). Με βάση αυτή την κλίμακα ο χρήστης καλείται να επιλέξει μεταξύ των εξής απαντήσεων:

- Πολύ Χαμηλή
- Χαμηλή
- Μέτρια
- Υψηλή
- Πολύ Υψηλή

Οι απαντήσεις αυτές με τη σειρά που εμφανίζονται λαμβάνουν τα αντίστοιχα ποσοστά: μικρότερο ή ίσο του 10%, 10-30%, 30-50%, 50-70% και τέλος 70-90%. Πιο συγκεκριμένα λοιπόν για τους κινδύνους που εντοπίσαμε οι πιθανότητες εμφάνισής τους δίνονται στον παρακάτω πίνακα:

Κίνδυνος	**Πιθανότητα**				
	Πολύ Χαμηλή	**Χαμηλή**	**Μέτρια**	**Υψηλή**	**Πολύ Υψηλή**
1.Ασαφείς/παρερμηνευμένοι στόχοι και σκοπός του έργου			X		
2.Μη ρεαλιστικά χρονοδιαγράμματα και προϋπολογισμός				X	
3.Ανάπτυξη λανθασμένων λειτουργιών στο λογισμικό	X				
4.Συνεχείς αλλαγές στις απαιτήσεις					X
5.Αποτυχία της Διοίκησης στη συμμετοχή των χρηστών στο έργο		X			

6.Ελλείψεις προσωπικού		X			
7.Ελλείψεις στην αποτελεσματική μεθοδολογία διαχείρισης του έργου		X			
8.Έλλειψη εφεδρικού σχεδίου απρόσκοπτης λειτουργίας του συστήματος				X	
9.Αδυναμία διαχείρισης προβλημάτων/συμβάντων			X		
10.Λάθος ανάπτυξη στο περιβάλλον επικοινωνίας των χρηστών		X			

Πίνακας 12: Πιθανότητα Εμφάνισης των Κινδύνων

Μετά τον πίνακα Πιθανότητας Εμφάνισης των Κινδύνων ακολουθεί ο πίνακας των Συνεπειών που μπορεί να επιφέρει η κάθε απειλή. Για κάθε χαρακτηριστικό του έργου που θίγεται, όπως για παράδειγμα κόστος, αξιοπιστία, χρόνος υλοποίησης και άλλα, χαρακτηρίζεται συνολικά η συνέπεια ως: πολύ χαμηλή αν οι απώλειες είναι μηδαμινές, χαμηλή αν είναι μικρότερες του 5%, ως μέτρια αν πρόκειται το ποσοστό να κυμανθεί ανάμεσα στο 5-10%, υψηλές όταν αναφέρονται στο 10-20% και πολύ υψηλές όταν είναι μεγαλύτερες από το 20% του συνολικού έργου.

Κίνδυνος	**Συνέπειες-Επιπτώσεις**				
	Πολύ Χαμηλή	**Χαμηλή**	**Μέτρια**	**Υψηλή**	**Πολύ Υψηλή**
1.Ασαφείς/παρερμηνευμένοι στόχοι και σκοπός του έργου				X	
2.Μη ρεαλιστικά χρονοδιαγράμματα και προϋπολογισμός					X
3.Ανάπτυξη λανθασμένων λειτουργιών στο λογισμικό			X		
4.Συνεχείς αλλαγές στις απαιτήσεις			X		
5.Αποτυχία της Διοίκησης στη συμμετοχή των χρηστών στο έργο			X		
6.Ελλείψεις προσωπικού				X	
7.Ελλείψεις στην αποτελεσματική μεθοδολογία διαχείρισης του έργου				X	
8.Έλλειψη εφεδρικού σχεδίου απρόσκοπτης λειτουργίας του συστήματος					X
9.Αδυναμία διαχείρισης προβλημάτων/συμβάντων					X
10.Λάθος ανάπτυξη στο περιβάλλον επικοινωνίας των χρηστών			X		

Πίνακας 13: Πιθανότητα Συνεπειών-Επιπτώσεων

Αφού πραγματοποιήθηκε ο εντοπισμός κάθε κινδύνου, η πιθανότητα εμφάνισής του και στη συνέχεια το σύνολο των επιπτώσεων του, σειρά έχει η δημιουργία συγκεντρωτικών πινάκων που θα παρουσιάζουν το επίπεδο της συνολικής έκθεσης του έργου λογισμικού στον κάθε κίνδυνο. Το επίπεδο έκθεσης μπορεί να χαρακτηριστεί είτε ως Υψηλό, είτε ως Μέτριο, είτε ως Χαμηλό. Ανάγκη για άμεσες και ριζικές αλλαγές επιβάλλεται κυρίως στον χαρακτηρισμό «Υψηλό». Σύμφωνα με το πρότυπο του Ινστιτούτου Διαχείρισης Έργων ισχύει ότι:

Έκθεση = Πιθανότητα Εμφάνισης * Επιπτώσεις

Κίνδυνος	**Επίπεδο Έκθεσης**		
	Χαμηλό	**Μέτριο**	**Υψηλό**
1.Ασαφείς/παρερμηνευμένοι στόχοι και σκοπός του έργου		X	
2.Μη ρεαλιστικά χρονοδιαγράμματα και προϋπολογισμός			X
3.Ανάπτυξη λανθασμένων λειτουργιών στο λογισμικό	X		
4.Συνεχείς αλλαγές στις απαιτήσεις		X	
5.Αποτυχία της Διοίκησης στη συμμετοχή των χρηστών στο έργο	X		
6.Ελλείψεις προσωπικού		X	
7.Ελλείψεις στην αποτελεσματική μεθοδολογία διαχείρισης του έργου		X	
8.Έλλειψη εφεδρικού σχεδίου απρόσκοπτης λειτουργίας του συστήματος			X
9.Αδυναμία διαχείρισης προβλημάτων/συμβάντων			X
10.Λάθος ανάπτυξη στο περιβάλλον επικοινωνίας των χρηστών	X		

Πίνακας 14: Έκθεση των Κινδύνων

4.3 Προγραμματισμός Διαχείρισης Κινδύνων

Στη φάση αυτή η ομάδα που ασχολείται με τη διαδικασία διαχείρισης των κινδύνων πρέπει να βρει την κατάλληλη μέθοδο αντιμετώπισης του κάθε κινδύνου. Όπως αναφέρθηκε στο κεφάλαιο 3, οι μέθοδοι αντιμετώπισης των απειλών είναι η αποφυγή, η μεταφορά, η μείωση/μετριασμός και η αποδοχή.

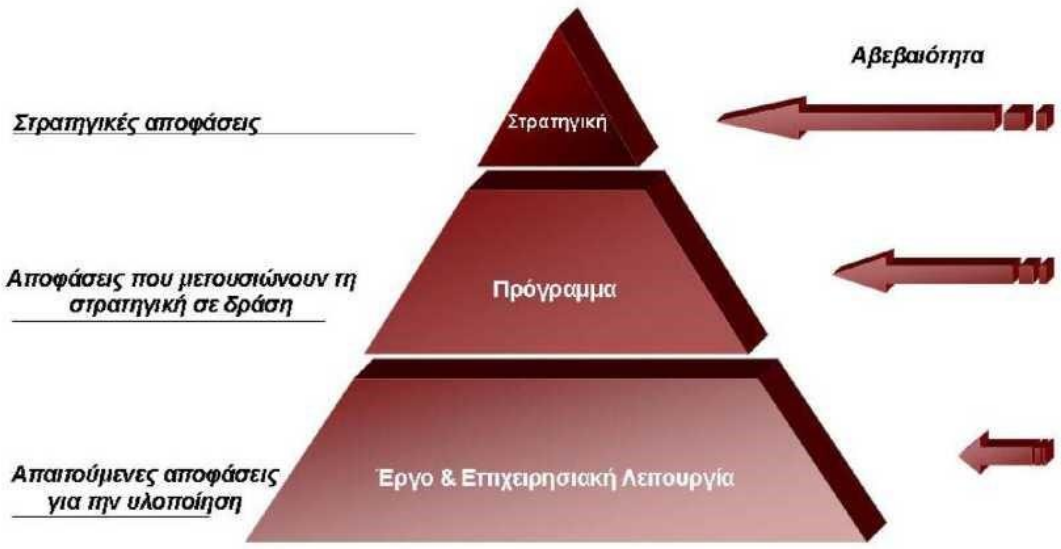
Η επιλογή της κατάλληλης στρατηγικής σχετίζεται με τη σοβαρότητα της συνέπειας και της φύσης του κινδύνου, καθώς και την επάρκεια των πόρων. Στον παρακάτω πίνακα θα αναφερθούν οι κίνδυνοι και η μέθοδος αντιμετώπισης του καθενός.

Κίνδυνος	**Μέθοδοι Αντιμετώπισης**
1.Ασαφείς/παρερμηνευμένοι στόχοι και σκοπός του έργου	αποφυγή
2.Μη ρεαλιστικά χρονοδιαγράμματα και προϋπολογισμός	μείωση/μετριασμός
3.Ανάπτυξη λανθασμένων λειτουργιών στο λογισμικό	μείωση/μετριασμός
4.Συνεχείς αλλαγές στις απαιτήσεις	μείωση/μετριασμός
5.Αποτυχία της Διοίκησης στη συμμετοχή των χρηστών στο έργο	αποφυγή
6.Ελλείψεις προσωπικού	μείωση/μετριασμός
7.Ελλείψεις στην αποτελεσματική μεθοδολογία διαχείρισης του έργου	μεταφορά
8.Έλλειψη εφεδρικού σχεδίου απρόσκοπτης λειτουργίας του συστήματος	μεταφορά
9.Αδυναμία διαχείρισης προβλημάτων/συμβάντων	μεταφορά
10.Λάθος ανάπτυξη στο περιβάλλον επικοινωνίας των χρηστών	αποφυγή

Πίνακας 15: Σχέδια Αντιμετώπισης Κινδύνων

4.4 Έλεγχος Κινδύνων

Όπως φαίνεται και στο παρακάτω σχήμα, η αβεβαιότητα στη λήψη αποφάσεων είναι φθίνουσα από το στρατηγικό προς το επιχειρησιακό επίπεδο / επίπεδο διαχείρισης έργων. Το επίπεδο εφαρμογής της προτεινόμενης μεθοδολογίας είναι ουσιαστικά το ενδιάμεσο επίπεδο, με έναν σημαντικό βαθμό αβεβαιότητας, που θα πρέπει όμως να ξεπεραστεί αποτελεσματικά, προκειμένου να μετουσιωθεί η στρατηγική σε δράση.



Εικόνα 7: Ιεραρχία του κινδύνου

Στη συνέχεια δίνεται σύντομη περιγραφή των κινδύνων που έχουν προσδιοριστεί, αναφέρονται τα αντίστοιχα KRI που προέρχονται από τη βιβλιοθήκη ITIL, καθώς και το σύνολο των ενεργειών που απαιτούνται για την αντιμετώπισή του κάθε κινδύνου.

1.Ασαφείς/παρερμηνευμένοι στόχοι και σκοπός του έργου

Οι διάφοροι εμπλεκόμενοι σε ένα έργο ανάπτυξης λογισμικού έχουν τους δικούς τους στόχους, οι οποίοι συχνά έρχονται σε αντιπαράθεση. Για παράδειγμα, οι χρήστες απαιτούν ένα φιλικό προς το χρήστη σύστημα με πολλές λειτουργίες για να μπορούν να υποστηρίξουν τα καθήκοντα τους, ενώ από την άλλη πλευρά τα μέλη της ομάδας ανάπτυξης, ένα ισχυρό σύστημα με ενδιαφέρουσες τεχνικές προκλήσεις. Αυτές οι διαφορετικές προσδοκίες δημιουργούν θεμελιώδεις συγκρούσεις και ταυτόχρονα ασαφείς ή παρεξηγημένους στόχους/σκοπούς του έργου.

Κίνδυνος	KRI	Στρατηγική Απάντηση
Ασαφείς/παρερμηνευμένοι στόχοι και σκοπός του έργου	Τεκμηριωμένοι στόχοι, ρόλοι και προσδοκίες, Αριθμός προσδιορισθέντων κινδύνων, Επιπτώσεις των κινδύνων που αναλαμβάνονται στην οργάνωση, Δίαυλοι επικοινωνίας, Αριθμός των νέων υπηρεσιών, Ευθύνες κινδύνου, Συμβάντα λόγω λήψης αποφάσεων, Ποσοστό των στόχων που παρακολουθούνται, Εισαγωγή νέων τεχνολογιών	• Ύπαρξη διαχείρισης καθ' όλη τη διάρκεια του κύκλου ζωής του έργου • Διαχωρισμός του έργου σε ελεγχόμενα τμήματα • Σταθεροποίηση των απαιτήσεων και των προδιαγραφών όσο το δυνατόν νωρίτερα

Πίνακας 16: KRI, Στρατηγική Απάντηση για τον κίνδυνο 1

2.Μη ρεαλιστικά χρονοδιαγράμματα και προϋπολογισμός

Ο κίνδυνος αυτός δημιουργεί δυσκολίες στο σωστό προγραμματισμό του έργου. Το χρονοδιάγραμμα και ο προϋπολογισμός θεωρούνται παράγοντες που είναι δύσκολο να εκτιμηθούν με ακρίβεια και συνέπεια. Πολύ συχνά μάλιστα, οι οργανισμοί ξεκινούν ένα μεγάλο έργο έχοντας υποτιμήσει το μέγεθος και την πολυπλοκότητά του.

Κίνδυνος	KRI	Στρατηγική Απάντηση
Μη ρεαλιστικά χρονοδιαγράμματα και προϋπολογισμός	Τεκμηριωμένοι στόχοι, ρόλοι και προσδοκίες, Ποσοστό των δαπανών πληροφορικής που υπερβαίνουν τον εγκεκριμένο προϋπολογισμό, Δείκτης των έργων / οφέλη μετά την εφαρμογή της στρατηγικής, Ποσοστό κέρδους ανά υπηρεσία, Αριθμός των πόρων, Αριθμός υπηρεσιών που	• Λεπτομερής ανάλυση κόστους • Αναλυτική εκτίμηση χρονοδιαγράμματος • Σχεδιασμός με βάση το κόστος • Σταδιακή ανάπτυξη • Επαναχρησιμοποίηση λογισμικού • Περιορισμός των απαιτήσεων • Συμμόρφωση της υλοποίησης

	σχετίζονται, Αριθμός αναγνωρισμένων κινδύνων, Ενημερώσεις ανάλυσης και επιπτώσεων κινδύνων, Συμβάντα λόγω λήψης αποφάσεων	με το σχέδιο ανάπτυξης λογισμικού • Συνδυασμός των εσωτερικών αξιολογήσεων με τα εξωτερικά σχόλια • Διαχωρισμός του έργου σε ελεγχόμενα τμήματα • Συμμετοχή της Διοίκησης καθ' όλη τη διάρκεια του κύκλου ζωής του έργου • Τακτική αξιολόγηση των κινδύνων • Υπολογισμός του κόστος και των επιπτώσεων που θα έχουν στο χρονοδιάγραμμα οι αλλαγές στις απαιτήσεις και στις προδιαγραφές. • Επανεξέταση της μέχρι τώρα προόδου και θέσπιση των στόχων για την επόμενη φάση του έργου

Πίνακας 17: KRI, Στρατηγική Απάντηση για τον κίνδυνο 2

3. Ανάπτυξη λανθασμένων λειτουργιών στο λογισμικό

Ο κίνδυνος αυτός αναφέρεται τη σωστή λειτουργικότητα του συστήματος τόσο σε επίπεδο χρηστών όσο και από τεχνικής άποψης. Συχνά, οι προγραμματιστές και οι αναλυτές σκέφτονται πρόσθετες δυνατότητες ή αλλαγές στο σύστημα που, κατά την άποψή τους, θα το κάνουν καλύτερο και πιο ελκυστικό. Τα νέα στοιχεία που ενσωματώνονται δεν είναι πάντα εύχρηστα ή μπορεί να αποτελούν περιττές δαπάνες.

Κίνδυνος	KRI	Στρατηγική Απάντηση
Ανάπτυξη λανθασμένων λειτουργιών στο λογισμικό	Αριθμός λειτουργιών με καλή / κακή ανατροφοδότηση, Αριθμός παραπόνων, Αξιολόγηση εμπειρογνωμόνων σχετικά με τις λειτουργίες, Αριθμός δοκιμών,	• Ανάλυση της υπάρχουσας οργάνωσης • Ανάλυση της αποστολής • Εννοιολογική διαμόρφωση των

	Αριθμός προσδιορισθέντων κινδύνων, Αριθμός μεταβλητών που δοκιμάστηκαν, Αριθμός ενδιαφερομένων, Αριθμός σφαλμάτων που εντοπίστηκαν στο «ζωντανό» περιβάλλον και δεν είχαν ανιχνεύθηκαν στο περιβάλλον δοκιμής, Αριθμός προβλημάτων που διαπιστώθηκαν σε κρίσιμα σημεία, Χρόνος δοκιμών, Παρερμηνεία των απαιτήσεων	λειτουργιών • Έρευνες μεταξύ των χρηστών • Προτυποποίηση • Έγκαιρη δημιουργία εγχειριδίων χρηστών • Διαχωρισμός του έργου σε ελεγχόμενα τμήματα • Σταθεροποίηση των απαιτήσεων και των προδιαγραφών όσο το δυνατόν νωρίτερα

Πίνακας 18: KRI, Στρατηγική Απάντηση για τον κίνδυνο 3

4.Συνεχείς αλλαγές στις απαιτήσεις

Καθώς οι ανάγκες των χρηστών αλλάζουν, το ίδιο συμβαίνει και με τις απαιτήσεις του έργου. Η διαχείριση της αλλαγής περιλαμβάνει ένα σύνολο από συνοδευτικές παρεμβάσεις στο έργο, όπως για παράδειγμα, την κατανόηση του κόστους και την εκτίμηση της πιθανής αντίδρασης των θιγόμενων από την αλλαγή τμημάτων του έργου. Συνεχείς και ανεξέλεγκτες αλλαγές στις απαιτήσεις θα οδηγήσουν αναπόφευκτα σε καθυστέρηση στο χρονοδιάγραμμα του έργου.

Κίνδυνος	KRI	Στρατηγική Απάντηση
Συνεχείς αλλαγές στις απαιτήσεις	Αριθμός ενημερώσεων στο πρόγραμμα, Τεκμηριωμένοι στόχοι, ρόλοι και προσδοκίες, Αριθμός μετρήσεων, Ποσοστό των στόχων που παρακολουθούνται, Ποσοστό των νέων υπηρεσιών, Εισαγωγή νέων τεχνολογιών	• Υψηλό κόστος αλλαγών • Σταδιακή ανάπτυξη • Απόκρυψη λεπτομερειών/ Γενίκευση σε επίπεδα • Συμμόρφωση της υλοποίησης με το σχέδιο ανάπτυξης λογισμικού • Ύπαρξη διαχείρισης καθ' όλη τη διάρκεια του κύκλου ζωής του έργου • Ανάπτυξη σχεδίου διαχείρισης της μετάβασης στην νέα κατάσταση • Συμμετοχή των χρηστών

		καθ' όλη τη διάρκεια του κύκλου ζωής του έργου • Εξασφάλιση ότι υπάρχει μια συντονιστική επιτροπή για το έργο • Τακτική αξιολόγηση των κινδύνων

Πίνακας 19: KRI, Στρατηγική Απάντηση για τον κίνδυνο 4

5.Αποτυχία της Διοίκησης στη συμμετοχή των χρηστών στο έργο

Παρόλο που η ιδέα της ανάμειξης του χρήστη στην διαδικασία ανάπτυξης του λογισμικού είναι ελκυστική, η επιτυχία της εξαρτάται από την επιθυμία της Διοίκησης και την δυνατότητα του χρήστη να διαθέσει χρόνο στην ομάδα ανάπτυξης. Συχνά, οι χρήστες έχουν άλλες υποχρεώσεις και δεν μπορούν να έχουν πλήρη συμμετοχή στην ανάπτυξη του λογισμικού ή κάποια μέλη του έργου, μπορεί να μην έχουν τον κατάλληλο χαρακτήρα και προσωπικότητα για συμμετέχουν εντατικά σε μία ομάδα.

Κίνδυνος	KRI	Στρατηγική Απάντηση
Αποτυχία της διαχείρισης στη συμμετοχή των χρηστών στο έργο	Μείωση / αύξηση της ικανοποίησης των χρηστών, Αριθμός αιτήσεων σχετικά με καθυστερήσεις ή παράπονα, Ικανοποίηση των χρηστών ανά υπηρεσία, Αριθμός ατόμων που απάντησαν στα ερωτηματολόγια, Αριθμός των χρηστών που είναι πρόθυμοι να δώσουν ανατροφοδότηση για τις υπηρεσίες, Παρανοήσεις στην επικοινωνία	• Εξασφάλιση ότι υπάρχει μια συντονιστική επιτροπή για το έργο • Συνεχής συμμετοχή χρηστών • Εκπαίδευση των χρηστών σχετικά με τον αντίκτυπο των αλλαγών κατά τη διάρκεια του έργου • Σταθεροποίηση των απαιτήσεων και των προδιαγραφών όσο το δυνατόν νωρίτερα

Πίνακας 20: KRI, Στρατηγική Απάντηση για τον κίνδυνο 5

6.Ελλείψεις προσωπικού

Τα άτομα που εμπλέκονται στο έργο ενδέχεται να μην έχουν επαρκή γνώση της τεχνολογίας, ή της επιχείρησης, ή μπορεί να μην έχουν την εμπειρία να χειριστούν το έργο. Η έλλειψη εμπειρίας, οι ανεπαρκείς δεξιότητες και οι μη ρεαλιστικές προσδοκίες των ικανοτήτων του προσωπικού, αυξάνουν την πιθανότητα εμφάνισης αυτού του κινδύνου και μπορεί να επηρεάσουν το επιθυμητό αποτέλεσμα.

Κίνδυνος	KRI	Στρατηγική Απάντηση
Ελλείψεις Προσωπικού	Τεκμηρίωση, Συχνότητα εκπαίδευσης, Δεξιότητες προσωπικού, Πληρωμές, Ποσοστό των διαύλων επικοινωνίας που χρησιμοποιούνται, Ποσοστό της διαθεσιμότητας, Περιστατικά που προκύπτουν, Παρερμηνεία των απαιτήσεων, Εισαγωγή νέων τεχνολογιών	• Στελέχωση με κορυφαία ταλέντα • Αντιστοίχηση των θέσεων εργασίας • Οικοδόμηση ομάδας • Ανύψωση ηθικού • Πολύπλευρη/διαγώνια κατάρτιση • Έγκαιρη εκπαίδευση ανθρώπων-κλειδιά.

Πίνακας 21: KRI, Στρατηγική Απάντηση για τον κίνδυνο 6

7.Ελλείψεις στην αποτελεσματική μεθοδολογία διαχείρισης του έργου

Η διαδικασία διαχείρισης κινδύνων θα πρέπει να ξεκινάει από την αρχική ενημέρωση σχετικά με το έργο, μέχρι την ολοκλήρωση και την παράδοση του στους χρήστες. Ένα σημαντικό ζήτημα στη διαχείριση κινδύνων είναι πιο μέρος του έργου (κύριος του έργου, ανάδοχος, υπεργολάβοι, προμηθευτές) και με τι κόστος, είναι υπεύθυνο για τον κάθε κίνδυνο. Για παράδειγμα, η κύρια ανησυχία για τον κύριο του έργου εντοπίζεται στον κίνδυνο του να μην ολοκληρωθεί το έργο εντός του χρονικού αλλά και οικονομικού προϋπολογισμού, ο ανάδοχος του έργου επικεντρώνει το ενδιαφέρον του σε κινδύνους που θα επηρεάσουν ενδεχομένως το οικονομικό όφελος του, ενώ οι προγραμματιστές ενδιαφέρονται κυρίως για τους κινδύνους που σχετίζονται με την υλοποίηση και την ασφάλεια του συστήματος.

Κίνδυνος	KRI	Στρατηγική Απάντηση
Ελλείψεις στην αποτελεσματική μεθοδολογία διαχείρισης του έργου	Ποσοστό κατανεμημένων πόρων/προσωπικού, Τεκμηριωμένοι στόχοι, ρόλοι και προσδοκίες, Αναλογία των έργων / οφέλη μετά την εφαρμογή της στρατηγικής, Αριθμός των πόρων, Αριθμός υπηρεσιών που σχετίζονται, Συμβάντα που οφείλονται στη λήψη αποφάσεων, Αποτυχημένες προσδοκίες, Εισαγωγή νέων τεχνολογιών	• Ανάθεση ευθύνης • Τακτική αξιολόγηση των κινδύνων • Διαχωρισμός του έργου σε ελεγχόμενα τμήματα • Υπολογισμός του κόστος και των επιπτώσεων που θα έχουν στο χρονοδιάγραμμα οι αλλαγές στις απαιτήσεις και στις προδιαγραφές • Σταθεροποίηση των απαιτήσεων και των προδιαγραφών όσο το δυνατόν νωρίτερα • Επανεξέταση της μέχρι τώρα προόδου και θέσπιση των στόχων για την επόμενη φάση του έργου

Πίνακας 22: KRI, Στρατηγική Απάντηση για τον κίνδυνο 7

8.Έλλειψη εφεδρικού σχεδίου απρόσκοπτης λειτουργίας του συστήματος

Για τους κινδύνους με ενδεχόμενες σημαντικές επιπτώσεις στο έργο, μπορεί να είναι σκόπιμο να αναπτυχθούν εφεδρικά σχέδια, έτοιμα για εφαρμογή, εφόσον οι προγραμματισμένες δράσεις αντιμετώπισης αποτύχουν και ο κίνδυνος εμφανιστεί. Τα σχέδια έκτακτης ανάγκης είναι κάτι ανάλογο με την προετοιμασία σχεδίων αποκατάστασης από καταστροφές. Ένα εφεδρικό σχέδιο θα πρέπει να είναι πλήρως ορισμένο, προγραμματισμένο και κοστολογημένο. Θα πρέπει επίσης να ορίζονται σαφείς συνθήκες ενεργοποίησης, οι οποίες θα καθορίζουν πότε ο κίνδυνος έχει συμβεί και ως εκ τούτου πότε το εφεδρικό σχέδιο θα πρέπει να εφαρμοστεί. Ο στόχος του σχεδίου έκτακτης ανάγκης είναι η ελαχιστοποίηση των επιπτώσεων του κινδύνου, η πρόληψη των αλυσιδωτών επιπτώσεων του σε άλλους τομείς του έργου, καθώς συμβάλλει και στην αποκατάσταση του ελέγχου του έργου.

Κίνδυνος	KRI	Στρατηγική Απάντηση
Έλλειψη εφεδρικού σχεδίου απρόσκοπτης λειτουργίας του συστήματος	Αριθμός περιστατικών, Αριθμός επαναλαμβανόμενων περιστατικών, Χρόνος επίλυσης, Μέσος χρόνος απόκρισης, Παράπονα χρηστών/πελατών, Αριθμός προβλημάτων που δεν έχουν επιλυθεί, Αριθμός προβλημάτων που καθυστερεί η επίλυσή τους, Αριθμός διακοπών του συστήματος, Στατιστικά χρήσης του συστήματος	• Λειτουργία συστημάτων UPS • Ύπαρξη ομάδων standby από εξειδικευμένα άτομα για δυνατότητα υποστήριξης 24/7 • Διαρκείς έλεγχοι στον όγκο δεδομένων των εφαρμογών και στην αποθηκευτική ικανότητα του συστήματος • Αποτελεσματική και αδιάλειπτη λειτουργία της διαδικασίας backup για τις εφαρμογές. • Δημιουργία disaster recovery site σε εναλλακτική τοποθεσία με δυνατότητα πλήρους επαναφοράς του συστήματος και των εφαρμογών σε ελάχιστο χρόνο • Υλοποίηση της διαδικασίας online replication από την κύρια στην εναλλακτική τοποθεσία

Πίνακας 23: KRI, Στρατηγική Απάντηση για τον κίνδυνο 8

9.Αδυναμία διαχείρισης προβλημάτων/συμβάντων

Ο μοναδικός τρόπος αντιμετώπισης των προβλημάτων και των δυσκολιών που ανακύπτουν στην πορεία εκτέλεσης των εργασιών είναι η γνωστοποίηση όλων των πτυχών σε όλους τους εμπλεκόμενους και η εφαρμογή της καλύτερης λύσης που θα δοθεί από τα πιο έμπειρα στελέχη της ομάδας.

Η λύση των προβλημάτων απαιτεί μία διαδικασία τεσσάρων βημάτων:

- Ορισμός του προβλήματος
- Εντοπισμός της αιτίας του προβλήματος
- Προσδιορισμός πιθανών λύσεων
- Απομάκρυνση της αιτίας ή λήψη διορθωτικής ενέργειας

Η έγκαιρη αναγνώριση των μελλοντικών προβλημάτων και η προετοιμασία βάσει σχεδίου, αυξάνουν τις πιθανότητες επιτυχίας του έργου και μειώνουν τις συγκρούσεις.

Κίνδυνος	KRI	Στρατηγική Απάντηση
Αδυναμία διαχείρισης προβλημάτων/ συμβάντων	Αριθμός περιστατικών, Αριθμός επαναλαμβανόμενων περιστατικών, Μέσος χρόνος απόκρισης, Χρόνος επίλυσης, Προσπάθεια επίλυσης αυτών των περιστατικών, Αριθμός αιτήσεων, Αριθμός προβλημάτων που δεν έχουν επιλυθεί, Αριθμός συμβάντων ανά γνωστό πρόβλημα	• Προσπάθεια εντοπισμού της πηγής του προβλήματος • Προσδιορισμός του λόγου που δεν έχει επιλυθεί το πρόβλημα • Αξιολόγηση του αντίκτυπου της επανάληψης ενός προβλήματος στον οργανισμό • Προσπάθεια εντοπισμού των περιστατικών όσο το δυνατόν νωρίτερα • Διαμόρφωση εργαλείων διαχείρισης γεγονότων • Διαθεσιμότητα πληροφοριών από γνωστά σφάλματα (θα δώσει τη δυνατότητα στο προσωπικό διαχείρισης συμβάντων να μάθει από προηγούμενα περιστατικά και να αναζητήσει τρόπους αντιμετώπισης) • Ύπαρξη ειδικευμένου προσωπικού στις δοκιμές και στον έλεγχο ποιότητας • Παρότρυνση όλου του προσωπικού (τεχνικές ομάδες καθώς και χρήστες) να καταγράφει όλα τα περιστατικά που προκύπτουν • Κίνητρα στο προσωπικό για να χρησιμοποιεί τη βάση δεδομένων της γνώσης • Ενθάρρυνση της χρήσης web-based εφαρμογών αυτοβοήθειας (οι οποίες μπορούν να επιταχύνουν την αντιμετώπιση των κινδύνων και να μειώσουν τις

		απαιτήσεις σε πόρους) • Συνεχής δίαυλος επικοινωνίας μεταξύ της ομάδας διαχείρισης συμβάντων και της ομάδας διαχείρισης προβλημάτων

Πίνακας 24: KRI, Στρατηγική Απάντηση για τον κίνδυνο 9

10.Λάθος ανάπτυξη στο περιβάλλον επικοινωνίας των χρηστών

Το περιβάλλον επικοινωνίας των χρηστών ενσωματώνει μια πληθώρα εργαλείων, στο κέντρο των οποίων βρίσκεται η δημιουργία περιεχομένου από τους ίδιους τους χρήστες, η διαμοίραση υλικού πολλαπλών μορφών, η ανοιχτή επικοινωνία και η αλληλεπίδραση μεταξύ τους. Επιπλέον, παρέχει τη δυνατότητα άμεσης συγκέντρωσης και εκμετάλλευσης της γνώσης των χρηστών για διάφορα ζητήματα με σκοπό την υιοθέτηση κατευθύνσεων και τη λήψη αποφάσεων.

Κίνδυνος	KRI	Στρατηγική Απάντηση
Λάθος ανάπτυξη στο περιβάλλον επικοινωνίας των χρηστών	Αριθμός λειτουργιών με καλή / κακή ανατροφοδότηση, Αριθμός παραπόνων, Αξιολόγηση εμπειρογνωμόνων σχετικά με τις λειτουργίες, Αριθμός δοκιμών, Αριθμός προσδιορισθέντων κινδύνων, Αριθμός μεταβλητών που δοκιμάστηκαν, Αριθμός ενδιαφερομένων, Αριθμός σφαλμάτων που εντοπίστηκαν στο «ζωντανό» περιβάλλον και δεν είχαν ανιχνευθεί στο περιβάλλον δοκιμής, Αριθμός προβλημάτων που διαπιστώθηκαν σε κρίσιμα σημεία, Χρόνος δοκιμών	• Προτυποποίηση των σεναρίων, ανάλυση εργασιών • Διαχωρισμός του έργου σε ελεγχόμενα τμήματα • Ανάλυση της υπάρχουσας οργάνωσης • Εννοιολογική διαμόρφωση των λειτουργιών • Έρευνες μεταξύ των χρηστών • Προτυποποίηση • Έγκαιρη δημιουργία εγχειριδίων χρηστών • Σταθεροποίηση των απαιτήσεων και των προδιαγραφών όσο το δυνατόν νωρίτερα

Πίνακας 25: KRI, Στρατηγική Απάντηση για τον κίνδυνο 10

4.5 Παρακολούθηση Κινδύνων

Κατά τη διάρκεια του κύκλου ζωής ενός έργου μπορεί να εμφανιστούν νέοι κίνδυνοι, να αυξηθεί ή να μειωθεί η έκθεση παλιότερων κινδύνων, ή να παρατηρηθεί ότι δεν είναι αποτελεσματικά τα σχέδια αντιμετώπισης που έχουν οριστεί από την ομάδα διαχείρισης. Για τους παραπάνω λόγους γίνεται αντιληπτό ότι η παρακολούθηση των κινδύνων αποτελεί ουσιαστικά μια επαναληπτική διαδικασία και όχι το τελευταίο στάδιο της διαχείρισης κινδύνων.

Οι βασικές λειτουργίες που γίνονται σε αυτό το στάδιο είναι οι εξής:

- Παρακολούθηση των προσδιορισμένων κινδύνων
- Παρακολούθηση υλοποίησης ενεργειών αντιμετώπισης των κινδύνων
- Εντοπισμός νέων κινδύνων
- Διαχείριση νέων κινδύνων που εμφανίζονται
- Έλεγχος των σχεδίων αντιμετώπισης κινδύνων
- Αναθεώρηση των σχεδίων αντιμετώπισης

4.6 Φύλλα Κινδύνου

Όλη η διαδικασία της διαχείρισης των κινδύνων, καταγράφεται σε ειδικές φόρμες που ονομάζονται «φύλλα κινδύνων» (risk sheets).

Συγκεκριμένα, το φύλλο κινδύνου:

- Αποτελεί το βασικό εργαλείο της διαδικασίας Διαχείρισης Κινδύνου
- Αναφέρεται σε ένα συγκεκριμένο πίνακα και εκεί καταγράφονται όλες οι απαραίτητες ενέργειες για την διαχείριση των παραγόντων κινδύνου που έχουν προσδιοριστεί.
- Απαιτεί τον καθορισμό του πιθανού Υπεύθυνου Διαχείρισης για κάθε παράγοντα κινδύνου

Δύο ενδεικτικά παραδείγματα φύλλων κινδύνου φαίνονται στους παρακάτω πίνακες (πηγή IRM).

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #1				
Προσδιορισμός κινδύνου				
Όνομα κινδύνου :	Ανάπτυξη λανθασμένων λειτουργιών στο λογισμικό			
Σύντομη περιγραφή :	Ελλιπής δημιουργία της βάσης δεδομένων. Κατά τη μεταφορά δεδομένων προέκυψε κακή αντιστοίχιση δεδομένων.			
Κατηγορία κινδύνου :	Τεχνολογικός			
Ημερομηνία αναγνώρισης :	26/05/2014			
Υπεύθυνος:	Η. Αυγερίκου - Σαμωνά			
Ανάλυση κινδύνου				
Πιθανότητα εμφάνισης	Συνέπεια / επίπτωση	Έκθεση	Προτεραιότητα	Ημερομηνία ενημέρωσης
1	3	1	4	27/05/2014
Αντιμετώπιση κινδύνου				
Δείκτης παρακολούθησης:	Αξιολόγηση εμπειρογνωμόνων σχετικά με τις λειτουργίες			
Προπομπός κινδύνου :	Σε κάποια έκδοση η βάση δεδομένων δε λειτουργεί σωστά στο σύστημα testing (UAT – Users Acceptance Testing)			
Στρατηγική αντιμετώπισης :	Μείωση/Μετριασμός			
Ημερομηνία Ενημέρωσης :	27/05/2014			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα :	Έγκαιρη διάγνωση του κινδύνου, μεγαλύτερη συχνότητα UAT			
Διορθωτικά μέτρα :				
Εναλλακτικό σχέδιο :				
Σχέδιο μετάπτωσης :				
Σχέδιο αποφυγής :				
Σχέδιο μεταφοράς :				
Σχέδιο αποδοχής :				
Παρακολούθηση κινδύνου				
Παρακολούθηση :	Καθημερινή			
Κατάσταση :	Ανοιχτή			
Ημερομηνία Κλεισίματος :				
Ημερομηνία Ελέγχου :	30/05/2014			

Πίνακας 26: Φύλλο Κινδύνου #1

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #2				
Προσδιορισμός κινδύνου				
Όνομα κινδύνου :	Συνεχείς αλλαγές στις απαιτήσεις			
Σύντομη περιγραφή :	Νέα προσθήκη στις απαιτούμενες λειτουργίες της εφαρμογής με αποτέλεσμα την ανακατασκευή μεγάλου μέρους αυτής.			
Κατηγορία κινδύνου :	Εξωτερικός			
Ημερομηνία αναγνώρισης :	29/05/2014			
Υπεύθυνος:	Η. Αυγερίκου - Σαμωνά			
Ανάλυση κινδύνου				
Πιθανότητα εμφάνισης	Συνέπεια / επίπτωση	Έκθεση	Προτεραιότητα	Ημερομηνία ενημέρωσης
4	3	2	2	30/05/2014
Αντιμετώπιση κινδύνου				
Δείκτης παρακολούθησης:	Ανάπτυξη σχεδίου διαχείρισης της μετάβασης στην νέα κατάσταση			
Προπομπός κινδύνου :	Ύπαρξη εντόνων αντιδράσεων από την ομάδα εργασίας			
Στρατηγική αντιμετώπισης :	Μείωση/Μετριασμός			
Ημερομηνία Ενημέρωσης :	30/05/2014			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα :	Έγκαιρη διάγνωση του κινδύνου, ενημέρωση της Διοίκησης			
Διορθωτικά μέτρα :				
Εναλλακτικό σχέδιο :	Συχνότερες ενημερωτικές συναντήσεις			
Σχέδιο μετάπτωσης :				
Σχέδιο αποφυγής :				
Σχέδιο μεταφοράς :				
Σχέδιο αποδοχής :				
Παρακολούθηση κινδύνου				
Παρακολούθηση :	Εβδομαδιαία			
Κατάσταση :	Ανοιχτή			
Ημερομηνία Κλεισίματος :				
Ημερομηνία Ελέγχου :	30/05/2014			

Πίνακας 27: Φύλλο Κινδύνου #2

4.7 Αποτελέσματα

Η εφαρμογή του παραπάνω μοντέλου στη μηχανογράφηση ενός μεγάλου Τραπεζικού Ιδρύματος, έδωσε τη δυνατότητα για την αξιολόγηση της προτεινόμενης μεθοδολογίας και τον έλεγχο της αξιοπιστίας των αποτελεσμάτων που παρέχει.

Εκ των πραγμάτων, η πλήρης εφαρμογή της μεθοδολογίας σε όλο της το εύρος δεν είναι εφικτή στα πλαίσια μιας ερευνητικής εργασίας, επιπλέον για να γίνει σωστή αξιολόγηση όλων των παραμέτρων και συστατικών της, απαιτείται η παρακολούθησή της για ένα μεγάλο χρονικό διάστημα.

Παρ' όλα αυτά η έστω και περιορισμένη πιλοτική εφαρμογή της μεθοδολογίας, με πραγματικά δεδομένα και καταστάσεις, ήταν ιδιαίτερα χρήσιμη και συνέβαλλε σε μεγάλο βαθμό στην επίδειξη των πλεονεκτημάτων της και στην ενθάρρυνση για ευρεία εφαρμογή της. Με βάση μάλιστα τις εκτιμήσεις των συμμετεχόντων στη διαδικασία πιλοτικής εφαρμογής, το προτεινόμενο μοντέλο ανάλυσης και διαχείρισης κινδύνου χαρακτηρίστηκε ως ιδιαίτερα εύχρηστο, αξιόπιστο και λειτουργικό.

5. Συμπεράσματα και μελλοντικές επεκτάσεις

Σε αυτό το κεφάλαιο αναφέρονται τα συμπεράσματα που απορρέουν από την παρούσα εργασία, καθώς και οι μελλοντικές επεκτάσεις της έρευνας που πραγματοποιήθηκε.

5.1 Συμπεράσματα

Η κατανόηση των παραγόντων που συμβάλλουν στον κίνδυνο των έργων λογισμικού γίνεται όλο και πιο απαραίτητη τα τελευταία χρόνια. Αυτό είναι αποτέλεσμα του μεγέθους, της πολυπλοκότητας και της στρατηγικής σημασίας των πληροφοριακών συστημάτων που αναπτύσσονται διεθνώς.

Η προτεινόμενη μεθοδολογία αποτελεί ένα ολοκληρωμένο και συνεκτικό πλαίσιο διαχείρισης κινδύνου σε έργα λογισμικού. Κύριο στόχο αποτελεί η ενσωμάτωση σε μια ολοκληρωμένη μεθοδολογία όλων των διαδικασιών και μεθοδολογιών ανάλυσης και διαχείρισης κινδύνου, με βάση την οποία θα πραγματοποιείται διαχείριση των κινδύνων συνολικά ενός προγράμματος, αλλά και διαχείριση κινδύνων των επιμέρους έργων, τόσο ως προς την παρακολούθηση και διαχείρισή τους, όσο και ως προς τον έλεγχο των οικονομικών τους στοιχείων και των παραμέτρων απόδοσης.

Συνοπτικά, τα γενικά συμπεράσματα που απορρέουν από την ανάλυση που παρατέθηκε στα προηγούμενα κεφάλαια έχουν ως εξής:

- Η αναπτυχθείσα μεθοδολογία αντιμετωπίζει με ενιαίο και συνεκτικό τρόπο το πρόβλημα της διαχείρισης κινδύνου.
- Η αναπτυχθείσα μεθοδολογία ενσωματώνει σε μια γενική προσέγγιση μεθοδολογίες και πρακτικές από τον χώρο της διαχείρισης κινδύνου, καθώς και από τον χώρο του εσωτερικού ελέγχου.
- Η αναπτυχθείσα μεθοδολογία προτείνει κατάλληλο πλαίσιο ομαδικής διαχείρισης κινδύνων, με ομαδικές ανασκοπήσεις μεταξύ όλων των εμπλεκόμενων φορέων.
- Η πιλοτική εφαρμογή της μεθοδολογίας στην διαχείριση κινδύνων ενός μεγάλου Τραπεζικού Ιδρύματος, επιβεβαίωσε τη λειτουργικότητά της, την αξιοπιστία των παραγόμενων αποτελεσμάτων και την αποτελεσματικότητά της.

5.2 Μελλοντικές Επεκτάσεις

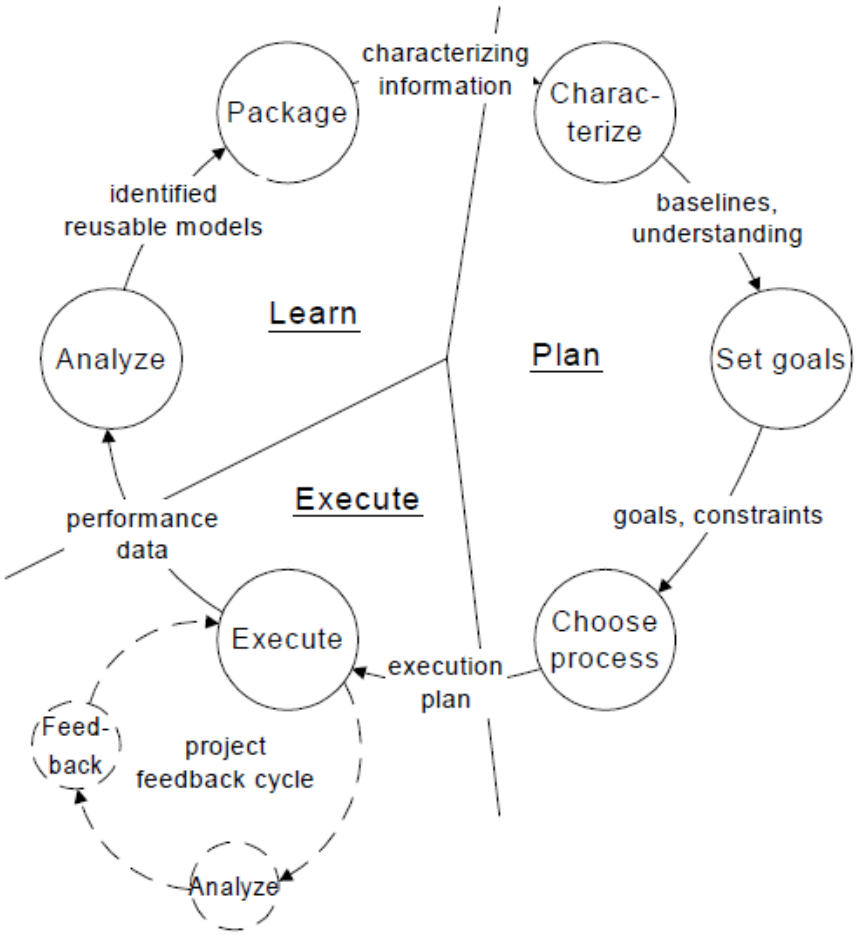
Σε αυτή την ενότητα θα παρουσιάσουμε πως η μέθοδος **RiskIT** μπορεί να ενσωματωθεί ή να συνεργαστεί με άλλα πλαίσια.

5.2.1 QIP

Η **QIP** (Quality Improvement Paradigm) είναι μια συστηματική διαδικασία για συνεχή βελτίωση των υπηρεσιών διαχείρισης κινδύνων και αποτελείται από έξι βασικές δραστηριότητες [12]:

1. **Χαρακτηρισμός (Characterize):** Κατανόηση του περιβάλλοντος με βάση τα διαθέσιμα δεδομένα, τα πρότυπα, την εμπειρία και τις γνώσεις. Καθιέρωση και δημιουργία μιας βάσης με τις υφιστάμενες διαδικασίες της οργάνωσης και χαρακτηρισμός της κρισιμότητας αυτών των διεργασιών.
2. **Ορισμός στόχων (Set goals):** Με βάση το χαρακτηρισμό του περιβάλλοντος, καθορισμός μετρήσιμων στόχων για το έργο και την οργανωτική απόδοση και βελτίωση.
3. **Επιλογή διαδικασίας (Choose process):** Με βάση το χαρακτηρισμό και τους στόχους, θα επιλεγούν οι διαδικασίες, τα εργαλεία και οι τεχνικές που είναι κατάλληλες για το έργο, αφού επιβεβαιωθεί ότι συνάδουν με τους στόχους και τους περιορισμούς που έχουν καθοριστεί.
4. **Εκτέλεση (Execute):** Εκτέλεση των επιλεγμένων διαδικασιών και παροχή ενημέρωσης σχετικά με την πρόοδο.
5. **Ανάλυση (Analyze):** Στο τέλος κάθε έργου, αναλύονται τα στοιχεία και οι πληροφορίες που συγκεντρώθηκαν για να αξιολογηθούν οι τρέχουσες πρακτικές, να καθοριστούν τα προβλήματα και να διατυπωθούν συστάσεις για μελλοντικά έργα.
6. **Πακέτο (Package):** Αποθήκευση της εμπειρίας που αποκτήθηκε με τη μορφή νέων ή επικαιροποιημένων μοντέλων, εγγράφων και άλλων μορφών γνώσης.

Ο κύκλος της QIP μπορεί επίσης να θεωρηθεί ότι αποτελείται από τρεις διαφορετικές λειτουργίες: τον προγραμματισμό, την εκτέλεση και τη μάθηση, όπως φαίνεται στην Εικόνα 8. Η εικόνα δείχνει επίσης και την εσωτερική ανάδραση που χρησιμοποιείται για τον έλεγχο του έργου.

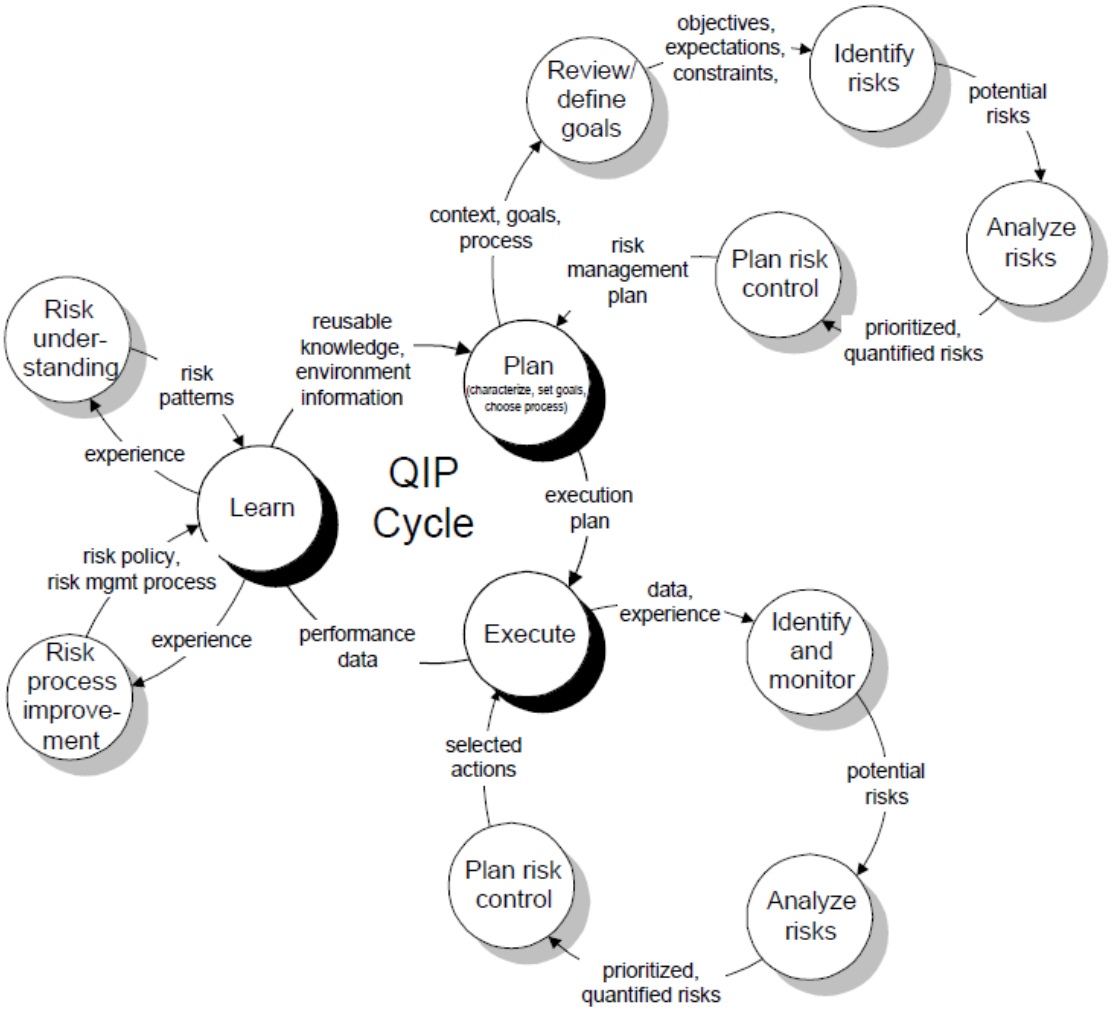


Εικόνα 8: Ο κύκλος και οι λειτουργίες της QIP

Όταν εφαρμοστεί και ολοκληρωθεί η διαδικασία RiskIT, αντιμετωπίζεται από τη σκοπιά και την εμπειρία της QIP, για να προσδιορίσουν τα στάδια όπου η διαδικασία διαχείρισης των κινδύνων πρέπει να βελτιωθεί.

Ο **σχεδιασμός** αντιπροσωπεύει τον πρώτο κύκλο της διαδικασίας RiskIT, ενώ ο κύκλος της διαχείρισης κινδύνων τροφοδοτεί το βήμα της **εκτέλεσης** των επιλεγμένων διαδικασιών για να πραγματοποιηθεί η παρακολούθηση και ο έλεγχος των κινδύνων. Το στάδιο της **μάθησης** αναλύει την εμπειρία και τα δεδομένα που συλλέχτηκαν σχετικά με τους κινδύνους και παράγει «πακεταρισμένα» και επαναχρησιμοποιήσιμα κομμάτια γνώσης, τα οποία στη συνέχεια αποθηκεύονται στη βάση δεδομένων της γνώσης για να χρησιμοποιηθούν σε μελλοντικά έργα.

Όλες οι δραστηριότητες της QIP και της RiskIT απεικονίζονται στην Εικόνα 9.

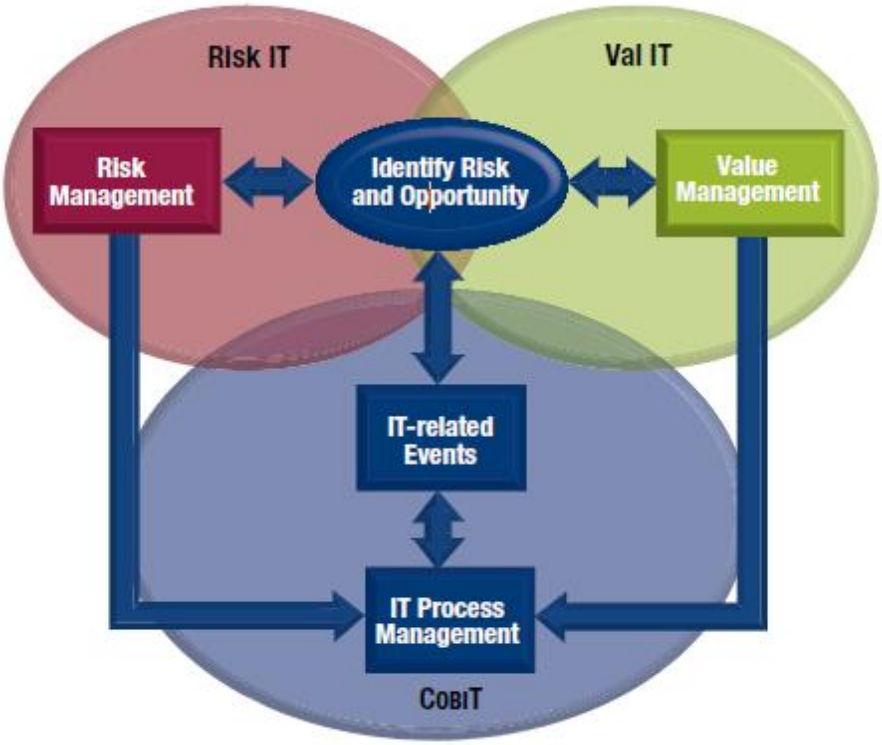


Εικόνα 9: Οι δραστηριότητες της QIP και της RiskIT

5.2.2 COBIT και Val IT

Το πλαίσιο ελέγχου **COBIT** (Control Objectives for Information and Related Technology) αναπτύχθηκε από την ISACA και είναι ένα σύνολο πολιτικών, διαδικασιών, πρακτικών και οργανωσιακών δομών σχεδιασμένων να παρέχουν ασφάλεια σχετικά με το ότι οι επιχειρηματικοί στόχοι θα υλοποιηθούν και οποιεσδήποτε αρνητικές καταστάσεις θα παρεμποδιστούν, θα εξαλειφθούν ή θα διορθωθούν. Το πλαίσιο Val IT περιγράφει πώς πρέπει να υλοποιηθούν οι διαδικασίες με απώτερο σκοπό τη μεγιστοποίηση της απόδοσης του οργανισμού.

Η παρακάτω εικόνα δείχνει την αλληλεπίδραση της διαδικασίας RiskIT με τα πλαίσια COBIT και Val IT [5].

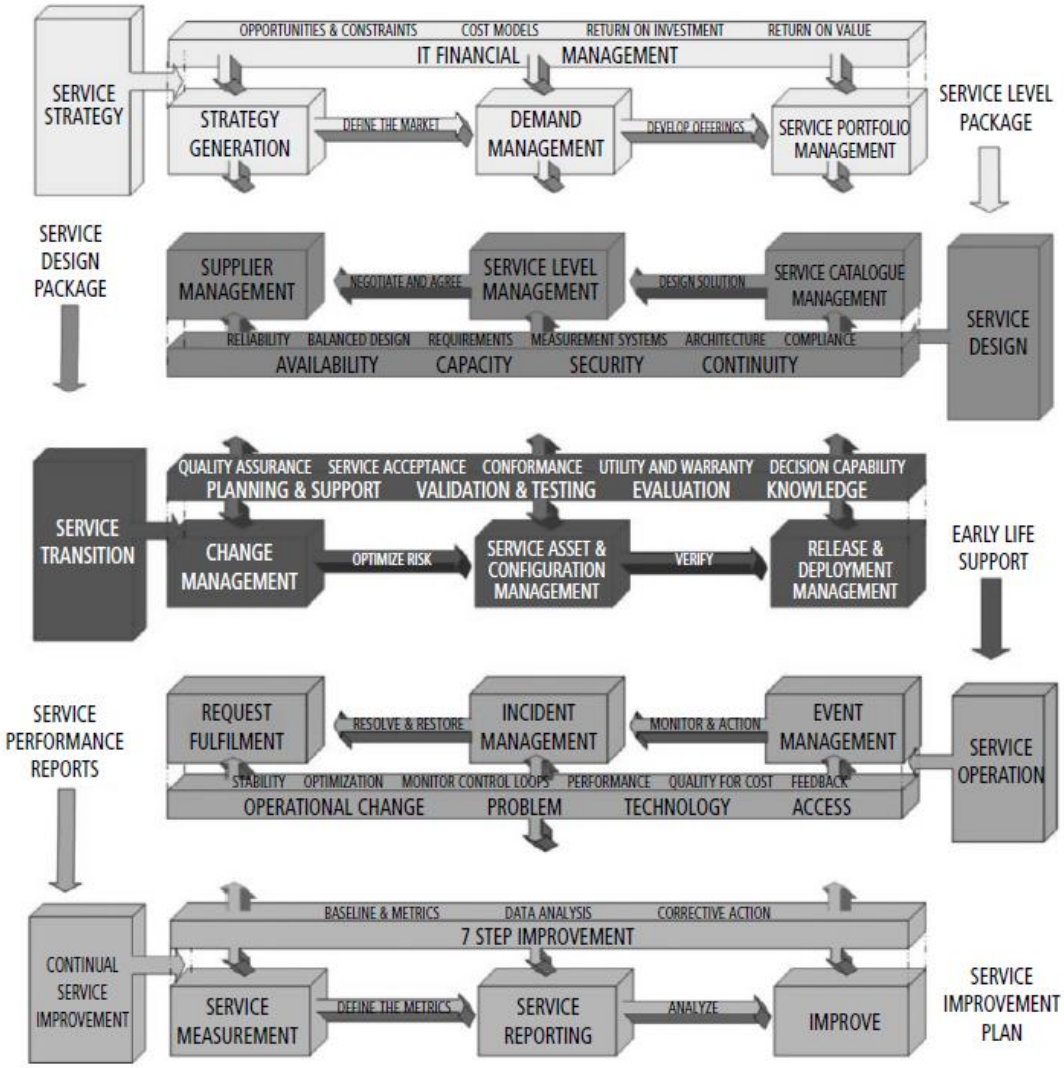


Εικόνα 10: Αλληλεπίδραση της RiskIT με τα πλαίσια COBIT και Val IT.

Η συνεργασία αυτών των πλαισίων έχει ως στόχο να αναπτύξει και προωθήσει ένα επίσημο, έγκυρο, διεθνές σύνολο γενικώς αποδεκτών προτύπων για την τεχνολογία των πληροφοριακών συστημάτων, για καθημερινή χρήση από τους διευθυντές και τους ελεγκτές, πλαίσιο αναφοράς για σκοπούς ελέγχου Πληροφοριακών Συστημάτων και βασικές πρακτικές που υποστηρίζουν την αποτελεσματική εφαρμογή της Εταιρικής Διακυβέρνησης μέσω της Πληροφορικής.

5.2.3 Κατασκευή λογισμικού Διαχείρισης Κινδύνου

Όπως θα παρατηρήσατε η διαχείριση κινδύνου είναι μια πολύπλοκη και χρονοβόρα διαδικασία. Η πολυπλοκότητα αυτή θα αυξηθεί με μια δυναμική ενσωμάτωση της βιβλιοθήκης ITIL στη μέθοδο RiskIT [8]. Αυτό φαίνεται από την επόμενη εικόνα:



Εικόνα 11: Η απεικόνιση των διαδικασιών της ITIL σε υψηλό επίπεδο

Είναι πλέον σαφές ότι για την εφαρμογή της διαχείρισης κινδύνου σε επιχειρησιακό επίπεδο, με μια ολοκληρωμένη μεθοδολογία, θα πρέπει να υπάρχει μια αυτοματοποιημένη διαδικασία η οποία θα υλοποιείται και θα ελέγχεται από ένα λογισμικό το οποίο:

- χρησιμοποιεί αλγορίθμους υψηλού επιπέδου
- ενσωματώνει όλες τις διαδικασίες της μεθοδολογίας
- βασίζεται σε ένα DBMS για την διαχείριση των δεδομένων
- θα μπορεί να εξάγει τις απαραίτητες αναφορές για κάθε διαδικασία
- θα λειτουργεί σαν σύστημα συναγερμού για τις επιπτώσεις των κινδύνων
- θα έχει την μορφή client-server για χρήση από μεγάλο αριθμό ενδιαφερομένων
- θα έχει δυνατότητες διασύνδεσης με λογισμικά διαχείρισης έργου
- θα έχει εύχρηστο περιβάλλον για τους χρήστες

Η κατασκευή ενός λογισμικού με τις προδιαγραφές που αναφέραμε είναι ο επόμενος στόχος μας και ελπίζουμε να τον υλοποιήσουμε είτε με την εκπόνηση διδακτορικής διατριβής, η οποία θα επεκτείνει την παρούσα εργασία, είτε με πιθανή συνεργασία μας με κάποιο Μεγάλο Οργανισμό.

Αναφορές

[1] PMI, A guide to the project management body of knowledge: PMBOK guide. - 3rd ed., Project Management Institute, 2004. pp. 8, 237-268.

[2] "Critical Success Factors". Retrieved 29/5/2014, from http://www.mindtools.com/pages/article/newLDR_80.htm

[3] Mark Beasley, Bruse Branson, Bonnie Hancock, Developing Key Risk Indicators to strengthen Enterprise Risk Management. Coso, 2010. pp. 1-5.

[4] Cruz M., Modeling Measuring and Hedging Operational Risk, John Wiley & Sons, LTD, 2002. pp. 233-270.

[5] The RiskIT Framework, ISACA, 2009, ISBN 978-1-60420-111-6. pp. 13, 28, 31-33.

[6] Jyrki Kontio, The Riskit Method for Software Risk Management, version 1.00, Computer Science Technical Reports. University of Maryland. USA, 1997. pp. 14-41.

[7] Jake Kouns and Daniel Minoli, Information Technology Risk Management In Enterprise Environments. Canada: Willey, 2010. pp. 11, 92-94, 130-136.

[8] Alison Cartlidge, Ashley Hanna, Colin Rudd, Ivor Macfarlane, John Windebank, Stuart Rance. An Introductory Overview of ITIL V3. itSMF Ltd, 2007. pp. 12-40, 50.

[9] Graham Williams, Everything you wanted to know about Management of Risk (M_o_R) in less than 1000 words. White Paper. The Stationery Office: 2011. pp. 3.

[10] Michael Dallas, Management of Risk: Guidance for Practitioners and the international standard on risk management, ISO 31000:2009, APM Group Ltd, Whitepaper, 2013, pp. 5.

[11] Barry W. Boehm, Software Risk Management: Principles and Practices, 1991. pp. 13.

[12] Jyrki Kontio, Software Engineering Risk Management, Doctoral Dissertation, Helsinki University of Technology, 2001. pp. 101-106.

Βιβλιογραφία

Wideman M., Project and program risk management: a guide to managing project risks and opportunities, PMI, 1992.

Kevin Forsberg, Hal Mooz, Visualizing Project Management, Models and frameworks for mastering complex systems, Third Edition, PMP, CSEP - Howard Cotterman, John Wiley & Sons, Inc., 2005

B.W. Boehm, Tutorial: Software Risk Management, IEEE Computer Society Press, 1989.

Neumann, P., Computer-Related Risks, Addison-Wesley, 2000.

Davidson Frame J., Managing Risk in Organizations: A Guide for Managers. Jossey-Bass, 2003.

R. N. Charette, Software Engineering Risk Analysis and Management, New York: McGraw-Hill, 1989.

J. V. Michaels, Technical Risk Management, Upper Saddle River, NJ: Prentice Hall, 1996.

V.R. Basili, M.V. Zelkowitz, F. McGarry, J. Page, S. Waligora, and R. Pajerski, Software Process Improvement Program IEEE Software, 1995.