Πανεπιστήμιο Πειραιώς

Τμήμα Ψηφιακών Συστημάτων

Π.Μ.Σ. Ψηφιακά Συστήματα & Υπηρεσίες

Κατεύθυνση: Δικτυοκεντρικά Πληροφοριακά Συστήματα

Διπλωματική Εργασία:

«Διαχείριση Κινδύνου Δικτυοκεντρικού Συστήματος»

ΔΕΛΙΟΣ ΙΓΝΑΤΙΟΣ ΜΕ 11057

Επιβλέπων: Θεμιστοκλέους Μαρίνος

ΠΕΡΙΕΧΟΜΕΝΑ

ΛΙΣΤΑ ΠΙΝΑΚΩΝ

ΛΙΣΤΑ ΕΙΚΟΝΩΝ

ΚΕΦΑΛΑΙΟ 1

1.1. Περίληψη

Ένα έργο Πληροφορικής μεγάλου μεγέθους και πολυπλοκότητας εμπεριέχει ποικίλους κινδύνους που απειλούν την επιτυχία της εφαρμογής του. Στην σύγχρονη εποχή όπου οι νέες τεχνολογίες και τα πληροφορικά συστήματα έχουν εισβάλλει σημαντικά στην καθημερινότητά μας, συναντάται συχνά το φαινόμενο από οργανισμούς να βασίζουν ένα μεγάλο μέρος της λειτουργίας τους σε αυτά. Η παραμικρή δυσλειτουργεία, η διακοπή ή η παράνομη διείσδυση στα συστήματα αυτά μεταφράζεται σε κόστος είτε από άμεσες οικονομικές απώλειες είτε από αδυναμία του οργανισμού να λειτουργήσει αποδοτικά. Για να αποφευχθεί ένα σύνολο από ποικίλες απειλές που επιφέρει η υλοποίηση ενός έργου πληροφορικής μεγάλου μεγέθους και αξιόλογου προϋπολογισμού, κρίνεται απαραίτητη η επισήμανση και η αντιμετώπιση των κινδύνων που μπορούν να προκληθούν σε όλα τα στάδια επίτευξής του.

Σκοπός της Διπλωματικής αυτής Εργασίας είναι η περιγραφή των τεχνικών αναγνώρισης και αντιμετώπισης των πιθανών κινδύνων. Πιο συγκεκριμένα παρουσιάστηκαν όλα τα στάδια της διαδικασίας διαχείρισης κινδύνων 1) Εκτίμηση κινδύνων, 2) Επιλογή μεθόδων αντιμετώπισης κινδύνων και 3) Παρακολούθηση σχεδίου αντιμετώπισης κινδύνων. Κατά την εκτίμηση κινδύνων έγινε η παρουσίαση κάποιων πιθανών κινδύνων, των μεθόδων αξιολόγησης της σοβαρότητας αυτών, ως προς την πιθανότητα εμφάνισής τους και το μέγεθος των επιπτώσεών τους, στο επόμενο στάδιο προτάθηκαν μέθοδοι και πολιτικές αντιμετώπισής τους και στο τελευταίο παρουσιάστηκαν οι μέθοδοι παρακολούθησης του σχεδίου προστασίας του έργου.

Στο τέλος έγινε η εφαρμογή των διαδικασιών διαχείρισης κινδύνων στο έργο « ***Fleetbroadband Provisioning System*** ». Για το έργο αυτό απαριθμήθηκαν οι πληροφορίες που πρέπει να αναζητηθούν, οι κίνδυνοι που το απειλούν, έγινε αξιολόγηση της πιθανότητας εμφάνισης και των επιπτώσεων αυτών των κινδύνων και προτάθηκαν μέθοδοι αντιμετώπισης αυτών ανάλογα με την αξία του μετριασμού τους για την πορεία υλοποίησης του έργου.

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

1.2. Αντικείμενο της Εργασίας

Τα αντικείμενα της έρευνας είναι η θεωρητική ανάλυση της έννοιας «Διαχείριση Κινδύνων» μέσω της σχετικής βιβλιογραφίας, η διερεύνηση μίας μελέτης περίπτωσης (case study / use case) και η μελέτη και ανάλυση ενός συστήματος σχετικό με τη μελέτη περίπτωσης και τη διαχείριση κινδύνων.

Θεωρητική ανάλυση: Ανάλυση των βασικών εννοιών της έρευνας, του κύκλου ζωής της διαχείρισης κινδύνων και των μεθοδολογιών ασφάλειας των πληροφοριακών συστημάτων.

Μελέτη περίπτωσης: Ανάλυση του πληροφοριακού συστήματος Fleetbroadband Provisioning System το οποίο στη συνέχεια θα συνδεθεί με τη διαχείριση κινδύνων.

Μελέτη συστήματος: Ανάλυση της λειτουργίας του πληροφοριακού συστήματος Fleetbroadband Provisioning System, των προβλημάτων που παρουσιάστηκαν κατά τη διάρκειά της και της διαδικασίας διαχείρισης κινδύνων που έπρεπε να έχει λάβει χώρα ώστε να μειωθούν ή να αποφευχθούν τα προβλήματα αυτά.

1.3. Σκοπός και αντικειμενικοί στόχοι

Σκοπός της εργασίας είναι η ανάλυση της έννοιας «διαχείριση κινδύνου» και η μελέτη των παραγόντων που την πλαισιώνουν. Μέσα από αυτή την έρευνα θα γίνουν πλήρως κατανοητοί οι παράγοντες αυτοί και να είναι εφικτή η άρτια αντιμετώπιση του ρίσκου σε οποιαδήποτε δραστηριότητα ή έργο.

1.4. Δομή εργασίας

Η παρούσα εργασία αποτελείται από 7 κεφάλαια.
Στο **κεφάλαιο 1** γίνεται αναφορά στις έννοιες του κινδύνου, της διαχείρισης αυτού και του έργου και προσδιορίζονται ο σκοπός και τα αντικείμενα της έρευνας.
Στο **κεφάλαιο 2** δίνεται αναλυτικά η βιβλιογραφική επισκόπηση της έρευνας. Αρχικά, δίνονται κάποια γενικά στοιχεία για το έργο (project) και στη συνέχεια αναλύεται η έννοια της διαχείρισης κινδύνου (risk management) και ο κύκλος ζωής αυτής.
Στο **κεφάλαιο 3** αναφέρονται κάποια γενικά στοιχεία για τα πληροφοριακά έργα και τη σημαντικότητα της διαχείρισης κινδύνου σε αυτά. Επίσης αναφέρονται οι κυριότεροι μηχανισμοί ασφαλείας.

Στο **κεφάλαιο 4** αναφέρονται κάποια γενικά στοιχεία για την υπηρεσία Fleetbroadband και τον Inmarsat. Επίσης γίνεται μια γενική και τεχνική περιγραφή του δικτύου BGAN και τι είδους υπηρεσίες το Fleetbroadband Provisioning System.

Στο **κεφάλαιο 5** αναφέρεται η βασική περιγραφή του πληροφοριακού συστήματος Fleetbroadband Provisioning System καθώς και στην συνέχεια γίνεται ανάλυση αυτού.

Στο **κεφάλαιο 6** αναλύεται η διαδικασία διαχείρισης κινδύνων του συστήματος Fleetbroadband Provisioning System, λαμβάνοντας υπ' όψιν τα προβλήματα που προέκυψαν κατά τη διάρκεια της λειτουργίας του.

Στο **κεφάλαιο 7** αναφέρονται τα συμπεράσματα της έρευνας.

ΚΕΦΑΛΑΙΟ 2

2.1 Κίνδυνος

Ορισμός

Ο κίνδυνος γενικά μπορεί να ορισθεί ως ο συνδυασμός της πιθανότητας ενός γεγονότος και των συνεπειών του. Σε όλους τους τύπους των δραστηριοτήτων, υπάρχει το ενδεχόμενο για γεγονότα και συνέπειες που συνιστούν ευκαιρίες προς όφελος ή απειλές της επιτυχίας.

Η έννοια του κινδύνου χρησιμοποιείται παγκόσμια σε διαφορετικές εννοιολογικές περιοχές. Για παράδειγμα ενώ στον οικονομικό τομέα χρησιμοποιείται για να δηλώσει την πιθανότητα να συμβεί μια οικονομική απώλεια, στον ιατρικό τομέα χρησιμοποιείται για να δηλώσει την πιθανότητα μιας δυσλειτουργίας στην ζωή ενός ανθρώπου.

Στον τομέα της πληροφορικής η έννοια του κινδύνου είναι συνυφασμένη με σφάλματα ή προβλήματα που μπορεί να προκύψουν κατά την λειτουργία ενός πληροφοριακού συστήματος (πρόβλημα υλικού ή λογισμικού).

Στα έργα πληροφορικής δίνεται ιδιαίτερη έμφαση στους κινδύνους που προκύπτουν από τον κώδικα του λογισμικού, τις συγχωνεύσεις εταιρειών (συνένωση των πληροφοριακών συστημάτων των εταιρειών) και τις συμβάσεις για την συντήρηση των πληροφοριακών συστημάτων.

2.2 Διαχείριση Κινδύνου (Risk Management)

Η πιο απλή ερμηνεία για το τι είναι η διαχείριση κινδύνων είναι αυτό που υποδηλώνει και ο τίτλος της, δηλαδή είναι ένας τρόπος για το πώς να διαχειριζόμαστε και να αντιμετωπίζουμε κινδύνους. Πιο αναλυτικά μπορούμε να πούμε ότι συμπεριλαμβάνει όλες τις ενέργειες που εκτελούνται για να ελαχιστοποιηθούν οι αβεβαιότητες που συνδέονται με συγκεκριμένες δραστηριότητες ή γεγονότα. Στα πλαίσια των έργων η διαχείριση κινδύνων μειώνει τις επιπτώσεις των ανεπιθύμητων γεγονότων σε ένα έργο.

Η διαχείριση κινδύνων σε οποιοδήποτε έργο απαιτεί την λήψη αποφάσεων σε συγκεκριμένες δραστηριότητες που εκτελούνται.

2.3 Κύκλος Ζωής Διαχείριση Κινδύνου

Ένα έργο διαχείρισης κινδύνου περιλαμβάνει τις διαδικασίες του σχεδιασμού, του καθορισμού, της ανάλυσης, του σχεδιασμού αντιμετώπισης και της παρακολούθησης και ελέγχου του έργου.

Οι αντικειμενικοί στόχοι ενός έργου της διαχείρισης κινδύνου είναι να αυξήσει την πιθανότητα και την επίδραση των θετικών γεγονότων και να μειώσει την πιθανότητα και την επίδραση των αρνητικών γεγονότων σε ένα έργο.

Ο κίνδυνος είναι ένα γεγονός ή μια κατάσταση που με την εμφάνιση του σε ένα έργο μπορεί να έχει επίδραση σε τουλάχιστον έναν αντικειμενικό στόχο του έργου. Οι στόχοι ενός έργου μπορεί να περιλαμβάνουν παραμέτρους του όπως είναι το εύρος, ο σχεδιασμός, το κόστος και η ποιότητα του. Ένας κίνδυνος μπορεί να έχει ένα ή περισσότερα αίτια και αν προκύψει μπορεί να έχει μία ή περισσότερες επιδράσεις. Μια αιτία μπορεί να είναι μια απαίτηση, μια υπόθεση, ένας περιορισμός, ή μια περίπτωση που δημιουργεί την πιθανότητα αρνητικών ή θετικών αποτελεσμάτων. Ο κίνδυνος ενός έργου έχει τις ρίζες του στην αβεβαιότητα που είναι υπαρκτή σε όλα τα έργα.

Γνωστοί κίνδυνοι είναι αυτοί που έχουν προσδιοριστεί και αναλυθεί καθιστώντας δυνατό τον σχεδιασμό αντιμετώπισης τους. Ορισμένοι άγνωστοι κίνδυνοι δεν μπορούν να είναι διαχειρίσιμοι προληπτικά με αποτέλεσμα η ομάδα έργου θα πρέπει να δημιουργήσει ένα σχεδιασμό ενδεχομένων.

Οι οργανισμοί και οι επιχειρήσεις αντιλαμβάνονται τον κίνδυνο σαν αποτέλεσμα της αβεβαιότητας στους στόχους τους. Οι οργανισμοί και οι εμπλεκόμενοι σε ένα έργο είναι πρόθυμοι να αποδεχτούν ποικίλες βαθμίδες κινδύνων. Αυτό ονομάζεται ανοχή κινδύνου. Οι κίνδυνοι που αποτελούν απειλή για ένα έργο μπορεί να γίνουν αποδεκτοί εάν βρίσκονται μέσα στα όρια της ανοχής κινδύνου και σε ισορροπία με τις ανταμοιβές που μπορεί να αποκομιστούν λαμβάνοντας αποφάσεις που εμπεριέχουν τους κινδύνους αυτούς.

Τα άτομα και οι ομάδες υιοθετούν συμπεριφορές προς τον κίνδυνο οι οποίες επηρεάζουν τον τρόπο που αντιδρούν. Αυτές οι συμπεριφορές καθοδηγούνται από την αντίληψη της κάθε ομάδας, τις ανοχές και άλλους παράγοντες που θα πρέπει να γίνονται σαφείς όποτε είναι δυνατό.

Σε κάθε έργο θα πρέπει να αναπτύσσεται μια συνεκτική προσέγγιση σε σχέση με τον κίνδυνο ενώ θα πρέπει να υπάρχει συνεχής επικοινωνία για τον κάθε πιθανό κίνδυνο και τον χειρισμό του.

Η απόκριση κάθε οργανισμού ως προς τους κινδύνους αντανακλά τον τρόπο που αντιλαμβάνονται την αποφυγή ή την επιλογή του κινδύνου.

Για να είναι επιτυχής στην ολοκλήρωση κάθε έργου ένας οργανισμός, θα πρέπει να δεσμεύεται πως θα ασχολείται με τη διαχείριση κινδύνου προληπτικά και με συνέπεια σε όλη τη διάρκεια ζωής του έργου. Θα πρέπει να γίνεται μια συνειδητή επιλογή προσδιορισμού των κινδύνων και να επιδιώκεται μια

αποτελεσματική διαχείριση κινδύνου ενός έργου σε όλα τα επίπεδα ενός οργανισμού ή μιας επιχείρησης. Ο κίνδυνος υπάρχει σε ένα έργο πριν ακόμα αρχίσει να υλοποιείται.

Προχωρώντας με την έναρξη ενός έργου χωρίς να έχει γίνει προηγουμένως προληπτικά μια προσεκτική διαχείριση κινδύνου, αυξάνει την επίδραση ενός κινδύνου που ενδεχομένως να παρουσιαστεί και είναι περισσότερο πιθανό να οδηγήσει στην αποτυχία του έργου.
Ένα έργο διαχείρισης κινδύνου αποτελείται από τις εξής διαδικασίες:

- **Σχεδιασμός Διαχείρισης Κινδύνου**

Είναι η διαδικασία ορισμού των ενεργειών διεξαγωγής της διαχείρισης κινδύνου σε ένα έργο.

- **Αναγνώριση Κινδύνων**

Είναι η διαδικασία καθορισμού των πιθανών κινδύνων που μπορεί να επηρεάσουν το έργο και η καταγραφή των χαρακτηριστικών τους.

- **Ποιοτική Ανάλυση Κινδύνων**

Είναι η διαδικασία ιεράρχησης των κινδύνων για περαιτέρω ανάλυση. Σε αυτή την ανάλυση γίνεται και η αξιολόγησή τους μέσω του συνδυασμού της πιθανότητας να συμβούν και της επίδρασής τους.

- **Ποσοτική Ανάλυση Κινδύνων**

Είναι η διαδικασία αριθμητικής ανάλυσης της επίδρασης των κινδύνων που έχουν καθοριστεί σε όλο το εύρος του έργου.

- **Σχεδιασμός Απόκρισης Κινδύνων**

Είναι η διαδικασία ανάπτυξης επιλογών και ενεργειών για να ενισχύσουν τις ευκαιρίες και να μειώσουν τις απειλές που θα υπάρξουν κατά τη διάρκεια του έργου.

- **Παρακολούθηση και Έλεγχος Κινδύνων**

Είναι η διαδικασία εφαρμογής του σχεδίου αντιμετώπισης κινδύνων, παρακολούθησης των προσδιορισμένων κινδύνων, καθορισμός νέων κινδύνων και αξιολόγηση της αποτελεσματικότητας της διαδικασίας διαχείρισης κινδύνου σε όλο το έργο.

2.3.1 Σχεδιασμός Διαχείρισης Κινδύνου

Ο σχεδιασμός της διαχείρισης κινδύνου είναι η διαδικασία καθορισμού των ενεργειών της διαχείριση κινδύνου που θα διεξαχθούν για το έργο. Ο προσεκτικός και σαφής σχεδιασμός ενισχύει την πιθανότητα της επιτυχίας για τις επόμενες 5 διαδικασίες διαχείρισης κινδύνου όπως παρουσιάζονται στη συνέχεια.
Ο σχεδιασμός της διαχείρισης κινδύνου είναι σημαντικό να εξασφαλίσει ότι ο βαθμός και ο τύπος της διαχείρισης κινδύνου είναι ανάλογα με τους κινδύνους και τη σπουδαιότητα του έργου στον οργανισμό. Ο σχεδιασμός είναι επίσης σημαντικό να παρέχει επαρκείς πόρους και χρόνο για τις δραστηριότητες της διαχείρισης του κινδύνου. Επίσης κατά το σχεδιασμό θα πρέπει να δημιουργηθεί μια συμφωνημένη βάση για την αξιολόγηση των κινδύνων. Η διαδικασία του σχεδιασμού της διαχείρισης κινδύνου πρέπει να ξεκινά πριν την έναρξη του έργου και να ολοκληρώνεται κατά τη διάρκεια του σχεδιασμού του έργου. Οι βασικές πληροφορίες που είναι απαραίτητες και πρέπει να προσδιοριστούν για το σωστό σχεδιασμό αναλύονται στη συνέχεια.

- **Καθορισμός πλαισίου του έργου**

Δίνει μια γενική άποψη για το έργο και για την επίδραση της διαχείρισης κινδύνου σε αυτό.

- **Σχεδιασμός Διαχείρισης Κόστους**

Αποτελεί σημαντική πληροφορία η γνώση του προϋπολογισμού διαχείρισης κινδύνου.

- **Σχεδιασμός Διαχείρισης Προγραμματισμού**

Είναι απαραίτητη η γνώση του προγράμματος εργασιών για τον χρονικό προσδιορισμός της διαχείρισης κινδύνου.

- **Σχεδιασμός Διαχείρισης Επικοινωνίας**

Είναι σημαντικό να υπάρχει επικοινωνία μεταξύ των ομάδων του έργου για τη σωστή διαχείριση κινδύνου.

- **Περιβαλλοντικοί Παράγοντες Επιχείρησης**

Επηρεάζουν την συμπεριφορά μιας επιχείρησης στην αντιμετώπιση των κινδύνων.

- **Περιουσιακά στοιχεία επιχείρησης**

Τα περιουσιακά στοιχεία της επιχείρησης που μπορεί να επηρεάσουν τη διαδικασία σχεδιασμού διαχείρισης κινδύνων περιλαμβάνουν:

- Κατηγορίες κινδύνων
- Ορισμούς κανόνων
- Πρότυπα έκθεσης κινδύνων
- Ρόλοι και υπευθυνότητες
- Επιχειρησιακά επίπεδα αποφάσεων
- Μητρώα εμπλεκομένων

2.3.2 Αναγνώριση Κινδύνων

Η αναγνώριση κινδύνων είναι η διαδικασία προσδιορισμού των κινδύνων που μπορούν να επηρεάσουν ένα έργο και η καταγραφή των χαρακτηριστικών τους. Οι εμπλεκόμενοι στις ενέργειες προσδιορισμού των κινδύνων είναι οι ακόλουθοι:
Ο διευθυντής του έργου, τα μέλη της ομάδας έργου, η ομάδα διαχείρισης κινδύνου, οι πελάτες, οι τελικοί χρήστες, οι εμπλεκόμενοι και οι ειδικοί διαχείρισης κινδύνου. Η αναγνώριση κινδύνων είναι μια επαναληπτική διαδικασία καθώς νέοι κίνδυνοι μπορεί να εξελιχθούν ή να εμφανιστούν κατά τη διάρκεια

του κύκλου ζωής του έργου. Η συχνότητα επανάληψης της διαδικασίας και οι συμμετέχοντες κάθε φορά μπορεί να είναι διαφορετικοί.

Η μορφή της διαχείρισης των κινδύνων πρέπει να μοιάζει σε όλες τις περιπτώσεις για να είναι δυνατή η σύγκριση των επιδράσεων των κινδύνων στο έργο.
Για τον προσδιορισμό των κινδύνων θα πρέπει ιδανικά να γνωρίζουμε τα εξής:

- **Σχεδιασμός διαχείρισης κινδύνου**

Είναι η διαδικασία ορισμού των ενεργειών διεξαγωγής της διαχείρισης κινδύνου σε ένα έργο.

- **Εκτίμηση κόστους δραστηριοτήτων**

Το κόστος κάθε δραστηριότητας καθορίζει το κατά πόσο θα ληφθεί ή όχι σοβαρά υπόψη η δραστηριότητα στην διαχείριση κινδύνου.

- **Εκτίμηση της διάρκειας της κάθε δραστηριότητας**

Σημαντικό ρόλο στη διαχείριση κινδύνου παίζουν τα επιτρεπτά χρονικά περιθώρια της κάθε δραστηριότητας ή ολόκληρου του έργου.

- **Εύρος και πλαίσιο έργου**

Θα πρέπει να ληφθούν υπόψη οι διάφορες υποθέσεις όσον αφορά το πλαίσιο του έργου, και η πιθανότητα να συμβεί κάποια από αυτές.

- **Εμπλεκόμενοι στο έργο**

Οι πληροφορίες όσον αφορά τους εμπλεκόμενους στο έργο είναι πολύ χρήσιμες καθώς αυτοί μπορεί να καθορίσουν τους κινδύνους του έργου.

- **Σχεδιασμός Διαχείρισης Κόστους**

Αποτελεί σημαντική πληροφορία η γνώση του προϋπολογισμού διαχείρισης κινδύνου.

- **Σχεδιασμός Διαχείρισης Προγραμματισμού**

Η αναγνώριση των κινδύνων απαιτεί και την καλή γνώση του προγράμματος εργασιών.

- **Σχεδιασμός Ποιότητας**

Η αναγνώριση των κινδύνων απαιτεί τη γνώση των απαιτούμενων ποιοτικών χαρακτηριστικών των εργασιών.

- **Έγγραφα έργου**

Είναι σημαντικό να γνωρίζουμε τα έγγραφα του έργου που περιγράφουν διεργασίες ή περιλαμβάνουν πληροφορίες που μπορεί να φανούν χρήσιμες στη διαχείριση κινδύνου.

- **Περιβαλλοντικοί παράγοντες**

Όπως και στο σχεδιασμό του κινδύνου, έτσι και στον καθορισμό τους, είναι καλό να υπάρχει γνώση των περιβαλλοντικών παραγόντων.

- **Περιουσιακά στοιχεία επιχείρησης**

Τα περιουσιακά στοιχεία της επιχείρησης που μπορεί να επηρεάσουν τη διαδικασία σχεδιασμού διαχείρισης κινδύνων περιλαμβάνουν:

  - Αρχεία έργου
  - Διαδικασίες ελέγχου έργου
  - Πρότυπα έκθεσης κινδύνων

Αναγνώριση κινδύνων: Εργαλεία και Τεχνικές

- **Έγγραφα Ολοκληρωμένων Έργων**

Μια ολοκληρωμένη ανασκόπηση των εγγράφων ενός έργου, που περιλαμβάνει τα σχέδια, τις υποθέσεις, συμβόλαια και προηγούμενα αρχεία έργων, καθώς επίσης και οποιαδήποτε άλλη πληροφορία.

- **Τεχνικές Συλλογής Πληροφοριών**

Μερικά παραδείγματα συλλογής πληροφοριών που χρησιμοποιούνται για τον προσδιορισμό κινδύνων:

- **Brainstorming**

Ο σκοπός του brainstorming είναι να δημιουργηθεί μια περιεκτική λίστα κινδύνων του έργου. Η ομάδα έργου χρησιμοποιεί το brainstorming συνήθως σε μια ομάδα ειδικών που δεν αποτελούν μέρος της ομάδας ανάλυσης κινδύνου. Η διαδικασία του brainstorming συντονίζεται από ένα άτομο, και χρησιμοποιεί είτε αδόμητη συζήτηση, είτε μια περισσότερο δομημένη διαδικασία. Είναι δυνατό να χρησιμοποιηθούν κατηγορίες κινδύνων, όπως μια αναλυτική δομή (πίνακας) κινδύνων ως βάση για τη διαδικασία. Οι κίνδυνοι που παράγονται από τη συζήτηση αυτή κατηγοριοποιούνται με βάση τους τύπους κινδύνου και γίνονται πιο σαφείς.

- **Τεχνική Delphi**

Η τεχνική Delphi είναι ένας τρόπος να αποκτήσεις την κοινή συναίνεση των ειδικών. Οι ειδικοί κινδύνου του έργου συμμετέχουν σε αυτή τη διαδικασία ανώνυμα. Ο συντονιστής χρησιμοποιεί ένα ερωτηματολόγιο για να συλλέξει ιδέες για σημαντικούς κινδύνους του έργου. Οι απαντήσεις συλλέγονται και στη συνέχεια δίνονται πάλι στους ειδικούς για περαιτέρω σχολιασμό. Η απαραίτητη συναίνεση όσον αφορά τους κινδύνους, δίνεται μετά από μερικές επαναλήψεις της διαδικασίας. Η τεχνική Delphi βοηθάει στην αποφυγή πόλωσης όσον αφορά τα δεδομένα και αποτρέπει αδικαιολόγητη επιρροή ενός ατόμου στο τελικό αποτέλεσμα.

- **Συνεντεύξεις**

Οι συνεντεύξεις έμπειρων στελεχών του έργου, των εμπλεκομένων και διάφορων ειδικών του έργου μπορεί να οδηγήσει στον προσδιορισμό κινδύνων.

- **Ανάλυση αιτίου – αποτελέσματος**

Η ανάλυση αυτή αποτελεί μια συγκεκριμένη τεχνική για τον προσδιορισμό ενός προβλήματος, τα υποκείμενα αίτια που οδηγούν σε αυτό, ενώ επίσης οδηγεί και στην ανάπτυξη προληπτικών ενεργειών.

- **Ανάλυση Λίστας Ελέγχου**

Οι λίστες προσδιορισμού κινδύνων αναπτύσσονται βασισμένες σε ιστορικά δεδομένα και συσσωρευμένες γνώσεις από προηγούμενα έργα, καθώς και από άλλες πηγές πληροφοριών. Τα κατώτερα στρώματα της δομής πόρων του έργου μπορεί επίσης να χρησιμοποιηθούν ως λίστα ελέγχου κινδύνων. Ενώ μια τέτοια λίστα μπορεί να είναι γρήγορη και απλή, είναι αδύνατο να είναι πολύ αναλυτική. Η ομάδα κινδύνου θα πρέπει να είναι σίγουρη πως υπάρχουν κίνδυνοι που δεν εμφανίζονται στη λίστα. Η λίστα μπορεί μετά το τέλος του έργου να χρησιμοποιηθεί ξανά και να ενσωματωθεί σε μελλοντικά έργα.

- **Ανάλυση Υποθέσεων**

Κάθε έργο και κάθε προσδιορισμένος κίνδυνος έργου είναι βασισμένος σε υποθέσεις. Η ανάλυση υποθέσεων ερευνά την εγκυρότητα των υποθέσεων σε περίπτωση που εμφανιστούν στο έργο. Επίσης προσδιορίζει τους κινδύνους του έργου λόγω ανακριβειών, ασταθών παραγόντων, ασυνεπειών ή και ανολοκλήρωτων υποθέσεων.

- **Τεχνικές Διαγραμμάτων**

Οι τεχνικές διαγραμμάτων περιλαμβάνουν:

- Διαγράμματα αιτίων και αποτελεσμάτων. Αυτά είναι επίσης γνωστά ως διαγράμματα Ishikawa και είναι χρήσιμα για τον προσδιορισμό αιτίων κινδύνων.
- Διαγράμματα ροής διαδικασιών. Αυτά δείχνουν τον τρόπο με τον οποίο τα διάφορα στοιχεία του συστήματος συσχετίζονται.
- Διαγράμματα επιρροής. Είναι γραφικές αναπαραστάσεις καταστάσεων που δείχνουν επιρροές και άλλες σχέσεις μεταξύ μεταβλητών και αποτελεσμάτων.

- **Ανάλυση SWOT**

Η τεχνική αυτή εξετάζει το έργο από όλες τις πλευρές SWOT (strengths – δυνάμεις, weaknesses – αδυναμίες, opportunities – ευκαιρίες, και threats – απειλές), και τον τρόπο με τον οποίο οι εσωτερικές αυτές παράμετροι είναι δυνατό να αυξήσουν τα αρνητικά αποτελέσματα των κινδύνων. Η τεχνική αρχίζει με τον προσδιορισμό των δυνάμεων και των αδυναμιών της επιχείρησης, εστιάζοντας είτε στην οργάνωση του έργου, είτε στην ευρύτερη επιχείρηση. Ο προσδιορισμός των παραγόντων αυτών γίνεται συνήθως με τη χρήση της τεχνικής brainstorming. Στη συνέχεια η ανάλυση SWOT προσδιορίζει οποιεσδήποτε ευκαιρίες που είναι δυνατό να προκύψουν εκμεταλλευόμενοι τις δυνάμεις της επιχείρησης, και τις απειλές που μπορεί να εμφανιστούν λόγω των αδυναμιών της. Η ανάλυση SWOT επίσης εξετάζει το βαθμό στον οποίο οι δυνάμεις της επιχείρησης αντισταθμίζουν τις απειλές και οι ευκαιρίες που παρουσιάζονται μπορεί να χρησιμοποιηθούν για να ξεπεραστούν οι αδυναμίες.

- **Κρίση Εμπειρογνωμόνων**

Οι κίνδυνοι μπορεί να προσδιοριστούν απευθείας από ειδικούς με σχετική εμπειρία σε παρόμοια έργα ή σε αντίστοιχους επιχειρηματικούς τομείς. Τέτοιοι ειδικοί θα πρέπει να βρίσκονται από τον project manager του έργου και να καλούνται ώστε να εξετάσουν όλες τις πτυχές του έργου ώστε να προτείνουν πιθανούς κινδύνους βασισμένοι σε προηγούμενη εμπειρία. Η γνώμη των ειδικών θα πρέπει να λαμβάνεται υπόψη σε αυτή τη διαδικασία.

Αναγνώριση κινδύνων: Συμπεράσματα

- **Μητρώο Κινδύνων**

Τα βασικά συμπεράσματα της διαδικασίας Αναγνώρισης Κινδύνων αποτελούν τις αρχικές εισόδους στο μητρώο κινδύνων. Το μητρώο αυτό περιέχει τελικά τα αποτελέσματα άλλων διαδικασιών διαχείρισης κινδύνου, που έχουν ως αποτέλεσμα αύξηση του επιπέδου και του περιεχομένου της πληροφορίας που αφορά τους κινδύνους κατά τη διάρκεια του χρόνου. Η προετοιμασία του μητρώου κινδύνων αρχίζει με τη διαδικασία Αναγνώρισης Κινδύνων (με τις πληροφορίες που παρουσιάζονται στη συνέχεια) και στη συνέχεια γίνεται διαθέσιμο και στις υπόλοιπες διαδικασίες project και risk management.

- **Λίστα προσδιορισμένων κινδύνων**

Οι προσδιορισμένοι κίνδυνοι περιγράφονται με τις απαραίτητες λεπτομέρειες ώστε να γίνονται κατανοητοί. Η δομή των κινδύνων της λίστας θα πρέπει να είναι απλή και να αναφέρει το γεγονός που μπορεί να εμφανιστεί, προκαλώντας κάποια επίπτωση, ή κάποιο αίτιο που μαζί με ένα γεγονός θα επιφέρει κάποια αποτελέσματα. Επιπλέον, οι αιτίες των κινδύνων μπορεί να γίνουν περισσότερο προφανείς μέσα από αυτή τη διαδικασία. Οι αιτίες αυτές αποτελούν θεμελιώδεις προϋποθέσεις για την αύξηση των προσδιορισμένων κινδύνων και θα πρέπει να καταγράφονται για να χρησιμοποιηθούν σε μελλοντικό προσδιορισμό των κινδύνων του υπάρχοντος ή κάποιου μελλοντικού έργου.

- **Λίστα πιθανών αποκρίσεων**

Οι πιθανές αποκρίσεις σε έναν κίνδυνο μπορεί ορισμένες φορές να προσδιοριστούν κατά τη διάρκεια της διαδικασίας Σχεδιασμού Αποκρίσεων Κινδύνων

2.3.3 Ποιοτική Ανάλυση Κινδύνων

Είναι η διαδικασία ιεράρχησης των κινδύνων για περαιτέρω ανάλυση. Σε αυτή την ανάλυση γίνεται και η αξιολόγησή τους μέσω του συνδυασμού της πιθανότητας να συμβούν και της επίδρασής τους. Οι οργανισμοί μπορούν να βελτιώσουν την επίδοση σε ένα έργο εστιάζοντας σε κινδύνους υψηλή προτεραιότητας. Η διαδικασία Ποιοτικής Ανάλυσης Κινδύνου αξιολογεί την προτεραιότητα των προσδιορισμένων κινδύνων χρησιμοποιώντας τη σχετική πιθανότητα εμφάνισης, τις αντίστοιχες επιδράσεις στο έργο με την εμφάνιση κάποιου κινδύνου καθώς επίσης και άλλους παράγοντες όπως ο χρόνος απόκρισης κα η ανοχή της εταιρίας στον κίνδυνο που σχετίζεται με μεγέθη όπως είναι το κόστος, ο προγραμματισμός, το εύρος του έργου και η ποιότητα. Η αποτελεσματική αξιολόγηση των κινδύνων θα πρέπει να λαμβάνει σοβαρά υπόψη τις διάφορες συμπεριφορές απέναντι στον κίνδυνο των βασικών συμμετεχόντων στη διαδικασία ποιοτικής ανάλυσης κινδύνου. Όπου εμφανίζονται τέτοιες συμπεριφορές και δημιουργούν προβλήματα στην αξιολόγηση των κινδύνων θα πρέπει να λαμβάνονται και οι αντίστοιχες διορθωτικές αποφάσεις.

Ορίζοντας τα διάφορα επίπεδα πιθανότητας και επίδρασης των κινδύνων είναι δυνατόν να μειώσουμε την αρνητική επιρροή των υποκειμενικών απόψεων. Επίσης η αξιολόγηση της ποιότητας της διαθέσιμης πληροφορίας που αφορά τους κινδύνους του έργου βοηθάει στο να αντιληφθούμε τη σπουδαιότητα του κάθε κινδύνου στο έργο.

Η Ποιοτική Ανάλυση Κινδύνου είναι συνήθως μια αποδοτική διαδικασία που συμβάλει στην ιεράρχηση του Σχεδιασμού Απόκρισης Κινδύνων καθώς και στην Ποσοτική Ανάλυση Κινδύνου. Η Ποιοτική Ανάλυση

Κινδύνου πρέπει να επανεξετάζεται κατά τη διάρκεια του κύκλου ζωής του έργου και να ενημερώνεται με οποιαδήποτε αλλαγή κινδύνου του έργου.

- **Μητρώο Κινδύνων**

Το μητρώο κινδύνων έχει αναλυθεί προηγουμένως.

- **Σχεδιασμός Διαχείρισης Κινδύνων**

Βασικά στοιχεία του σχεδιασμού διαχείρισης κινδύνων που χρησιμοποιούνται στην Ποιοτική Ανάλυση Κινδύνων περιλαμβάνουν τους ρόλους και τις ευθύνες των στελεχών που διεξάγουν την ανάλυση κινδύνου, τον προϋπολογισμό, τον προγραμματισμό των ενεργειών της ανάλυσης κινδύνου, τις κατηγορίες κινδύνων, τον πίνακα πιθανοτήτων και επιπτώσεων καθώς και τις ανοχές των συμμετεχόντων ως προς τον κίνδυνο. Αυτές οι πληροφορίες συχνά προσαρμόζονται στο έργο κατά τη διάρκεια του Σχεδιασμού Ανάλυσης Κινδύνων. Αν δεν είναι διαθέσιμοι τότε, αναπτύσσονται κατά τη διαδικασία Ποιοτικής Ανάλυσης.

- **Πεδίο Εφαρμογής Έργου**

Έργα κοινά ή επαναλαμβανόμενα τείνουν να έχουν καλά καθορισμένους κινδύνους. Έργα που είναι πολύ περίπλοκα ή υψηλής τεχνολογίας τείνουν να έχουν μεγαλύτερη αβεβαιότητα. Αυτές οι παράμετροι εξετάζονται κατά την αρχική δήλωση του πεδίου εφαρμογής του έργου.

- **Εταιρικά Περιουσιακά Στοιχεία**

Τα εταιρικά περιουσιακά στοιχεία που μπορεί να επηρεάσουν τη διαδικασία Ποιοτικής Ανάλυσης περιλαμβάνουν (αλλά δεν περιορίζονται σε):

- Πληροφορίες προηγούμενων ίδιων ολοκληρωμένων έργων
- Εξέταση παρόμοιων έργων από ειδικούς διαχείρισης κινδύνου
- Βάσεις δεδομένων που μπορεί να είναι διαθέσιμες από τη βιομηχανία ή και ιδιοκτήτες

Ποιοτική Ανάλυση Κινδύνων: Εργαλεία και Τεχνικές

- **Πιθανότητα Κινδύνου και Εκτίμηση Επιπτώσεων**

Η εκτίμηση πιθανότητας κινδύνων ερευνά την πιθανότητα κάθε κίνδυνος να παρουσιαστεί. Η εκτίμηση επιπτώσεων των κινδύνων μελετά το πιθανό αποτέλεσμα που θα έχει σε ένα αντικειμενικό στόχο του έργου, όπως είναι το πρόγραμμα, το κόστος, η ποιότητα ή η επίδοση, περιλαμβάνοντας είτε αρνητικά αποτελέσματα λόγω απειλών, είτε θετικά αποτελέσματα λόγω ευκαιριών.

Η πιθανότητα και η επίπτωση εκτιμώνται για κάθε προσδιορισμένο κίνδυνο. Οι κίνδυνοι μπορεί να εκτιμηθούν μέσω συνεντεύξεων ή συναντήσεων με επιλεγμένους συμμετέχοντες όσους είναι οικείοι με τους ως προς συζήτηση κινδύνους. Επίσης περιλαμβάνονται μέλη της ομάδας έργου καθώς και πρόσωπα εκτός έργου που έχουν τις απαραίτητες γνώσεις.

Ο βαθμός της πιθανότητας κάθε κινδύνου και το αποτέλεσμα σε κάθε αντικειμενικό σκοπό του έργου αξιολογείται κατά τη διάρκεια των συνεντεύξεων ή των συναντήσεων. Επίσης περιλαμβάνονται και επεξηγηματικές λεπτομέρειες που δικαιολογούν την εκτίμηση και το αποτέλεσμα του κάθε κινδύνου. Αυτοί κατατάσσονται σε σχέση με τους ορισμούς που έχουν δοθεί στην αρχική φάση του σχεδιασμού διαχείρισης κινδύνου. Κίνδυνοι χαμηλής πιθανότητας και αποτελέσματος επίσης περιλαμβάνονται σε μια λίστα για μελλοντική παρακολούθηση.

- **Πίνακας Πιθανοτήτων και Επιπτώσεων**

Οι κίνδυνοι μπαίνουν σε προτεραιότητα για μελλοντική ποσοτική ανάλυση και απόκριση βασιζόμενοι στη βαθμολόγησή τους. Συνήθως οι κανόνες βαθμολόγησης μπαίνουν στην αρχή του έργου και αποτελούν περιουσιακό στοιχείο της εταιρίας. Οι κανόνες μπορεί να προσαρμοστούν στο συγκεκριμένο έργο στη διαδικασία Σχεδιασμού Διαχείρισης Κινδύνων. Εκτίμηση της σημαντικότητας του κάθε κινδύνου άρα και προτεραιότητά του γίνεται με τη χρήση ενός πίνακα, του πίνακα πιθανοτήτων και επιπτώσεων. Αυτός ο πίνακας καθορίζει συνδυασμούς πιθανότητας και αποτελέσματος που οδηγεί στην κατάταξη των κινδύνων ως χαμηλής, μεσαίας ή υψηλής προτεραιότητας.

Η κατάταξη των κινδύνων βοηθά στις αποφασισμένες αποκρίσεις. Για παράδειγμα οι κίνδυνοι που έχουν αρνητικό αποτέλεσμα στους στόχους του έργου (απειλές) και είναι στη ζώνη υψηλού κινδύνου στον πίνακα χρειάζονται διαχείριση με υψηλή προτεραιότητα και επιθετικές στρατηγικές απόκρισης. Οι απειλές χαμηλού κινδύνου δεν χρειάζονται κάποια ιδιαίτερη ενέργεια, μόνο τοποθετούνται σε μια λίστα παρακολούθησης.

Ομοίως οι ευκαιρίες που μπορεί να δώσουν μεγαλύτερο όφελος θα πρέπει να στοχοποιούνται πρώτα. Οι ευκαιρίες που δίνουν μικρότερο όφελος θα πρέπει να βρίσκονται υπό παρακολούθηση.

- **Εκτίμηση Ποιότητας Δεδομένων Κινδύνου**

Η ποιοτική ανάλυση κινδύνου απαιτεί ακριβή στοιχεία για να είναι αξιόπιστη. Η ανάλυση της ποιότητας των δεδομένων κινδύνου είναι μια τεχνική αξιολόγησης του βαθμού χρησιμότητάς τους στην ανάλυση κινδύνου. Περιλαμβάνει την ακρίβεια, την ποιότητα, την αξιοπιστία των δεδομένων κινδύνου. Αν η ποιότητα δεν είναι αποδεκτή, ίσως να είναι απαραίτητη η συλλογή στοιχείων καλύτερης ποιότητας.

- **Κατηγοριοποίηση Κινδύνων**

Οι κίνδυνοι ενός έργου μπορεί να κατηγοριοποιηθούν ως προς την πηγή τους, την περιοχή του έργου που θα επηρεαστεί και κάθε άλλη κατηγορία που μπορεί να δημιουργηθεί. Η ομαδοποίηση των κινδύνων ως προς κοινή αιτία οδηγεί σε πιο αποτελεσματική αντιμετώπισή τους.

- **Εκτίμηση Επειγόντων Κινδύνων**

Επείγοντες θεωρούνται οι κίνδυνοι που χρειάζονται βραχυπρόθεσμη αντιμετώπιση. Η προτεραιότητα του κάθε κινδύνου μπορεί να περιλαμβάνει και το χρόνο αντίδρασης, προειδοποιητικά σημεία καθώς και τη βαθμολόγησή τους. Σε ορισμένες ποιοτικές αναλύσεις η εκτίμηση της άμεσης αντιμετώπισης ενός κινδύνου μπορεί να συνδυαστεί με την κατάταξη του κάθε κινδύνου που απορρέει από τον πίνακα πιθανοτήτων και αποτελέσματος, έτσι ώστε να πάρουμε την τελική σημασία του κάθε κινδύνου.

- **Κρίση Εμπειρογνωμόνων**

Η γνώμη των εμπειρογνωμόνων είναι απαραίτητη για να εκτιμηθεί η πιθανότητα και το αποτέλεσμα κάθε κινδύνου και να προσδιοριστεί η θέση του στον πίνακα πιθανοτήτων και αποτελέσματος. Οι εμπειρογνώμονες έχουν πρόσφατη εμπειρία από παρόμοια έργα. Επίσης όσοι ασχολούνται με το συγκεκριμένο έργο έχουν σημαντική γνώση για αυτό. Η εμπειρία τους λαμβάνεται υπόψη μέσω συνεντεύξεων και συναντήσεων κατά τη διαδικασία αυτή.

Ποιοτική Ανάλυση Κινδύνων: Συμπεράσματα

- **Ενημέρωση Μητρώου Κινδύνων**

Το μητρώο κινδύνων δημιουργείται κατά τη διαδικασία Προσδιορισμού Κινδύνων. Το μητρώο κινδύνων ενημερώνεται με πληροφορίες από την Ποιοτική Ανάλυση Κινδύνων και το ενημερωμένο μητρώο περιλαμβάνεται στα έγγραφα του έργου. Οι ενημερώσεις του μητρώου κατά την Ποιοτική Ανάλυση Κινδύνου περιλαμβάνουν:

- **Σχετική κατάταξη ή λίστα προτεραιότητας κινδύνων**

Ο πίνακας πιθανοτήτων και αποτελεσμάτων μπορεί να χρησιμοποιηθεί για να ταξινομήσει τους κινδύνους με βάση την ατομική τους σημασία. Χρησιμοποιώντας συνδυασμούς της πιθανότητας εμφάνισης ενός κινδύνου και του αποτελέσματος στους στόχους του έργου, εάν εμφανιζόταν, οι κίνδυνοι παίρνουν προτεραιότητα ο ένας ως προς τον άλλο και ταξινομούνται ως υψηλού, μέτριου και χαμηλού κινδύνου. Οι κίνδυνοι μπορεί να πάρουν προτεραιότητα ξεχωριστά για το πρόγραμμα, το κόστος και το αποτέλεσμά τους, καθώς οι εταιρίες μπορεί να ενδιαφέρονται περισσότερο για την επίτευξη συγκεκριμένων στόχων. Ο project manager μπορεί να με βάση τη λίστα προτεραιοτήτων να δώσει μεγαλύτερη σημασία στους κινδύνους που έχουν μεγαλύτερη σημασία ως προς τους στόχους της εταιρίας, έτσι ώστε οι αποκρίσεις να οδηγήσουν σε καλύτερα αποτελέσματα.

- **Κατηγοριοποίηση κινδύνων**

Η κατηγοριοποίηση των κινδύνων μπορεί να αποκαλύψει κοινά αίτια κινδύνων σε διάφορες περιοχές του έργου που χρίζουν ιδιαίτερης προσοχής. Η ανακάλυψη συγκεκριμένων αιτίων κινδύνου μπορεί να οδηγήσει σε πιο αποτελεσματική αντιμετώπισή του.

- **Αίτια κινδύνου ή περιοχές του έργου που χρειάζονται συγκεκριμένη προσοχή**

Η ανακάλυψη συγκεκριμένων αιτίων κινδύνου μπορεί να οδηγήσει σε πιο αποτελεσματική αντιμετώπισή του.

- **Λίστα κινδύνων που χρειάζονται βραχυπρόθεσμες δράσεις**

Οι κίνδυνοι που πρέπει να αντιμετωπιστούν άμεσα και αυτοί που μπορεί να αντιμετωπιστούν αργότερα μπορεί να μπουν σε διαφορετικές λίστες.

- **Λίστα κινδύνων που χρειάζονται επιπλέον ανάλυση και δράση**

Ορισμένοι κίνδυνοι χρειάζονται περισσότερη ανάλυση συνήθως Ποιοτική.

- **Λίστα παρακολούθησης των κινδύνων χαμηλής προτεραιότητας**

Οι κίνδυνοι που δεν έχουν εκτιμηθεί ως πολύ σημαντικοί κατά την Ποιοτική Ανάλυση, μπορεί να μπουν σε μια λίστα παρακολούθησης για μελλοντική παρακολούθηση.

- **Τάσεις στα αποτελέσματα της ποιοτικής ανάλυσης κινδύνων**

Η επανάληψη της ανάλυσης μπορεί να αποκαλύψει τάσεις και μπορεί να οδηγήσει σε δράσεις ή περαιτέρω ανάλυση κάνοντάς τους περισσότερο ή λιγότερο σημαντικούς.

2.3.4 Ποσοτική Ανάλυση Κινδύνων

Η Ποσοτική Ανάλυση Κινδύνου είναι η διαδικασία αριθμητικής ανάλυσης των αποτελεσμάτων που έχουν οι προσδιορισμένοι κίνδυνοι συνολικά στο έργο. Η Ποσοτική Ανάλυση Κινδύνου γίνεται για κινδύνους που έχουν ιεραρχηθεί προηγουμένως κατά τη διεργασία Ποιοτικής Ανάλυσης Κινδύνου και οι οποίοι έχουν ουσιαστική επίδραση στις απαιτήσεις του έργου. Η Ποσοτική Ανάλυση Κινδύνου αναλύει τα αποτελέσματα των κινδύνων. Επίσης μπορεί να χρησιμοποιηθεί είτε για αριθμητική εκτίμηση του κάθε κινδύνου ξεχωριστά είτε λαμβάνοντας υπόψη όλους τους κινδύνους συνολικά που επηρεάζουν το έργο.
Αποτελεί την ποσοτική προσέγγιση των αποφάσεων σε περιβάλλον αβεβαιότητας.
Η Ποσοτική Ανάλυση ακολουθεί την Ποιοτική Ανάλυση, αν και σε ορισμένες περιπτώσεις δεν είναι αναγκαία. Η διαθεσιμότητα σε χρόνο και χρήμα καθώς και η ανάγκη ή όχι ποιοτικών και ποσοτικών

συμπερασμάτων για τους κινδύνους και τις επιδράσεις τους στο έργο θα προσδιορίσει και τις μεθόδους που θα χρησιμοποιηθούν. Η Ποσοτική Ανάλυση θα πρέπει να επαναλαμβάνεται μετά από κάθε σχέδιο απόκρισης κινδύνου ως μέρος της παρακολούθησης και του ελέγχου των κινδύνων για να καθοριστεί αν ο συνολικός κίνδυνος για το έργο έχει μειωθεί ικανοποιητικά.

- **Μητρώο Κινδύνων**

Το μητρώο κινδύνων έχει αναλυθεί προηγουμένως.

- **Σχεδιασμός Διαχείρισης Κινδύνων**

Τα παραπάνω δεδομένα εισόδου έχουν αναλυθεί σε προηγούμενες παραγράφους.

- **Σχεδιασμός Διαχείρισης Κόστους**

Ο σχεδιασμός διαχείρισης κόστους του έργου δημιουργεί τα κριτήρια για το σχεδιασμό, τη δόμηση, την εκτίμηση και τον έλεγχο των εξόδων του έργου. Οι έλεγχοι αυτοί βοηθούν στον προσδιορισμό και της δομής και του ελέγχου του κόστους του έργου και στον προσδιορισμό της ποσοτικής ανάλυσης του προϋπολογισμού.

- **Σχεδιασμός Διαχείρισης Προγράμματος**

Ο σχεδιασμός διαχείρισης προγράμματος του έργου βοηθά αντίστοιχα με το σχεδιασμό του κόστους στον καλύτερο έλεγχο και στην πιο αποτελεσματική προσέγγιση του προγράμματος.

- **Επιχειρησιακές Διαδικασίες**

Οι επιχειρησιακές διαδικασίες βοηθούν και μπορούν να επηρεάσουν την Ποσοτική Ανάλυση Κινδύνου ως εξής:

  - Με πληροφόρηση προηγουμένων ίδιων ολοκληρωμένων έργων
  - Μελέτη παρόμοιων έργων από ειδικούς
  - Βάσεις δεδομένων διαθέσιμες από τη βιομηχανία ή επιχειρησιακές

Ποσοτική Ανάλυση Κινδύνων: Εργαλεία και Τεχνικές

- **Συλλογή Δεδομένων και Τεχνικές Αναπαράστασης**
- **Συνεντεύξεις**

Οι τεχνικές συνεντεύξεων βασίζονται στην εμπειρία και στα ιστορικά δεδομένα για να ποσοτικοποιήσουν την πιθανότητα και το αποτέλεσμα των κινδύνων στους αντικειμενικούς στόχους του έργου. Η απαραίτητη πληροφορία εξαρτάται από τον τύπο της κατανομής πιθανοτήτων που θα χρησιμοποιηθεί. Για παράδειγμα, οι πληροφορίες θα συλλέγονταν για το αισιόδοξο, το απαισιόδοξο και το πιο πιθανό σενάριο για τις πιο συχνά χρησιμοποιούμενες κατανομές.

- **Πιθανοτικές Κατανομές**

Οι συνεχείς πιθανοτικές κατανομές, που χρησιμοποιούνται εκτενώς στη μοντελοποίηση και στην προσομοίωση, αναπαριστούν την αβεβαιότητα τιμών όπως διάρκειες προγράμματος διαφόρων ενεργειών του έργου και κόστη κομματιών του έργου. Οι διακριτές κατανομές μπορεί να χρησιμοποιηθούν για να αναπαρασταθούν αβέβαια γεγονότα όπως το αποτέλεσμα ενός τέστ ή ένα πιθανό σενάριο σε ένα δέντρο αποφάσεων.

- **Ποσοτική Ανάλυση Κινδύνων και Τεχνικές Μοντελοποίησης**

Οι πιο συχνά χρησιμοποιούμενες τεχνικές περιλαμβάνουν προσεγγίσεις ανάλυσης σχετικές είτε με γεγονότα είτε με το έργο.

- **Ανάλυση Ευαισθησίας**

Η ανάλυση ευαισθησίας βοηθά στον προσδιορισμό των κινδύνων που έχουν τη μεγαλύτερη πιθανή επίπτωση στο έργο. Εξετάζει την έκταση στην οποία η αβεβαιότητα του κάθε μέρους του έργου επηρεάζει τον στόχο που εξετάζεται, όταν όλα τα υπόλοιπα αβέβαια μέρη έχουν τις βασικές τους τιμές. Τυπικό δείγμα ανάλυσης ευαισθησίας είναι το διάγραμμα «ανεμοστρόβιλος» (tornado diagram) το οποίο είναι χρήσιμο για τη σύγκριση παραμέτρων σχετικής σημαντικότητας και επίδρασης οι οποίες έχουν μεγαλύτερο βαθμό αβεβαιότητας σε σχέση με άλλες περισσότερο σταθερές.

- **Αναμενόμενη ανάλυση νομισματικής αξίας**

Η αναμενόμενη ανάλυση νομισματικής αξίας (Expected Monetary Value) είναι μια στατιστική μέθοδος που υπολογίζει το μέσο αποτέλεσμα όταν συμβούν ή όχι μελλοντικά σενάρια (αποτελεί δηλαδή ανάλυση με αβεβαιότητα). Η ανάλυση EMV των ευκαιριών εκφράζεται γενικά με θετικές τιμές, ενώ η ανάλυση των απειλών με αρνητικές. Η ανάλυση EMV απαιτεί υποθέσεις ουδέτερου ρίσκου για να εφαρμοστεί. Η EMV ενός έργου υπολογίζεται πολλαπλασιάζοντας την τιμή του πιθανού αποτελέσματος με την πιθανότητα εμφάνισης και προσθέτοντας τα γινόμενα που προκύπτουν. Μια κοινή χρήση ανάλυσης τέτοιου τύπου αποτελούν τα Δέντρα Αποφάσεων.

- **Μοντελοποίηση και προσομοίωση**

Η προσομοίωση ενός έργου χρησιμοποιεί ένα μοντέλο που μεταφράζει τις προσδιορισμένες με λεπτομέρεια αβεβαιότητες του έργου στο πιθανό αποτέλεσμα στους στόχους του έργου. Προσομοιωτές ολοκλήρωσης χρησιμοποιούν συνήθως τη μέθοδο Monte Carlo. Σε μια προσομοίωση, ένα μοντέλο υπολογίζεται πολλές φορές (ολοκλήρωση) με τις εισόδους (κόστος, διάρκεια εργασιών) να διαλέγονται τυχαία σε κάθε επανάληψη, από τις κατανομές πιθανότητας της κάθε μεταβλητής. Η πιθανοτική κατανομή (συνολικό κόστος ή ημερομηνία ολοκλήρωσης του έργου) υπολογίζεται από τις επαναλήψεις. Για μια ανάλυση κινδύνου κόστους, η προσομοίωση χρησιμοποιεί εκτιμήσεις κόστους. Για μια ανάλυση κινδύνου προγραμματισμού χρησιμοποιείται το διάγραμμα προγράμματος και εκτιμήσεις διάρκειας.

- **Κρίση Εμπειρογνωμόνων**

Η κρίση των εμπειρογνωμόνων (ιδανικά θα πρέπει οι ειδικοί να έχουν σχετική και πρόσφατη εμπειρία) είναι απαραίτητη για τον προσδιορισμό των πιθανών επιπτώσεων στο κόστος και στον προγραμματισμό, και για τον προσδιορισμό των εισόδων (όπως για παράδειγμα οι πιθανοτικές κατανομές) στα διάφορα εργαλεία που θα χρησιμοποιηθούν.

Ποσοτική Ανάλυση Κινδύνων: Συμπεράσματα

- **Ενημερώσεις Μητρώου Κινδύνων**

Το μητρώο κινδύνων ενημερώνεται με τα αποτελέσματα της ποσοτικής ανάλυσης κινδύνων που περιλαμβάνει λεπτομέρειες ως προς την ποσοτική προσέγγιση, τα δεδομένα εξόδου και ενδεχόμενες συστάσεις.

- **Πιθανοτική Ανάλυση του έργου**

Γίνονται εκτιμήσεις για τα πιθανά αποτελέσματα του κόστους και του προγράμματος καταχωρώντας τις ημερομηνίες ολοκλήρωσης μαζί με συνδεδεμένα επίπεδα εμπιστοσύνης. Το αποτέλεσμα αυτό που συχνά εκφράζεται ως μια σωρευτική κατανομή, μπορεί να χρησιμοποιηθεί μαζί με τις ανοχές κινδύνου των εμπλεκομένων για να εμποδίσουν την χρήση αποθεματικών επείγουσας επέμβασης που αφορούν το κόστος και το χρόνο. Τα αποθεματικά αυτά χρειάζονται για να επαναφέρουν στόχους του έργου που έχουν υπερβεί τα όρια, σε επίπεδα αποδεκτά από την επιχείρηση.

- **Πιθανότητα Επίτευξης Στόχων Κόστους και Χρόνου**

Με τους κινδύνους που αντιμετωπίζει το έργο, η πιθανότητα επίτευξης των στόχων του έργου με το συγκεκριμένο σχεδιασμό, μπορεί να εκτιμηθεί με χρήση των αποτελεσμάτων ποσοτικής ανάλυσης κινδύνων.

- **Λίστα Προτεραιοτήτων Ποσοτικοποιημένων Κινδύνων**

Η λίστα κινδύνων περιλαμβάνει αυτούς που αποτελούν μεγαλύτερη απειλή ή παρουσιάζουν μεγαλύτερες ευκαιρίες για το έργο. Περιλαμβάνονται οι κίνδυνοι που έχουν το μεγαλύτερο αποτέλεσμα σε ένα ενδεχόμενο κόστος και αυτοί που είναι περισσότερο πιθανό να επηρεάσουν το κρίσιμο μονοπάτι. Οι κίνδυνοι αυτοί μπορεί να προσδιοριστούν σε ορισμένες περιπτώσεις μέσω ενός διαγράμματος tornado που παράγεται από μια ανάλυση προσομοίωσης.

- **Τάσεις Ποσοτικής Ανάλυσης Αποτελεσμάτων**

Με την επανάληψη της ανάλυσης φανερώνονται πολλές φορές τάσεις που οδηγούν σε συμπεράσματα που επηρεάζουν τις αποκρίσεις στους κινδύνους. Νέες ιδέες μπορεί να προκύψουν μέσα από τη

διαδικασία Ποσοτικής Ανάλυσης Κινδύνων που αλλάζοντας τις πληροφορίες ιστορικού μιας επιχείρησης που αφορούν τον προγραμματισμό, κόστη, την ποιότητα και τις επιδόσεις. Αυτά τα ιστορικά στοιχεία μπορεί να πάρουν μια μορφή αναφοράς ποσοτικής ανάλυσης κινδύνων. Η αναφορά μπορεί να είναι χωρισμένη ή συνδεδεμένη με το μητρώο κινδύνων.

2.3.5 Σχεδιασμός Απόκρισης Κινδύνων

Είναι η διαδικασία ανάπτυξης επιλογών και ενεργειών για να ενισχύσουν τις ευκαιρίες και να μειώσουν τις απειλές που θα υπάρξουν κατά τη διάρκεια του έργου.
Ακολουθεί την ποιοτική και ποσοτική ανάλυση. Περιλαμβάνει τον προσδιορισμό και την ανάθεση σε συγκεκριμένα άτομα να αναλάβουν τον σχεδιασμό της απόκρισης σε κάθε κίνδυνο. Ο Σχεδιασμός Απόκρισης είναι μια διαδικασία κατά τη διάρκεια της οποίας αντιμετωπίζονται οι κίνδυνοι με βάση την προτεραιότητα τους, εισάγει πόρους και απαραίτητες δράσεις στον προϋπολογισμό και στον προγραμματισμό του έργου όπου είναι απαραίτητο.
Η αντιμετώπιση κάθε κινδύνου θα πρέπει να είναι ρεαλιστική όσον αφορά το περιβάλλον του έργου, αποδοτική όσον αφορά το κόστος και το χρόνο και να συμφωνούν με αυτή όλοι οι εμπλεκόμενοι του έργου.

- **Μητρώο Κινδύνων**

Το μητρώο κινδύνων έχει αναλυθεί παραπάνω.

- **Σχεδιασμός Διαχείρισης Κινδύνων**

Τα παραπάνω δεδομένα εισόδου έχουν αναλυθεί σε προηγούμενες παραγράφους.

Σχεδιασμός Απόκρισης Κινδύνων: Εργαλεία και Τεχνικές

Υπάρχουν διαθέσιμες διάφορες στρατηγικές απόκρισης στους κινδύνους. Θα πρέπει κάθε φορά να διαλέγεται η στρατηγική ή οι στρατηγικές που είναι πιο αποτελεσματικές για τον κάθε κίνδυνο. Εργαλεία ανάλυσης κινδύνου, όπως τα δέντρα αποφάσεων, μπορεί να χρησιμοποιηθούν για να επιλεγούν οι πιο αποτελεσματικές αποκρίσεις. Συγκεκριμένες ενέργειες αναπτύσσονται για να υλοποιηθεί η κάθε στρατηγική, συμπεριλαμβάνοντας βασικές και δευτερεύουσες στρατηγικές, όπου κρίνεται απαραίτητο.

Ένα εφεδρικό σχέδιο μπορεί να αναπτυχθεί για υλοποίηση αν η επιλεγμένη στρατηγική αποδειχθεί λιγότερο αποτελεσματική από το αναμενόμενο, ή αν εμφανιστεί ένας αποδεκτός κίνδυνος. Δευτερεύοντες κίνδυνοι (δηλαδή κίνδυνοι που προκύπτουν από τις στρατηγικές) θα πρέπει επίσης να επανεξετάζονται. Ένα αποθεματικό επείγουσας επέμβασης πολύ συχνά διατίθεται για τον χρόνο ή το κόστος. Αν αναπτυχθεί, μπορεί να περιλαμβάνει ταυτοποίηση των συνθηκών που ενεργοποιούν τη χρήση του.

- **Στρατηγικές Αρνητικών Κινδύνων ή Απειλών**

Τρεις από τις στρατηγικές που ακολουθούν ασχολούνται με απειλές ή κινδύνους που έχουν αρνητικά αποτελέσματα στους στόχους του έργου σε περίπτωση που εμφανιστούν. Η τέταρτη στρατηγική, η αποδοχή, μπορεί να χρησιμοποιηθεί είτε για αρνητικούς κινδύνους ή απειλές, είτε για θετικούς κινδύνους ή ευκαιρίες. Οι στρατηγικές αυτές είναι η αποφυγή, η μεταφορά, ο μετριασμός και η αποδοχή.

- **Αποφυγή**

Η αποφυγή του κινδύνου περιλαμβάνει την αλλαγή του σχεδιασμού του έργου για την πλήρη εξάλειψη του κινδύνου. Ο project manager μπορεί επίσης να απομονώσει τους στόχους του έργου από την επίδραση του κινδύνου, ή να αλλάξει τον στόχο που επηρεάζεται. Παραδείγματα περιλαμβάνουν την επέκταση του προγράμματος, την αλλαγή της στρατηγικής ή τη μείωση του πεδίου δράσης του έργου. Η πιο ριζοσπαστική στρατηγική αποφυγής είναι η παύση του έργου τελείως. Ορισμένοι κίνδυνοι που εμφανίζονται νωρίς στο έργο μπορούν να αποφευχθούν διευκρινίζοντας απαιτήσεις, αποκτώντας πληροφορίες, βελτιώνοντας την επικοινωνία ή αποκτώντας ειδικές και επιπλέον γνώσεις.

- **Μεταφορά**

Η μεταφορά κινδύνων απαιτεί τη μεταφορά ορισμένων ή όλων των αρνητικών αποτελεσμάτων ή απειλών, μαζί με την ευθύνη της απόκρισης σε έναν εξωτερικό συνεργάτη. Η μεταφορά του κινδύνου απλώς δίνει την ευθύνη διαχείρισης σε έναν εξωτερικό συνεργάτη, δεν εξαλείφει τον κίνδυνο. Η μεταφορά ευθύνης ενός κινδύνου είναι περισσότερο αποτελεσματική σε περιπτώσεις έκθεσης σε οικονομικούς κινδύνους. Η μεταφορά κινδύνου σχεδόν πάντα περιλαμβάνει την πληρωμή στον εξωτερικό συνεργάτη που αναλαμβάνει την αντιμετώπιση του κινδύνου. Τα εργαλεία μεταφοράς ποικίλουν και περιλαμβάνουν (χωρίς να είναι αυστηρά περιορισμένα σε) χρήση ασφάλιστρων, εγγυητικών επιστολών, ενταλμάτων, εγγυήσεων κλπ. Τα συμβόλαια επίσης μπορεί να χρησιμοποιηθούν για τη μεταφορά του κινδύνου σε μια

άλλη ομάδα. Για παράδειγμα, όταν ένας αγοραστής έχει ικανότητες που ο πωλητής δεν διαθέτει, μπορεί να είναι καλύτερα να μεταφερθεί δουλειά και το αντίστοιχο ρίσκο στον αγοραστή μέσω συμβολαίου.

- **Μετριασμός**

Η μείωση του κινδύνου σημαίνει τη μείωση της πιθανότητας και του αποτελέσματος ενός σοβαρού κινδύνου, σε αποδεκτά όρια. Οι ενέργειες που γίνονται για τη μείωση της πιθανότητας και του αποτελέσματος ενός κινδύνου που ίσως εμφανιστεί στο έργο είναι περισσότερο αποτελεσματικές από την προσπάθεια διόρθωσης της ζημιάς μετά την εμφάνιση του κινδύνου. Παραδείγματα μείωσης του κινδύνου είναι η υιοθέτηση λιγότερο πολύπλοκων διαδικασιών, η διεξαγωγή περισσότερων ελέγχων ή η επιλογή καλύτερου προμηθευτή. Όπου δεν είναι εφικτό να μειωθεί η πιθανότητα εμφάνισης, η μείωση του αποτελέσματος μπορεί να επικεντρωθεί σε διασυνδέσεις του αποτελέσματος που καθορίζουν τη σοβαρότητά του. Για παράδειγμα, ο σχεδιασμός ενός εφεδρικού συστήματος μπορεί να μειώσει το αποτέλεσμα μιας ζημιάς του αρχικού.

- **Αποδοχή**

Η στρατηγική αυτή υιοθετείται επειδή σπάνια είναι δυνατό να εξαλειφθούν όλοι οι κίνδυνοι και οι απειλές από ένα έργο. Η στρατηγική υποδεικνύει ότι η ομάδα έργου έχει αποφασίσει να μην αλλάξει το σχεδιασμό του έργου για να αντιμετωπίσει έναν κίνδυνο, ή αδυνατεί να προσδιορίσει διαφορετική στρατηγική απόκρισης. Η στρατηγική αυτή μπορεί να είναι είτε ενεργητική είτε παθητική. Η παθητική αποδοχή δεν απαιτεί καμία ενέργεια, εκτός από να καταγράψει τη στρατηγική, αφήνοντας την ομάδα έργου να ασχοληθεί με τους κινδύνους καθώς συμβαίνουν. Η πιο κοινή ενεργητική στρατηγική αποδοχής είναι να δημιουργηθεί ένα αποθεματικό επείγουσας επέμβασης, που περιλαμβάνει χρόνο, χρήματα και πόρους, έτσι ώστε να είναι δυνατός ο χειρισμός των κινδύνων.

- **Στρατηγικές Θετικών Κινδύνων ή Ευκαιριών**

Τρεις από τις τέσσερις αποκρίσεις ασχολούνται με κινδύνους με πιθανά θετικά αποτελέσματα στους στόχους του έργου. Η τέταρτη στρατηγική, η αποδοχή, μπορεί να χρησιμοποιηθεί για αρνητικούς κινδύνους ή απειλές, όπως και για θετικούς κινδύνους και ευκαιρίες. Οι στρατηγικές αυτές που περιγράφονται παρακάτω είναι η εκμετάλλευση, η διανομή, η ενίσχυση και η αποδοχή.

- **Εκμετάλλευση**

Η στρατηγική αυτή επιλέγεται για κινδύνους με θετικά αποτελέσματα, όπου η επιχείρηση θέλει να είναι σίγουρη ότι η ευκαιρία θα πραγματοποιηθεί. Η στρατηγική αυτή επιδιώκει να εξαλείψει την αβεβαιότητα που εμφανίζεται με τον θετικό κίνδυνο, εξασφαλίζοντας ότι η ευκαιρία θα εμφανιστεί σίγουρα. Για παράδειγμα μια επιχείρηση μπορεί να αναθέσει το έργο στους πιο αποτελεσματικούς υπαλλήλους για να μειώσει το χρόνο και το κόστος ολοκλήρωσης του έργου.

- **Διαμερισμός**

Η στρατηγική αυτή εννοεί πως ένας θετικός κίνδυνος και η ευκαιρία που συνεπάγεται, μοιράζεται σε έναν εξωτερικό συνεργάτη που μπορεί να συλλάβει καλύτερα την ευκαιρία για το όφελος του έργου. Παραδείγματα αποτελούν οι συνεργασίες εταιριών έτσι ώστε όλοι οι συνεργαζόμενοι να επωφεληθούν από τις ενέργειες που θα γίνουν.

- **Ενίσχυση**

Η στρατηγική αυτή χρησιμοποιείται για να αυξηθεί η πιθανότητα και/ή τα αποτελέσματα μιας ευκαιρίας. Προσδιορίζοντας και μεγιστοποιώντας τις βασικές κινητήριες δυνάμεις των θετικών αυτών κινδύνων, είναι πιθανό να αυξηθεί η πιθανότητα εμφάνισής τους. Παράδειγμα αποτελεί η χρήση περισσότερων πόρων για να τελειώσει μια ενέργεια νωρίτερα.

- **Αποδοχή**

Αποδοχή μιας ευκαιρίας είναι το να την εκμεταλλευτεί η εταιρία χωρίς όμως να επιδιώκει κάτι τέτοιο ενεργά.

- **Ενδεχόμενες Στρατηγικές Αντιμετώπισης**

Ορισμένες αποκρίσεις σχεδιάζονται για χρήση μόνο αν ένα συγκεκριμένο γεγονός εμφανιστεί. Για κάποιους κινδύνους είναι καταλληλότερο για την ομάδα έργου να φτιάξει ένα σχέδιο απόκρισης που θα εκτελεστεί μόνο κάτω από προκαθορισμένες συνθήκες. Θεωρείται πως θα υπάρχει προειδοποίηση για να

υλοποιηθεί το σχέδιο. Τα γεγονότα που ενεργοποιούν μια τέτοια στρατηγική θα πρέπει να προσδιορίζονται και να ακολουθούνται.

- **Κρίση Εμπειρογνωμόνων**

Η κρίση εμπειρογνωμόνων είναι η γνώση μιας ομάδας ανθρώπων που χρησιμοποιείται για τις ενέργειες που πρέπει να γίνουν για ένα συγκεκριμένο και προσδιορισμένο κίνδυνο.

Σχεδιασμός Απόκρισης Κινδύνων: Συμπεράσματα

- **Ενημέρωση Μητρώου Κινδύνων**

Κατά τη διαδικασία Σχεδιασμού Αποκρίσεων Κινδύνων επιλέγονται κατάλληλες αποκρίσεις, όπως έχει συμφωνηθεί, και περιλαμβάνονται στο μητρώο κινδύνων. Το μητρώο κινδύνων θα πρέπει να έχει γραφτεί με λεπτομέρεια που αντιστοιχεί στην προτεραιότητα του κάθε κινδύνου και στη σχεδιασμένη απόκριση. Συνήθως οι υψηλοί και μέτριοι κίνδυνοι γράφονται με λεπτομέρεια. Οι κίνδυνοι που κρίνονται ως χαμηλής προτεραιότητας περιλαμβάνονται σε μια λίστα παρακολούθησης για περιοδικό έλεγχο. Τα στοιχεία του μητρώου κινδύνων σε αυτό το σημείο μπορεί να περιλαμβάνουν:

- Προσδιορισμένους κινδύνους, τις περιγραφές τους, τις περιοχές του έργου που επηρεάζονται, τα αίτια, και πως μπορεί να επηρεάσουν τους στόχους του έργου
- Τα πρόσωπα που είναι υπεύθυνα για τον κάθε κίνδυνο αναλαμβάνουν τις ευθύνες τους
- Τις εξόδους από τη διαδικασία Ποιοτικής Ανάλυσης Κινδύνου, συμπεριλαμβανομένου τις λίστες προτεραιότητας των κινδύνων
- Συμφωνημένες στρατηγικές αποκρίσεων
- Συγκεκριμένες ενέργειες για την υλοποίηση της επιλεγμένης στρατηγικής απόκρισης
- Συμπτώματα και στοιχεία που δείχνουν ότι ένας κίνδυνος μπορεί να εμφανιστεί
- Ενέργειες σχετικές με τον προϋπολογισμό και τον προγραμματισμό που είναι απαραίτητες για την υλοποίηση των επιλεγμένων αποκρίσεων
- Σχέδια επείγουσας ανάγκης που απαιτείται να εκτελεστούν
- Εφεδρικά σχέδια που θα χρησιμοποιηθούν ως αντίδραση σε έναν κίνδυνο που έχει εμφανιστεί και η βασική απόκριση είναι τελικά ανεπαρκής
- Ορισμένους κινδύνους που είναι αναμενόμενο να παραμείνουν και μετά από την εφαρμογή των σχεδιασμένων αποκρίσεων, καθώς και τους κινδύνους που έχουν γίνει σκόπιμα αποδεκτοί

- Δευτερεύοντες κινδύνους που εμφανίζονται ως άμεσο αποτέλεσμα μιας απόκρισης κινδύνου
- Αποθεματικά που υπολογίζονται βασιζόμενα στην ποσοτική ανάλυση κινδύνων του έργου και στο κατώφλι κινδύνου της εταιρίας.

- **Αποφάσεις Συμβολαίων Λόγω Κινδύνων**

Αποφάσεις για μεταφορά του κινδύνου, όπως συμφωνίες για ασφάλιση, υπηρεσίες και άλλα στοιχεία, επιλέγονται επίσης σε αυτή τη διαδικασία. Αυτό μπορεί να συμβεί ως αποτέλεσμα μείωσης ή μεταφοράς μέρους ή όλης της απειλής, ή ενίσχυσης ή μοιράσματος μέρους ή όλης της ευκαιρίας. Το είδος του συμβολαίου που επιλέγεται παρέχει επίσης έναν μηχανισμό διαμοιρασμού των κινδύνων.

- **Ενημέρωση Σχεδιασμού Έργου**

Στοιχεία του σχεδιασμού διαχείρισης του έργου που μπορεί να ενημερωθούν περιλαμβάνουν:

- **Σχεδιασμό Προγραμματισμού Έργου**

Ο σχεδιασμός προγραμματισμού έργου ενημερώνεται για να αντικατοπτρίσει τις αλλαγές που γίνονται στη διαδικασία και στις ενέργειες λόγω των αποκρίσεων κινδύνου. Μπορεί να περιλαμβάνει αλλαγές στην ανοχή ή στη συμπεριφορά των πόρων ως προς την ποσότητα εργασιών, καθώς και στο πρόγραμμα χρονικά.

- **Σχεδιασμό Κόστους Έργου**

Ο σχεδιασμός κόστους έργου ενημερώνεται για να αντικατοπτρίσει τις αλλαγές που γίνονται στη διαδικασία και στις ενέργειες λόγω των αποκρίσεων κινδύνου. Μπορεί να περιλαμβάνει αλλαγές στην ανοχή ή στη συμπεριφορά σχετικά με τη λογιστική του κόστους, την παρακολούθηση και τις αναφορές, καθώς και ενημερώσεις στον προϋπολογισμό και στην κατανάλωση των αποθεματικών.

- **Σχεδιασμό Ποιότητας Έργου**

Ο σχεδιασμός ποιότητας έργου ενημερώνεται για να αντικατοπτρίσει τις αλλαγές που γίνονται στη διαδικασία και στις ενέργειες λόγω των αποκρίσεων κινδύνου. Μπορεί να περιλαμβάνει αλλαγές στην

ανοχή ή στη συμπεριφορά σχετικά με τις απαιτήσεις, την διαβεβαίωση ποιότητας, ή τον έλεγχο ποιότητας, καθώς και ενημερώσεις των εγγράφων με τις απαιτήσεις του έργου.

- **Σχεδιασμό Προμηθειών Έργου**

Ο σχεδιασμός προμηθειών έργου ενημερώνεται για να αντικατοπτρίσει τις αλλαγές που γίνονται στη στρατηγική, όπως εναλλαγές στις αποφάσεις μεταξύ κατασκευής ή αγοράς ορισμένων στοιχείων ή στους τύπους συμβολαίων, που επηρεάζονται από τις αποκρίσεις κινδύνου.

- **Σχεδιασμό Ανθρωπίνων Πόρων Έργου**

Ο σχεδιασμός ανθρωπίνων πόρων έργου, που είναι μέρος του σχεδιασμού ανθρωπίνων πόρων, ενημερώνεται για να αντικατοπτρίσει τις αλλαγές που γίνονται στην οργανωτική δομή του έργου και στις εφαρμογές των πόρων, που οφείλονται στις αποκρίσεις κινδύνου. Μπορεί να περιλαμβάνει αλλαγές στην ανοχή ή στη συμπεριφορά σχετικές με την κατανομή του προσωπικού, καθώς και με την ποσότητα των εργασιών που αναθέτεται στους πόρους.

- **Αναλυτική Δομή Εργασιών**

Η αναλυτική δομή εργασιών μπορεί να αλλάξει λόγω του νέου φόρτου εργασιών ή των αλλαγών του που οφείλονται στις αποκρίσεις των κινδύνων.

- **Βασικό Χρονοδιάγραμμα**

Το βασικό χρονοδιάγραμμα μπορεί να αλλάξει λόγω του νέου φόρτου εργασιών ή των αλλαγών του που οφείλονται στις αποκρίσεις των κινδύνων.

- **Βασικό Κόστος Επίδοσης**

Το βασικό κόστος επένδυσης μπορεί να αλλάξει λόγω του νέου φόρτου εργασιών ή των αλλαγών του που οφείλονται στις αποκρίσεις των κινδύνων.

- **Ενημερώσεις Εγγράφων Έργου**

Η ενημέρωση των εγγράφων του έργου περιλαμβάνει:

- **Ενημερώσεις Παραδοχών**

Νέες πληροφορίες γίνονται διαθέσιμες με την εφαρμογή των αποκρίσεων κινδύνων, οπότε οι διάφορες παραδοχές που έχουν γίνει αλλάζουν. Η ενημέρωση των παραδοχών λόγω των αλλαγμένων πληροφοριών είναι απαραίτητη και γίνεται είτε στη δήλωση του πεδίου εφαρμογής του έργου είτε σε ξεχωριστά έγγραφα.

- **Ενημερώσεις τεχνικών εγγράφων**

Νέες πληροφορίες γίνονται διαθέσιμες με την εφαρμογή των αποκρίσεων κινδύνων, επομένως τεχνικές προσεγγίσεις ή παραδοτέα που έχουν αποφασιστεί θα πρέπει να επανεξεταστούν.

2.3.6 Παρακολούθηση και Έλεγχος Κινδύνων

Είναι η διαδικασία εφαρμογής του σχεδίου αντιμετώπισης κινδύνων, παρακολούθησης των προσδιορισμένων κινδύνων, καθορισμός νέων κινδύνων και αξιολόγηση της αποτελεσματικότητας της διαδικασίας διαχείρισης κινδύνου σε όλο το έργο.
Η αντιμετώπιση των κινδύνων που έχουν συμπεριληφθεί στον προγραμματισμό του έργου εκτελούνται καθ'όλη τη διάρκεια ζωής του έργου ενώ παράλληλα θα πρέπει να είναι συνεχής η παρακολούθηση και ο έλεγχος για τυχόν νέους κινδύνους.
Η διαδικασία παρακολούθησης και ελέγχου των κινδύνων απαιτεί τη χρήση πληροφορίας που παρέχεται κατά τη διάρκεια του έργου. Επίσης χρησιμοποιείται για τον προσδιορισμό των παρακάτω:

- Αν οι αρχικές υποθέσεις του έργου είναι ακόμη έγκυρες.
- Αν η ανάλυση που έχει γίνει δείχνει ότι ένας κίνδυνος έχει ξεπεραστεί ή έχει αλλάξει.
- Αν οι διαδικασίες της διαχείρισης κινδύνου ακολουθούνται.

- Αν η αρχική πρόβλεψη κόστους και σχεδιασμού όσον αφορά τον κίνδυνο θα πρέπει να αλλάξει σε σχέση με την τρέχουσα εκτίμηση κινδύνου.

Η παρακολούθηση και ο έλεγχος των κινδύνων μπορεί να περιλαμβάνει εναλλακτικές στρατηγικές, διορθωτικές ενέργειες και αλλαγή στον προγραμματισμό του έργου. Το άτομο που αναλαμβάνει να διαχειριστεί το κάθε πιθανό ενδεχόμενο που αφορά έναν κίνδυνο θα πρέπει να αναφέρει περιοδικά στον διαχειριστή του έργου τυχόν αναπάντεχα φαινόμενα, να κρίνει αν είναι ή όχι αποτελεσματικό το υπάρχον πλάνο διαχείρισης του κινδύνου και να προτείνει αλλαγές εάν κάτι τέτοιο θεωρηθεί αναγκαίο.
Τέλος τα δεδομένα που αφορούν ένα κίνδυνο, ανεξάρτητα από το αν θα παρουσιαστεί ή όχι κατά τη διάρκεια του έργου, διατηρούνται στη βάση δεδομένων του οργανισμού που το εκτελεί και δύναται να χρησιμοποιηθούν για μελλοντικά έργα.

- **Μητρώο Κινδύνων**

Το μητρώο κινδύνων έχει σημαντικές εισόδους για το έργο και περιλαμβάνει τους προσδιορισμένους κινδύνους και τους υπεύθυνους, συμφωνημένες αποκρίσεις, συγκεκριμένες ενέργειες υλοποίησης, συμπτώματα και προειδοποιητικά σημάδια κινδύνων, δευτερεύοντες κινδύνους, λίστα παρακολούθησης κινδύνων χαμηλής προτεραιότητας, καθώς και αποθεματικά χρόνου και κόστους.

- **Σχεδιασμός Διαχείρισης Έργου**

Ο σχεδιασμός διαχείρισης έργου εμπεριέχει το σχεδιασμό διαχείρισης κινδύνων, που περιλαμβάνει ανοχές κινδύνου, πρωτόκολλα και αναθέσεις ανθρώπων (συμπεριλαμβανομένου υπεύθυνων κινδύνου) και χρόνου, καθώς και άλλους πόρους στο σχεδιασμό διαχείρισης κινδύνων.

- **Πληροφορίες Προόδου Εργασιών**

Οι πληροφορίες προόδου εργασιών που σχετίζονται με διάφορα αποτελέσματα προόδου, περιλαμβάνουν:

- Κατάσταση Παραδοτέων
- Πρόοδο προγράμματος
- Υφιστάμενα Κόστη
- Αναφορές Προόδου

Οι αναφορές προόδου παίρνουν πληροφορίες από μετρήσεις προόδου και τις αναλύουν, παρέχοντας πληροφορίες προόδου των εργασιών του έργου, συμπεριλαμβάνοντας ανάλυση διακύμανσης, δεδομένα εκτελεσθείσας αξίας, και δεδομένα προβλέψεων.

Παρακολούθηση και Έλεγχος Κινδύνων: Εργαλεία και Τεχνικές

- **Επανεκτίμηση Κινδύνων**

Η Παρακολούθηση και ο Έλεγχος των Κινδύνων έχει ως αποτέλεσμα τον προσδιορισμό νέων κινδύνων, επανεκτίμηση τωρινών κινδύνων, και το κλείσιμο των παλαιότερων κινδύνων. Η επανεκτίμηση των κινδύνων του έργου θα πρέπει να προγραμματίζεται τακτικά. Η επανάληψη της διαδικασίας επανεκτίμησης εξαρτάται από την πρόοδο του έργου σε σχέση με τους στόχους του.

- **Έλεγχος Κινδύνων**

Ο έλεγχος κινδύνων εξετάζει και καταγράφει την αποτελεσματικότητα των αποκρίσεων σε σχέση με τους προσδιορισμένους κινδύνους και τα αίτιά τους, καθώς και ως προς την αποτελεσματικότητα της διαδικασίας διαχείρισης κινδύνων. Ο διαχειριστής του έργου είναι υπεύθυνος για τη διασφάλιση εκτέλεσης των ελέγχων με τη σωστή συχνότητα, όπως καθορίζεται στο σχεδιασμό διαχείρισης έργου. Οι έλεγχοι κινδύνων μπορεί να συμπεριλαμβάνονται στις καθιερωμένες συναντήσεις για την πρόοδο του έργου, ή σε ξεχωριστές συναντήσεις. Ο τρόπος που γίνεται ο έλεγχος και οι σκοποί του θα πρέπει να έχουν καθοριστεί πριν την εφαρμογή του.

- **Ανάλυση Διακύμανσης και Τάσης**

Πολλές διαδικασίες ελέγχου χρησιμοποιούν ανάλυση διακύμανσης για να συγκρίνουν τα σχεδιασμένα με τα πραγματικά αποτελέσματα. Για τους σκοπούς της παρακολούθησης και ελέγχου των γεγονότων κινδύνου, θα πρέπει να επανεξετάζονται οι τάσεις που εμφανίζονται κατά την εκτέλεση του έργου χρησιμοποιώντας πληροφορίες επίδοσης. Ανάλυση εκτελεσθείσας αξίας και άλλες μέθοδοι ανάλυσης διακύμανσης και τάσεων του έργου μπορεί να χρησιμοποιηθούν για την παρακολούθηση της συνολικής επίδοσης του έργου. Τα αποτελέσματα από μια τέτοια ανάλυση μπορεί να προβλέψουν πιθανή παρέκκλιση του έργου από τους στόχους κόστους και προγραμματισμού. Μια τέτοια παρέκκλιση μπορεί να δείχνει τυχόν εμφάνιση απειλών ή ευκαιριών.

- **Μέτρηση Τεχνικών Επιδόσεων**

Η μέτρηση τεχνικών επιδόσεων συγκρίνει τους τεχνικούς στόχους που πραγματοποιήθηκαν κατά τη διάρκεια του έργου με την τεχνική πρόοδο που υπάρχει στον αρχικό σχεδιασμό του έργου. Απαιτεί τον προσδιορισμό των ποσοτικά μετρήσιμων τεχνικών στόχων, που θα συγκριθούν με τους αρχικά προσδιορισμένους. Οι μετρήσεις τεχνικής επίδοσης μπορεί να περιλαμβάνουν χρόνους αλληλεπίδρασης, αριθμό ελαττωματικών στοιχείων, χωρητικότητα αποθήκευσης και άλλα. Τυχόν αποκλίσεις σε σχέση με το αρχικό πλάνο βοηθούν στην πρόβλεψη επίτευξης του αρχικού πλάνου του έργου, και μπορεί να εκθέσει και τυχόν τεχνικούς κινδύνους που θα εμφανιστούν.

- **Ανάλυση Αποθεματικών**

Κατά τη διάρκεια εκτέλεσης του έργου, ορισμένοι κίνδυνοι μπορεί να εμφανιστούν, με θετικές ή αρνητικές επιπτώσεις στα αποθεματικά προϋπολογισμού και προγραμματισμού. Η ανάλυση αποθεματικών συγκρίνει την ποσότητα αποθεματικών που απομένει με την ποσότητα του κινδύνου που απομένει σε κάθε χρονική στιγμή του έργου, με σκοπό να προσδιοριστεί εάν τα αποθεματικά που υπάρχουν είναι επαρκή.

- **Συναντήσεις Κατάστασης Έργου**

Η διαχείριση κινδύνων του έργου θα πρέπει να αποτελεί μέρος της συζήτησης στις συναντήσεις που γίνονται περιοδικά για τον έλεγχο του έργου. Ο χρόνος που απαιτείται για το λόγο αυτό ποικίλλει ανάλογα με τους κινδύνους που έχουν προσδιοριστεί, την προτεραιότητά τους, και τη δυσκολία απόκρισης. Η διαχείριση κινδύνων είναι πιο εύκολη όσο συχνότερα γίνεται. Συχνές συζητήσεις από τους εμπλεκομένους για τους κινδύνους αυξάνει την πιθανότητα προσδιορισμού τους, καθώς και ευκαιριών από μπορεί να εμφανιστούν.

Παρακολούθηση και Έλεγχος Κινδύνων: Συμπεράσματα

- **Ενημέρωση Μητρώου Κινδύνων**

Ένα ενημερωμένο μητρώο κινδύνων περιλαμβάνει:

Αποτελέσματα επανεξέτασης κινδύνων, ελέγχου κινδύνων, και περιοδικής αναθεώρησης κινδύνων. Τα αποτελέσματα αυτά μπορεί να περιλαμβάνουν προσδιορισμό νέων γεγονότων κινδύνου και ενημερώσεις πιθανότητας, αποτελέσματος, προτεραιότητας, σχεδίων απόκρισης, υπευθυνότητας και άλλως στοιχείων

του μητρώου κινδύνων. Πραγματικά αποτελέσματα των κινδύνων του έργου και των αποκρίσεών τους. Οι πληροφορίες αυτές μπορεί να βοηθήσουν τους διαχειριστές του έργου στο σχεδιασμό ρίσκου στην επιχείρησή τους, καθώς και σε μελλοντικά έργα.

- **Ενημέρωση Διαδικασιών Επιχείρησης**

Οι έξι διαδικασίες Διαχείρισης Κινδύνου Έργου παράγουν πληροφορίες που μπορεί να χρησιμοποιηθούν για μελλοντικά έργα, και θα πρέπει να καταγραφούν ως περιουσιακά στοιχεία της επιχείρησης. Τα περιουσιακά στοιχεία που μπορεί να ενημερωθούν περιλαμβάνουν:

- Πρότυπα για το σχεδιασμό διαχείρισης κινδύνου, που περιλαμβάνουν τον πίνακα πιθανοτήτων και αποτελεσμάτων, και το μητρώο κινδύνων
- Αναλυτική Δομή Κινδύνων
- Διδάγματα από τις δραστηριότητες διαχείρισης κινδύνου του έργου.

Τα έγγραφα αυτά θα πρέπει να ενημερώνονται σωστά κατά το κλείσιμο του έργου. Περιλαμβάνονται τελικές εκδόσεις καταλόγου κινδύνων, πρότυπα σχεδιασμού διαχείρισης κινδύνου, λίστας ελέγχου και αναλυτικής δομής κινδύνων.

- **Αιτήματα Αλλαγής**

Η υλοποίηση σχεδίων επείγουσας επέμβασης μπορεί να καταλήξει σε κάποιο αίτημα αλλαγής. Τα αιτήματα αυτά ετοιμάζονται και υποβάλλονται κατά τη διάρκεια κατάλληλης διαδικασίας. Επίσης μπορεί να περιέχουν διορθωτικές και προληπτικές ενέργειες.

- **Προτεινόμενες διορθωτικές αλλαγές**. Οι προτεινόμενες διορθωτικές αλλαγές περιλαμβάνουν σχέδια επείγουσας επέμβασης και λύσεις. Οι λύσεις είναι αποκρίσεις που δεν είχαν σχεδιαστεί αρχικά αλλά είναι απαραίτητες για αναδυόμενους κινδύνους που ήταν απροσδιόριστοι ή παθητικά αποδεκτοί.
- **Προτεινόμενες προληπτικές ενέργειες**. Οι προτεινόμενες προληπτικές ενέργειες αποτελούν γραπτές οδηγίες εκτέλεσης μιας ενέργειας που μπορεί να μειώσει την πιθανότητα εμφάνισης αρνητικών συνεπειών σχετικών με κινδύνους του έργου.

- **Ενημέρωση Σχεδιασμού Διαχείρισης Έργου**

Εάν οι εγκεκριμένες αιτήσεις αλλαγής έχουν επίδραση στη διαδικασία διαχείρισης κινδύνων, τα αντίστοιχα έγγραφα στοιχείων του σχεδιασμού διαχείρισης του έργου αναθεωρούνται και επανεκδίδονται για να αντικατοπτρίσουν τις εγκεκριμένες αλλαγές. Τα στοιχεία του σχεδιασμού διαχείρισης έργου που ενημερώνονται είναι τα ίδια με αυτά της διαδικασίας Σχεδιασμού Αποκρίσεων Κινδύνων.

- **Ενημέρωση Εγγράφων Έργου**

Τα έγγραφα έργου που μπορεί να ενημερωθούν από τη διαδικασία Παρακολούθησης και Ελέγχου των Κινδύνων είναι ίδια με αυτά της διαδικασίας Σχεδιασμού Αποκρίσεων Κινδύνων.

ΚΕΦΑΛΑΙΟ 3

3.1 Βασικές Αρχές Διαχείρισης κινδύνων στα Έργα Πληροφορικής

3.1.1 Σκοπός της Διαχείρισης Κινδύνων

Η διαχείριση κινδύνων στα έργα πληροφορικής έχει διαφορετικά ζητήματα που πρέπει να επιλύσει (σε σχέση με τα έργα μη πληροφορικής). Βοηθάει στη διάσωση έργων από την αποτυχία εξαιτίας διαφορετικών παραγόντων, όπως μη ολοκλήρωση των έργων μέσα στο καθορισμένο χρονοδιάγραμμα και προϋπολογισμό, και μη ικανοποίησης των απαιτήσεων του πελάτη.

Η διαχείριση κινδύνων εξετάζει τα έργα από διαφορετικές οπτικές γωνίες για να διασφαλίσει ότι οι απειλές που μπορούν να θέσουν σε κίνδυνο τα έργα έχουν προσδιορισθεί, αναλυθεί και έχουν ληφθεί οι κατάλληλες στρατηγικές για να μετριάσουν και να ελέγξουν τους κινδύνους. Οι στρατηγικές μετριασμού των κινδύνων δεν σημαίνουν απαραίτητα ότι θα καταργήσουμε από το έργο τις δραστηριότητες που εμπεριέχουν κίνδυνο.

Στις εταιρείες πληροφορικής πολλές δραστηριότητες μπαίνουν σε φάση υλοποίησης, ακόμα και εάν οι εταιρείες γνωρίζουν ότι αυτές οι δραστηριότητες εμπεριέχουν υψηλό κίνδυνο. Πολλές φορές οι δραστηριότητες που εμπεριέχουν υψηλούς κινδύνους είναι σημαντικές για μια επιχείρηση, για να αποκτήσει η επιχείρηση στρατηγικό πλεονέκτημα έναντι των ανταγωνιστών της.

Ο κύριος σκοπός της διαχείρισης κινδύνων σε ένα έργο είναι να γνωρίζει όλους τους κινδύνους, να εκτιμήσει την σοβαρότητά τους και τις πιθανές συνέπειες που μπορεί να προκαλέσουν και να καθορίσει τα στάδια αντιμετώπισης και εξάλειψης των κινδύνων ανάλογα με την φύση τους. Η κεντρική ιδέα είναι η εξάλειψη οποιουδήποτε αναπάντεχου προβλήματος που μπορεί να προκύψει κατά την διάρκεια του έργου, με το να είναι έτοιμοι και σε εγρήγορση για όλα τα ενδεχόμενα τόσο ο διευθυντής του έργου όσο και η ομάδα του έργου. Ο σωστός σχεδιασμός και η καλή προετοιμασία οδηγούν στην ελαχιστοποίηση των αβεβαιοτήτων, οι οποίες μπορεί να οδηγήσουν σε ολοκλήρωση του έργου με προβλήματα, ή ακόμα χειρότερα και σε πρόωρο τερματισμό του έργου.

Η διαχείριση κινδύνων στην τεχνολογία λογισμικού, και κατ’ επέκταση στα έργα πληροφορικής, χρησιμοποιεί μια πολύ προσεκτική προσέγγιση λαμβάνοντας όλα τα δυνατά προληπτικά μέτρα, έτσι ώστε να γίνει η ολοκλήρωση ενός έργου μέσα στον καθορισμένο χρόνο και προϋπολογισμό. Στην πραγματικότητα στα έργα που λαμβάνονται υπόψη οι κίνδυνοι το τελικό αποτέλεσμα είναι πολύ καλύτερο τόσο από πλευράς τελικού κόστους και χρόνου υλοποίησης όσο και από την πλευρά της ποιότητας των παραδοτέων. Χωρίς την διαχείριση κινδύνων θα υπήρχε μεγάλη πιθανότητα οι εταιρείες που υλοποιούν έργα να χάσουν τόσο έσοδα όσο και την φήμη τους στους πελάτες (όπως και συμβαίνει άλλωστε), ή ακόμα χειρότερα να οδηγηθούν σε ολοκληρωτική πτώχευση οι συμμετέχοντες επιχειρήσεις / οργανισμοί σε ένα έργο.

3.2 Η Διαχείριση Κινδύνων και οι Διαστάσεις της

Η διαχείριση κινδύνων στην τεχνολογία λογισμικού υπάρχει και χρησιμοποιείται εδώ και αρκετές δεκαετίες. Ωστόσο, όπως αναφέρθηκε και νωρίτερα, τα τελευταία χρόνια έχει αποκτήσει καθολική αναγνώριση και αποδοχή από την κοινότητα της τεχνολογίας λογισμικού. Στα έργα πληροφορικής που υλοποιήθηκαν μέχρι και τις αρχές του 21ου αιώνα χρησιμοποιούνταν διαφορετικές και κατά περίπτωση προσεγγίσεις για την διαχείριση κινδύνων, χωρίς παρόλα αυτά να εφαρμόζονται κάποιες συγκεκριμένες μεθοδολογίες. Η ολοένα και αυξανόμενη πολυπλοκότητα των έργων πληροφορικής οδήγησε τις εταιρείες να κατανοήσουν την σπουδαιότητα της διαχείρισης κινδύνων, γιατί πολύ απλά βοηθάει στην εξάλειψη των αβεβαιοτήτων και μειώνει την πιθανότητα να αποτύχει κάποιο έργο.

3.3 Διαχείριση Κινδύνων Πληροφορικής σε Εταιρείες

Το αποτέλεσμα ενός έργου πληροφορικής, είτε είναι προϊόν λογισμικού είτε υπηρεσία πρέπει να έχει σχεδιαστεί σωστά για να μπορέσει να λειτουργήσει αποδοτικά στο περιβάλλον στο οποίο λειτουργεί η επιχείρηση. Είναι σημαντικό να κατανοήσουμε το αντίκτυπο που θα έχει για την επιχείρηση ένα προϊόν λογισμικού το οποίο είτε δυσλειτουργεί, είτε δεν εκπληρώνει τους στόχους για τους οποίους είχε σχεδιαστεί. Σε κάθε περίπτωση όλοι οι κίνδυνοι (ή οι περισσότεροι) που προέρχονται από την τεχνολογία των πληροφοριών θα μπορούσαν να έχουν εξαλειφθεί, εάν κατά το έργο πληροφορικής που απέδωσε το/α συγκεκριμένο/α παραδοτέο/α είχαν ληφθεί υπόψη οι κίνδυνοι που σχετίζονται τόσο με την ανάπτυξη του προϊόντος όσο και με την λειτουργία του.

Πρέπει να κατανοήσουμε ότι τα προϊόντα λογισμικού συντηρούνται και επεκτείνονται σε όλη τη διάρκεια του κύκλου ζωής τους μέχρι να βγουν εκτός παραγωγής. Επιπλέον, πρέπει να έχουμε στο μυαλό μας ότι το πληροφοριακό περιβάλλον της επιχείρησης μεταβάλλεται και δεν μένει σταθερό (π.χ. αλλαγή δικτυακής υποδομής, μεταβολή τελικών χρηστών, νέες πολιτικές ασφάλειας κλπ).

Συνεπώς, η ιδιαίτερη φύση των έργων πληροφορικής και η μεταβλητότητα του πληροφοριακού περιβάλλοντος πρέπει να ληφθούν υπόψη κατά το σχεδιασμό και την ανάπτυξη του προϊόντος λογισμικού.

Στα έργα πληροφορικής παίζει πολύ μεγάλο ρόλο η εμπειρία του διευθυντή του έργου στους τομείς του σχεδιασμού, της ανάπτυξης και του ελέγχου του τελικού προϊόντος, έτσι ώστε να μπορέσει να τους απεικονίσει με ακρίβεια στο σχέδιο διοίκησης του έργου και να δώσει τις σωστές κατευθυντήριες γραμμές στην ομάδα του έργου.

Το καλό τεχνικό υπόβαθρο του διευθυντή ενός έργου πληροφορικής θα βοηθήσει στο να υπάρχει:

- Καλύτερη κατανόηση των τεχνικών δυσκολιών
- Έγκαιρος προσδιορισμός των κινδύνων
- Καλύτερη επικοινωνία με την ομάδα έργου
- Αποφυγή παρανοήσεων μεταξύ των συμμετεχόντων στο έργο
- Αποτελεσματικότερη παρακολούθηση της πορείας ανάπτυξης του προϊόντος

Είναι απαραίτητο να κατανοήσουμε τους κινδύνους που απορρέουν από την χρήση της τεχνολογίας της πληροφορικής σε μια επιχείρηση έτσι ώστε να μπορέσουμε να κατανοήσουμε το περιβάλλον στο οποίο θα κληθεί να λειτουργήσει το προϊόν λογισμικού που θα υλοποιηθεί ως αποτέλεσμα του έργου.
Μία από τις ιδιαιτερότητες των έργων πληροφορικής είναι το ότι δεν μπορούμε να είμαστε σίγουροι ότι το αποτέλεσμα του έργου είναι «καλό» εάν δεν δουλέψει σε πραγματικές συνθήκες (στο περιβάλλον παραγωγής της εταιρείας). Σε ένα κατασκευαστικό έργο γνωρίζουμε πως εάν έχουμε τηρήσει τους κανόνες των τεχνικών επιμελητηρίων και τις προδιαγραφές του έργου το αποτέλεσμα θα είναι άρτιο.

Όμως σε ένα έργο πληροφορικής εάν το λογισμικό ή υπηρεσία δεν λειτουργήσει σε περιβάλλον παραγωγής και δεν δοκιμαστεί έντονα δεν μπορούμε να είμαστε σίγουροι ότι το αποτέλεσμα είναι άρτιο. Για αυτό ακριβώς το λόγο πρέπει να κατανοήσουμε τους κινδύνους πληροφορικής σε μια επιχείρηση έτσι ώστε κατά την εκτέλεση ενός έργου πληροφορικής να τους λάβουμε υπόψη για να δημιουργήσουμε έναν όσο το δυνατόν αρτιότερο αποτέλεσμα.

Εάν δεν το κάνουμε αυτό υπάρχει ο κίνδυνος να μην πάρει αποδοχή το λογισμικό από την εταιρεία και όλο το έργο να βγει εκτός πλάνου στην καλύτερη περίπτωση. Στην χειρότερη περίπτωση μπορεί το έργο να ακυρωθεί με όλες τις αρνητικές συνέπειες για όλους τους συμμέτοχους στο έργο. Στα έργα πληροφορικής το έργο ολοκληρώνεται όταν το λογισμικό ή η υπηρεσία λειτουργήσει πλήρως και αποδοτικά στο περιβάλλον της επιχείρησης. Εάν αυτό δεν συμβεί τότε το έργο δεν θα παραδοθεί.
Συνεπώς, είναι λάθος να μην ληφθούν υπόψη οι κίνδυνοι της πληροφορικής στις εταιρείες, γιατί και το ίδιο το λογισμικό που αναπτύσσεται θα κληθεί να τους αντιμετωπίσει αφού θα λειτουργήσει στο περιβάλλον της επιχείρησης.

3.4 Πολιτική προστασίας – μηχανισμοί ασφαλείας

3.4.1 Γενική αρχή κανόνων ασφαλείας

Γενική αρχή κανόνων ασφαλείας αποτελεί η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ) που έχει ως στόχο της την προστασία του απορρήτου των επιστολών, της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε τρόπο καθώς και την ασφάλεια των δικτύων και πληροφοριών. Στην έννοια της προστασίας του απορρήτου των επικοινωνιών περιλαμβάνεται και ο έλεγχος της τήρησης των όρων και της διαδικασίας άρσης του απορρήτου, που προβλέπονται από τον νόμο.

Από πρακτική άποψη, η ασφάλεια μπορεί να έγκειται στην επαρκή προστασία ανθρώπων και αγαθών, για την οποία μπορεί να λαμβάνονται διάφορα μέτρα προστασίας από πιθανούς κινδύνους. Για παράδειγμα, η φυσική ασφάλεια ενός κτηρίου έγκειται στην αποτροπή εισόδου κακόβουλων ατόμων και στην αποτροπή ζημιών από φυσικές καταστροφές. Αντίστοιχα, η ασφάλεια μίας ηλεκτρονικής βάσης δεδομένων έγκειται στην προστασία των δεδομένων από καταστροφή, διαγραφή, αλλοίωση ή αποκάλυψη σε μη εξουσιοδοτημένους χρήστες. Θα πρέπει να ορίζονται, να τεκμηριώνονται, να εφαρμόζονται και να αναθεωρούνται συγκεκριμένες διαδικασίες ασφάλειας.

Οι διαδικασίες ασφάλειας καθορίζονται από την ΑΔΑΕ και ορίζουν συγκεκριμένες ενέργειες των εργαζομένων και των συνεργατών τους, των χρηστών και των συνδρομητών, του προσώπου που ασχολείται με την παροχή δικτύων ή/και υπηρεσιών ηλεκτρονικών επικοινωνιών, την αλληλουχία των ενεργειών, τους υπεύθυνους για την εκτέλεσή τους και τον τρόπο και τα μέσα τεκμηρίωσής τους.

3.4.2 Γενική αρχή ασφαλούς μεταφοράς δεδομένων μέσω διαδικτύου

Για την ασφάλεια και την διασφάλιση του απορρήτου των εφαρμογών διαδικτύου έχουν αναπτυχθεί διάφορα πρωτόκολλα και εφαρμογές που βασίζονται στις γενικές αρχές κρυπτογράφησης. Ανάλογα και με τον τύπο της εφαρμογής έχουν προτυποποιηθεί και συγκεκριμένα πρωτόκολλα .

Οι πάροχοι διαδικτυακών υπηρεσιών οφείλουν να κάνουν χρήση των ευρέως αποδεκτών τεχνικών και πρωτοκόλλων ασφαλείας των εφαρμογών διαδικτύου. Ενδεικτικά αναφέρονται για εφαρμογές παγκοσμίου ιστού (www) το πρωτόκολλο SSL (Secure Sockets Layer) , για εφαρμογές ηλεκτρονικού ταχυδρομείου το S/MIME, το PEM (Privacy Enhanced Mail) και το PGP (Pretty Good Privacy)και για ηλεκτρονικές πληρωμές μέσω πιστωτικών καρτών το πρωτόκολλο SET (Secure Electronic Transaction). Δεδομένου ότι τα νέα πρωτόκολλα και τεχνολογίες θα ανακύπτουν με την πρόοδο της επιστήμης των υπολογιστών, η ΑΔΑΕ θα εκδίδει τεχνικές οδηγίες και συστάσεις προς τους παρόχους διαδικτύου σχετικά με τα νέα πρωτόκολλα και τις τεχνολογίες.

Οι πάροχοι διαδικτύου είναι υποχρεωμένοι να ακολουθούν τα εκάστοτε ευρέως χρησιμοποιούμενα πρωτοκόλλα και τεχνολογίες, είτε αυτόβουλα είτε έπειτα από έλεγχο και αντίστοιχη οδηγία από την ΑΔΑΕ.

3.4.3 Γενική αρχή των υποχρεώσεων των παροχέων διαδικτυακών υπηρεσιών

Πρωταρχικό στοιχείο για την διασφάλιση του απορρήτου των επικοινωνιών στο διαδίκτυο αποτελεί η ύπαρξη πολιτικής ασφάλειας στους παρόχους, η οποία αφορά τους χρήστες, τους χρήστες του παρόχου και στα συστήματα που εμπλέκονται στην επικοινωνία από και προς το Διαδίκτυο.

Η γενική αρχή που θα πρέπει να ακολουθήσει ο πάροχος πρέπει να ανταποκρίνεται στις ειδικές απαιτήσεις της ασφάλειας του, να καθορίζει την πολιτική πρόσβασης σε συστήματα και πληροφορίες, την πολιτική αποδεκτής χρήσης , τι ενέργειες που ακολουθούνται για την διατήρηση τις ασφάλειας και τα μέτρα που εφαρμόζονται σε περιπτώσεις παραβίασης ή έκτακτης ανάγκης. Μέσω της γενικής αρχής των παροχέων διαδικτύου προστατεύονται και διασφαλίζονται τα δεδομένα επικοινωνίας των χρηστών και των χρηστών του παρόχου, το απόρρητο των επικοινωνιών, η προστασία των υπολογιστικών συστημάτων και των δικτυακών υποδομών και η προστασία των διαδικτυακών υπηρεσιών και εφαρμογών.

Η πολίτικη ασφάλειας που ακολουθεί ο πάροχος θα πρέπει να συμφωνεί με την γενική αρχή της ΑΔΑΕ, γι αυτό και θα υπόκειται σε έλεγχο από αυτήν τόσο ως προς την αποτελεσματικότητα της αλλά και ως προς τον βαθμό εφαρμογής της. Η φύση των επενδύσεων που γίνονται από τους παρόχους για την διατήρηση της ασφάλειας και της ακεραιότητας του δικτύου πρέπει να ακολουθεί την αρχή της αναλογικότητας, η οποία λαμβάνει υπόψη της το μέγεθος του παρόχου και των αριθμό των χρηστών παρόχου.

Σύμφωνα λοιπόν με την ΑΔΑΕ ο πάροχος υποχρεούται να τηρεί τα παρακάτω:

- Να διαθέτει και να τηρεί πολιτική πρόσβασης για τα συστήματα τα οποία αναφέρονται σε εξωτερικές συνδέσεις, επικοινωνίες δεδομένων, τηλεπικοινωνιακές συσκευές και λογισμικά προγράμματα. Καθώς και να λαμβάνει όλα τα απαραίτητα και πρόσφορα μέτρα για τη φυσική προστασία των εγκαταστάσεών του, για τον έλεγχο της φυσικής πρόσβασης, ώστε αυτή να επιτρέπεται μόνο σε εξουσιοδοτημένα πρόσωπα. Να ενημερώνουν τους χρήστες σχετικά με τα μέτρα προστασίας που μπορούν να λαμβάνουν για την διασφάλιση του απορρήτου των επικοινωνιών και των δεδομένων τους π.χ. την χρήση συγκεκριμένου λογισμικού ή τεχνολογιών κρυπτογράφησης.

- Να ενημερώνουν τους χρήστες για δεδομένα επικοινωνίας τα οποία πιθανόν να αποθηκεύονται σε αντίγραφα ασφαλείας αλλά και να του κοινοποιούν το μέγιστο χρονικό διάστημα για το οποίο τα δεδομένα θα είναι αποθηκευμένα. Να λαμβάνουν υπόψη και να εφαρμόζουν στο τμήμα της πολιτικής τους τις διατάξεις της νομοθεσίας για την επεξεργασία των δεδομένων επικοινωνίας.

- Να χρησιμοποιούν συστήματα ανίχνευσης επισυνδέσεων για την ενίσχυση προστασίας του δικτύου, 24 ώρες το 24ωρο. Η διακοπή των συστημάτων αυτών επιτρέπεται μόνο σε περιπτώσεις συντήρησης ή κάποιας βλάβης του συστήματος.

- Να διαθέτει απαραίτητο λογισμικό για την προστασία από Ιούς όλων των υπηρεσιών και εφαρμογών που προσφέρει στους χρήστες.

- Να αναπτύξει και να συντηρεί ένα σχέδιο εκτάκτου ανάγκης του συστήματος μετά από κακόβουλες επιθέσεις περιλαμβάνοντας την εκτέλεση αντίγραφων ασφαλείας, την παροχή διαδικασιών για συνέχιση της λειτουργίας σε περίπτωση ανάγκης και την ανάκτηση από μια επίθεση. Επιπλέον, να παραδίδει την πιο πρόσφατη πολιτική Αντιγράφων Ασφάλειας κάθε φορά που επιτελείται κάποια σημαντική αλλαγή σε αυτήν.

- Να διαθέτει σαφή Διαδικασία Χειρισμού Περιστατικών Ασφαλείας (ΔΧΠΑ) τα οποία απειλούν την ασφάλεια των επικοινωνιακών υποδομών αλλά και την διασφάλιση του απορρήτου των επικοινωνιών που διεξάγονται μέσω του παρόχου. Επιπλέον οφείλει να την ανανεώνει και να ελέγχει σε τακτικά διαστήματα την ετοιμότητα ενεργοποίησης όλων των μηχανισμών και προσώπων της ΔΠΧΑ καθώς επίσης και να την παραδίδει στην ΑΔΑΕ κάθε φορά για έλεγχο.

- Να διαθέτει ομάδα ελέγχου ασφάλειας του δικτύου του και κατά τους ελέγχους, να επιτρέπει την πρόσβαση στο δίκτυο ως το επίπεδο που κρίνεται αναγκαίο για την εκτέλεση τους καθώς και ομάδα αντιμετώπισης Ιών που θα μπορεί να παραπέμψει και ένα χρήστη που χρήζει βοήθειας, στην αρμόδια εταιρεία όταν της ζητηθεί.

- Να συγκροτεί ομάδα αποτίμησης κίνδυνου, που θα περιλαμβάνει τόσο τεχνικό προσωπικό (προγραμματιστές, τεχνικούς ασφάλειας κτλ) όσο και ανώτερα στελέχη, ώστε η αποτίμηση να είναι όσο το δυνατόν πιο ολοκληρωμένη.

3.4.4 Γενική αρχή δικαιωμάτων των χρηστών διαδικτυακών υπηρεσιών

Η γενική αρχή των δικαιωμάτων των χρηστών προσδιορίζει τις ειδικές απαιτήσεις σχετικά με τους συνδρομητές ή χρήστες των παρεχομένων διαδικτυακών υπηρεσιών με βάση τα δικαιώματα αυτών.
Πιο συγκεκριμένα προσδιορίζει τις απαιτήσεις των χρηστών από τον πάροχο διαδικτυακών υπηρεσιών, που είναι οι εξής:

Το πρόσωπο που ασχολείται με την παροχή διαδικτυακών υπηρεσιών ή και ηλεκτρονικών επικοινωνιών οφείλει να διατηρεί αρχείο που αναφέρει αναλυτικά τους μηχανισμούς ελέγχου πρόσβασης και αυθεντικοποίησης που χρησιμοποιούνται για την πρόσβαση των συνδρομητών ή χρηστών του στις υπηρεσίες ή/και τα δίκτυα που παρέχει.

Το πρόσωπο που ασχολείται με την παροχή διαδικτυακών υπηρεσιών ή και ηλεκτρονικών επικοινωνιών οφείλει να διαμορφώσει και να ακολουθεί συγκεκριμένη διαδικασία διαχείρισης των λογαριασμών πρόσβασης των συνδρομητών ή χρηστών στις υπηρεσίες ή/και τα δίκτυα που παρέχει , στην οποία θα περιγράφεται με σαφήνεια ο τρόπος προσθήκης και κατάργησης λογαριασμών πρόσβασης, καθώς και η απόδοση του ονόματος χρήστη και του κωδικού πρόσβασης στους συνδρομητές ή χρήστες των παρεχομένων δικτύων ή υπηρεσιών, στην περίπτωση που αυτά καθορίζονται αρχικά από αυτό.
Στην περίπτωση αυτή, το πρόσωπο που ασχολείται με την παροχή δικτύων ή/και υπηρεσιών ηλεκτρονικών επικοινωνιών οφείλει να δημιουργεί τους αρχικούς κωδικούς πρόσβασης με τρόπο που να αποτρέπει τον εύκολο προσδιορισμό τους.

Επιπρόσθετα, οφείλει να ενημερώνει με κάθε πρόσφορο μέσο τους συνδρομητές ή χρήστες των παρεχομένων δικτύων ή υπηρεσιών σχετικά με την αναγκαιότητα αλλαγής του αρχικού κωδικού πρόσβασης, καθώς και σχετικά με ενδεδειγμένους κανόνες δημιουργίας ισχυρών κωδικών πρόσβασης.
Το πρόσωπο που ασχολείται με την παροχή δικτύων ή/και υπηρεσιών ηλεκτρονικών επικοινωνιών οφείλει να διαθέτει διαδικασία σύμφωνα με την οποία διενεργείται περιοδικός έλεγχος σχετικά με την αλλαγή του αρχικού κωδικού πρόσβασης από τους συνδρομητές ή χρήστες των παρεχομένων δικτύων ή υπηρεσιών και εξασφαλίζει την εκ νέου ενημέρωσή τους σχετικά με την αναγκαιότητα αλλαγής των κωδικών πρόσβασης σε περίπτωση που δεν έχουν προβεί στην σχετική αλλαγή, σύμφωνα με την Πολιτική Ελέγχου Εφαρμογής της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών.
Σε περίπτωση που το πρόσωπο που ασχολείται με την παροχή δικτύων ή/και υπηρεσιών ηλεκτρονικών επικοινωνιών προσφέρει τη δυνατότητα στους συνδρομητές ή χρήστες των παρεχομένων δικτύων ή υπηρεσιών να αποκτήσουν πρόσβαση σε δεδομένα επικοινωνίας τους (ενδεικτικά, εξερχόμενες κλήσεις, ηλεκτρονικό ταχυδρομείο) μέσω συγκεκριμένης ιστοθέσης (web account), οφείλει να χρησιμοποιεί τους ευρέως αποδεκτούς μηχανισμούς ασφαλούς αυθεντικοποίησης και κρυπτογράφησης και να περιγράφει αυτούς σε σχετικό αρχείο το οποίο οφείλει να διατηρεί.

Το πρόσωπο που ασχολείται με την παροχή δικτύων ή/και υπηρεσιών ηλεκτρονικών επικοινωνιών οφείλει να ενημερώνει τους συνδρομητές ή χρήστες των παρεχομένων δικτύων ή υπηρεσιών σχετικά με τους κανόνες ενδεδειγμένης συμπεριφοράς αναφορικά με την προστασία των κωδικών πρόσβασης που κατέχουν, με έντυπη ή ηλεκτρονική ενημέρωση, τουλάχιστον κατά την σύναψη της μεταξύ τους σύμβασης, καθώς και σε εύκολα προσβάσιμο σημείο του ισοτόπου του. Οι κανόνες αυτοί θα πρέπει να ακολουθούν τις ευρέως αποδεκτές και διεθνείς πρακτικές.

3.4.5 Πλαίσιο χρήσης μηχανισμών ασφαλείας στο διαδίκτυο

Μια ολοκληρωμένη υλοποίηση Διαδικτυακής επικοινωνίας θα πρέπει να περιλαμβάνει επαρκείς μεθόδους κρυπτογράφησης (encryption), χρησιμοποίηση επαλήθευσης ή προσδιορισμού ταυτότητας (authentication) από τους χρήστες, και ένα σχέδιο διαχείρισης που θα ενσωματώνει αποδοτικές μεθόδους κλειδιών και κωδικών πρόσβασης.

Υπάρχουν περιπτώσεις που οι κωδικοί πρόσβασης δεν αρκούν και χρειάζεται ένα είδος δυναμικής πιστοποίησης των δεδομένων. Αυτό επιτυγχάνεται με μια σειρά από διαφορετικές τεχνολογίες όπως οι γεννήτριες δυναμικών κωδικών, τεχνικές βασισμένες στην κρυπτογραφία, καθώς και ψηφιακές υπογραφές και πιστοποιητικά.

Επίσης, ο πάροχος διαδικτύου θα πρέπει να προστατεύει τους διακομιστές του δίκτυού του και να παρέχει την δυνατότητα ανάκτησης των αρχείων του σε περίπτωση απώλειας αυτών. Οι διαχειριστές δικτύου θα πρέπει να παρέχουν μεθόδους εφεδρικών αντιγράφων όπως η πλήρη, η αυξητική και η διαφορική αντιγραφή αρχείων.

Άλλη μια μέθοδος είναι η Δικτυακή αντιγραφή αρχείων στην οποία κρυπτογραφημένα δεδομένα με αυτόματο και ασφαλή τρόπο αντιγράφονται και αποθηκεύονται σε μια περιοχή εκτός του εσωτερικού δίκτυού του παρόχου του διαδικτύου.

Επιπλέον, απαραίτητη είναι η χρήση λογισμικού κατά των κακόβουλων επιθέσεων, αυτό γίνεται κυρίως με την χρήσης αναχωμάτων ασφάλειας (firewalls), για την προστασία από ιούς.

Επιπλέον, οι εξυπηρετητές (servers) των εφαρμογών ηλεκτρονικού ταχυδρομείου μπορεί να είναι αρχικοποιημένοι ώστε κάθε μήνυμα να υπογράφεται χρησιμοποιώντας την ψηφιακή υπογραφή του αποστολέα, να απαγορεύουν την αποστολή μηνυμάτων σε μη κατάλληλους προορισμούς και να ανιχνεύουν τα κατάλληλα προγράμματα για αποστολή / λήψη μηνυμάτων. Οι χρήστες θα πρέπει να συμμορφώνονται με τους κανόνες ασφαλείας που ορίζει ο πάροχος διαδικτύου είτε ενυπόγραφα είτε ηλεκτρονικά, καθώς επίσης δεν θα πρέπει να δημοσιοποιούν υλικό σε ακατάλληλους ή παράνομους ηλεκτρονικούς τόπους.

Παρακάτω περιγράφονται εκτενέστερα οι μέθοδοι της κρυπτογράφησης, της αυθεντικοποίησης και οι μηχανισμοί προστασίας από ιούς.

Κρυπτογράφηση

Η κρυπτογραφία είναι μια επιστήμη που βασίζεται στα μαθηματικά για την κωδικοποίηση και αποκωδικοποίηση των δεδομένων. Οι μέθοδοι κρυπτογράφησης καθιστούν τα ευαίσθητα προσωπικά δεδομένα προσβάσιμα μόνο από όσους είναι κατάλληλα εξουσιοδοτημένοι. Εξασφαλίζουν έτσι το απόρρητο στις ψηφιακές επικοινωνίες αλλά και στην αποθήκευση ευαίσθητων πληροφοριών. Η κρυπτογράφηση στο διαδίκτυο έχει σκοπό την διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της μη αποποίησης ευθύνης στις συναλλαγές προστατεύοντας έτσι την ιδιωτικότητα του χρήστη. Για αυτό και οι πάροχοι οφείλουν να εφαρμόζουν αλγορίθμους και τεχνικές κρυπτογράφησης τόσο στα συστήματα και τις εφαρμογές τους όσο και στην μετάδοση των δεδομένων, ακολουθώντας διεθνή πρότυπα, καθώς υποχρεούνται να ενημερώνουν για τις τεχνικές τους την ΑΔΑΕ. Η ΑΔΑΕ από την μεριάς της οφείλει να εκδίδει τεχνικές οδηγίες και συστάσεις που θα καθορίζουν το μήκος του κλειδιού ανά πεδίο κρυπτογράφησης. Το επίπεδο της κρυπτογράφησης πρέπει να είναι τέτοιο ώστε η παραβίαση να μην είναι δυνατή σε λογικό χρόνο και με λογικούς υπολογιστικούς πόρους.

Αναγνώριση και ταυτοποίηση

Όλοι οι χρήστες του συστήματος (τεχνικό προσωπικό, διαχειριστές, προγραμματιστές, κοινοί χρήστες κλπ.), θα πρέπει να έχουν ένα μοναδικό αναγνωριστικό (user ID), για καθαρά προσωπική τους χρήση στο σύστημα. Με αυτόν τον τρόπο είναι δυνατός ο εντοπισμός του υπεύθυνου ατόμου για όλες τις δραστηριότητες που γίνονται στο πληροφοριακό σύστημα του οργανισμού. Επιπλέον, τα user IDs δεν πρέπει να φανερώνουν τα δικαιώματα του χρήστη στο σύστημα. Μια ομάδα μπορεί να μοιράζεται το ίδιο user ID για την εκτέλεση συγκεκριμένων εργασιών στο σύστημα, μόνο σε εξαιρετικές περιπτώσεις, και εφόσον κάτι τέτοιο είναι απαραίτητο για τον οργανισμό. Σε μια τέτοια περίπτωση θα πρέπει να υπάρχει ειδική έγκριση από τη διοίκηση του οργανισμού, όπως επίσης και να χρησιμοποιηθεί κάποιος μηχανισμός που θα καθορίζει τις ευθύνες των μελών της ομάδας.

Υπάρχουν διάφορες διαδικασίες αυθεντικοποίησης που μπορούν να χρησιμοποιηθούν για την επιβεβαίωση της ταυτότητας ενός χρήστη. Τα συνθηματικά είναι ο πλέον συνηθισμένος τρόπος, ο οποίος βασίζεται στη χρήση ενός μυστικού, γνωστού μόνο στο χρήστη. Άλλοι μηχανισμοί αυθεντικοποίησης περιλαμβάνουν συνδυασμούς κρυπτογραφίας και πρωτοκόλλων εξακρίβωσης της ταυτότητας του χρήστη.

Διάφορα αντικείμενα, όπως έξυπνες κάρτες, τα οποία έχει στην κατοχή του ο χρήστης, μπορούν επίσης να χρησιμοποιηθούν για αυθεντικοποίηση στο σύστημα. Ένας άλλος τρόπος εξακρίβωσης της ταυτότητας, περιλαμβάνει την εξέταση διάφορων βιομετρικών χαρακτηριστικών του χρήστη, όπως είναι τα δακτυλικά αποτυπώματα. Ο συνδυασμός πολλαπλών τεχνολογιών εξακρίβωσης της ταυτότητας, έχει ως αποτέλεσμα ισχυρότερη αυθεντικοποίηση.

Προστασία από ιούς

Ο πάροχος θα πρέπει να διαθέτει κατάλληλο λογισμικό για την προστασία από ιούς για όλες τις υπηρεσίες και εφαρμογές που προσφέρει στους χρήστες . Για παράδειγμα υπηρεσία e-mail απαιτεί χρήση e-mail scanner. Θα πρέπει επίσης να εγκαθιστά μονίμως μνήμη (memory resident) των υπολογιστικών συστημάτων λογισμικό προστασίας από ιούς το οποίο θα εξετάζει αυτομάτως όλα τα εισερχόμενα μηνύματα. Επίσης, και οι χρήστες από την άλλη θα πρέπει να προστατεύονται ομοίως και θα πρέπει να ελέγχονται αλλά και να ενημερώνονται από τον πάροχο σχετικά με το πως μπορούν να προστατευθούν επιπλέον. Θα πρέπει να υλοποιηθούν οι κατάλληλοι μηχανισμοί για την αποτροπή και τον εντοπισμό κακόβουλου λογισμικού. Η προστασία απέναντι στο κακόβουλο λογισμικό θα πρέπει να βασίζεται στην ενημέρωση του προσωπικού για την ασφάλεια του οργανισμού, τα κατάλληλα δικαιώματα προσπέλασης και τους μηχανισμούς διαχείρισης αλλαγών στο σύστημα.
Οι παρακάτω μηχανισμοί ελέγχου έχουν ιδιαίτερη σημασία για την προστασία αρχείων που εξυπηρετούν μεγάλο αριθμό σταθμών εργασίας.

- Μια επίσημη πολιτική που να επιβάλει την ύπαρξη των κατάλληλων αδειών χρήσης λογισμικού και να απαγορεύει τη χρήση μη εξουσιοδοτημένου λογισμικού.
- Μια επίσημη πολιτική που να προστατεύει το πληροφοριακό σύστημα από λογισμικό και αρχεία που μπορούν να εισέλθουν στο σύστημα από κάποιο εξωτερικό δίκτυο ή μέσο αποθήκευσης.
- Εγκατάσταση και τακτική ενημέρωση προγραμμάτων antivirus για τον έλεγχο προσωπικών υπολογιστών και αποθηκευτικών μέσων.
- Τακτικός έλεγχος του χρησιμοποιούμενου λογισμικού και των αρχείων του συστήματος. Οποιαδήποτε αλλαγή θα πρέπει να ερευνάται. Ο έλεγχος αρχείων και αποθηκευτικών μέσων για ιούς πριν από τη χρήση τους.Ο έλεγχος των εισερχόμενων ηλεκτρονικών μηνυμάτων για ιούς. Ο συγκεκριμένος έλεγχος μπορεί να γίνει σε διάφορα σημεία του συστήματος, όπως τους εξυπηρετητές ηλεκτρονικού ταχυδρομείου, τους προσωπικούς υπολογιστές κλπ. Την εκπαίδευση των χρηστών και ύπαρξη διαδικασιών για την αντιμετώπιση ιών.

- Την ύπαρξη σχεδίου επιχειρησιακής συνέχειας στην περίπτωση εκτεταμένων ζημιών στο σύστημα από ιούς.
- Την ύπαρξη διαδικασιών για τον έλεγχο της ακρίβειας της πληροφόρησης για ιούς.

3.5 Προστασία Πληροφοριακών Συστημάτων

3.5.1 Έλεγχος Πρόσβασης

Βασική προϋπόθεση στην ασφάλεια των συστημάτων της εταιρείας είναι ο έλεγχος πρόσβασης στα συστήματα της τόσο από φυσική άποψη στο υλικό κομμάτι, φυλάσσοντας και προστατεύοντας τους servers της και τα υπόλοιπα υπολογιστικά συστήματα σε ασφαλείς χώρους, εξασφαλίζοντας περιορισμένη και ελεγχόμενη πρόσβαση σε αυτά, όσο και ο έλεγχος πρόσβασης των απομακρυσμένων χρηστών της στις υπηρεσίες της και της εφαρμογές της. Η πρόσβαση θα πρέπει να επιτρέπεται μόνο σε εξουσιοδοτημένους χρήστες καθότι απειλές μπορεί να δεχτούν τα συστήματα και από εσωτερικούς χρήστες, όχι μόνο από εξωτερικούς. Οι απειλές εκ των έσω μπορεί να είναι η διαρροή ευαίσθητων πληροφοριών, κρούσματα ιών, απάτες από κακόβουλους χρήστες κ.α τα οποία χρήζουν αντίστοιχης αντιμετώπισης. Για αυτό απαραίτητη προϋπόθεση για ολοκληρωμένη ασφάλεια είναι και η προστασία από εσωτερικές απειλές.
Η πρόσβαση θα επιτρέπεται μόνο μέσω διαδικασιών αυθεντικοποίησης και ταυτοποίησης. Η έξυπνη κάρτα (smart card) είναι μια κάρτα που ενσωματώνει ένα μικροεπεξεργαστή, ο οποίος βρίσκεται κάτω από μια επαφή από χρυσό, προσαρμοσμένο στη μια πλευρά της. Τα δεδομένα στην έξυπνη κάρτα δεν είναι εύκολο να παραλλαχθούν ή και να διαγραφούν, γιατί ο μικροεπεξεργαστής της δεν περιέχει δεδομένα για το χρήστη. Ο μικροεπεξεργαστής της κάρτας και ο υπολογιστής, με τον οποίο συνδέεται, επικοινωνούν πριν ο μικροεπεξεργαστής επιτρέψει την πρόσβαση στα δεδομένα που περιέχονται στη μνήμη της κάρτας. Με τον τρόπο αυτό αποτρέπεται η παραχάραξη των δεδομένων κι έτσι ο χρήστης διασφαλίζεται, αν η κάρτα του βρεθεί σε διαφορετικά από τα δικά του χέρια.

Η τροφοδοσία της κάρτας με ενέργεια εξασφαλίζεται από τον αναγνώστη έξυπνης κάρτας (smart card reader), στον οποίο εισάγεται η κάρτα προκειμένου να χρησιμοποιηθεί. Αυτός μπορεί να επικοινωνήσει με κάποιο κεντρικό υπολογιστή, όπου υπάρχουν τα στοιχεία του χρήστη, προκειμένου να εξασφαλιστεί η πρόσβαση σε δεδομένα.

3.5.2 Έλεγχος Προσπέλασης

Απαραίτητη προϋπόθεση ασφαλής λειτουργίας των πληροφοριακών συστημάτων είναι ο έλεγχος. Από τη στιγμή που έχει διακριβωθεί η ταυτότητα ενός χρήστη μέσω του έλεγχου πρόσβασης, το σύστημα θα πρέπει να φροντίζει έτσι ώστε ο χρήστης αυτός να μπορεί να ενεργήσει μόνο στα πλαίσια των κανόνων που καθορίζονται από την πολιτική ασφάλειας. Αυτό επιτυγχάνεται εφαρμόζοντας ελέγχους προσπέλασης. Σχετικά με τους ελέγχους προσπέλασης ισχύουν οι ακόλουθες έννοιες:

- Υποκείμενα. Πρόκειται για τις ενεργές οντότητες στο σύστημα (χρήστες, διεργασίες, υπηρεσίες)
- Αντικείμενα. Με τον όρο αυτό περιγράφονται οι πόροι ή οι παθητικές οντότητες στο σύστημα (αρχεία, συσκευές, προγράμματα)
- Τρόπος προσπέλασης. Ο όρος αυτός αναφέρεται στην ενέργεια που πραγματοποιεί ένα υποκείμενο σε ένα αντικείμενο π.χ. ανάγνωση, εγγραφή, εκτέλεση, αναφορά ιδιοχαρακτηριστικών.

Ο έλεγχος προσπέλασης συνίσταται στην εξέταση αν το υποκείμενο έχει δικαίωμα για τον συγκεκριμένο τρόπο προσπέλασης στο αντικείμενο, και στην απαγόρευση της ενέργειας, αν τελικά δεν υπάρχει το σχετικό δικαίωμα. Η επιλογή της πολίτικης έλεγχου προσπέλασης εξαρτάται από τα επιμέρους χαρακτηριστικά του περιβάλλοντος που πρόκειται να προστατευτεί.

Οι τρεις βασικές προσεγγίσεις ελέγχου προσπέλασης είναι οι εξής:

- Η κατά-διάκριση (Discretionary Access Control - DAC). Μια αρκετά διαδεδομένη προσέγγιση κυρίως σε στρατιωτικούς οργανισμούς, από όπου και προέρχεται, είναι η υποχρεωτική (mandatory) προσέγγιση. Σύμφωνα με αυτή την προσέγγιση, επιτρεπτές είναι μόνο οι ενέργειες που προβλέπονται και προδιαγράφονται στην πολιτική ασφάλειας. Οτιδήποτε δεν περιλαμβάνεται στην πολιτική ασφάλειας απαγορεύεται, ανεξάρτητα από τις συνθήκες ή τις συνέπειες που η απαγόρευση αυτή μπορεί να επιφέρει. Η προσέγγιση αυτή είναι αρκετά δημοφιλής στην ανάπτυξη πολιτικών ασφάλειας πληροφοριακών συστημάτων, παρόλο που οι πολιτικές ασφάλειας που την ακολουθούν συχνά αποδεικνύονται άκαμπτες και αναποτελεσματικές. Είναι προφανές ότι οι προδιαγραφές και οδηγίες ασφάλειας δε μπορούν να είναι τόσο λεπτομερείς, ούτε τέτοιες που να μπορούν να καλύψουν το σύνολο των δυνατών περιπτώσεων που απαιτείται κάποια ενέργεια από

τους χρήστες του πληροφοριακού συστήματος. Ειδικά σε δυναμικά περιβάλλοντα με συχνές αλλαγές, η προσέγγιση αυτή είναι λιγότερο αποτελεσματική από τις άλλες προσεγγίσεις .

- Η κατά-απαίτηση (Mandatory Access Control - MAC). Για τις πολιτικές ασφάλειας που διαμορφώνονται με βάση την προσέγγιση διακριτού (discretionary) ελέγχου, όλες οι ενέργειες που δεν περιλαμβάνονται στις απαγορευμένες θεωρούνται επιτρεπτές και σύμφωνες με την πολιτική.

Έτσι, στην περίπτωση που απαιτείται κάποια ενέργεια η οποία δεν περιλαμβάνεται στην πολιτική ασφάλειας, θεωρείται ότι ο χρήστης θα δράσει με τρόπο που συμβαδίζει με τους στόχους της πολιτικής ασφάλειας. Η προσέγγιση αυτή, είναι ευκολότερα να γίνει αποδεκτή από τους χρήστες των πληροφοριακών συστημάτων που καλούνται να εφαρμόσουν την πολιτική ασφάλειας, διότι είναι αντίστοιχη με τον τρόπο που ισχύει η νομοθεσία ενός κράτους: οι πολίτες γνωρίζουν ότι οι ενέργειες τους θεωρούνται νόμιμες, εκτός αν ανήκουν σε αυτές που απαγορεύονται. Το προτέρημα της προσέγγισης αυτής έναντι των υπολοίπων είναι η μεγαλύτερη αποδοχή των πολιτικών ασφάλειας από τους χρήστες των πληροφοριακών συστημάτων.
Από την άλλη πλευρά, η μεγάλη ευελιξία των πολιτικών αυτών μπορεί να οδηγήσει σε μείωση του επιπέδου ασφάλειας, αυξάνοντας την επικινδυνότητα.

- Η βασισμένη-σε-ρόλους (Role-Based Access Control). Σύμφωνα με την προσέγγιση αυτή, οι οδηγίες ασφάλειας που προδιαγράφονται στην πολιτική εφαρμόζονται, μπορούν και να παρακαμφθούν όμως όταν υπάρχουν αντικρουόμενες απαιτήσεις. Επίσης οι πολιτικές αυτές μπορεί να παρακαμφθούν και στην περίπτωση που τα προσδοκώμενα οφέλη από τη μη τήρηση των οδηγιών αυτών (εξαιρουμένου του προσωπικού-ατομικού οφέλους) υπερτερούν των οφελών που θα προκύψουν από την εφαρμογή των οδηγιών της πολιτικής ασφάλειας, σε όρους επιχειρηματικών στόχων και στόχων ασφάλειας. Τα πλεονεκτήματα αυτής της προσέγγισης γίνονται περισσότερο φανερά σε ειδικές περιπτώσεις που δε θα μπορούσαν να έχουν προβλεφθεί και συμπεριληφθεί στις οδηγίες μιας πολιτικής ασφάλειας. Στις περιπτώσεις αυτές, η δράση των χρηστών είναι πιο ευέλικτη, σε σχέση με τις άλλες προσεγγίσεις. Το μειονέκτημα της ‘κατά περίπτωση’ πολιτικής ασφάλειας συνδέεται με τη δυνατότητα παράκαμψης της πολιτικής κατά την κρίση των χρηστών του πληροφοριακού συστήματος. Η δυνατότητα επιλογής για τη συμμόρφωση ή μη με την πολιτική ασφάλειας σε σχέση με τα αναμενόμενα οφέλη από την εφαρμογή της πολιτικής εισάγει το στοιχείο της υποκειμενικότητας, καθώς εναπόκειται στους χρήστες του πληροφοριακού συστήματος να αξιολογήσουν και να κρίνουν τις πιθανές συνέπειες και τα πιθανά οφέλη από την εφαρμογή των οδηγιών ασφάλειας.

Οι δυο πρώτες κατηγορίες χαρακτηρίζονται ως κλασσικές, καθώς έχουν αναγνωρίσει και εφαρμοστεί από τους ερευνητές και επαγγελματίες ασφάλειας για πολύ καιρό. Τα τελευταία χρόνια κατά γενική ομολογία υπάρχουν μοντέλα έλεγχου προσπέλασης που έχουν τα χαρακτηριστικά και των δυο προσεγγίσεων όπως τα βασισμένα σε ρόλους μοντέλα., τα οποία έχουν μονοπωλήσει τα τελευταία χρόνια το ενδιαφέρον των ερευνητών.

3.5.3 Προστασία Βάσεων Δεδομένων

Όσον αφορά την ασφάλεια βάσεων δεδομένων, θα πρέπει να λαμβάνεται υπ' όψιν ότι η βάση δεδομένων είναι ένα σύστημα που εκτελείται σε έναν υπολογιστή, πάνω από ένα λειτουργικό σύστημα, και έτσι επηρεάζεται άμεσα από τους μηχανισμούς ασφάλειας που παρέχει ο συνδυασμός αυτός υλικού/λογισμικού. Αν για παράδειγμα το λειτουργικό σύστημα δεν παρέχει επαρκείς μηχανισμούς διακρίβωσης ταυτότητας, η βάση δεδομένων θα πρέπει να υλοποιήσει δικούς της. Επίσης, αν η βάση δεδομένων αποθηκεύεται σε αρχεία που δεν προστατεύονται επαρκώς από το λειτουργικό σύστημα, οι μηχανισμοί ελέγχου πρόσβασης που υλοποιούνται από τη βάση δεδομένων μπορούν να παρακαμφθούν, απλά διαβάζοντας ή τροποποιώντας τα αρχεία σε επίπεδο λειτουργικού συστήματος.
Βασικοί κανόνες για την προστασία των βάσεων είναι ότι τόσο κατά τη φάση της επεξεργασίας των πληροφοριών όσο και κατά τη φάση της μετάδοσης πρέπει αφενός να εκτελεστούν στο σύνολο τους όλες οι δοσοληψίες και αφετέρου ότι να εφαρμόζονται όλοι οι κανόνες ακεραιότητας που έχουν ορισθεί για τη βάση δεδομένων.
Σε γενικές γραμμές μία βάση δεδομένων θα πρέπει να διαφυλάσσει την εμπιστευτικότητα των πληροφοριών την παρέχοντα πρόσβαση σε εξουσιοδοτημένους χρήστες, την ακεραιότητα των πληροφοριών της καθώς και την διαθεσιμότητα τους.
Η εμπιστευτικότητα των πληροφοριών επιτυγχάνεται με τον έλεγχο πρόσβασης στις Βάσεις Δεδομένων, ώστε να διαπιστώνεται αν ένας χρήστης έχει το δικαίωμα να χρησιμοποιήσει το σύστημα βάσεων δεδομένων ή όχι. Για διακρίβωση της ταυτότητας των χρηστών διατίθενται οι παρακάτω τεχνικές:

- Διακρίβωση ταυτότητας με όνομα χρήστη-συνθηματικό.

Η βάση δεδομένων διαθέτει κατάλογο με τις έγκυρες αντιστοιχίες ονομάτων χρηστών και συνθηματικών ώστε να αποφασίζει για το αν τα παρουσιασθέντα διαπιστευτήρια είναι έγκυρα. Η τεχνική αυτή είναι χρήσιμη όταν το λειτουργικό σύστημα δεν παρέχει αξιόπιστους μηχανισμούς διακρίβωσης ταυτότητας των χρηστών ή όταν πραγματοποιούνται συνδέσεις μέσω δικτύου στη βάση δεδομένων, οπότε η ταυτότητα του χρήστη στο λειτουργικό σύστημα δεν είναι διαθέσιμη ή αξιόπιστη.

- Διακρίβωση ταυτότητας από το λειτουργικό σύστημα.

Σ’ αυτή την περίπτωση η πρόσβαση στην ΒΔ στηρίζεται στους μηχανισμούς του λειτουργικού συστήματος για την διακρίβωση ταυτότητας. Από τη στιγμή που ένας χρήστης έχει αναγνωριστεί από το λειτουργικό σύστημα και ο χρήστης λειτουργικού συστήματος είναι εξουσιοδοτημένος να χρησιμοποιεί τη βάση δεδομένων, δεν ζητείται κανένα πρόσθετο στοιχείο για την προσπέλαση του χρήστη στη βάση δεδομένων.

Η τεχνική αυτή δεν μπορεί να χρησιμοποιείται ως αποκλειστικός μηχανισμός διακρίβωσης ταυτότητας σε συστήματα όπου επιτρέπεται δικτυακή πρόσβαση στη βάση δεδομένων, καθώς χρειάζεται κάθε χρήστης να έχει λογαριασμό στο λειτουργικό σύστημα. Επίσης, πρέπει να χρησιμοποιείται μόνον όταν το λειτουργικό σύστημα έχει επαρκώς αξιόπιστους μηχανισμούς διακρίβωσης ταυτότητας.

- Διακρίβωση ταυτότητας μέσω καθολικών υπηρεσιών καταλόγου.

Ο χρήστης εισάγει ένα όνομα και ένα συνθηματικό και για διακρίβωση του το σύστημα διασυνδέεται με καθολικές υπηρεσίες καταλόγου. Η προσέγγιση αυτή έχει το πλεονέκτημα ότι προωθεί τη χρήση κεντρικού σημείου φύλαξης των διαπιστευτηρίων σύνδεσης. Έχοντας ένα κεντρικό σημείο φύλαξης, είναι δυνατόν όλες οι ενότητες λογισμικού που απαιτούν πιστοποίηση (λειτουργικό σύστημα, βάση δεδομένων κ.λπ.) να συνδιαλέγονται με το σημείο αυτό, ούτως ώστε κάθε χρησιμοποιεί ένα μόνο ζεύγος διαπιστευτηρίων για προσπέλαση σε όλους τους πόρους.

3.5.4 Προστασία Δικτύων Υπολογιστικών Συστημάτων

Βασική προϋπόθεση για ορθή υλοποίηση της πολιτικής ασφαλείας μιας εταιρείας είναι ότι θα πρέπει να διασφαλίζει την ασφάλεια των δικτύων των υπολογιστικών συστημάτων της εταιρείας. Τα δίκτυα της εταιρείας συνίσταται από τη διασύνδεση δυο ή περισσοτέρων υπολογιστικών συστημάτων κατά τρόπο ώστε να παρέχεται η δυνατότητα στους χρήστες να επωφελούνται από ολόκληρο το υπολογιστικό δυναμικό. Αυτό πραγματοποιείται μέσω της ανταλλαγής πληροφοριών μεταξύ των χρηστών και της κοινής χρήσης των διαθέσιμων υπολογιστικών πόρων. Για αυτό το λόγο η εταιρεία πρέπει να προνοεί και για την προστασία από απειλές των δικτύων της.

Η διασύνδεση ενός εταιρικού δικτύου με το Διαδίκτυο ή άλλα εξωτερικά μη έμπιστα δίκτυα, καθιστά ολόκληρη την εταιρική πληροφορική υποδομή ευάλωτη σε μια σειρά από απειλές που δύναται να προσβάλλουν την ασφάλεια της επιχείρησης. Για αυτό τον λόγο συνίσταται η χρήση πρωτόκολλων για ασφαλή επικοινωνία όπως το HTTPS και SSL.

Η χωρίς προστασία παροχή υπηρεσιών επιτρέπει την εκμετάλλευση πιθανών υπαρκτών αδυναμιών από τρίτους, με σκοπό την παραβίαση της ασφάλειας. Για το λόγο αυτό, κρίνεται απαραίτητη η υλοποίηση εξειδικευμένων μηχανισμών ασφάλειας όπως Firewall, Web Access Systems, Mail Security Systems, Network IPS/IDS.

Η εταιρεία εξασφαλίζει την προστασία των δικτύων της μέσω ενός ολοκληρωμένου πακέτου ασφαλείας το End Point Security System, το οποίο στοχεύει στην υλοποίηση υπηρεσιών ασφάλειας στην πύλη του δικτύου (Gateway Security) από και προς το διαδίκτυο.

Οι βασικές υπηρεσίες είναι:

- Firewall
- Antivirus
- Antisyare
- Antispam
- URL Filtering
- DMZ (De Military Zone)
- Intrusion Detection / Prevention Systems

3.5.5 Παραδείγματα Πρωτόκολλων Ασφαλής Επικοινωνίας

Απαραίτητο μέτρο για ασφαλή σύνδεση και ανταλλαγή πληροφοριών ιδίως μέσω διαδικτύου είναι η χρήση και εφαρμογή πρωτόκολλων για ασφαλή επικοινωνία. Τα πρωτόκολλα αυτά παρέχουν επιπλέον ασφάλεια στην διακίνηση πληροφοριών μέσω δικτύων και στηρίζονται κυρίως στη μέθοδο της κρυπτογράφησης.

3.5.5.1 Πρωτόκολλο HTTPS (Secure HTTP)

Το σύστημα αυτό σχεδιάστηκε αρχικά από την εταιρία Netscape Communications Corporation για να χρησιμοποιηθεί σε sites όπου απαιτείται αυθεντικοποίηση χρηστών και κρυπτογραφημένη επικοινωνία. Σήμερα χρησιμοποιείται ευρέως στο διαδίκτυο όπου χρειάζεται αυξημένη ασφάλεια διότι διακινούνται ευαίσθητες πληροφορίες. Το HTTPS δεν είναι ξεχωριστό πρωτόκολλο όπως μερικοί νομίζουν, αλλά αποτελεί συνδυασμό του απλού HTTP πρωτοκόλλου και των δυνατοτήτων κρυπτογράφησης που παρέχει το πρωτόκολλο Secure Sockets Layer (SSL). Η κρυπτογράφηση που χρησιμοποιείται διασφαλίζει ότι τα κρυπτογραφημένα δεδομένα δεν θα μπορούν να υποκλαπούν από άλλους κακόβουλους χρήστες ή από επιθέσεις man-in-the-middle.

Για να χρησιμοποιηθεί το HTTPS σε έναν εξυπηρετητή (server), θα πρέπει ο διαχειριστής του να εκδώσει ένα πιστοποιητικό δημοσίου κλειδιού. Στην συνέχεια το πιστοποιητικό αυτό θα πρέπει να υπογραφεί από μία αρχή πιστοποίησης (certificate authority), η οποία πιστοποιεί ότι ο εκδότης του πιστοποιητικού είναι νομότυπος και ότι το πιστοποιητικό είναι έγκυρο. Με τον τρόπο αυτό οι χρήστες μπορούν να δουν την υπογραφή της αρχής πιστοποίησης και να βεβαιωθούν ότι το πιστοποιητικό είναι έγκυρο και ότι κανένας κακόβουλος χρήστης δεν το έχει πλαστογραφήσει.
Όπως αναφέρθηκε προηγουμένως, το HTTPS χρησιμοποιείται κυρίως όταν απαιτείται μεταφορά ευαίσθητων προσωπικών δεδομένων. Το επίπεδο προστασίας των δεδομένων εξαρτάται από το πόσο σωστά έχει εφαρμοστεί η διαδικασία ασφάλειας και από το πόσο ισχυροί είναι οι αλγόριθμοι κρυπτογράφησης που χρησιμοποιούνται.
Όσον αφορά την χρήση και τις συναλλαγές μέσω πιστωτικών καρτών, πολλοί χρήστες θεωρούν ότι το HTTPS προστατεύει ολοκληρωτικά τον αριθμό της πιστωτικής τους κάρτας από κατάχρηση, αυτό όμως δεν ισχύει. Το HTTPS χρησιμοποιεί την κρυπτογράφηση για να μεταδώσει τον αριθμό από τον υπολογιστή του πελάτη προς τον εξυπηρετητή. Η μετάδοση είναι ασφαλής και τα δεδομένα φτάνουν στον εξυπηρετητή χωρίς κανείς να μπορέσει να τα υποκλέψει. Παρόλα αυτά υπάρχει το ενδεχόμενο διάφοροι χάκερ να έχουν επιτεθεί στον εξυπηρετητή και από εκεί να έχουν υποκλέψει τα ευαίσθητα προσωπικά δεδομένα.

3.5.5.2 Πρωτόκολλο SSL (Secure Sockets Layer)

Το πρωτόκολλο SSL αναπτύχθηκε από την εταιρεία Netscape και σχεδιάστηκε για να παρέχει ασφάλεια κατά την μετάδοση ευαίσθητων δεδομένων στο διαδίκτυο. Η έκδοση 3.0 του πρωτοκόλλου κυκλοφόρησε από την Netscape το 1996 και αποτέλεσε την βάση για την μετέπειτα ανάπτυξη του πρωτοκόλλου TLS (Transport Layer Security), το οποίο πλέον τείνει να αντικαταστήσει το SSL. Τα δύο αυτά

πρωτόκολλα χρησιμοποιούνται ευρέως για ηλεκτρονικές αγορές και χρηματικές συναλλαγές μέσω του διαδικτύου.

Το SSL χρησιμοποιεί μεθόδους κρυπτογράφησης των δεδομένων που ανταλλάσσονται μεταξύ δύο συσκευών (συνηθέστερα Ηλεκτρονικών Υπολογιστών) εγκαθιδρύοντας μία ασφαλή σύνδεση μεταξύ τους μέσω του διαδικτύου. Το πρωτόκολλο αυτό χρησιμοποιεί το TCP/IP για τη μεταφορά των δεδομένων και είναι ανεξάρτητο από την εφαρμογή που χρησιμοποιεί ο τελικός χρήστης. Για τον λόγο αυτό μπορεί να παρέχει υπηρεσίες ασφαλούς μετάδοσης πληροφοριών σε πρωτόκολλα ανώτερου επιπέδου όπως για παράδειγμα το HTTP, το FTP, το telnet κοκ.

Το SSL προσφέρει συνοπτικά τις ακόλουθες υπηρεσίες:

- Πιστοποίηση του server από τον client.
- Πιστοποίηση του client από τον server
- Εγκαθίδρυση ασφαλούς κρυπτογραφημένου διαύλου επικοινωνίας μεταξύ των δύο μερών.

Ένα μειονέκτημα της χρήσης του πρωτοκόλλου SSL είναι ότι αυξάνει τα διακινούμενα πακέτα μεταξύ των δύο μηχανών και συνεπώς καθυστερεί την μετάδοση των πληροφοριών επειδή χρησιμοποιεί μεθόδους κρυπτογράφησης και αποκρυπτογράφησης. Ειδικότερα οι διάφορες καθυστερήσεις εντοπίζονται στα εξής σημεία:

Στην αρχική διαδικασία χειραψίας όπου κανονίζονται οι λεπτομέρειες της σύνδεσης και ανταλλάσσονται τα κλειδιά της συνόδου.

Στην διαδικασία κρυπτογράφησης και αποκρυπτογράφησης που γίνεται στους δύο υπολογιστές με αποτέλεσμα να δαπανώνται υπολογιστικοί πόροι και χρόνος.

Στην καθυστέρηση μετάδοσης των κρυπτογραφημένων δεδομένων αφού αυτά αποτελούνται από περισσότερα bytes σε σχέση με την αρχική μη κρυπτογραφημένη πληροφορία.

Λόγω αυτών των επιβαρύνσεων που εισάγει το πρωτόκολλο SSL, χρησιμοποιείται πλέον μονάχα σε περιπτώσεις όπου πραγματικά χρειάζεται ασφαλής σύνδεση (πχ μετάδοση κωδικών χρήστη ή αριθμών πιστωτικών καρτών μέσω του διαδικτύου) και όχι σε περιπτώσεις απλής επίσκεψης σε μία ιστοσελίδα.

3.5.5.3 End point Security Systems

Αποτελεί πολύ βασικό μέτρο για την ασφάλεια των συστημάτων της εταιρείας. Στόχος του πακέτου αυτού είναι να προστατεύει όλους τους υπολογιστές και τα δεδομένα της εταιρείας, να ελέγχει τις εξωτερικές συσκευές και τις εφαρμογές καθώς και την πρόσβαση στο δίκτυο, παρέχοντας στην εταιρεία ασφάλεια και συμβατότητα με τις κανονιστικές ρυθμίσεις και εσωτερικές πολιτικές.

Επίσης ασφαλίζει τους υπολογιστές και τα ευαίσθητα δεδομένα με τεχνολογίες anti-virus, anti-spyware και firewall. Ελαχιστοποιεί τις επιπτώσεις στους υπολογιστές προσφέροντας προστασία δεδομένων και προστασία από ιούς και malware.

Ελέγχει αυτόματα τόσο τους υπολογιστές υπό διαχείριση, όσο και τους ''άγνωστους'' υπολογιστές επισκεπτών για τυχόν μη ενημερωμένα προγράμματα ασφάλειας, πριν αποκτήσουν πρόσβαση στο δίκτυο.

Σταματά τους hackers με το ενσωματωμένο client firewall που υποστηρίζει κεντρική διαχείριση και είναι ενσωματωμένο στον anti-virus agent. Και γενικότερα βοηθά στην αύξηση της παραγωγικότητας των συστημάτων χωρίς να τα επιβραδύνει, ή να καταλύει πόρους του συστήματος. Η εταιρεία για την ακρίβεια χρησιμοποιεί το Synematic Endpoint Protection 11.

ΚΕΦΑΛΑΙΟ 4

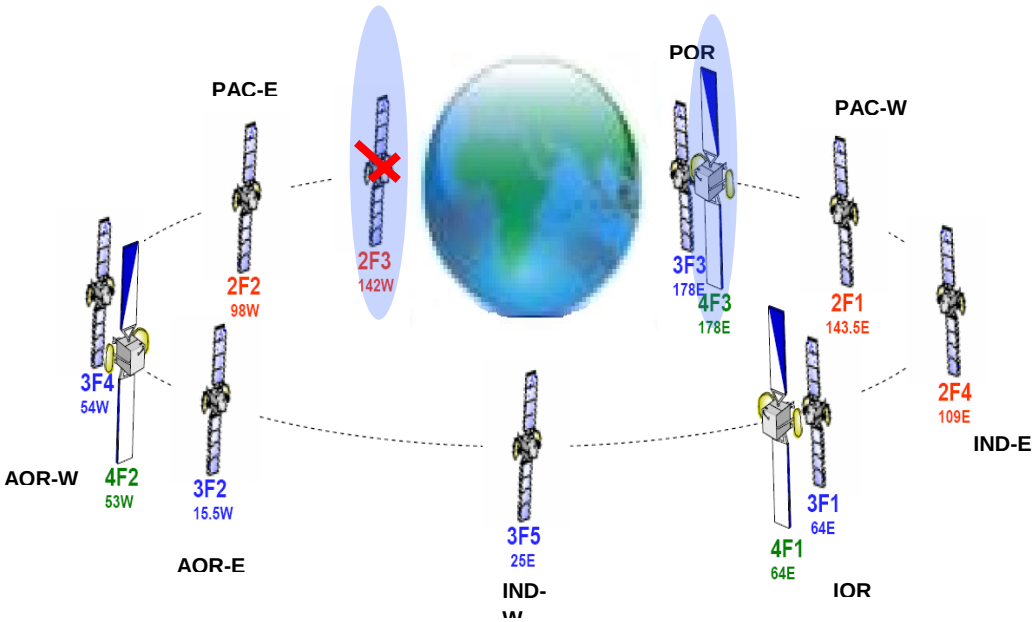
4.1 Inmarsat - Υπηρεσία Fleetbroadband

4.1.1 Εισαγωγή

Η υπηρεσία Fleetbroadband (FBB) παρέχεται μέσω των δορυφόρων 4ης γενιάς του Inmarsat 4F1 AMERICAS, 4F2 EMEA και 4F3 APAC, του επίγειου δίκτυού BGAN και τον συμβατών κινητών δορυφορικών σταθμών Inmarsat (User Terminal, UT). Το δίκτυο BGAN αποτελείται από τρεις δορυφορικούς πρόσβασης (Satellite Access Station, SAS) οι οποίοι βρίσκονται στο Burum (Ολλανδία) στο Fucino (Ιταλία) και στην Χαβάη. Οι δυο αυτοί Δορυφορικοί Σταθμοί πρόσβασης συνδέονται μεταξύ τους και συνδέουν ο καθένας τα δυο δορυφορικά συστήματα 4F1 και 4F2 με τα επίγεια δίκτυα (PSTN, ISDN, PLMN, IP κτλ). Η υπηρεσία FBB προσφέρει υψηλές ταχύτητες μετάδοσης πακέτων δεδομένων (συμμετρικές η μη εξαρτάται από το δορυφορικό τερματικό) και φωνής. Υποστηρίζει την ταυτόχρονη χρήση φωνής (voice) και δεδομένων (data) από ένα δορυφορικό τερματικό (UT). Το δορυφορικό τερματικό θα πρέπει να είναι συμβατό με το επίγειο δίκτυο BGAN του Inmarsat. Τα δορυφορικά τερματικά υποστηρίζουν την σύνδεση διαφόρων τύπων εξωτερικών συσκευών και υπολογιστών

4.1.2 Δορυφόροι Inmarsat

Οι δορυφόροι Inmarsat συνολικά 10 σε λειτουργία και βρίσκονται στη γεωστατική τροχιά (35,786 km από το ύψος τις θάλασσας) πάνω από τον ισημερινό της Γης και καλύπτουν όλες τις ωκεάνιες περιοχές καθώς και το μεγαλύτερο κομμάτι ξηράς εκτός των πόλων (γεωγραφικά πλάτη +/-75^{o})

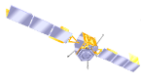
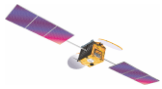
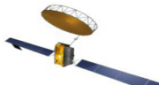


Εικόνα 1: Δορυφόροι Inmarsat

Ο δεύτερος δορυφόρος 3ης γενιάς 2F3 τέθηκε εκτός λειτουργίας τον Απρίλιο του 2006. Ο τρίτος δορυφόρος 4ης γενιάς 3F4 εκτοξεύτηκε από το Κέντρο Εκτόξευσης της ILS στο Διαστημικό Κέντρο Μπαικονουρ στο Καζαχστάν με φορέα Proton-M τον Μάρτιο του 2008

4.1.3 Δορυφόροι Inmarsat 4ης Γενιάς

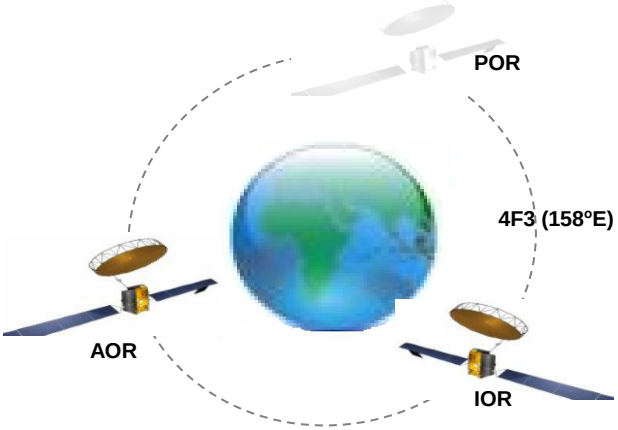
Οι δορυφόροι 4ης Γενιάς είναι από τα πλέον σύγχρονα δορυφορικά τηλεπικοινωνιακά συστήματα εμπορικής χρήσης και τέθηκαν σε λειτουργία το 2005. Έχουν 16 φορές μεγαλύτερη χωρητικότητα από τους δορυφόρους 3ης γενιάς, 3πλασιο βάρος και 60 φορές περισσότερη ισχύ και αναμένεται να παραμείνουν σε λειτουργία ως το 2020. Η συνολική στιγμιαία χωρητικότητα κάθε δορυφόρου είναι περίπου 400Mbit/s. Η συνολική στιγμιαία χωρητικότητα του δικτύου με τον 3ο δορυφόρο θα είναι περίπου 1.2GB

Satellites	4	4+1 Spare	2+1
Year Operational	1990	1996	2005
Coverage	Global	Global+7 Wide Spot	Global+19 Wide Regional +228 Narrow Spot
Bandwidth(MHz)	20	60	126
Mobile link EIRP	39dbW/(7.95KW)	49dBW/(79.4KW)	67dbW /(5MW)
Channelization	4 Channels between 2X4.5+7.3MHz+5.2MHz	46 Channels between 0.9-2.2MHz	630 Channels at 200Khz spacing
Voice (4.8Kbps)	250	1000	18000
M4 GAN (64Kbps)	N/A	200	2250
BGAN(432Kbps)	N/A	N/A	>600
Solar Array Span(m)	14.5	20.7	48
Satellite Dry Mass (Kg)	700	1000	3300
Total Launch Mass(Kg)	1500	2050	6000
Manufacturer(Bus)	British Aerospace	Lockheed Martin	Astrium
Manufacturer(Payload)	Hughes	Marconi	Astrium

Πίνακας 1: Δορυφόροι Inmarsat με το πέρας του χρόνου

Αυτή τη στιγμή η κάλυψη για της υπηρεσίες BGAN (Broadband Global Area Network, land), FBB (Fleet Broadband , maritime) and SBB (Swift Broadband, aeronautical) παρέχεται από τους δορυφόρους 4F1-AOR, 4F2-IOR και 4F3-POR στις περιοχές του Ατλαντικού, Ινδικού και Ειρηνικού ωκεανού.



Εικόνα 2: Δορυφόροι Inmarsat 4ης γενιάς

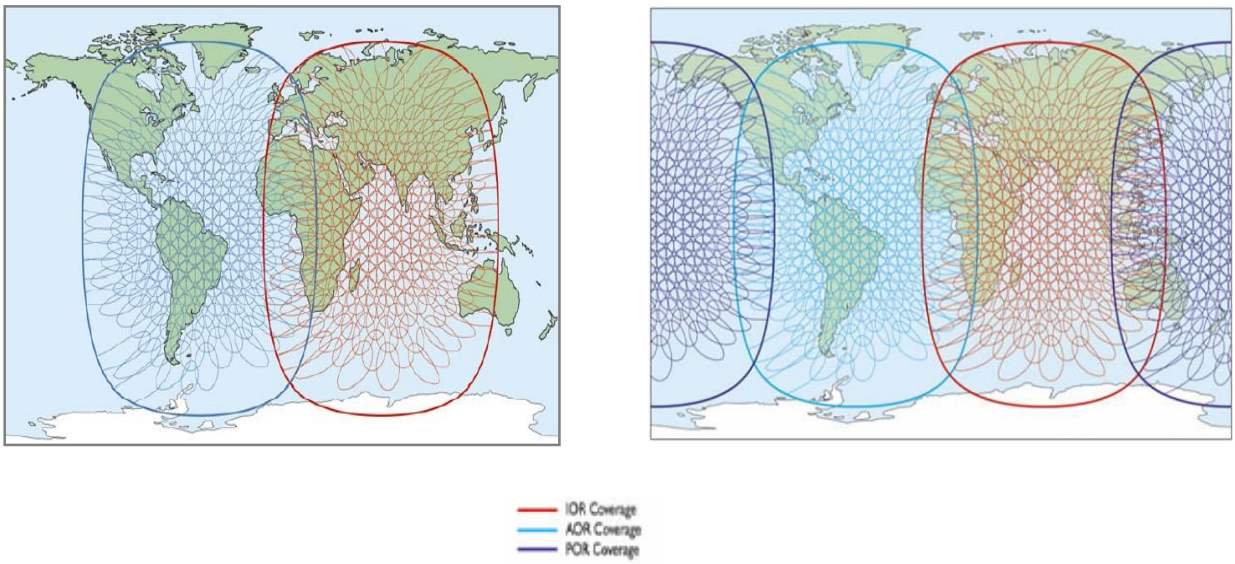
4.1.4 Γεωγραφική Κάλυψη Δορυφόρων Inmarsat 4ης Γενιάς

Η δορυφορική κάλυψη από τον κάθε δορυφόρο παρέχεται σε 3 επίπεδα μέσα από διαφορετικούς τύπους δεσμών. Συγκεκριμένα οι 3 τύποι είναι οι παγκόσμιες δέσμες (Global Beams), οι τοπικές δέσμες (Regional beams), και οι λεπτές δέσμες (Spot beams).Κάθε δορυφόρος υποστηρίζει μια παγκόσμια δέσμη, 19 τοπικές δέσμες και 228 λεπτές δέσμες.

Οι παγκόσμιες δέσμες χρησιμεύουν για την αποστολή μεταδόσεων και πληροφοριών στα δορυφορικά τερματικά (UT) σχετικά με τα Πρωτεύοντα Φέροντα Διαμεριζόμενης Πρόσβασης (Primary Shared Access Bearers) δηλαδή τις συχνότητες των φερόντων στην τοπική δέσμη. Οι τοπικές δέσμες χρησιμεύουν για την αποστολή πληροφοριών και ανταλλαγή σηματοδοσίας από και προς τα δορυφορικά τερματικά (UT) για την εγγραφή στο δίκτυο. Δεν υποστηρίζουν μεταφορά φωνής η δεδομένων μόνο μηνυμάτων SMS. Οι υπάρχουσες υπηρεσίες B/Mini-M/GAN/Swift/Fleet θα περνάνε μέσα από αυτές τις δέσμες κατά την αλλαγή παροχής των υπηρεσιών από τους I3 δορυφόρους στους I4. Οι λεπτές δέσμες χρησιμεύουν για την αποστολή φωνής, δεδομένων (streaming ροής, background IP) και ISDN.

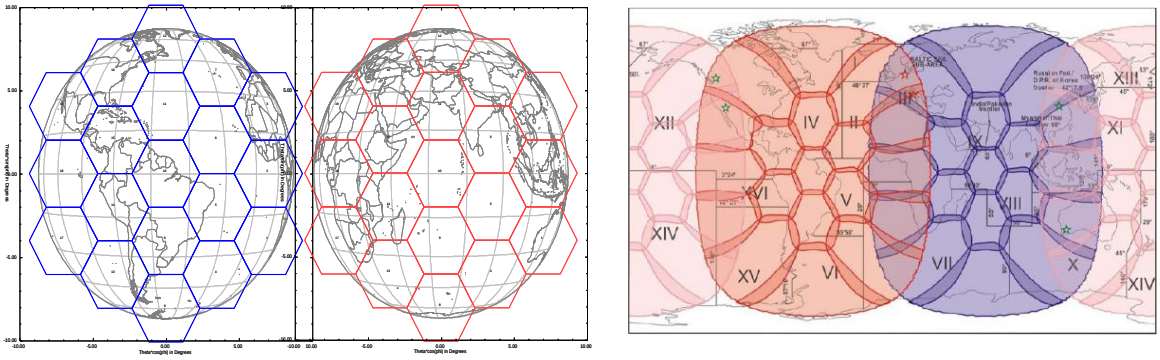
Στο παρακάτω σχήμα φαίνονται οι παγκόσμιες και λεπτές δέσμες των δορυφόρων:

4F2-IOR(53° E) 4F1-AOR(64°E) 4F2-IOR(53° E) 4F1-AOR(64°E) 4F3 POR (158°E)



Εικόνα 3 : Οι παγκόσμιες και λεπτές δέσμες των δορυφόρων Inmarsat 4ης γενιάς

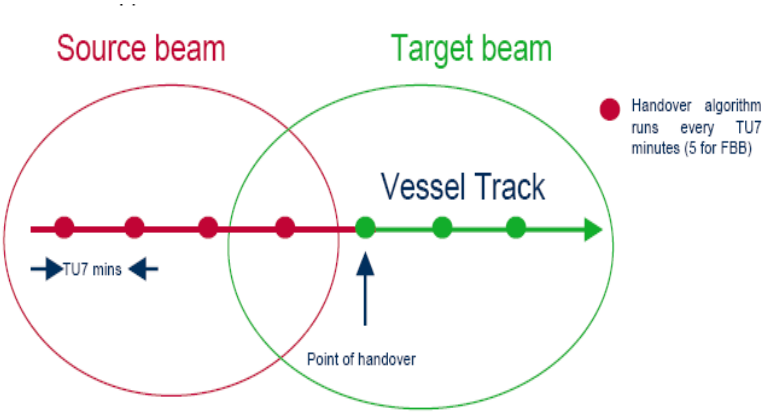
Στο παρακάτω σχήμα φαίνονται οι τοπικές δέσμες



Εικόνα 4: Οι τοπικές δέσμες των δορυφόρων Inmarsat 4ης γενιάς

4.1.5 Μεταπομπή Τερματικού Χρήστη – UT Handover

Οι δυο τύποι δορυφορικών τερματικών υποστηρίζουν τη μεταπομπή μέσα από της λεπτές δέσμες (spot beam handover). Η μεταπομπή συνδέσεων μεταγωγής πακέτου όπως είναι οι Standard και Streaming IP είναι χωρίς απώλειες 'lossless' και έτσι η σύνδεση δεν διακόπτεται κατά την μεταπομπή. Αντιθέτως οι συνδέσεις μεταγωγής κυκλώματος είναι με απώλειες 'lossy' και έτσι η σύνδεση διακόπτεται μερικώς κατά την μεταπομπή (η σύνδεση διακόπτεται μολονότι το κύκλωμα βρίσκεται ακόμα ενεργό στο τέλος της μεταπομπή)



Εικόνα 5: Μεταπομπή Τερματικού Χρήστη – UT Handover

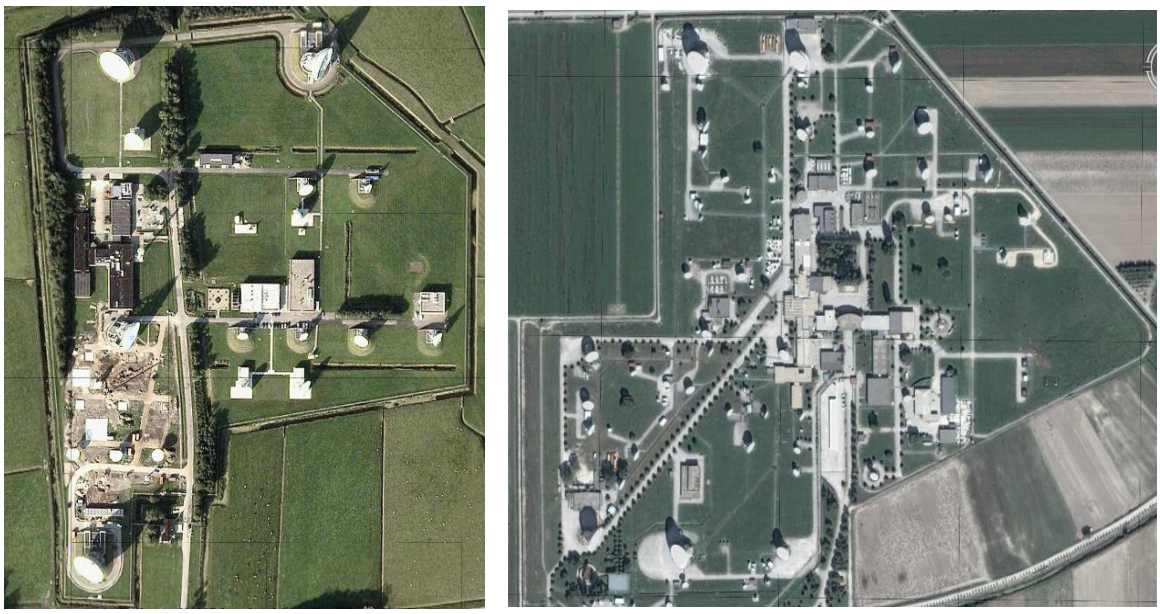
Η μεταπομπή μεταξύ δεσμών διαφορετικών δορυφόρων δεν υποστηρίζεται και οι σύνδεση διακόπτεται.

4.1.6 Δορυφορικοί Σταθμοί Πρόσβασης - Satellite Access Stations (SAS)

Οι Δορυφορικοί Σταθμοί Πρόσβασης αποτελούν τμήμα του Δικτύου Ραδιο-Πρόσβασης (RAN) του επίγειου δικτύου BGAN και ανήκουν στον Inmarsat . Μέχρι αυτή τη στιγμή υπάρχει ένας σταθμός με 2 RAN στο Burum της Ολλανδίας, ένας στο Fucino της Ιταλίας και επίσης υπάρχει τέταρτος σταθμός με 2 RAN στη Hawai για την διασύνδεση του 4F3 με τα επίγεια δίκτυα. Όλοι οι δορυφόροι διασυνδέονται με τουλάχιστον 2 Δορυφορικούς Σταθμούς Πρόσβασης. Οι δορυφορικοί σταθμοί πρόσβασης διασυνδέονται μεταξύ τους. Ο σταθμός στο Burum λειτουργεί ως πρωτεύον σταθμός και εξυπηρετεί την κίνηση από και προς τα επίγεια δίκτυα και τους δορυφόρους 4F1 (AOR) και 4F2 (IOR). Σε περίπτωση βλάβης στο Burum η κίνηση μετάγεται στον σταθμό στο Fucino ο οποίος λειτουργεί ως εφεδρικός.

Οι Δορυφορικοί Σταθμοί Πρόσβασης συνδέονται με το Σύστημα Εμπορικής Υποστήριξης (Business Support System, BSS) στα κεντρικά του Inmarsat στο Λονδίνο για διαδικασίες τιμολόγησης της κίνησης και για διαδικασίες σχετικές με το customer care.

Στις παρακάτω φωτογραφίες φαίνονται οι Δορυφορικοί Σταθμοί Πρόσβασης στο Burum και στο Fucino.



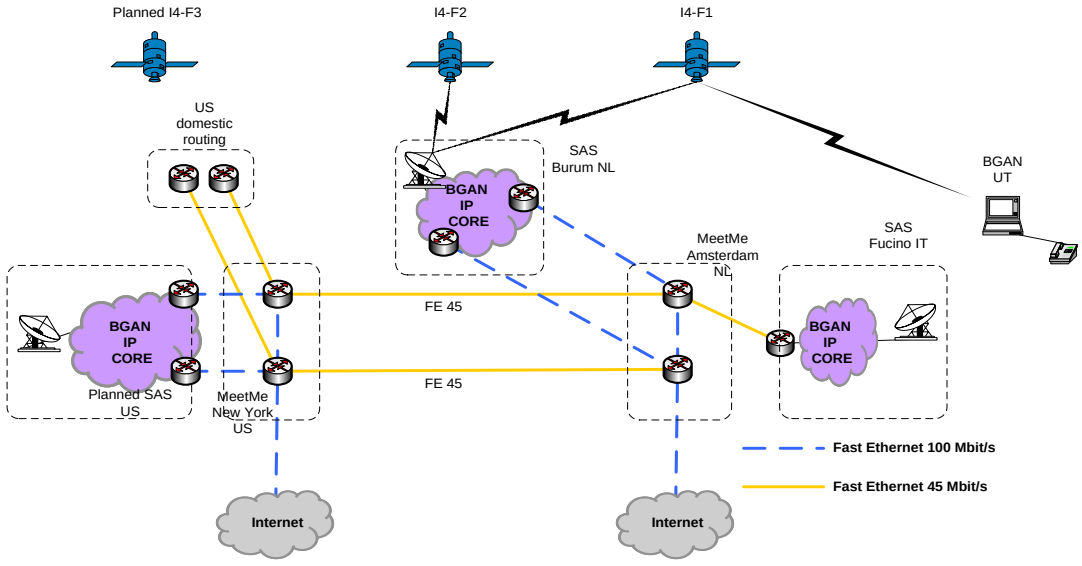
SAS Burum **SAS Fucino**

Εικόνα 6: Δορυφορικοί Σταθμοί Πρόσβασης στο Burum και στο Fucino

4.1.7 Διασύνδεση Δορυφορικών Σταθμών Πρόσβασης (SAS)

Οι δορυφορικοί Σταθμοί Πρόσβασης διασυνδέονται μεταξύ τους καθώς επίσης συνδέονται με τα Σημεία Συνάντησης (Meet-Me-Points, MMP).

Ο δορυφορικός σταθμός στο Burum διασυνδέεται με το Σημείο Συνάντησης (MMP) στο Άμστερνταμ μέσω δυο κυκλωμάτων Fast Ethernet 100Mb/s, ενώ ο Δορυφορικός Σταθμός Πρόσβασης στο Fucino διασυνδέεται με το (MMP) στο Άμστερνταμ μέσω ενός κυκλώματος Fast Ethernet 45Mb/s.



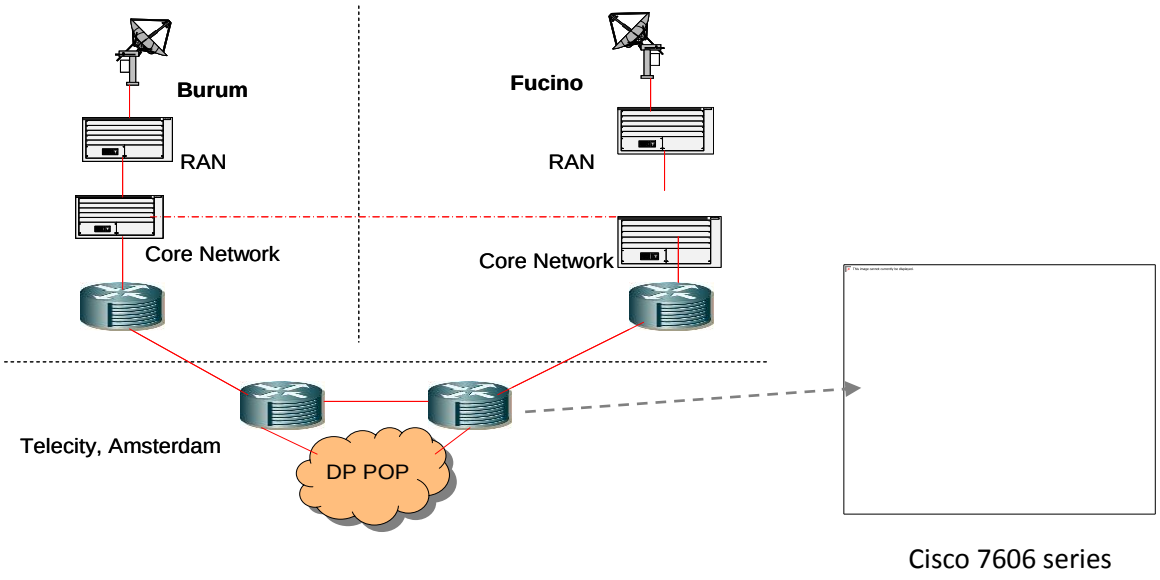
Εικόνα 7: Διασύνδεση Δορυφορικών Σταθμών Πρόσβασης (SAS)

4.1.8 Σημείο Συνάντησης (Meet-Me-Point, MMP)

Ο Inmarsat λειτουργεί και διαχειρίζεται δυο Σημεία Συνάντησης (Meet-Me-Points, MMP) τα οποία βρίσκονται σε κεντρικούς Κόμβους Εναλλαγής Internet (Internet Exchanges) κίνησης . Το ένα Σημείο Συνάντησης βρίσκεται στο Άμστερνταμ και ονομάζεται Telecity, ενώ το δεύτερο βρίσκεται στη Νέα Υόρκη και ονομάζεται Telx. Τα Σημεία Συνάντησης έχουν δημιουργηθεί με σκοπό να διευκολύνουν την διασύνδεση των DP παρόχων με τις υποδομές του επίγειου δικτύου BGAN. Ο εξοπλισμός των παροχών οι οποίοι διαθέτουν δικό τους Σημείο Παρουσίας (PoP) μπορεί να συστεγαστεί στις εγκαταστάσεις του ενός η των δυο Σημείων Συνάντησης για αποδοτικότερη διασύνδεση η μπορεί να τοποθετηθεί σε άλλο απομακρυσμένο σημείο το οποίο συνδέεται με το MMP.

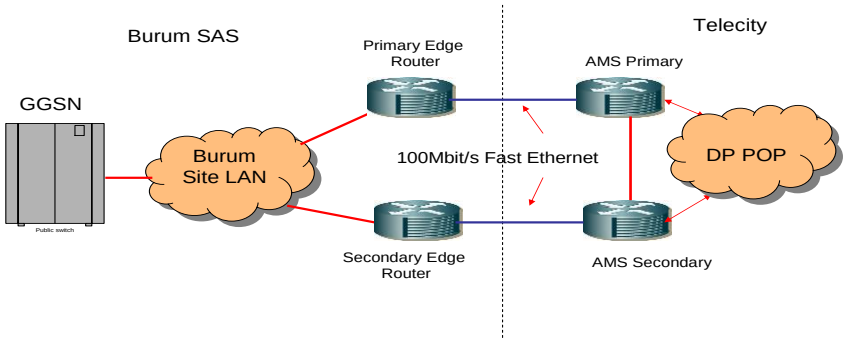
Τα Σημεία Συνάντησης του Άμστερνταμ (Telecity) και Νέας Υόρκης (Telx) συνδέονται με διπλά κυκλώματα Fast Ethernet 45Mb/s over DS-3.

Παρακάτω φαίνονται παραδείγματα της διασύνδεσης των Δορυφορικών Σταθμών Πρόσβασης (SAS) στο Burum και στο Fucino με το Σημείο Συνάντησης (MMP) του Άμστερνταμ (Telecity).



Εικόνα 8: Διασύνδεση Δορυφορικών Σταθμών Πρόσβασης (SAS) με το Σημείο Συνάντησης (MMP) του Άμστερνταμ (Telecity)

Επικεντρώνοντας στον Δορυφορικό Σταθμό Πρόσβασης στο Burum το επίγειο δίκτυο BGAN συνδέεται με τα επίγεια δίκτυα μεταγωγής πακέτου (packet switched data networks) δεδομένων μέσω δυο ακραίων δρομολογητών (border edge routers). Οι ακραίοι δρομολογητές συνδέονται με το GGSN του δικτύου κορμού BGAN μέσω του τοπικού δικτύου του σταθμού.

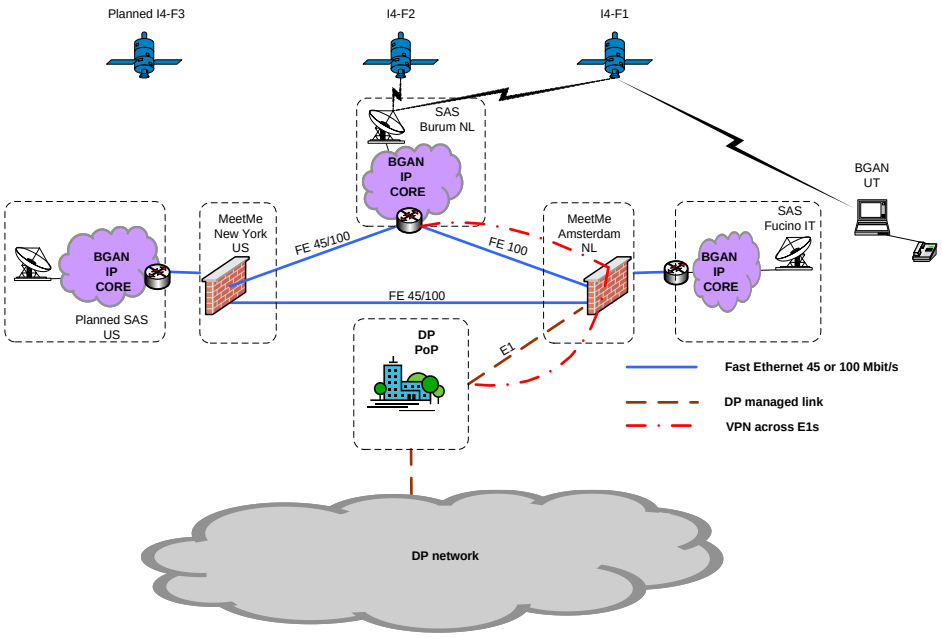


Εικόνα 9: Διασύνδεση Δορυφορικού Σταθμού Πρόσβασης με τα επίγεια δίκτυα (packet switched data networks)

Οι ακραίοι δρομολογητές συνδέονται σε δυο αντίστοιχους δρομολογητές (τον πρωτεύοντα και δευτερεύοντα) στο Σημείο Συνάντησης (MMP) του Amsterdam (Telecity) μέσω διπλού κυκλώματος Fast Ethernet 100Mb/s.
Ο πρωτεύων και δευτερεύων δρομολογητής του Inmarsat στο Telecity (AMS-MMP) είναι Cisco 7606 series.

4.1.9 Σημείο Παρουσιας (Point of Presence,PoP)

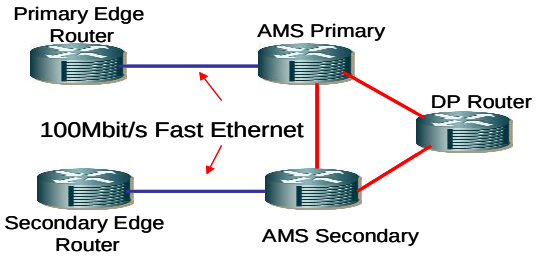
Ένα Σημείο Παρουσίας (PoP) παρέχει στους DP τη δυνατότητα καλύτερης διαχείρισης και ελέγχου των υπηρεσιών που παρέχονται προς τους πελάτες. Δίνει επίσης την δυνατότητα και διαφοροποίησης των υπηρεσιών μέσω της παροχής υπηρεσιών προστιθέμενης άξιας (value added services) μέσω του Σημείου Παρουσίας (PoP)



Εικόνα 10: Διάγραμμα διασύνδεσης DP PoP - BGAN - DP Ground Network

4.1.10 Διασύνδεση Σημείου Παρουσίας (PoP) με δίκτυο BGAN

Ο αρχικός σχεδιασμός του Σημείου Παρουσίας της Otesat-Maritel προβλέπει την διασύνδεση των δρομολογητών του Σημείου Συνάντησης (πρωτεύοντα και του δευτερεύοντα δρομολογητή) σε κοινό τερματισμό (δρομολογητή) στο σημείο εισόδου του Σημείου Παρουσίας της Otesat-Maritel μέσω ψηφιακής δομημένης μισθωμένης γραμμής E1 (G.703 & G.704).



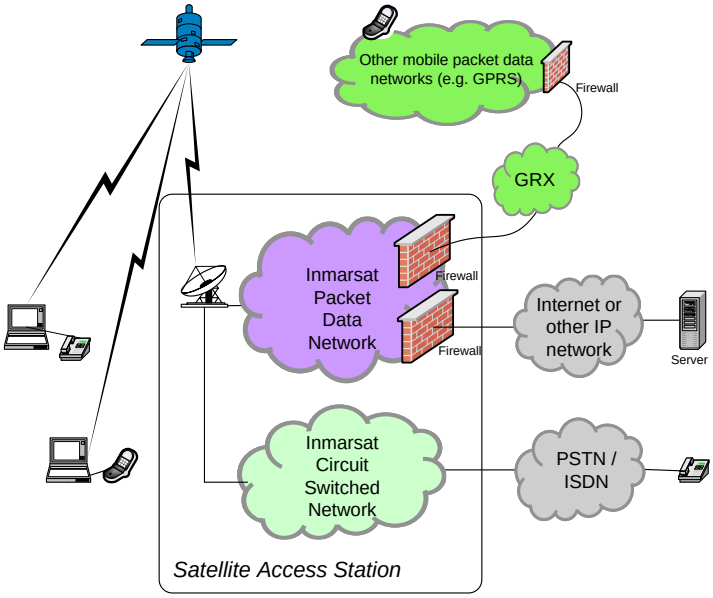
Εικόνα 11: Διασύνδεση Σημείου Παρουσίας (PoP) με δίκτυο BGAN

Η φυσική τερματική αντίσταση των διεπαφών είναι 120Ω και οι συνδετήρες (connectors) είναι τύπου RJ-45

4.2 Δίκτυο BGAN

4.2.1. Γενική Περιγραφή Δικτύου BGAN

Το δίκτυο BGAN παρέχει σε δορυφορικά τερματικά (UT) (μέσω των δορυφόρων τέταρτης γενιάς I4) πρόσβαση σε επίγεια δίκτυα μεταγωγής πακέτου και κυκλώματος διαμέσου των Δορυφορικών Σταθμών Πρόσβασης (SAS)



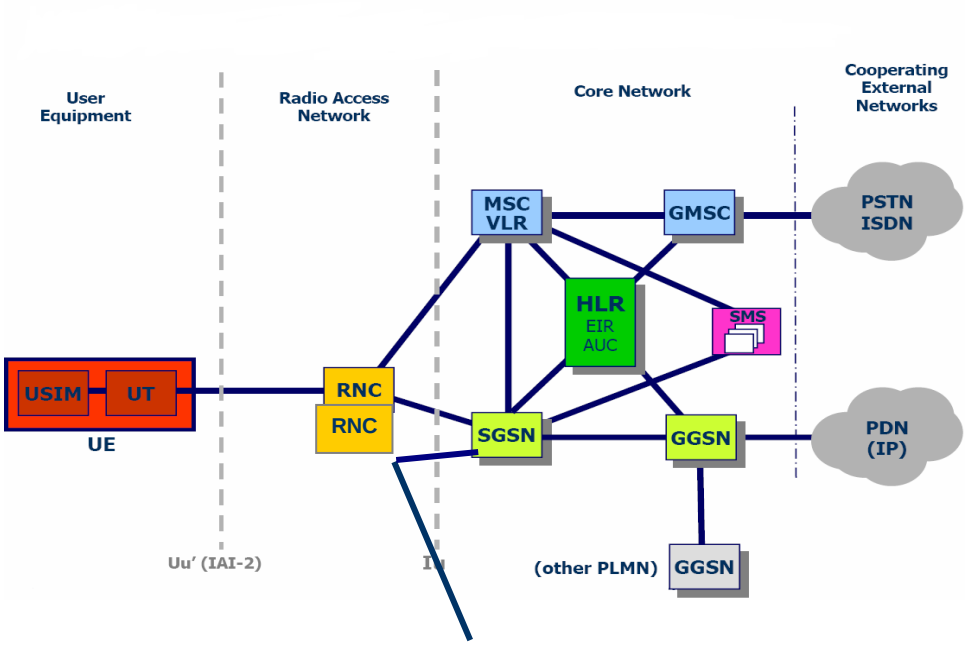
Εικόνα 12: Περιγραφή Δικτύου BGAN

Το δίκτυο μεταγωγής κυκλώματος χρησιμοποιείται για τις τηλεφωνικές και ISDN κλήσεις (circuit switched voice) και συνδέει τον δορυφορικό σταθμό πρόσβασης (SAS) με τα επίγεια δίκτυα μεταγωγής κυκλώματος (PSTN, ISDN etc).

Το δίκτυο μεταγωγής πακέτου χρησιμοποιείται για την σύνδεση πακέτων δεδομένων (packed data) και συνδέει τον δορυφορικό σταθμό πρόσβασης (SAS) με το Internet η άλλα IP δίκτυα.

4.2.2 Τεχνική Περιγραφή Επίγειας Υποδομής Δικτύου BGAN

Η υπηρεσία Fleetbroadband παρέχεται μέσω των δορυφόρων τέταρτης γενιάς (I4) και του επίγειου δικτύου 3ης γενιάς (3G) BGAN του Inmarsat το οποίο είναι και συμβατό με άλλα αντίστοιχα ασύρματα τηλεπικοινωνιακά δίκτυα 3η γενιάς . Το δίκτυο αποτελεί δορυφορικό κομμάτι του πρωτοκόλλου τρίτης γενιάς UMTS (Satellite –Universal Mobile Telecommunication System, S-UMTS) και βασίζεται στην αρχιτεκτονική που περιγράφεται στις προδιαγραφές 3GPP/ETSI UMTS Release 4 εκτός από την τεχνολογία της Ράδιο Διεπαφής (Air Interface). Το UMTS ορίζει την διεπαφή ως Uu (Uu Interface). Η τεχνολογία της Ράδιο Επαφής στο Δίκτυο Ασύρματης Πρόσβασης (Radio Access Network, RAN) του δικτύου Inmarsat είναι η δεύτερη γενιά του Inmarsat Air Interface 2 (IAI2) . Αποτελείται από δύο κύρια τμήματα. Το Δίκτυο Ασύρματης Πρόσβασης (Radio Access Network, RAN) και το Δίκτυο Κορμού (Core Network, CN).

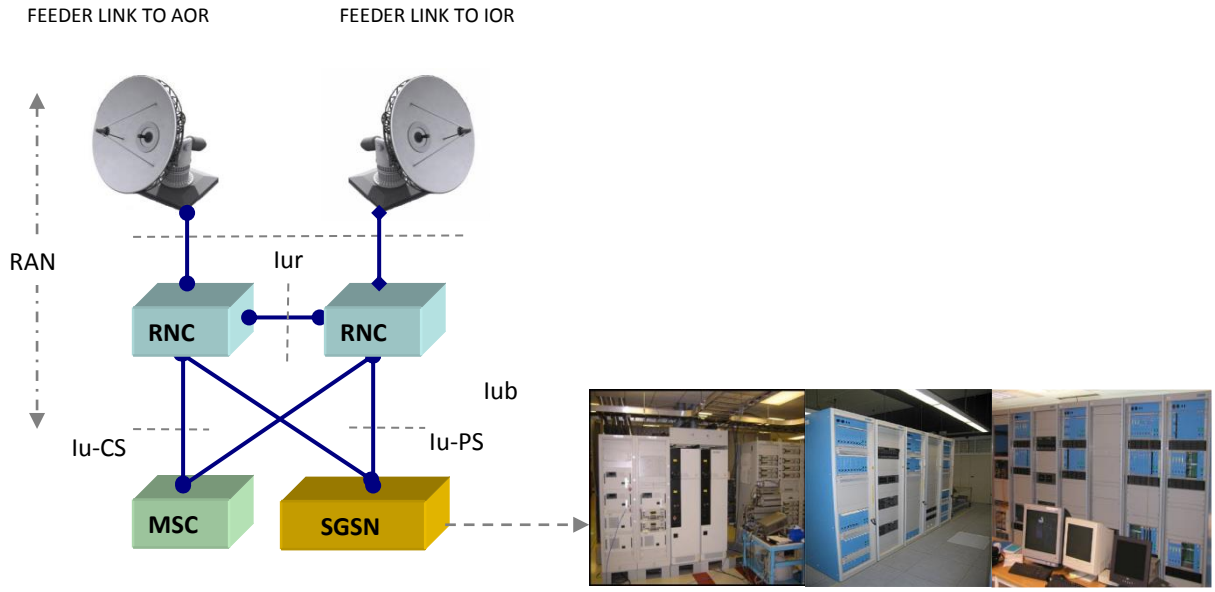


Εικόνα 13: Διάγραμμα Επίγειας Υποδομής Δικτύου BGAN

4.2.3 Δίκτυο Ράδιο-Πρόσβασης - RAN

Το Δίκτυο Ασύρματης Πρόσβασης (RAN) περιλαμβάνει όλα τα υποσυστήματα (Node B) που σχετίζονται με την εκπομπή και την λήψη των ηλεκτρομαγνητικών κυμάτων (παραβολικές κεραίες, κυματοδηγοί, μικροκυματικοί πομποδέκτες) στις μικροκυματικές συχνότητες στην περιοχή 4-6 GHz (Feeder Links) καθώς και τους Ελεγκτές Ράδιο Δικτύου (Radio Network Controller, RNC). Συνδέεται με το

δίκτυο κορμού μέσω των διεπαφών Iu οι οποίες μεταφέρουν κίνηση φωνής και δεδομένων (voice and data traffic) καθώς επίσης και σηματοδοσία (signaling). Το Δίκτυο Ασύρματης Πρόσβασης είναι κατασκευασμένο την Thrane & Thrane.



Εικόνα 14: Δίκτυο Ράδιο-Πρόσβασης - RAN

4.2.3.1 Node B (SAS RF Subsystem)

Το υποσύστημα Node B περιλαμβάνει τις κεραίες (με παραβολικά κάτοπτρα), τους κυματοδηγούς, τους μικροκυματικούς πομποδέκτες, και τις λοιπές διαδικασίες επεξεργασίας σήματος, (φιλτράρισμα, δια/αποδιαμόρφωση, κωδικο/αποκωδικοποίηση άνω/κατω μετατροπή συχνότητας, έλεγχος επιπέδων ισχύος εκπομπής κτλ).

4.2.3.2 RNC (Radio Network Controller)

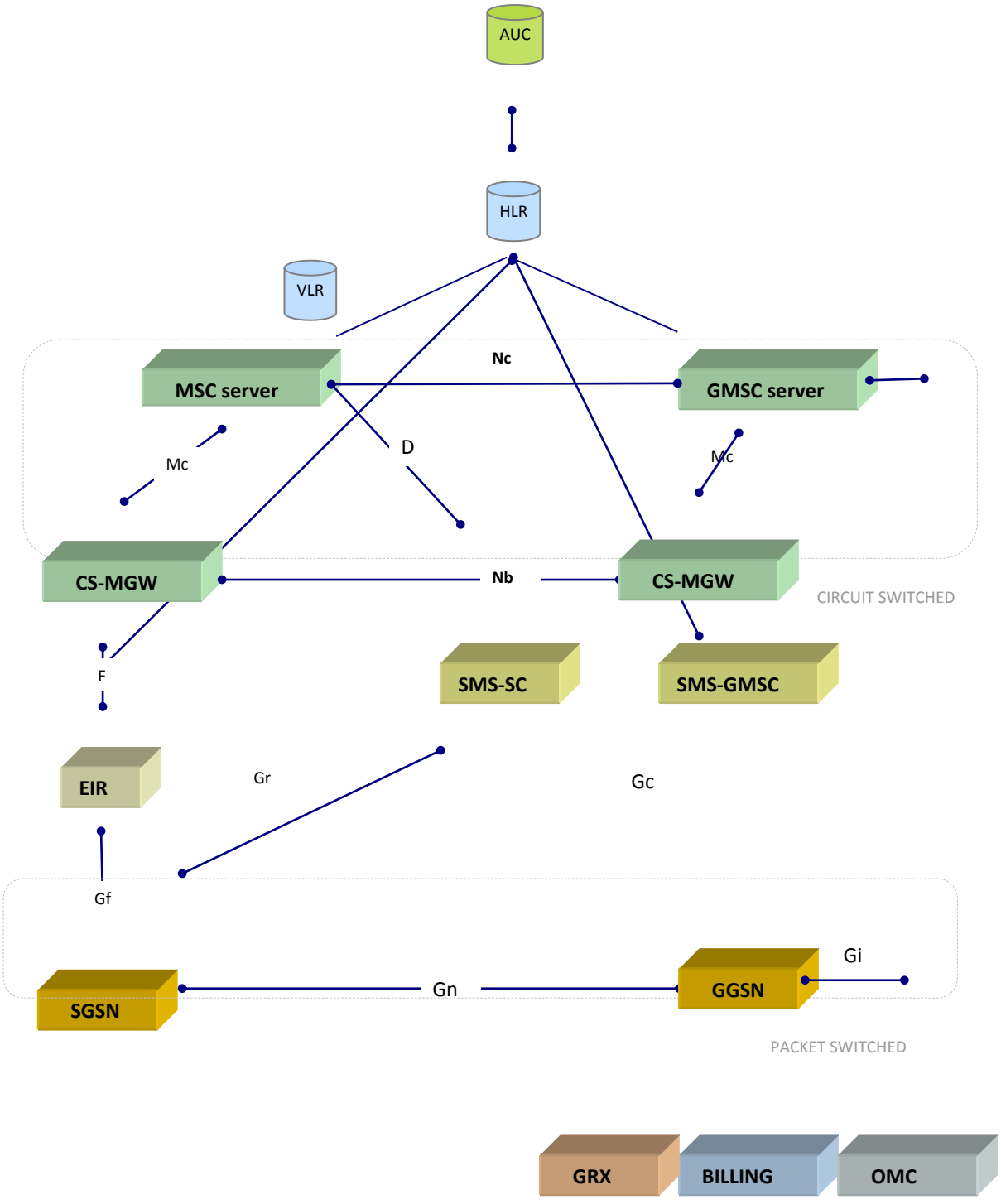
Ο ελεγκτής Ράδιο Δικτύου ελέγχει τις λειτουργίες των Node B. Τα Node B συνδέονται στον Ελεγκτή Ράδιο Δικτύου μέσω της διεπαφής (Iub interface) . Οι βασικές λειτουργίες είναι η διαχείριση των Ράδιο Πόρων (Radio Resource) ή Ράδιο καναλιών (Radio Resource Management) στην διεπαφή Iur (Iur interface) και επίγειων καναλιών προς τα Κέντρα Μεταγωγής δηλαδή των διαθέσιμων συχνοτήτων φερόντων, διαχείριση κινητικότητας χρηστών (Mobility Management) και είναι το σημείο όπου κρυπτογραφούνται τα δεδομένα προτού ληφθούν αποσταλούν από και προς τον δορυφόρο. Επίσης κατανέμει και αναθέτει ζεύγη ελεύθερων καναλιών επικοινωνίας και ελέγχου (Forward και Return transmission/reception and signaling channels), πραγματοποιεί τον Έλεγχο Υποδοχής (Admission Control) των UTs, καθώς επίσης Έλεγχο Επιπέδων Ισχύος των Node Bs και UTs. Το RNC συνδέει τα δίκτυα μεταγωγής κυκλώματος με το (Mobile Switching Center, MSC) μέσω της διεπαφής (Iu-CS) και τα δίκτυα μεταγωγής πακέτου με το (Serving GRPS Node, SGSN) μέσω της διεπαφής (Iu-PS). Επίσης οι Ελεγκτές Ράδιο Δικτύου συνδέονται μεταξύ τους μέσω των ραδιοεπαφών Iur (Iur Interface) οι οποίες χρησιμοποιούνται για τις διαδικασίες μεταπομπής (handovers).

4.2.3.3 Δίκτυο Κορμού - CN

Το δίκτυο κορμού, είναι ανεξάρτητο από την τεχνολογία ασύρματης πρόσβασης του Δικτύου Ράδιο-Προσβασης (RAN) και περιλαμβάνει όλο το υπόλοιπο τμήμα του δικτύου 3ης γενιάς μαζί με τα δίκτυα μεταγωγής κυκλώματος (circuit switched) και πακέτου(packet switched). Περιλαμβάνει όλα τα υποσυστήματα που σχετίζονται με την πιστοποίηση του χρήστη, την χρέωση, την δρομολόγηση των κλήσεων, των διαχωρισμό και την μεταγωγή των κλήσεων στα κατάλληλα δίκτυα, την σηματοδοσία, και τις διεπαφές για την διασύνδεση με τα επίγεια κυκλώματα.

Τα δίκτυα μεταγωγής κυκλώματος (circuit switched) μεταφέρουν τις φωνητικές κλήσεις, τις ISDN κλήσεις καθώς επίσης και μηνύματα SMS.

Τα δίκτυα μεταγωγής πακέτων (packet switched) μεταφέρουν τα δεδομένα των IP συνδέσεων. Το UMTS Δίκτυο Κορμού στηρίζεται σε εξοπλισμό της Ericcson.



Εικόνα 15: Δίκτυο Κορμού - CN

Το Δίκτυο Κορμού BGAN (CN) διαχωρίζεται σε επίπεδο μεταγωγής κυκλώματος και μεταγωγής πακέτου. Μερικές από τις οντότητες του δικτύου BGAN είναι:

4.2.3.3.1 Κέντρο μεταγωγής κινητών σταθμών - Mobile-Services Switching Center (MSC)

Το κέντρο μεταγωγής κινητών σταθμών είναι ένα εξελιγμένο τηλεφωνικό κέντρο το οποίο υποστηρίζει κλήσεις μεταγωγής κυκλώματος, διαχείριση κινητικότητας χρηστών (mobility management) και παρέχει υπηρεσίες φωνής, δεδομένων, fax και SMS στους κινητούς σταθμούς που μετακινούνται στην περιοχή ελέγχου του.

Αποτελείται από τα εξής πεδία:

- Circuit Switched Media Gateway (**CS-MGW**).
  Ελέγχει όλα τα κανάλια μεταφοράς πληροφορίας των χρηστών.

- Mobile-services Swtiching Center Server (**MSC server**).
  Είναι υπεύθυνος για τον έλεγχο των κλήσεων.

Η λειτουργικότητα του εξυπηρετητή του MSC (MSC server) επιτρέπει των διαχωρισμό μεταξύ του επιπέδου ελέγχου (σηματοδοσίας) και επιπέδου χρήστη (φορέας στα στοιχεία δικτύου που ονομάζονται Πύλες Μέσων, Media Gateways), και εγγυάται περισσότερο βελτίωση τοποθέτησης των στοιχείων (element) στο δίκτυο. Ο MSC server και το MGW καθιστούν δυνατή τη διασύνδεση κλήσεων μεταγωγής κυκλώματος χρησιμοποιώντας IP, ATM, AAL2 καθώς και TDM.

Ο MSC συνδέεται με τα:

- HLR για την απόκτηση δεδομένων σχετικά με τις κάρτες SIM και τους αριθμούς κλήσης MSISDN.
- RAN το οποίο διαχειρίζεται την ράδιο-επικοινωνία με τα κινητά τερματικά (UT).
- VLR για το καθορισμό της θέσης των άλλων κινούμενων συνδρομητών.
- Άλλα MSCs για την πραγματοποίηση διαδικασιών όπως μεταπομπές (handovers).

Η λειτουργίες του MSC είναι οι εξής:

- Παράδοση κλήσεων σε συνδρομητές όπως φτάνουν στην περιοχή εξυπηρέτησης που βασίζεται σε πληροφορίες που παρέχονται από το VLR.
- Συνδέσεις εξερχόμενων κλήσεων (από το κινητό τερματικό) προς άλλα τερματικά η σταθερά επίγεια δίκτυα.
- Παράδοση των SMS από τους συνδρομητές στο SMSC και αντίστροφα.
- Κανονίζει τις μεταπομπές από RNC σε RNC.
- Διεκπεραιώνει μεταπομπές από αυτό το MSC προς και από άλλα.
- Υποστηρίζει συμπληρωματικές υπηρεσίες όπως τηλεσυνδιασκέψεις, κράτηση κλήσης κτλ.
- Δημιουργεί πληροφορίες για τα συστήματα χρέωσης.

4.2.3.3.2 Πύλη Κέντρο Μεταγωγής Κινητών Επικοινωνιών - Gateway Mobile-Services Switching Center (GMSC)

Είναι το MSC που υλοποιεί την δρομολόγηση των κλήσεων στην τοποθεσία που βρίσκεται ο κινητός σταθμός. Καθορίζει ποιο Visited MSC(V-MSC) βρίσκεται ο συνδρομητής ο οποίος καλείται και συνδέεται με τα δίκτυα μεταγωγής κυκλώματος PSTN και ISDN. Δρομολογεί κλήσεις από τερματικό προς τερματικό καθώς επίσης κλήσεις από σταθερά τηλέφωνα (ξηράς) προς το τερματικό.

Αποτελείται από τα εξής:

- Circuit Switched Media Gateway (**CS-MGW**).
  Ελέγχει όλα τα κανάλια μεταφοράς πληροφορίας των χρηστών.

- Gateway Mobile-services Swtiching Center Server (G**MSC server**).
  Είναι υπεύθυνος για τον έλεγχο και την δρομολόγηση των κλήσεων προς τους κινητούς σταθμούς.

4.2.3.3.3 Καναχωρητής ταυτότητας εξοπλισμού - Equipment Identity Register (EIR)

Αποθηκεύεται η Διεθνής ταυτότητα εξοπλισμού κινητού σταθμού - Internation Mobile Equipment Identity (IMEI) της συσκευής. Διατηρεί λίστα με όλα τα κινητά τερματικά (αναγνωρίζονται από το IMEI) που απαγορεύεται να χρησιμοποιήσουν το δίκτυο η βρίσκονται υπό επιτήρηση. Συχνά βρίσκεται ενσωματωμένο στο HLR και χρησιμεύει στον εντοπισμό κλεμμένων τερματικών.

4.2.3.3.4 Οικείος καταχώρησης θέσης αναζήτησης - Home Location Register (HLR)

Βάση δεδομένων (database) στην οποία αποθηκεύονται πληροφορίες για τον κάθε συνδρομητή χρήστη δορυφορικού τερματικού FBB που είναι εξουσιοδοτημένος να χρησιμοποιήσει το δίκτυο κορμού BGAN-CN. Συνήθως υπάρχει μια ανά δίκτυο άλλα μπορεί να είναι και περισσότερες.

- Αποθηκεύει πληροφορίες και κλειδιά (IMSI, ICCID,MSISDN,AMSISDN κτλ) για την κάθε SIM κάρτα - Μονάδα Ταυτότητας Χρηστή (Subscriber Identity Module, SIM) που έχει εκδοθεί από τον διαχειριστή του δικτύου.
- Αποθηκεύει την τωρινή θέση του χρήστη (VLR και GGSN).
- Αποθηκεύει GRPS ρυθμίσεις σχετικές με την πρόσβαση του συνδρομητή στις υπηρεσίες μεταγωγής πακέτου(packet switched).
- Αποθηκεύει τις υπηρεσίες που έχει αιτηθεί ή λάβει ο συνδρομητής.

Η λειτουργία του HLR είναι:

Να διαχειριστεί την κινητικότητα των συνδρομητών (subscriber's mobility) ενημερώνοντας για την θέση τους σε περιοχές διαχείρισης οι οποίες ονομάζονται Περιοχές Εντοπισμού/Θέσης (Location Areas, LA), και οι οποίες αναγνωρίζονται μέσω ενός μοναδικού κωδικού που ονομάζεται Κωδικός περιοχής εντοπισμού Location Area Code,LAC). Καθώς ο συνδρομητής κινείται από μια περιοχή εντοπισμού (LA) σε κάποια άλλη το HLR ενημερώνει τις τρέχουσες πληροφορίες περιοχής εντοπισμού στη βάση παίρνοντας της πληροφορίες από το RAN.

Να αποστείλει τα στοιχεία συνδρομητή σε ένα VLR η GGSN όταν ο συνδρομητής εισέρχεται στην περιοχή (κατά την διαδικασία της περιαγωγής).

Μεσολαβεί μεταξύ του GMSC or SMSSC και το τρέχων VLR του συνδρομητή για την παράδοση των εισερχομένων κλήσεων ή μηνυμάτων σε αυτόν.

Διαγράφει τα στοιχεία συνδρομητή από προηγούμενα VLR όταν ο χρήστης έχει μετακινηθεί σε κάποια άλλη περιοχή μακριά από αυτό.

Επίσης ο HLR συνδέεται με τα

- GMSC για την διαχείριση εισερχομένων (ως προς το τερματικό) κλήσεων
- VLR για την διαχείριση αιτημάτων σύνδεσης από κινητούς δορυφορικούς σταθμούς (UT) στο δίκτυο.

- SMSC για την διαχείριση εισερχομένων μηνυμάτων SMS (ως προς το τερματικό)
- Το Σύστημα Αυτόματου Τηλεφωνητή (Voice Mail System) για την παράδοση ειδοποιήσεων στο τερματικό ότι εκκρεμεί κάποιο νέο μήνυμα.

4.2.3.3.5 Καταχωρητής θέσης αναζήτησης επισκεπτών - Visit or Location Register (VLR)

Βάση δεδομένων προσωρινής αποθήκευσης στοιχείων συνδρομητή που έχουν εισέλθει στην περιοχή την οποία εξυπηρετεί. Κάθε Node B κόμβος εξυπηρετείται αποκλειστικά από ένα VLR, συνεπώς ένας συνδρομητής δεν μπορεί να βρίσκεται ταυτόχρονα σε δυο VLR. Συνήθως βρίσκεται μαζί με το Κίτρο Μεταγωγής (MSC)

Οι πληροφορίες που αποθηκεύονται στο VLR παρέχονται είτε από το HLR είτε από τον Κινητό Σταθμό (UT) και περιλαμβάνουν

- Τον αριθμό IMSI.
- Στοιχειά Πιστοποίησης/Αναγνώρισης.
- Τον αριθμό MSISDN.
- Υπηρεσίες που επιτρέπεται να χρησιμοποιήσει ο χρήστης.
- Σημείο Πρόσβασης για GPRS υπηρεσίες (Access Point, AP) για το οποίο υπάρχει συνδρομή. Κάθε σημείο πρόσβασης είναι ουσιαστικά ένα IP δίκτυο (μαζί με τις αντίστοιχες ρυθμίσεις) με συγκεκριμένη ονομασία και αναγνωρίζεται ως Δίκτυο Σημείου Πρόσβασης (Access Point Network, APN).
- Την διεύθυνση του HLR του συνδρομητή.

Συνδέεται με τα εξής:

- Επισκεπτόμενο MSC (Visited MSC, V-MSC) για την παροχή δεδομένων τα οποία χρειάζονται από το V-MSC κατά την διάρκεια των διαδικασιών που εκτελεί (π.χ. πιστοποίηση η την προετοιμασία έναρξης τηλεφωνήματος). Το V-MSC είναι το MSC της περιοχής που βρίσκεται ο συνδρομητής εκείνη τη στιγμή.
- HLR για να ζητήσει στοιχειά για τα κινητά τερματικά που έχουν προσκολληθεί στην περιοχή που εξυπηρετεί.
- Άλλα VLR για τη μεταφορά προσωρινών στοιχείων που σχετίζονται με το κινητό δορυφορικό τερματικό όταν μεταπηδά σε νέες περιοχές που ελέγχονται από νέα VLR (όπως πχ ο κωδικός TMSI).

Η λειτουργία του VLR είναι η εξής:

- Ενημέρωση του HLR ότι ο συνδρομητής έχει αφιχθεί σε μια περιοχή που εξυπηρετείται από το συγκεκριμένο VLR
- Να εντοπίσει την ακριβή θέση του χρηστή μέσα στην περιοχή εντοπισμού του VLR (Location Area, LA) όταν δεν έχει ενεργές κλήσεις.
- Να καθορίσει σε ποιες υπηρεσίες επιτρέπεται να έχει πρόσβαση ο συνδρομητής.
- Να αναθέσει τους αριθμούς υπό περιαγάγει κατά την επεξεργασία εισερχομένων κλήσεων (προς το κινητό)
- Να καθαρίσει το καταχωρημένο αρχείο συνδρομητή (subscriber record) όταν ο συνδρομητής αλλάξει κατάσταση σε ανενεργός και ενώ βρίσκεται μέσα στην περιοχή εντοπισμού του VLR. Το VLR διαγράφει τότε όλα τα στοιχειά του συνδρομητή μετά από κάποιο προκαθορισμένο χρονικό διάστημα αδράνειας (κατά το οποίο ο συνδρομητής παραμένει ανενεργός όπως πχ όταν έχει κλείσει το τερματικό του, η όταν έχει μεταπηδήσει σε περιοχή μη επαρκούς κάλυψης για αρκετό χρονικό διάστημα)
- Να διαγράψει κατόπιν εντολής από το HLR τα στοιχειά του συνδρομητή από την βάση όταν μετακινείται σε περιοχές δικαιοδοσίας κάποιου άλλου VLR

4.2.3.3.6 Κέντρο Μεταγωγής Σύντομων Μηνυμάτων SMS - Short Messaging Service Switching Center (SMS-SC)

Το δίκτυο BGAN έχει το δικό του Κέντρο Μεταγωγής SMS. Δίνει την δυνατότητα αποστολής μηνυμάτων SMS από τα δορυφορικά τερματικά σε άλλα τηλέφωνα που υποστηρίζουν SMS. Ο Inmarsat συνεργάζεται με την KPN για την διαχείριση ολόκληρης της κίνησης SMS προς και από το δίκτυο BGAN.

Ο DP μπορεί να παρέχει υπηρεσίες SMS σε τερματικά FBB μέσω οποιασδήποτε πύλης (gateway) τρίτου παρόχου με τον οποίο συνεργάζεται και εφόσον υπάρχει συμφωνία διασύνδεσης με την KPN.

4.2.3.3.7 Πύλη Υποστήριξης Υπηρεσιών GRPS - Gateway GRPS Support Node (GGSN)

Αποθηκεύονται πληροφορίες που λαμβάνονται από το HLR και τον SGSN. Χρησιμοποιούνται στη διαχείριση μεταφοράς των πακέτων (packet transport management) και ως πύλη μεταξύ της GPRS ραχοκοκαλιάς του δικτύου BGAN και άλλων δικτύων μεταγωγής πακέτου όπως IP δίκτυα, ιδιωτικά δίκτυα, internet). Μετατρέπει τα πακέτα που έρχονται από το SGSN στο κατάλληλο Πρωτόκολλο Πακέτων Δεδομένων (Packet Data Protocol) και τα τροφοδοτεί στο κατάλληλο δίκτυο μεταγωγής πακέτου. Στην αντίστροφη κατεύθυνση οι διευθύνσεις PDP των εισερχομένων πακέτων μετατρέπονται στις διευθύνσεις FBB/BGAN του χρηστή (προορισμού) και τροφοδοτούνται στο αρμόδιο SGSN. Για αυτό το σκοπό το GGSN αποθηκεύει τις τρέχουσες διευθύνσεις SGSN του χρηστή και το προφίλ του στον καταχωρητή θέσης (location register). Το GGSN είναι υπεύθυνο για την IP διευθυνσιοδότηση και είναι ο προεπιλεγμένος δρομολογητής για το συνδεδεμένο κινητό τερματικό. Το GGSN υποστηρίζει λειτουργίες χρέωσης και πιστοποίησης.

4.2.3.3.8 Κόμβοι Υποστήριξης Υπηρεσιών GPRS - Serving GPRS Support Node (SGSN)

Η λειτουργία του αναφέρεται στην διαχείριση μεταφοράς των πακέτων και αποθηκεύει δυο είδη πληροφοριών, subscription information και location information.

Το SGSN είναι υπεύθυνο για την παράδοση των πακέτων από και προς τους κινητούς δορυφορικούς σταθμούς (UT) μέσα στη γεωγραφική περιοχή που εξυπηρετεί. Η λειτουργίες του περιλαμβάνουν την δρομολόγηση και μεταφορά πακέτων, διαχείριση κινητικότητας χρηστή (προσκόλληση/αποκόλληση από το δίκτυο, διαχείριση περιοχής εντοπισμού/θεσης κινητού δορυφορικού σταθμού), διαχείριση λογικών συνδέσεων, λειτουργίες πιστοποίησης και χρέωσης . Ο καταχωρητής θέσης του SGSN αποθηκεύει πληροφορίες σχετικές με την τρέχουσα θέση ταυ κινητού δορυφορικού σταθμού (τρέχουσα δέσμη που εξυπηρετεί, τρέχων VLR) και τα προφίλ χρηστή (πχ IMSI, διεύθυνση που χρησιμοποιείται στο δίκτυο μεταγωγής πακέτου) όλων των χρηστών που είναι καταχωρημένοι και έχουν εγγράφει σε αυτό το SGSN

Η λειτουργία του SGSN είναι η εξής:

- Εξόρυξη (detunnel) πακέτων GTP από το τούνελ με το GGSN (downlink).
- Εισαγωγή IP πακέτων στο τούνελ (tunnel) με το GGSN.

- Να διεκπεραιώσει την διαχείριση κινητικότητας χρήστη καθώς ένας κινητός σταθμός που βρίσκεται σε κατάσταση αναμονής (standby) μετακινείται από μια περιοχή δρομολόγησης (Routing Area, RA) σε άλλη.
- Πληροφορίες/δεδομένα χρέωσης χρήστη.

4.2.3.3.9 Κέντρο Πιστοποίησης Συνδρομητών - Authentication Center (AuC)

Το Κέντρο Πιστοποίησης παράγει και αποθηκεύει όλα τα κλειδιά πιστοποίησης και κρυπτογράφησης. Χρησιμοποιείται για την επαλήθευση κάθε SIM κάρτας που προσπαθεί να αποκτήσει πρόσβαση στο Δίκτυο Κορμού. Εάν η επαλήθευση είναι σωστή τότε επιτρέπεται στο HLR να διαχειριστεί την SIM κάρτα καθώς και τις διαθέσιμες υπηρεσίες.

Επίσης παράγει κλειδιά κρυπτογράφησης τα οποία χρησιμοποιούνται με την σειρά τους για να κρυπτογραφήσουν την διακινούμενη πληροφορία.

Το AuC συνδέεται με το MSC, το οποίο ζητά μια καινούργια δέσμη δεδομένων για ένα IMSI αφού χρησιμοποιηθούν τα προηγούμενα. Έτσι εξασφαλίζεται ότι τα ίδια κλειδιά και αντιδράσεις πρόκλησης (challenge responses) δεν θα χρησιμοποιηθούν δεύτερη φορά για το ίδιο κινητό.

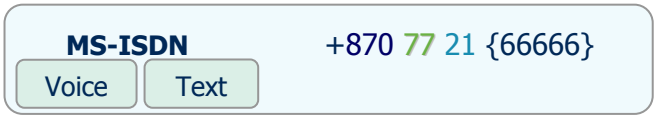
4.2.4 Αριθμοδότηση

4.2.4.1 MSISDN (Mobile Services International Subscriber Dialing Number)

Πρόκειται για τον αριθμό κλήσης του χρηστή. Είναι μοναδικός αριθμός ο οποίος δίνεται ανά παρεχόμενη υπηρεσία η οποία έχει ενεργοποιηθεί κατά την συνδρομή στο δίκτυο BGAN/FBB.

Στην υπηρεσία FBB ο αριθμός MSISDN είναι κοινός για φωνητικές κλήσεις και SMS.

Είναι της εξής μορφής:



Εικόνα 16: Αριθμοδότηση MSISDN

4.2.4.2 **AMSISDN** (Additional MSISDN)

Οι πρόσθετοι αριθμοί κλήσης χρησιμοποιούνται για τις υπηρεσίες Fax και ISDN.

Είναι της εξής μορφής:

Εικόνα 17: Αριθμοδότηση AMSISDN

Η περίοδος καραντίνας για ένα MSISDN πριν αυτό αποδοθεί σε καινούργιο χρήστη είναι 40 μέρες. Ο Inmarsat δεν σχεδιάζει να αναθέσει εύρη αριθμών στους DP.

4.2.4.3 Χρυσοί Αριθμοί – Golden Numbers

Μερικοί χρυσοί αριθμοί που θα επιλεγούν από τον Inmarsat μπορεί να δεσμευτούν και να διατεθούν για σκοπούς προώθησης.

4.2.5 Κάρτες UMTS Subscriber Identity Module (USIM)

Οι κάρτες USIM με ενσωματωμένο ολοκληρωμένο κύκλωμα (IC) έχουν τις ίδιες φυσικές διαστάσεις με τις αντίστοιχες UMTS και GSM κάρτες. Υποστηρίζει διάφορες λειτουργίες όπως:

- Υποστήριξη μιας η περισσοτέρων εφαρμογών User Service Identity Module, USIM.
- Υποστήριξη ενός ή περισσοτέρων προφίλ χρήστη στην USIM.
- Ενημέρωση πληροφοριών σχετικών με την USIM.
- Λειτουργίες ασφάλειας.
- Πιστοποίηση χρήστη.
- Προαιρετική συμπερίληψη τρόπου πληρωμής.
- Προαιρετική ασφαλής λήψη (download) νέων εφαρμογών.

Η USIM κάρτα της υπηρεσίας FBB θα είναι μια κοινή (generic) χωρίς κάποια συγκεκριμένη προσαρμογή σε κάποιο DP. Ο DP ανατίθεται στη κάρτα την στιγμή της ενεργοποίησης.

Ο Inmarsat συνεργάζεται με την εταιρία Gemalto (πρώην Axalto) σαν τον κατά προτίμηση κατασκευαστή USIM καρτών.

4.2.5.1 Διεθνής Ταυτότητα Κινητού Συνδρομητή - International Mobile Subscriber Identity (IMSI)

Κάθε κάρτα SIM εχει ένα μοναδικο χαρακτηριστικο αριθμό ο οποίος ονομαζεται IMSI (International Mobile Subscriber Identity).

Το IMSI είναι ένα μοναδικό διεθνές αναγνωριστικό ενός χρήστη υπηρεσίας FBB. Είναι μοναδικό για κάθε SIM κάρτα και αποτελείται από τα ακόλουθα μέρη.

- CC (Country Code, αναγνωριστικό χώρας, 202 για Ελλάδα)
- NC (Network Code, αναγνωριστικό δικτύου, π.χ. 870 για Inmarsat).
- SN (Subscriber Number).

4.2.5.2 Ταυτότητα Κάρτας Ενσωματωμένου Ολοκληρωμένου Κυκλώματος - Integrated Circuit Card ID (ICCID)

Κάθε κάρτα SIM έχει δικό της ξεχωριστό σειριακό αριθμό 18 ψηφίων ο οποίος αναγράφεται στο πλαστικό τμήμα της κάρτας και ονομάζεται Ταυτότητα Κάρτας Ενσωματωμένου Ολοκληρωμένου κυκλώματος (ICCID).

.

4.2.6 Δορυφορικά τερματικά (User Terminals)

Οι χρήστες της υπηρεσίας FBB μπορούν να επιλέξουν μια σειρά από δορυφορικά τερματικά FBB (FBB UTs) με διαφορετικές δυνατότητες. Στην υπηρεσία FBB καθορίζονται δυο κύριοι τύποι/κλάσεις τερματικών η κλάση 8 (Class 8 UTs) και η κλάση 9 (Class 9 UTs). Η βασική διαφορά μεταξύ της κλάσης 8 και της κλάσης 9 είναι η διάμετρος της κεραίας.

Σε όλες τις περιπτώσεις ο όρος Εξοπλισμός χρήστη (User Equipment, UE) αναφέρεται σε μια λογική μονάδα που αποτελείται από τα εξής:

4.2.6.1 Τερματικο Εξοπλισμο (Terminal Equipment, TE)

Συσκευή τελικού χρήστη (end user) που αποτελεί την διεπαφή μέσω της οποίας ο χρήστης χρησιμοποιεί τις δορυφορικές υπηρεσίες (πχ laptop/desktop computer, PDA).

Συνδέεται στο τερματικό χρήστη UT.

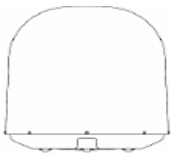
4.2.6.2 Τερματικό Χρήστη (User Terminal, UT)

Ράδιο τερματικό το οποίο χρησιμοποιείται για την επικοινωνία πάνω από τη δορυφορική διεπαφή το οποίο περιέχει τις λειτουργίες ενίσχυσης και την κεραία.

Το Τερματικό Χρήστη (UT) περιέχει μια έξυπνη κάρτα (smart card) η οποία ονομάζεται UMTS Subsciber Module (USIM) και αποθηκεύει την ταυτότητα χρήστη, εκτελεί τους αλγόριθμους πιστοποίησης, αποθηκεύει τα κλειδιά πιστοποίησης/κρυπτογράφισης και διατηρεί τις πληροφορίες του προφίλ τερματικού οι οποίες χρειάζονται από το τερματικό για τη χρήση της υπηρεσίας.

4.2.6.3 Δορυφορικά Τερματικά Κλάσης 8 & 9 (Class 8 & 9 UTs)

Τα τερματικά που υποστηρίζονται στην υπηρεσία FBB χωρίζονται σε 2 κλάσεις. Στην κλάση 8 η FB 500 και στην κλάση 9 η FB 250 . Οι κλάσεις τερματικών διαφέρουν μεταξύ τους στο μέγεθος της κεραίας και στις υπηρεσίες που υποστηρίζουν.



Hardware Definition	Class 8 - 'High Gain'	Class 9 - 'Low Gain'
Antenna Diameter approx	55cm	33cm
Antenna G/T (at 5o elevation)	-7dB/K	-15.5dB/K
Antenna EIRP	22dBW	15.1dBW
HPA Type	Linear	Linear
Approx Antenna weight	Directional/Stabilised	Directional/Stabilised
Product Data Features		
Standard IP Tx	192-432	78-239
Standard IP Rx	192-432	78-239
ISDN	Yes	No
Voice	4/64Kbps	4/64Kbps
3.1KHz (inc Fax)	Yes	Yes
SMS	Yes	Yes
IP 'Streaming Mode' (Throughput, Kbps)	32,64,128,256	32,64,(128)

Εικόνα 18: Χαρακτηριστικά και Υπηρεσίες τερματικών κλάσης 8 & 9

Και οι δυο κλάσεις τερματικών υποστηρίζουν την ταυτόχρονη χρήση μιας υπηρεσίας μεταγωγής κυκλώματος (Voice, ISDN, Fax -3.1KHz) και υπηρεσιών μεταγωγής πακέτου και ποιο συγκεκριμένα μέχρι 11 PDP contexts. Επίσης υποστηρίζουν πολλαπλούς χρηστές μέσω σύνδεσης πολλαπλών συσκευών τερματικού εξοπλισμού φωνής/δεδομένων/fax πάνω στο UT.

4.2.7 Διεθνής ταυτότητα εξοπλισμού κινητού σταθμού - Internation Mobile Equipment Identity (IMEI)

Το IMEI είναι ένας χαρακτηριστικός αριθμός, μοναδικός για κάθε δορυφορικό τερματικό FBB, και χρησιμοποιείται για την αναγνώριση του από το δίκτυο. Η πριμοδότηση ακολουθεί τις οδηγίες όπως περιγράφονται από την ένωση GSM PRD TW. 06 IMEI Allocation and Approval Guidelines v. 3.2.0. Αποτελείται από 5 κυρία τμήματα:

Country Code
Final Assembly Code
Manufacturer Code
Serial Number

Οι IMEI για κάθε ενεργή συσκευή σε ένα δίκτυο κινητής τηλεφωνίας αποθηκεύονται στον EIR (Equipment Identity Register), όπου κατατάσσονται σε 3 λίστες:

- Λευκή, αν είναι εξουσιοδοτημένη προς χρήση.
- Μαύρη, σε περίπτωση που είναι, π.χ. κλεμμένη.
- Γκρίζα, αν η συσκευή δεν έχει εγκριθεί ακόμη προς χρήση.

4.2.8 Ονομασία Σημείου Πρόσβασης Access Point Name (APN)

Η Ονομασία του Σημείου Πρόσβασης καθορίζει:

- Το δίκτυο στο όποιο θα συνδεθεί ο χρήστης και την δρομολόγηση της κίνησης (από ένα FBB τερματικό με μια κάρτα SIM η όποια έχει διατεθεί για αυτήν το σημείο πρόσβασης) σε ένα άλλο IP δίκτυο όπως το Internet η ένα εταιρικό δίκτυο.
- Τους τύπους των υπηρεσιών που είναι διαθέσιμοι.

- Το εύρος των IP διευθύνσεων που χρησιμοποιείται. Σε κάθε APN καθορίζεται και συνδυάζεται ένα σύνολο διευθύνσεων IP (IP address pool).

Κάθε DP πάροχος θα πρέπει να παρέχει στους συνδρομητές του με μια Ονομασία Σημείου Πρόσβασης. Η Ονομασία Σημείου Πρόσβασης είναι της μορφής otesat.bgan.inmarsat.com.
Ο Inmarsat διαχειρίζεται όλες τις ονομασίες Σημείου Πρόσβασης. Βάσει της βασικής προσφοράς υποδομής παρόχου DP infrastructure offering) ο Inmarsat ρυθμίζει και θα δοκιμάσει μια Ονομασία Σημείου Πρόσβασης (APN).

Η Ονομασία Σημείου Πρόσβασης προσδιορίζει ένα δίκτυο πακέτων δεδομένων το όποιο είναι ρυθμισμένο και προσβάσιμο από ένα GGSN. Μια Ονομασία Σημείου Πρόσβασης έχει διάφορα χαρακτηριστικά που σχετίζονται με την ρύθμιση της και που καθορίζουν τον τρόπο με τον όποιο οι χρηστές μπορούν να προσπελάσουν το δίκτυο σε εκείνο το σημείο εισόδου.

4.2.8.1 Επικοινωνία μεταξύ χρηστών του ιδίου APN

Όταν ο πάροχος DP διαθέτει δικό του APN έχει την δυνατότητα να ζητήσει από τον Inmarsat να επιτρέψει η να μην επιτρέψει την επικοινωνία μεταξύ χρηστών όντος του APN. Η κίνηση αυτή είναι μεταξύ δυο FBB τερματικών, και δρομολογείται από το δίκτυο BGAN του Inmarsat, χωρίς να καταλήξει σε άλλο IP δίκτυο. Εάν ο πάροχος DP δεν επιτρέπει αυτό τον τρόπο επικοινωνίας, η κίνηση θα σταλεί μέσα από το τούνελ (tunnel) προς το δίκτυο του DP παρόχου. Σε αυτή τη περίπτωση είναι ευθύνη του DP παρόδου να διαμοιράσει τη κίνηση και να εφαρμόσει στην υποδομή την πολιτική για την κίνηση τερματικού προς τερματικό (UT to UT traffic policy).

Η απευθείας επικοινωνία χρηστών μεταξύ διαφορετικών APN χωρίς δρομολόγηση πάνω από δημόσιες δικτυακές υποδομές συνήθως δεν επιτρέπεται.

4.2.9 Διευθυνσιοδότηση IP - IP Addressing

Η IP διευθυνσιοδότηση καθορίζεται από τις ανάγκες του DP παρόδου καθώς και των πελατών και περιλαμβάνει:

- Public dynamic IP addresses
- Private dynamic IP addresses
- Static IP addresses

Οι διευθύνσεις IP διαχειρίζονται από το δίκτυο του DP παρόχου και σχετίζονται με την Ονομασία Σημείου Πρόσβασης (APN). Ο πάροχος DP πρέπει να παρέχει στον Inmarsat τα εύρη δημοσίων διευθύνσεων (Public IP address ranges) και να συμφωνήσει για τις Ιδιωτικές διευθύνσεις IP (Private Addresses) που θα χρησιμοποιηθούν από τους πελάτες. Ο Inmarsat μπορεί να μην εκχωρήσει εύρη ιδιωτικών διευθύνσεων IP (Private Addresses) σε περίπτωση που συμπίπτουν/αλλεπικαλύπτονται με άλλα εύρη διευθύνσεων άλλων DP παρόχων.

Όταν ο DP πάροχος έχει δικό του Σημείο Παρουσίας PoP:

- Καθορίζει τις IP διευθύνσεις
- Διαχειρίζεται τα εύρη των IP διευθύνσεων
- Καθορίζει και θέτει σε εφαρμογή το σχέδιο δρομολόγησης IP (IP routing plan)

Η διαχείριση του εύρους των Διευθύνσεων IP (IP Address Range Management) και η ανάθεση των διευθύνσεων πραγματοποιούνται από έναν εξυπηρετητή RADIUS.

4.2.10 Υπηρεσία Απομακρυσμένης Πιστοποίησης Χρήστη μέσω κλήσης - Remote Authentication Dial-In User Service (RADIUS)

Ο Inmarsat ρυθμίζει και δοκιμάζει τους μηχανισμούς για την διασύνδεση του RADIUS server του παρόδου DP. Ο πάροχος DP διαθέτει έναν εξυπηρετητή RADIUS για τον έλεγχο του αριθμού των συνόδων (sessions) και την εγγύηση της ποιότητας υπηρεσίας (QoS).

4.2.11 Πλαίσιο Πρωτοκόλλου Πακέτων Δεδομένων - Packet Data Protocol (PDP) - PDP Context

Το πλαίσιο πρωτοκόλλου πακέτων δεδομένων είναι μια δομή δεδομένων που περιέχει τα στοιχεία συνόδου (session) του συνδρομητή, όταν ο συνδρομητής έχει μια ενεργή σύνοδο και βρίσκεται τόσο στο SGSN όσο και στο GGSN.

Όταν ένα δορυφορικό τερματικό (UT) θέλει να χρησιμοποιήσει την GPRS υπηρεσία, πρέπει πρώτα να συνδεθεί/προσκολληθεί (attach) στο δίκτυο και να ενεργοποιησει ενα πλαίσιο PDP. Τοτε ανατιθεται μια δομή δεδομένων πλαισιου PDP στο SGSN το οποίο επισκέπτεται ο συνδρομητής εκείνη τη στιγμή και

στο GGSN το οποίο εξυπηρετεί το Σημείο Πρόσβασης (Access Point) των συνδρομητών. Τα δεδομένα που εγγράφονται περιλαμβάνουν:

- Διεύθυνση IP του συνδρομητή - Subscriber's IP address
- Τον κωδικο IMSI του συνδρομητή Subscriber's IMSI
- Την Ταυτότητα Τούνελ Συνδρομητή - Subscriber's Tunnel ID
- Tunnel ID (TEID) at the GGSN
- Tunnel ID (TEID) at the SGSN
- Η ταυτότητα τούνελ Tunnel ID (TEID) είναι ένας αριθμός που ανατιθεται από το GSN και προσδιορίζει τα δεδομένα του τούνελ σε ενα συγκεκριμένο πλαίσιο PDP

Υπάρχουν δυο τύποι πλαισίων PDP:

- Πρωτεύον πλαίσιο PDP Primary PDP Context
- Έχει μια μοναδική διεύθυνση IP συνδεδεμένη μαζί του
- Δευτερεύον πλαίσιο - PDPSecondary PDP Context
- Μοιράζεται την διεύθυνση IP other ενα αλλο πλαίσιο PDP
- Δημιουργειται βαση ενός υπάρχοντος πλαισιου PDP (για να μοιραστεί την διεύθυνση IP)
- Μπορεί να έχει διαφορικές ρυθμίσεις Ποιότητας Υπηρεσίας (Quality of Service, QoS)
- Συνολικά μπορούν να συνυπάρξουν μέχρι και 11 πλαίσια PDP (με όλους τους συνδυασμούς πρωτευόντων και δευτερευόντων πλαισίων PDP)

4.2.12 Ποιότητα Υπηρεσίας – Quality of Service (QoS)

Το 3GPP (ETSI 23.107) πρωτόκολλο 3G UMTS υποστηρίζει 4 κλάσεις Ποιότητας Υπηρεσίας (QoS) που είναι:

- Conversational
- Bakcground
- Interactive
- Streaming

Οι DP πάροχοι θα πρέπει να λάβουν υπόψη τους τύπους των υπηρεσιών που παρέχονται στους πελάτες και την Ποιότητα Υπηρεσίας (QoS) που απαιτείται για κάθε προσφερόμενη υπηρεσία.

Ο όρος Ποιότητα Υπηρεσίας (QoS) έχει διάφορες σημασίες. Βάσει της Θεωρίας Τηλεπικοινωνιακής Κίνησης αναφέρεται στους μηχανισμούς ελέγχου κράτησης πόρων (resource reservation). Η Ποιότητα Υπηρεσίας μπορεί να παρέχει διαφορετικές προτεραιότητες σε διαφορετικούς χρήστες η ροές δεδομένων, η να εγγυηθεί ένα συγκεκριμένο επίπεδο επίδοσης σε μια ροή δεδομένων κατόπιν αιτήματος από την εφαρμογή (πρόγραμμα) η την πολιτική του παρόχου της υπηρεσίας. Οι εγγυήσεις Ποιότητας Υπηρεσίας είναι σημαντικές σε περιπτώσεις που η χωρητικότητα του δικτύου είναι περιορισμένη, όπως εφαρμογές μετάδοσης ροών πολυμεσικών δεδομένων (multimedia streaming) η φωνής πάνω από IP (VoIP) σε πραγματικό χρόνο που απαιτούν σταθερό ρυθμό μετάδοσης και είναι ευαίσθητα σε καθυστερήσεις . Η ποιότητα της υπηρεσίας περιλαμβάνει όλες τις πλευρές μιας σύνδεσης όπως χρονική απόκριση παροχής υπηρεσίας, ποιότητα φωνής, ηχώ (echo), απώλειες, αξιοπιστία (reliability), διαθεσιμότητα (availability), διατήρηση (sustainability) κτλ.

Το BGAN/FBB υποστηρίζει δυο κλάσεις υπηρεσιών :

- Background Class IP (Κλάση Υπόβαθρου). Δεν παρέχει εγγυημένο εύρος ζώνης (guaranteed bandwidth) στις συνδέσεις. Είναι κατάλληλη για εφαρμογές που βασίζονται σε TCP. Παραδείγματα εφαρμογών οι οποίες είναι κατάλληλες για συνδέσεις αυτού του τύπου είναι εφαρμογές γραφείου (Office applications) όπως email, MS Office, μεταφορά αρχείων, πρόσβαση στο Internet.
- Streaming Class IP (Κλάση Ροής) για τις υπηρεσίες κλάσης streaming με εγγυημένο εύρος ζώνης (bandwidth) για την διάρκεια της κάθε συνόδου (session) μέσω μιας ζεύξης με χαμηλής λανθάνουσας κατάστασης (latency). Αυτή η κλάση θα είναι διαθέσιμη κατά απαίτηση (on demand). Ο Inmarsat παρέχει υπηρεσία κλάσης 'ροής' με ταχύτητες 32, 64, 128, 256Kb/s. Ορισμένες ταχύτητες από αυτές δεν υποστηρίζονται από όλα τα δορυφορικά τερματικά. Είναι κατάλληλη για εφαρμογές που βασίζονται σε UDP.

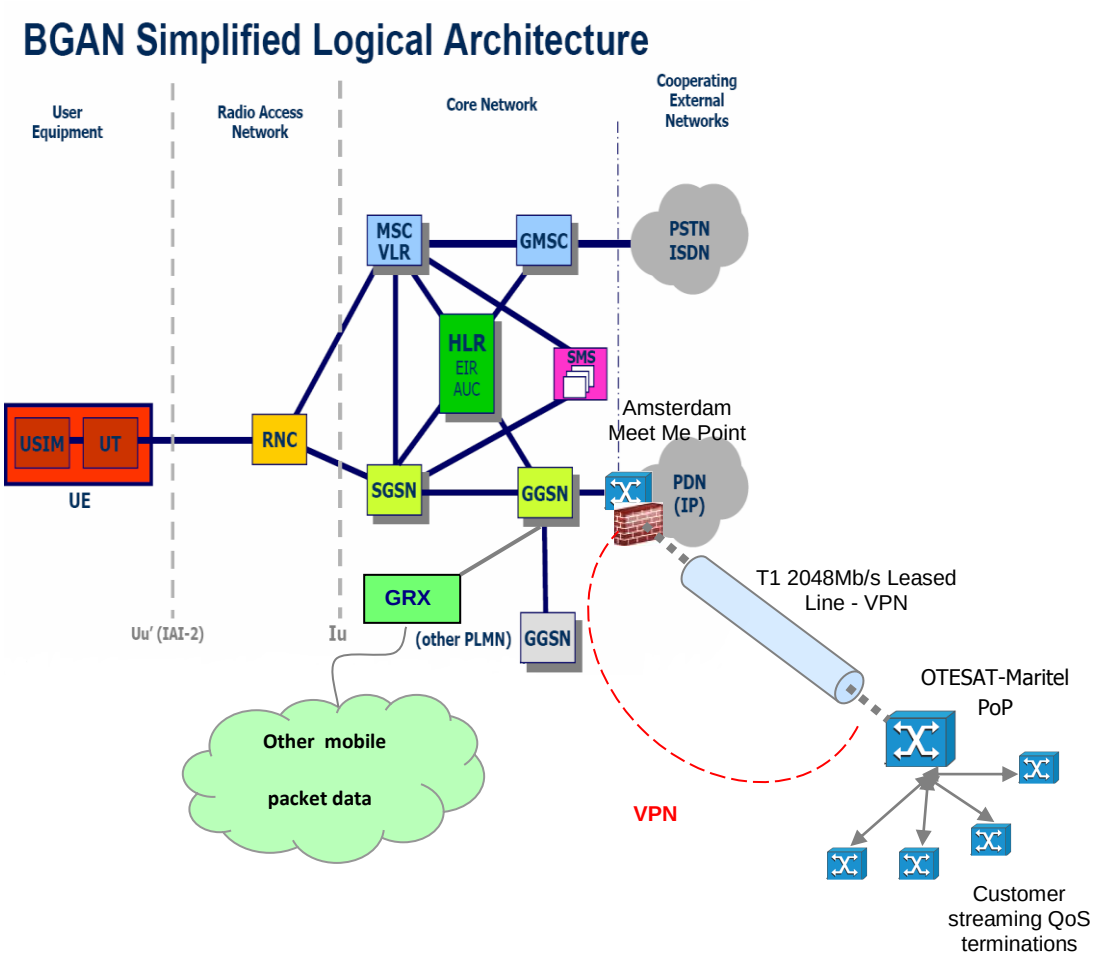
Η υπηρεσία ροής απαιτεί εγγυημένο εύρος ζώνης από την μια άκρη στην άλλη. Ο Inmarsat έχει εφαρμόσει και υποστηρίζει την Ποιότητα Υπηρεσίας (QoS) τόσο στο επίγειο δίκτυο BGAN όσο και στο δορυφορικό κομμάτι όπως αναφέρεται παρακάτω. Είναι μετά ευθύνη του Inmarsat, του παρόχου ή του πελάτη να αξιοποιήσει αυτές της πληροφορίες που διέρχονται μέσα από το δίκτυο BGAN και να παράσχει τα μέσα που θα επιτρέψουν την Ποιότητα Υπηρεσίας από άκρο σε άκρο (end-to-end QoS).

Για να εγγυηθεί την ποιότητα της υπηρεσίας ο Inmarsat:

- Παρέχει QoS στις δορυφορικές διεπαφές.
- Υποστηρίζει το 3GPP QoS στο επίγειο δίκτυο BGAN.

- Η κλάση της υπηρεσίας (Bakcground, Streaming) παρέχεται μέσω διαπραγμάτευσης του εξοπλισμού χρήστη (UT) και το δίκτυο κορμού BGAN κατά την ενεργοποίηση του πλαισίου PDP.

- Υποστηρίζει Διαφοροποιημένες Υπηρεσίες και την αντιστοίχηση/χαρτογραφηση (mapping) από το 3GPP QoS σε Σημεία Κώδικα Διαφοροποιημένων Υπηρεσιών (Differentiated Services Code Points, DSCP). Η σχέση ανάμεσα στα Σημεία Κώδικα Διαφοροποιημένων Υπηρεσιών και την συμπεριφορά ανά 'άλμα' (hop) είναι:
  - Κλάση Υποβάθρου (Background Class): Βέλτιστης προσπάθειας (best effort). Καμία ειδική μεταχείριση.
  - Κλάση Ροής (Streaming Class). Εξασφαλισμένη προώθηση και προτεραιότητα πάνω από τα πακέτο βέλτιστης προσπάθειας (best effort).
- Η αντιστοίχηση/χαρτογράφηση (mapping) της ροής upstream (αντίθετα προς το ρεύμα) καθορίζεται στον ορισμό του APN. Το δίκτυο BGAN αντιστοιχεί/χαρτογραφεί στην διεπαφή εξόδου Gi (outbound interface, η Gi interface) όπως περιγράφεται πιο πάνω. Το μαρκάρισμα (marking) Σημείου Κώδικα Διαφοροποιημένων Υπηρεσιών (DSCP) θα αντιγραφεί στην εξωτερική IP κεφαλίδα ασφαλείας (IP security header) όταν οδηγηθεί μέσα από το τούνελ (tunnel).
- Η αντιστοίχηση/χαρτογραφηση (mapping) της ροής downstream (στην κατεύθυνση ρεύματος) έχει καθοριστεί παγκόσμια για τα GGSN του Inmarsat. Τα πακέτα ροής (streaming packets) μπορούν να αποκτήσουν προτεραιότητα σε σχέση με τα πακέτα GTP (GPRS Tunneling Protocol). Χρησιμοποιούνται λειτουργίες Διαφοροποιημένων Υπηρεσιών (DiffServ) όπως το μαρκάρισμα, η ουρά αναμονής, τα χρονοδιαγράμματα και παράληψη των πακέτων.



Εικόνα 19: Αρχιτεκτονική BGAN

ΚΕΦΑΛΑΙΟ 5

5.1 Μελέτη Πληροφοριακού Συστήματος

Η θεώρηση του πληροφοριακού συστήματος δεν θα είναι υποτιθέμενη αλλά θα έχει αντίκτυπο σε πραγματικές συνθήκες. Πιο συγκεκριμένα, θα θεωρηθεί η εταιρεία Otesat – Maritel Δορυφορικές και Ναυτιλιακές Τηλεπικοινωνίες Α.Ε. και το πληροφοριακό σύστημα θα αφορά ένα σύστημα που θα αναπτυχθεί εσωτερικά από το δυναμικό της εταιρείας για την εξυπηρέτηση αναγκών της εταιρείας που έχουν προκύψει στο πλέον ανταγωνιστικό περιβάλλον των τηλεπικοινωνιών, όπως θα αναλυθεί στη συνέχεια.

5.2 Η εταιρεία Otesat - Maritel

Η Otesat-Maritel, μέλος του Ομίλου ΟΤΕ, παρέχει δορυφορικές υπηρεσίες Inmarsat και Iridium σε παγκόσμιο επίπεδο, σε ξηρά και θάλασσα και ολοκληρωμένες τηλεπικοινωνιακές λύσεις στην ελληνική και παγκόσμια ναυτιλιακή βιομηχανία.

Παράλληλα, η εταιρεία είναι σε θέση να εξυπηρετεί όλες τις τηλεπικοινωνιακές ανάγκες της Ελληνικής ναυτιλιακής βιομηχανίας, παρέχοντας όλα τα προϊόντα και τις υπηρεσίες του Ομίλου ΟΤΕ.

Η αγορά στην οποία απευθύνεται είναι στον κλάδο της Ναυτιλιακής Βιομηχανίας, σε εταιρείες Διαχείρισης Πλοίων, Εκκαθαρίστριες Εταιρείες, Κυβερνητικούς και Δημόσιους Οργανισμούς, παρόχους υπηρεσιών Inmarsat, ναυλομεσιτικά Γραφεία, νηογνώμονες, εταιρείες Εφοδιασμού Πλοίων, και οργανισμοί Λιμένων.

Τέλος άλλοι κλάδοι ενδιαφέροντος αποτελούν Μέσα Μαζικής Ενημέρωσης, Βιομηχανικές και Εμπορικές Εταιρείες, Εταιρείες Επίγειων Μεταφορών, Χρηματοπιστωτικοί Οργανισμοί, Κατασκευαστικές Εταιρείες, Ασφαλιστικές Εταιρείες, Ερευνητικά Κέντρα και Πάροχοι Υπηρεσιών Internet.

5.3 Παρεχόμενες Υπηρεσίες

Η εταιρεία παρέχει πιο συγκριμένα δορυφορικές τηλεπικοινωνιακές υπηρεσίες Inmarsat με παγκόσμια κάλυψη στα συστήματα Inmarsat B, C, mini-C, M, mini-M, GAN (M4), Fleet 77, 55, 33 μέσω των επίγειων σταθμών «ΘΕΡΜΟΠΥΛΑΙ» και συνεργατών καθώς και υπηρεσίες BGAN.

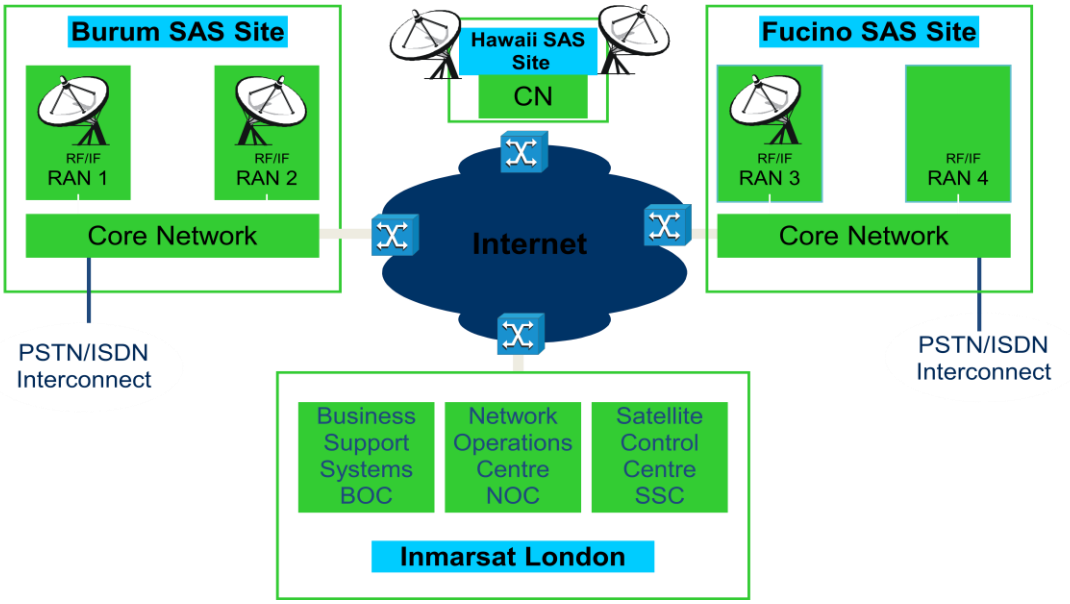
Επίσης η εταιρεία παρέχει FleetBroadband υπηρεσίες ως Distributor Partner του Inmarsat. Παράλληλα, παρεχόμενες δορυφορικές τηλεπικοινωνιακές υπηρεσίες αποτελούν αυτές του Iridium με πραγματική παγκόσμια κάλυψη, που συμπεριλαμβάνει όλες τις ωκεάνιες περιοχές καθώς και τους πόλους, ενώ παράλληλα ως μέλος του Ομίλου ΟΤΕ η Otesat-Maritel προσφέρει στη ναυτιλιακή βιομηχανία προϊόντα και υπηρεσίες του Ομίλου όπως τηλεπικοινωνιακά προϊόντα και υπηρεσίες ΟΤΕ, υπηρεσίες κινητής τηλεφωνίας Cosmote, υπηρεσίες Ip και Internet, υπηρεσίες φωνής και fax.

5.4 Πληροφοριακό Σύστημα Provisioning System για Υπηρεσίες Fleet Broadband

5.4.1 Βασική Περιγραφή Inmarsat Συστήματος FleetBroadband

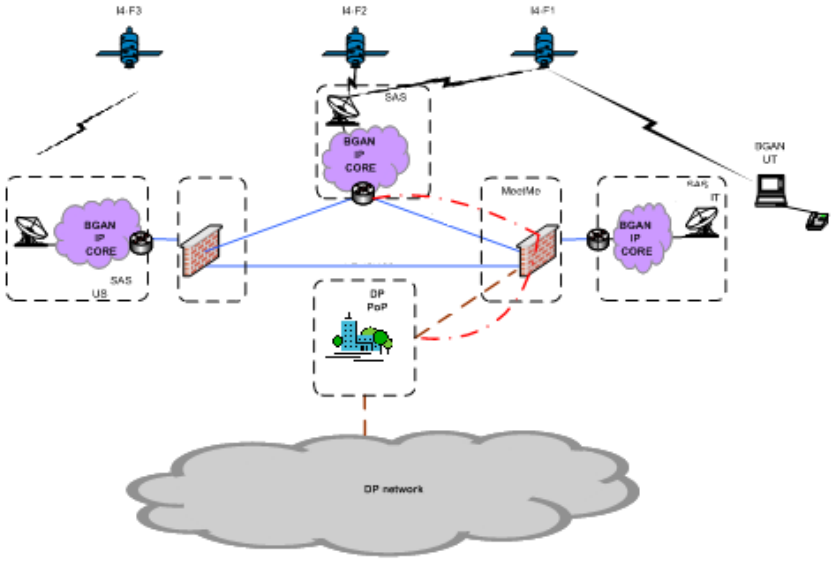
Σε αυτό το σημείο θα γίνει μια σύντομη περιγραφή της υπηρεσίας FleetBroadband και του δικτύου BGAN (Broadband Global Area Network) ώστε να γίνει αντιληπτή και κατανοητή η αναγκαιότητα, η βασική λειτουργία και η χρησιμότητα του πληροφοριακού συστήματος που θα αναλυθεί με την σκοπιά της διοίκησης έργου.

Η υπηρεσία Fleetbroadband (FBB) παρέχεται μέσω των δορυφόρων 4ης γενιάς του Inmarsat, του επίγειου δικτύου BGAN και των συμβατών κινητών δορυφορικών σταθμών Inmarsat (User Terminal, UT). Το δίκτυο BGAN αποτελείται δορυφορικούς σταθμούς πρόσβασης (Satellite Access Station, SAS) με διασύνδεση σε επίγεια δίκτυα (PSTN, ISDN, PLMN, IP κτλ).



Εικόνα 20: Επίγειο Δίκτυο BGAN & Fleetbroadband

Ο Inmarsat λειτουργεί και διαχειρίζεται τρεία Σημεία Συνάντησης (Meet-Me-Points, MMP) τα οποία βρίσκονται σε κεντρικούς Κόμβους Εναλλαγής Internet (Internet Exchanges) κίνησης . Τα Σημεία Συνάντησης έχουν δημιουργηθεί με σκοπό να διευκολύνουν την διασύνδεση των DP παρόχων με τις υποδομές του επίγειου δικτύου BGAN. Ένα Σημείο Παρουσίας (PoP) παρέχει στους DP τη δυνατότητα καλύτερης διαχείρισης και ελέγχου των υπηρεσιών που παρέχονται προς του πελάτες. Δίνει επίσης την δυνατότητα και διαφοροποίησης των υπηρεσιών μέσω της παροχής υπηρεσιών προστιθέμενης αξίας (value added services) μέσω του Σημείου Παρουσίας (PoP).



Εικόνα 21: BGAN - DP Ground Network

Έτσι, μέσω της παραπάνω αρχιτεκτονικής το Fleet Broadband, βασισμένο σε 3G δίκτυα προσφέρει συνεχή, παράλληλη πρόσβαση σε τηλεφωνία και data σε εξαιρετικά υψηλές ταχύτητες με δυνατότητα παγκόσμιας κάλυψης. Ο συνδρομητής δύναται την ίδια χρονική στιγμή να λαμβάνει μηνύματα ηλεκτρονικού ταχυδρομείου, να χρησιμοποιεί απαιτητικές σε bandwidth εφαρμογές αλλά και να πραγματοποιεί τηλεφωνικές κλήσεις οικονομικά και αξιόπιστα. Με εύκολο στην εγκατάσταση εξοπλισμό αλλά και δυνατότητα αφομοίωσης από πλοία κάθε είδους το εκάστοτε τερματικό υποστηρίζει πολλαπλές εφαρμογές για απρόσκοπτη επικοινωνία, ενημέρωση και ψυχαγωγία.

Οι αυξημένες απαιτήσεις της σύγχρονης ναυτιλίας δεν περιορίζονται μόνο σε θέματα ομαλής πλοήγησης αλλά επεκτείνονται και στους τομείς των επικοινωνιών. Η εκπλήρωση των ποικίλων εργασιών εν κινήσει περιλαμβάνει ενημέρωση σχετικά με τις αναμενόμενες καιρικές συνθήκες, σχεδιασμό πορείας ταξιδίου, παραγγελία αγαθών και αποθεμάτων, καθώς και επικοινωνία με τον έξω κόσμο. Το Fleet Broadband διεκπεραιώνει επιτυχώς όλα τα παραπάνω καθώς βασίζεται σε πρωτόκολλα IP που υποστηρίζουν πλήρως επικοινωνία και εφαρμογές μέσω αρχιτεκτονικής διαδικτύου αλλά και τις ήδη γνωστές υπηρεσίες τηλεφωνίας και δεδομένων που διέρχονται από τα κυκλώματα μεταγωγής του Inmarsat. Για τις επιχειρησιακές ανάγκες του κάθε οργανισμού που επιθυμεί μεγαλύτερη ασφάλεια στις ηλεκτρονικές εφαρμογές, υποστηρίζει Virtual Private Networks και λειτουργίες κωδικοποίησης – κρυπτογράφησης δεδομένων.

5.4.2 Ιδέα και Βασική Περιγραφή του Πληροφοριακού Συστήματος

Το έργο πληροφοριακού συστήματος που θα εξεταστεί θα αναληφθεί από την εταιρεία και αφορά ένα πληροφοριακό σύστημα provisioning μέσα από το οποίο θα μπορεί το customer care τμήμα της εταιρείας αλλά και οι πελάτες της να είναι σε θέση να πραγματοποιούν μια σειρά ενεργειών (πχ. ενεργοποιήσεις - απενεργοποιήσεις SIM καρτών και άλλων πρόσθετων υπηρεσιών της SIM κάρτα τους, διαχείριση, έλεγχο και παρακολούθηση χρήσης και τιμολόγησης υπηρεσιών) σε υπηρεσίες που σχετίζονται με Inmarsat FleetBroadband με αυτοματοποιημένο και άμεσης ανταπόκρισης τρόπο.

Αυτό το σύστημα, θα βοηθήσει τόσο την εταιρεία να μπορεί να παρέχει τις υπηρεσίες στους πελάτες της συνοδευόμενες από μια σειρά πρόσθετων λειτουργιών και δυνατοτήτων οι οποίες θα πραγματοποιούνται με γρήγορο, οργανωμένο, και αυτοματοποιημένο τρόπο, ενώ από πλευράς πελατών θα μπορούν να διαχειριστούν καλύτερα τις υπηρεσίες και την χρήση των SIM καρτών τους για λογαριασμό

του αυτού τους ή ως Ναυτιλιακές Εταιρείες για λογαριασμό του στόλου των πλοίων που διαχειρίζονται και επιβλέπουν.

Πιο αναλυτικά, οι υπηρεσίες στις οποίες πρέπει να είναι ικανό να ανταποκρίνεται η λειτουργία του υπό ανάπτυξης πληροφοριακού συστήματος είναι αυτές του Fleetbroadband συστήματος:

- **Telephony**

Πραγματοποίηση τηλεφωνικών κλήσεων σε σταθερούς και κινητούς προορισμούς με παράλληλη χρήση εφαρμογών δεδομένων. Το Fleetbroadband προσφέρει υπηρεσία φωνής (Circuit Switched voice) μέσω καναλιού φωνής με την χρησιμοποίηση τεχνολογίας συμπίεσης Inmarsat (AMBE+2) και προσφερόμενη ποιότητα φωνής 4kbps και επίσης μέσω PCM 3.1KHz (ITU G.711) καναλιού με ρυθμό μετάδοσης 64Kbps.

Παράλληλα πρόσθετες υπηρεσίες ανάλογων των κυψελωτών δικτύων πρέπει να υποστηρίζονται, όπως φαίνονται στον παρακάτω πίνακα.

CFU	Call Forwarding On Subscriber Busy
CFB	Call Forwarding Unconditional
CFNRy	Call Forwarding on No Reply
CFNRc	Call Forwarding on Mobile Subscriber Not reachable
CW	Call Waiting
HOLD	Call Hold
BAOC	Barring of All Outgoing Calls

Πίνακας 2: Υπηρεσίες τηλεφωνίας Fleetbroadband

- **ISDN**

Υπηρεσίες ISDN με ταχύτητες 56 ή 64 kbps με ανάλογες πρόσθετες δυνατότητες της τηλεφωνίας

- **Fax**

Υποστήριξη Group 3 Fax μέσω φωνής (3.1 kHz audio) αλλά και μέσω καναλιού ISDN UDI/RDI (Group 4 Fax).

- **Voicemail**

Προσωπική θυρίδα αποθήκευσης φωνητικών μηνυμάτων σε περιπτώσεις όπου ο συνδρομητής δεν είναι διαθέσιμος.

- **SMS**

Το FleetBroadband παρέχει υπηρεσία SMS. Το SMS αποτελείται από 160 χαρακτήρες.

- **Standard IP**

Η υπηρεσία Standard IP ενδείκνυται για πρόσβαση σε ηλεκτρονικό ταχυδρομείο, διαδίκτυο αλλά και σε περιβάλλον Intranet, καθώς και σε περιπτώσεις όπου απαιτείται μεταφορά αρχείων μεγάλου μεγέθους με μέγιστη ταχύτητα μεταφοράς δεδομένων μέχρι 432 kbps. Η λειτουργία αυτών των IP καναλιών είναι ανάλογη με την λειτουργία μιας ευρυζωνικής υπηρεσίας.

- **Streaming IP**

Εγγυημένες ταχύτητες από 32 μέχρι και 256 kbps. Σε περιπτώσεις όπου απαιτείται υψηλή ποιότητα επικοινωνίας, όπως για χρήση live video, store & forward, αλλά και videoconferencing. Συγκεκριμένα παρέχονται οι εξής ταχύτητες: 32, 64, 128 & 256 kbps τόσο για την παραλαβή όσο και για την λήψη δεδομένων.

Η ανάπτυξη ενός πληροφοριακού συστήματος κρίνεται επιτακτική ανάγκη για την επιβίωση μιας εταιρείας παροχής τέτοιων υπηρεσιών στον τομέα των δορυφορικών κινητών επικοινωνιών. Πληθώρα εφαρμογών μπορούν πλέον να αποκτήσουν πραγματική διάσταση και να αξιοποιηθούν και στον τομέα των δορυφορικών κινητών επικοινωνιών.

Η λήψη και αποστολή αλληλογραφίας με χρήση αξιόπιστων προγραμμάτων όπως Outlook αλλά και πρόσβαση σε γνωστές ιστοσελίδες διαχείρισης ηλεκτρονικού ταχυδρομείου όπως gmail, yahoo & hotmail, η έγκυρη up to date ενημέρωση καιρικών συνθηκών 24/7 και προειδοποίηση σε περίπτωση επικίνδυνων φαινομένων, η τηλεδιάσκεψη, το κατέβασμα αρχείων μεγάλου μεγέθους όπως οπτικοακουστικό υλικό αλλά και διαφόρων applications (π.χ. antivirus software) σε υψηλές ταχύτητες που ελαχιστοποιούν το απαιτούμενο κόστος, πλοήγηση στο διαδίκτυο σε ασφαλές περιβάλλον (ενημέρωση και ψυχαγωγία, πραγματοποίηση online αγορών, κλείσιμο εισιτηρίων) είναι μερικές από τις συνήθεις.

Παράλληλα, δίνεται η δυνατότητα με αξιόπιστα firewalls, να επιτυγχάνεται επιλεκτική πρόσβαση σε συγκεκριμένες ιστοσελίδες και light έκδοση γνωστών site (κείμενο χωρίς φωτογραφίες) για μικρότερη επιβάρυνση κόστους, η δυνατότητα για ασφαλείς επικοινωνίες και σύνδεση σε επιχειρησιακό intranet περιβάλλον μέσω Virtual Private Network για την ομαλή και απρόσκοπτη διαχείριση των εκάστοτε επιχειρησιακών αναγκών.

Τέλος σημαντικές κερδοφόρες εφαρμογές αποτελούν οι επικοινωνίες πληρώματος, όπως η τηλεφωνία, η πρόσβαση στο διαδίκτυο, η τηλεδιάσκεψη, ενημέρωση και ψυχαγωγία που μπορούν να

«τρέχουν» ταυτόχρονα σε πλοία που διαθέτουν εξοπλισμό Fleet Broadband καθώς και το η αποθήκευση και προώθηση video - οπτικοακουστικού υλικού εύκολα και γρήγορα με υψηλές.

Έτσι, για να μπορέσει ο πελάτης να είναι σε θέση να του παρέχονται οι παραπάνω υπηρεσίες και επίσης να δύναται να αξιοποιήσει τις εφαρμογές της τεχνολογίας Fleetbroadband, το προαναφερθέν πληροφοριακό σύστημα provisioning είναι επιτακτική ανάγκη για την εταιρεία.

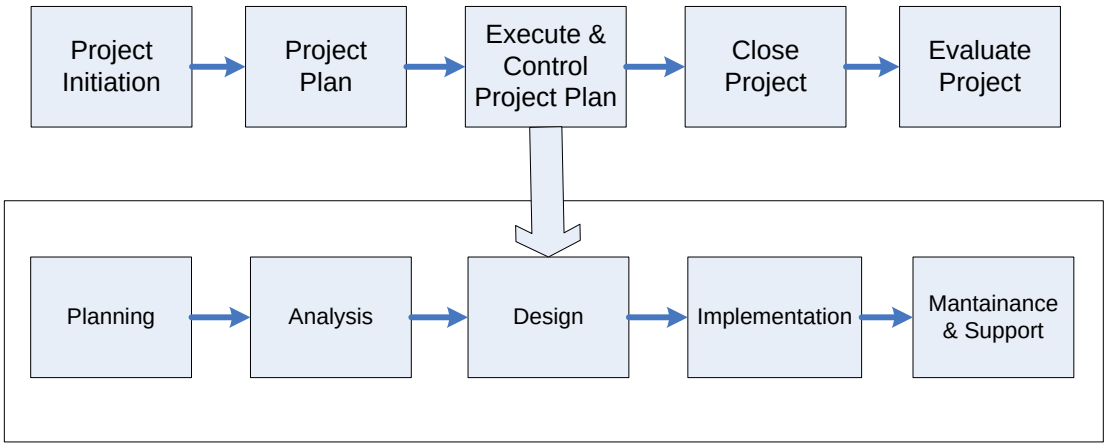
Ο πελάτης έτσι, θα μπορεί με το σχεδιαζόμενο πληροφοριακό σύστημα να έχει πρόσβαση σε ένα interface – γραφικό περιβάλλον το οποίο πρέπει να είναι ασφαλές και προσβάσιμο από το ίντερνετ για μεγαλύτερη ευκολία, και στο οποίο θα μπορεί αν είναι για παράδειγμα Ναυτιλιακή Εταιρεία να έχει την απαραίτητη πληροφορία για τις SIM κάρτες που λειτουργούν σε συστήματα FleetBroadband στο στόλο των πλοίων που ανήκουν στην ναυτιλιακή, και επίσης την δυνατότητας να κάνει κάποιες ενέργειες στις εκάστοτε SIM (απενεργοποιήσεις – ενεργοποιήσεις – παύση) ή να λάβει πληροφορίες κίνησης και τιμολόγησης για την κίνησή του σε πραγματικό χρόνο χωρίς να περιμένει την έκδοση τιμολογίου στο τέλος του μήνα ή ακόμα και να θέσει κανόνες firewall ανάλογα με το είδος των εφαρμογών που θέλει να χρησιμοποιήσει μέσω του δορυφορικού συστήματος.

Το σημαντικό σε αυτό το πληροφοριακό σύστημα είναι ότι όλες οι ενέργειες στις SIM κάρτες μπορούν να γίνουν με ηλεκτρονικό τρόπο, χωρίς την συμπλήρωση hardcopy φορμών, αποστολή emails, τηλεφωνικές επικοινωνίες για αιτήματα με το customer care της εταιρείας, ενέργειες γρήγορες, άμεσες, χωρίς γραφειοκρατία και διαδικασίες που να εξαρτώνται από τον συντονισμό πολλών τμημάτων της εταιρείας, και σίγουρα θα πρόκειται για ένα σύστημα που όλες οι πληροφορίες και οι ενέργειες θα είναι καταγεγραμμένες, οργανωμένες ώστε και η επίλυση τυχόν δυσλειτουργιών να είναι ευκολότερη από το support department της εταιρείας Otesat-Maritel.

Επομένως, το provisioning σύστημα της Otesat-Maritel για τις υπηρεσίες FleetBroadband του Inmarsat πρόκειται για ένα πλήρες πληροφοριακό σύστημα, αποτελούμενο από πολλά στοιχεία που πρέπει να αναλυθούν, να μελετηθούν, να σχεδιαστούν, να υλοποιηθούν και να συνεργαστούν ώστε να επιτευχθεί το τελικό αποτέλεσμα της επιτυχούς λειτουργίας προς εξυπηρέτηση των πελατών και της ίδιας της εταιρείας. Πρόκειται με άλλα λόγια για ένα έργο το οποίο πρέπει να ακολουθήσει το μοντέλο των φάσεων ανάπτυξης των έργων για να ολοκληρωθεί επιτυχώς στο επιθυμητό χρονικό διάστημα.

5.5 Ανάλυση Πληροφοριακού Συστήματος

Όπως κάθε έργο, έτσι και το έργο πληροφοριακού συστήματος στην προκειμένη περίπτωση της Otesat - Maritel, θα ακολουθήσει τον λεγόμενο Κύκλο Ζωής Έργου (Project Life Cycle), ο οποίος αναφέρεται σε μία λογική ακολουθία δραστηριοτήτων για την επίτευξη των σκοπών ή στόχων του Έργου. Κάθε Έργο λοιπόν διέρχεται από μία σειρά φάσεων κατά τη διάρκεια της ζωής του και τυπικά τα έργα ακολουθούν ένα μοντέλο κύκλου ζωής ανάλογο του σχήματος που ακολουθεί, χωρίς βέβαια να είναι δεσμευτικό για όλα τα έργα. Ανάλογα δηλαδή με τις συνθήκες και την περίπτωση έργου οι φάσεις προσαρμόζονται, αλλά γενικά ακολουθείται η παρακάτω αλληλουχία.



Εικόνα 22: Κύκλος ζωής Έργου

5.6 Περιγραφή Φάσεων Κύκλου Ζωής Έργου

Η πρώτη φάση είναι αυτή της Έναρξης του Έργου. Κατά τη φάση αυτή γίνεται η σύλληψη της ιδέας (concept development) όπου εντοπίζεται ένα επιχειρησιακό πρόβλημα ή μία ευκαιρία και παράγεται η λεγόμενη Έκθεση Επιχειρησιακής Σκοπιμότητας Έργου. Πριν από, κατά τη διάρκεια ή μετά την εκπόνηση της Έκθεσης Επιχειρησιακής Σκοπιμότητας Έργου εκπονούνται συνήθως η Ανάλυση Κόστους-Οφέλους και η Μελέτη Σκοπιμότητας για τον προσδιορισμό της εναλλακτικής λύσης με το μέγιστο καθαρό όφελος και για τη διερεύνηση του βαθμού στον οποίο κάθε εναλλακτική λύση αντιμετωπίζει το επιχειρησιακό πρόβλημα. Ως αποτέλεσμα της Έκθεσης Επιχειρησιακής Σκοπιμότητας Έργου, προτείνεται μία τελική συνιστώμενη λύση. Όταν η συνιστώμενη λύση εγκριθεί, διορίζονται το Επιτελικό Στέλεχος και ο Υπεύθυνος

Συντονιστής για να συμμετάσχουν στην εκπόνηση του «Τεχνικού Δελτίου Έργου», το οποίο περιγράφει συνοπτικά το αντικείμενο, τους στόχους, τις δραστηριότητες, τη δομή, τον προϋπολογισμό, το χρονοδιάγραμμα υλοποίησης, τους κινδύνους, τους περιορισμούς και τις υποθέσεις εργασίας για το Έργο. Όταν το Τεχνικό Δελτίο Έργου εγκριθεί, διορίζονται τα υπόλοιπα μέλη της Ομάδας Διαχείρισης Έργου.

Σε επόμενη φάση ακολουθεί ο λεγόμενος Προγραμματισμός Έργου. Η φάση αυτή περιλαμβάνει τον προγραμματισμό/ σχεδιασμό όλων των στοιχείων/ παραμέτρων του Έργου, έτσι ώστε να είναι έτοιμο προς υλοποίηση. Με άλλα λόγια, σε αυτή τη φάση δεν έχει ξεκινήσει η υλοποίηση του έργου, αλλά γράφονται όλα εκείνα τα απαραίτητα έγγραφα και σχέδια που θα αποτελέσουν αναφορά για την υλοποίηση. Σε αυτή την φάση θα δημιουργηθεί το λεγόμενο Πλάνο Έργου (Project Plan που εμπεριέχεται στην πρόταση έργου (Project Proposal). Έτσι για παράδειγμα, σε αυτή την φάση της μελέτης εκπονούνται σχέδια Χρονοδιαγράμματος Δραστηριοτήτων (καθορισμός της ακολουθίας δραστηριοτήτων και εργασιών, χρονικός προγραμματισμός), Διαχείρισης Πόρων (προσδιορισμός της εργασίας, του εξοπλισμού, των υλικών που απαιτούνται σε κάθε εργασία/στάδιο), Πρόγραμμα Κόστους (προσδιορισμός εσωτερικών και εξωτερικών μεγεθών κόστους και του χρόνου εμφάνισής τους), σχέδιο Διαχείρισης Κινδύνων (επισήμανση πιθανών κινδύνων και των ενεργειών για τον μετριασμό τους), σχέδιο Ποιότητας (ορισμός στόχων ποιότητας για τα παραδοτέα του Έργου και καθορισμός των διεργασιών διασφάλισης και ελέγχου ποιότητας), σχέδιο Διαχείρισης Ζητημάτων (καθορισμός διεργασίας για τον προσδιορισμό, εκτίμηση και επίλυση ζητημάτων σχετικών με το Έργο), σχέδιο Διαχείρισης Αλλαγών (καθορισμός διεργασίας για τη διαχείριση αλλαγών που έχουν άμεση επίπτωση στο Έργο), σχέδιο Αποδοχής Παραδοτέων (ορισμός κριτηρίων αποδοχής για τα παραδοτέα του Έργου και καθορισμός των διεργασιών για την εκτέλεση των δοκιμών αποδοχής), σχέδιο Επικοινωνίας (καθορισμός πληροφοριών προς διανομή στους ενδιαφερομένους και επιλογή των κατάλληλων μεθόδων για τη διανομή τους).

Στην επόμενη φάση, ακολουθεί η εκτέλεση και ο έλεγχος του Έργου, όπου όπως φαίνεται και από παραπάνω σχήμα απαρτίζεται από τις υποφάσεις του planning, analysis, design, implementation, maintenance & support. Η φάση αυτή περιλαμβάνει την εκτέλεση κάθε δραστηριότητας και εργασίας που ορίζεται στο Χρονοδιάγραμμα του Έργου. Παράλληλα, κατά την υλοποίηση των δραστηριοτήτων και των εργασιών εκτελείται μία σειρά από διαχειριστικές διαδικασίες για την παρακολούθηση και τον έλεγχο των εξής: χρόνου, πόρων, κόστους, κινδύνων, ποιότητας, ζητημάτων, αλλαγών, διαδικασίας αποδοχής παραδοτέων, επικοινωνίας, κλπ. Ο Φορέας Υλοποίησης φέρει την πλήρη ευθύνη για την επίτευξη όλων των αποτελεσμάτων του Έργου.

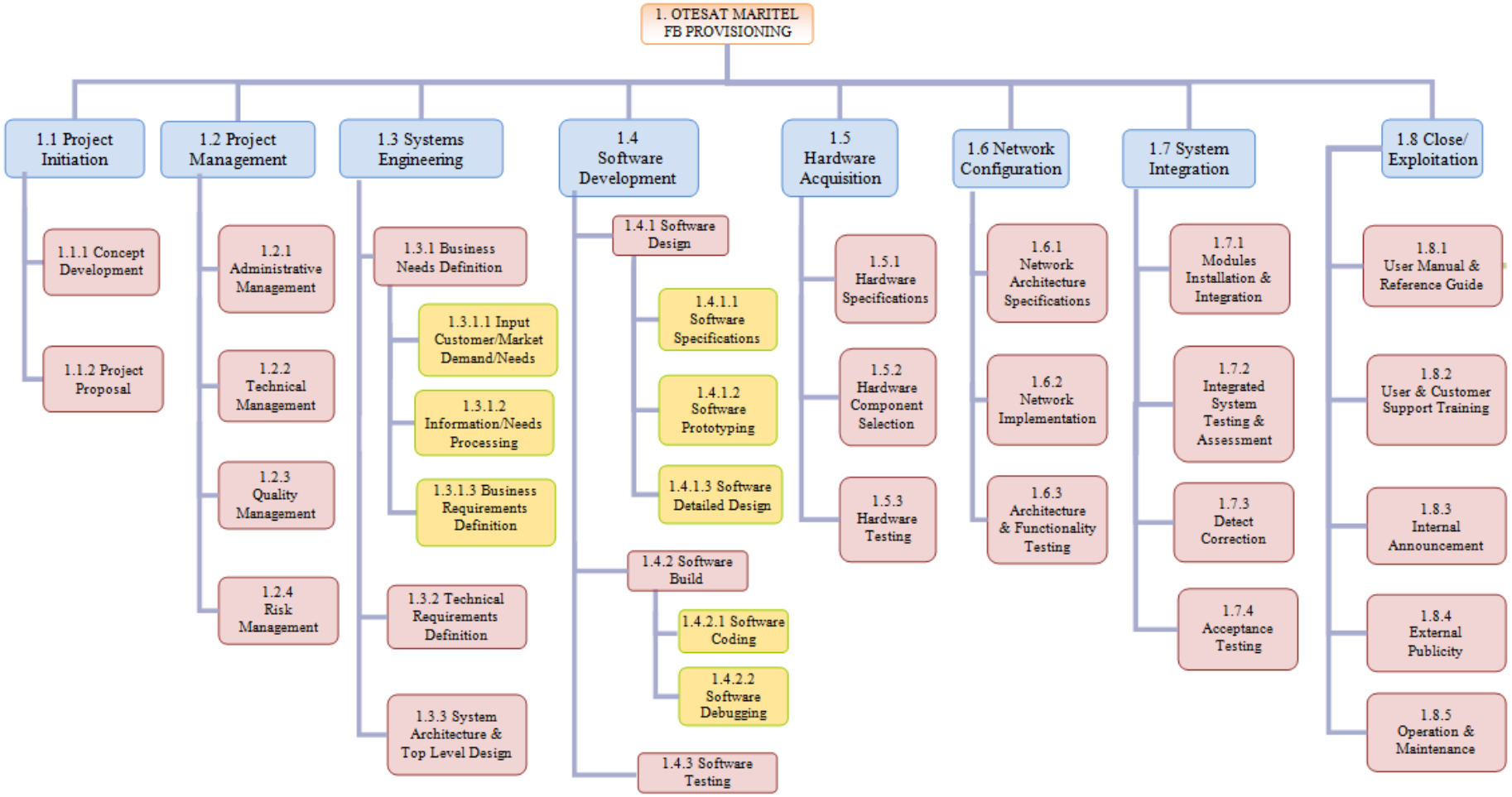
Τέλος με την φάση της ολοκλήρωσης του Έργου πραγματοποιούνται όλες οι δραστηριότητες και οι εργασίες που διασφαλίζουν την πλήρη αποπεράτωση του Έργου. Επίσης, περιλαμβάνει την αξιολόγηση των διαδικασιών που χρησιμοποιήθηκαν στο Έργο και των αποτελεσμάτων που επιτεύχθηκαν.

5.7 Ανάλυση και Περιγραφή WBS για το Provisioning Σύστημα

Στις προηγούμενες ενότητες δόθηκε η κατάλληλη πληροφορία για τον λόγο ύπαρξης και αναγκαιότητας του πληροφοριακού συστήματος και τις βασικές συνιστώσες που το απαρτίζουν ώστε να εξυπηρετείται η εταιρεία και οι πελάτες της. Έχοντας στη συνέχεια, αναπτύξει το γενικό μοντέλο διαίρεσης του συνολικού έργου σε φάσεις, είμαστε στη θέση στο στάδιο αυτό να παρουσιαστεί η λεγόμενη Αναλυτική Δομή Εργασιών ή αλλιώς Work Breakdown Structure του συγκεκριμένου έργου, του Πληροφοριακού Συστήματος Provisioning System της Otesat-Maritel για τις υπηρεσίες Ναυτιλιακών Δορυφορικών Επικοινωνιών FleetBroadband του δικτύου BGAN του Inmarsat (Broadband Global Area Network).

Η Αναλυτική Δομή Εργασιών (Work Breakdown Structure) είναι χρήσιμη διότι πρόκειται για μια διαδικασία με την οποία γίνεται μια προσπάθεια για μία προσανατολισμένη στα παραδοτέα ομαδοποίηση των συνιστωσών του Έργου, η οποία οργανώνει και ορίζει το συνολικό αντικείμενο του Έργου. Βασίζεται στην αρχή της υποδιαίρεσης των κύριων παραδοτέων ή υποπαραδοτέων του Έργου σε μικρότερες, καλύτερα διαχωρίσιμες συνιστώσες, μέχρις ότου τα παραδοτέα να προσδιορίζονται σε επαρκές επίπεδο ανάλυσης ώστε να υποστηρίζεται η ανάπτυξη των δραστηριοτήτων του Έργου (προγραμματισμός, εκτέλεση, έλεγχος και κλείσιμο). Η Αναλυτική Δομή Εργασιών Έργου περιλαμβάνει συνήθως τουλάχιστον τρία επίπεδα ανάλυσης και παρουσιάζεται συνήθως με τη μορφή διαγράμματος.

Παρακάτω λοιπόν παρατίθεται σε μορφή διαγράμματος η Δομή Ανάλυσης Εργασιών που δημιουργήθηκε για το συγκεκριμένο έργο που εξετάζεται. Όπως φαίνεται, από το εν λόγω διάγραμμα, αποτελείται από τέσσερα επίπεδα (4 levels) με χρωματική ομαδοποίηση των επιπέδων για καλύτερο οπτικό διαχωρισμό αυτών. Στο πρώτο επίπεδο (1) απεικονίζεται το συνολικό έργο (Otesat – Maritel FB Provisioning System) το οποίο απαρτίζεται από οκτώ (8) φάσεις που ανήκουν στο επίπεδο δύο (2), ενώ αυτές με την σειρά τους διασπώνται σε υποφάσεις και δραστηριότητες των επιπέδων τρία (3) και τέσσερα (4).



Εικόνα 23:Αναλυτική Δομή Εργασιών (Work Breakdown Structure) of FB Provisioning System

ΚΕΦΑΛΑΙΟ 6

6.1 Εφαρμογή Risk Management στο σύστημα Fleetbroadband Provisioning System

Στο κεφάλαιο αυτό θα αναλυθεί η διαδικασία διαχείρισης κινδύνων που αφορά τη λειτουργία του συστήματος Fleetbroadband Provisioning System.

Η διαδικασία διαχείρισης κινδύνων στο συγκεκριμένο σύστημα θα γίνει με βάση τα προβλήματα τα οποία ενδέχεται να προκύψουν κατά τη διάρκεια της λειτουργίας του. Στόχος είναι οι κίνδυνοι αυτοί να προσδιοριστούν, αναλυθούν, αξιολογηθούν και αντιμετωπιστούν τυχόν προβλήματα προβαίνοντας σε κάποιες κατάλληλες διορθωτικές ενέργειες.

6.2 Προσδιορισμός κινδύνων

Στη φάση αυτή πρέπει να εντοπιστούν οι πιθανοί κίνδυνοι χρησιμοποιώντας κάποια/ κάποιες από τις μεθόδους εντοπισμού (συνεντεύξεις, ομαδική παραγωγή ιδεών, ειδικές ομάδες, μέθοδος Delphi, ανάλυση SWOT, διαγραμματικές τεχνικές), να ταξινομηθούν στις διάφορες κατηγορίες και τέλος να φτιαχτεί το μητρώο κινδύνων, ένας συγκεντρωτικός πίνακας με τα παραπάνω στοιχεία.

Μερικοί από τους κινδύνους που μπορεί να προκύψουν είναι οι εξής:

- Ασυμβατότητα λογισμικού με τις απαιτήσεις
- Εξάντληση πόρων του συστήματος
- Λανθασμένη βάση δεδομένων αποθήκευσης των στοιχείων
- Ελλιπής ασφάλεια των προσωπικών δεδομένων των πελατών
- Δυσκολία σε αναβάθμιση – συντήρηση λογισμικού
- Έλλειψη διασυνδεσιμότητας των φορέων μέσω του συστήματος
- Λανθασμένος σχεδιασμός υλικού (αρχιτεκτονική συστήματος)
- Λανθασμένος σχεδιασμός λογισμικού (αρχιτεκτονική συστήματος)
- Ασυμβατότητα της τεχνολογίας του λογισμικού με τις υπάρχουσες κρατικές υποδομές ροής πληροφοριών (δικτυακή υποδομή)

- Χρήση νέων και μη δοκιμασμένων τεχνολογιών ανάπτυξης λογισμικού
- Μη αποδεκτή ποιότητα λογισμικού
- Ελλιπείς μηχανισμοί ελέγχου ασφάλειας του λογισμικού του πληροφοριακού συστήματος
- Αδυναμία Σύνδεσης με τον κεντρικό Η/Υ εξαιτίας υπερφόρτωσης των τηλεπικοινωνιακών δικτύων ή εξαιτίας της μειωμένης αξιοπιστίας του δικτύου

- Ανεπαρκής προστασία κρυπτογραφικών κλειδιών
- Ελλιπής επικύρωση της επεξεργασίας των δεδομένων
- Δυσλειτουργία του υλικού
- Ανεπαρκής έλεγχος του λογισμικού
- Σφάλματα λογισμικού
- Πολυπλοκότητα λογισμικού
- Μη ασφαλής αρχιτεκτονική δικτύου
- Προβλήματα επικοινωνίας με την εταιρεία ανάθεσης έργου

- Μη επαρκώς καθορισμένοι όροι του συμβολαίου μεταξύ του κράτους και του αναδόχου
- Μη διαθεσιμότητα ομάδας υποστήριξης του συστήματος
- Έλλειψη συνεργασίας μεταξύ των ομάδων κατασκευής του έργου.
- Ελλιπής φύλαξη του κτιρίου όπου στεγάζεται το πληροφοριακό σύστημα από εξειδικευμένα άτομα(φύλακες)
- Ελλιπής χρόνος προσαρμογής χρήσης του νέου πληροφοριακού συστήματος
- Ανεπαρκής ή λανθασμένος διαχωρισμός των καθηκόντων
- Ανεπαρκής επίβλεψη των εργαζομένων
- Έλλειψη διαδικασίας για την αφαίρεση των δικαιωμάτων πρόσβασης κατά την λήξη της απασχόλησης

- Ελλιπής σχεδιασμός τακτικών ελέγχων εύρυθμης λειτουργίας του λογισμικού
- Κίνδυνος εσφαλμένης εγκατάστασης υλικού ή λογισμικού από το προσωπικό της αναδόχου εταιρείας
- Ανεπαρκής κάλυψη του κτιρίου από σύστημα συναγερμού
- Ανεπαρκής κάλυψη του κτιρίου από σύστημα πυρανίχνευσης
- Ανεπαρκής κάλυψη του κτιρίου από σύστημα αναγνώρισης και ελέγχου ταυτότητας
- Έλλειψη οικονομικών πόρων
- Προβλήματα με την χρηματοδότηση του έργου
- Καταστροφή υλικού ή λογισμικού από τους χειριστές του συστήματος λόγω κακής χρήσης του
- Κλοπή υλικού από εργαζομένους
- Απεργίες εργαζομένων που διαχειρίζονται το πληροφοριακό σύστημα
- Κίνδυνος απροθυμίας προσαρμογής στην αλλαγή
- Καταστροφή εξοπλισμού από υγρά/τρόφιμα
- Διαρροή πληροφοριών
- Μη εξουσιοδοτημένη πρόσβαση στους χώρους του πληροφοριακού συστήματος
- Μη εξουσιοδοτημένη πρόσβαση στο πληροφοριακό σύστημα από τους εργαζόμενους
- Διαρροή κωδικών εισόδου και διαχείρισης του πληροφοριακού συστήματος
- Μη εξουσιοδοτημένες αλλαγές αρχείων
- Ακούσια αλλαγή των δεδομένων του πληροφοριακού συστήματος
- Έλλειψη κινήτρων για τους εργαζόμενους
- Έλλειψη ευαισθητοποίησης σε θέματα ασφάλειας
- Απώλεια συσκευών ταυτοποίησης προσώπου (ταυτότητες)
- Σύνδεση προσωπικών συσκευών στο εταιρικό δίκτυο

- Εγκατάσταση μη εξουσιοδοτημένου λογισμικού και εφαρμογών

- Ακούσια μεταφορά εμπιστευτικών δεδομένων του πληροφοριακού συστήματος εκτός γραφείου
- Λάθος κατανομή του κεφαλαίου
- Λανθασμένη κατανομή σημαντικότητας στις εφαρμογές του συστήματος
- Έλλειψη εφεδρικού σχεδίου απρόσκοπτης λειτουργίας του συστήματος
- Λανθασμένη πρόβλεψη απαιτούμενων πόρων υλικού
- Αλλαγή του χρονοδιαγράμματος λόγω λανθασμένου αρχικού προγραμματισμού
- Λανθασμένη κοστολόγηση του έργου
- Κοινή χρήση εμπιστευτικών δεδομένων με τους συνεργάτες και τους προμηθευτές
- Έλλειψη εμπειρίας και τεχνογνωσίας των προσώπων που είναι υπεύθυνα για την παρακολούθηση της υλοποίησης του έργου
- Λανθασμένες αποφάσεις διαχείρισης κινδύνων
- Κίνδυνος σεισμού
- Κίνδυνος κεραυνού
- Κίνδυνος πλημμύρας
- Κίνδυνος πυρκαγιάς
- Κίνδυνος διαρροής υδάτων
- Κίνδυνος αδυναμίας ηλεκτροδότησης του συστήματος λόγω ελλείψεων στην ηλεκτρολογική εγκατάσταση
- Κατολίσθηση – διάβρωση εδάφους
- Ηλιακές εκλάμψεις
- Σκόνη
- Βλάβη του συστήματος κλιματισμού
- Ηλεκτρομαγνητικές παρεμβολές
- Στατικός ηλεκτρισμός
- Έκρηξη ηφαιστείου

- Πυρηνικό ατύχημα
- Κίνδυνος εκρήξεων
- Έντομα/ τρωκτικά
- Κίνδυνος δονήσεων
- Καπνός / μικροσωματίδια
- Μαγνήτες/ μαγνητικά εργαλεία
- Αγωγές – Μηνύσεις

- Απώλεια καλής φήμης
- Κλοπή πνευματικής ιδιοκτησίας
- Αλλαγή σχεδιασμού συστήματος ή ματαίωση κατασκευής του λόγω πολιτικών αποφάσεων
- Κίνδυνος καταστροφής του πληροφοριακού συστήματος λόγω πολιτικής αστάθειας
- Κλοπή υλικού
- Βανδαλισμοί
- Εισβολείς (Hackers) – Υποκλοπή δεδομένων
- Εισβολείς (Hackers) – Καταστροφή δεδομένων
- Ηλεκτρονικοί Εγκληματίες(Μετάδοση κακόβουλου λογισμικού)
- Πρώην εργαζόμενοι που εργάζονται για ανταγωνιστές
- Κατασκοπεία
- Τρομοκρατικές επιθέσεις

Αφού προσδιοριστούν οι διάφοροι κίνδυνοι ταξινομούνται στις διάφορες κατηγορίες όπως φαίνεται στον παρακάτω Πίνακα 3.

Κατηγορίες κινδύνων	**Κίνδυνοι**
Τεχνολογικοί	• Ασυμβατότητα λογισμικού με τις απαιτήσεις • Εξάντληση πόρων του συστήματος • Λανθασμένη βάση δεδομένων αποθήκευσης των στοιχείων • Ελλιπής ασφάλεια των προσωπικών δεδομένων των πολιτών • Δυσκολία σε αναβάθμιση – συντήρηση λογισμικού • Έλλειψη διασυνδεσιμότητας του φορέων μέσω του συστήματος • Λανθασμένος σχεδιασμός υλικού (αρχιτεκτονική συστήματος) • Λανθασμένος σχεδιασμός λογισμικού (αρχιτεκτονική συστήματος) • Ασυμβατότητα της τεχνολογίας του λογισμικού με τις υπάρχουσες κρατικές υποδομές ροής πληροφοριών (δικτυακή υποδομή) • Χρήση νέων και μη δοκιμασμένων τεχνολογιών ανάπτυξης λογισμικού • Μη αποδεκτή ποιότητα λογισμικού • Ελλιπείς μηχανισμοί ελέγχου ασφάλειας του λογισμικού του πληροφοριακού συστήματος • Αδυναμία Σύνδεσης με τον κεντρικό Η/Υ εξαιτίας υπερφόρτωσης των τηλεπικοινωνιακών δικτύων ή εξαιτίας της μειωμένης αξιοπιστίας του δικτύου • Ανεπαρκής προστασία κρυπτογραφικών κλειδιών • Ελλιπής επικύρωση της επεξεργασίας των δεδομένων • Δυσλειτουργία του υλικού • Ανεπαρκής έλεγχος του λογισμικού • Σφάλματα λογισμικού • Πολυπλοκότητα λογισμικού • Μη ασφαλής αρχιτεκτονική δικτύου
Λειτουργικοί– Επιχειρησιακοί	• Προβλήματα επικοινωνίας με την εταιρεία ανάθεσης έργου • Μη επαρκώς καθορισμένοι όροι του συμβολαίου μεταξύ του κράτους και του αναδόχου • Μη διαθεσιμότητα ομάδας υποστήριξης του συστήματος Έλλειψη συνεργασίας μεταξύ των ομάδων κατασκευής του έργου. • Ελλιπής φύλαξη του κτιρίου όπου στεγάζεται το πληροφοριακό σύστημα από εξειδικευμένα άτομα(φύλακες) • Ελλιπής χρόνος προσαρμογής χρήσης του νέου πληροφοριακού συστήματος • Ανεπαρκής ή λανθασμένος διαχωρισμός των καθηκόντων • Ανεπαρκής επίβλεψη των εργαζομένων • Έλλειψη διαδικασίας για την αφαίρεση των δικαιωμάτων πρόσβασης κατά την λήξη της απασχόλησης • Ελλιπής σχεδιασμός τακτικών ελέγχων εύρυθμης λειτουργίας του λογισμικού • Κίνδυνος εσφαλμένης εγκατάστασης υλικού ή λογισμικού από το προσωπικό της αναδόχου εταιρείας λόγω έλλειψης τεχνικών γνώσεων ή εξαιτίας απλού ανθρώπινου σφάλματος του προσωπικού • Ανεπαρκής κάλυψη του κτιρίου από σύστημα συναγερμού

	• Ανεπαρκής κάλυψη του κτιρίου από σύστημα πυρανίχνευσης
Χρηματοοικονομικοί	• Έλλειψη οικονομικών πόρων • Προβλήματα με την χρηματοδότηση του έργου
Οργανωτικοί	• Λάθος κατανομή του κεφαλαίου • Λανθασμένη κατανομή σημαντικότητας στις εφαρμογές του συστήματος • Έλλειψη εφεδρικού σχεδίου απρόσκοπτης λειτουργίας του συστήματος • Λανθασμένη πρόβλεψη απαιτούμενων πόρων υλικού • Αλλαγή του χρονοδιαγράμματος λόγω λανθασμένου αρχικού προγραμματισμού • Λανθασμένη κοστολόγηση του έργου • Κοινή χρήση εμπιστευτικών δεδομένων με τους συνεργάτες και τους προμηθευτές • Έλλειψη εμπειρίας και τεχνογνωσίας των προσώπων που είναι υπεύθυνα για την παρακολούθηση της υλοποίησης του έργου • Λανθασμένες αποφάσεις διαχείρισης κινδύνων
Ανθρώπινοι	• Καταστροφή υλικού ή λογισμικού από τους χειριστές του συστήματος λόγω κακής χρήσης του • Κλοπή υλικού από εργαζομένους • Απεργίες εργαζομένων που διαχειρίζονται το πληροφοριακό σύστημα • Κίνδυνος απροθυμίας προσαρμογής στην αλλαγή • Καταστροφή εξοπλισμού από υγρά/τρόφιμα • Διαρροή πληροφοριών • Μη εξουσιοδοτημένη πρόσβαση στους χώρους του πληροφοριακού συστήματος • Μη εξουσιοδοτημένη πρόσβαση στο πληροφοριακό σύστημα από τους εργαζόμενους • Διαρροή κωδικών εισόδου και διαχείρισης του πληροφοριακού συστήματος • Μη εξουσιοδοτημένες αλλαγές αρχείων • Ακούσια αλλαγή των δεδομένων του πληροφοριακού συστήματος • Έλλειψη κινήτρων για τους εργαζόμενους • Έλλειψη ευαισθητοποίησης σε θέματα ασφάλειας • Σύνδεση προσωπικών συσκευών στο εταιρικό δίκτυο • Εγκατάσταση μη εξουσιοδοτημένου λογισμικού και εφαρμογών • Ακούσια μεταφορά εμπιστευτικών δεδομένων του πληροφοριακού συστήματος εκτός γραφείου • Έλλειψη απαιτούμενης εκπαίδευσης προσωπικού • Εσωτερικοί κίνδυνοι (δόλος)

	• Κίνδυνος σεισμού • Κίνδυνος Κεραυνού • Κίνδυνος πλημμύρας • Κίνδυνος πυρκαγιάς • Κίνδυνος διαρροής υδάτων Κίνδυνος αδυναμίας ηλεκτροδότησης του συστήματος λόγω ελλείψεων στην ηλεκτρολογική εγκατάσταση • Κατολίσθηση – διάβρωση εδάφους • Ηλιακές εκλάμψεις • Σκόνη • Βλάβη του συστήματος κλιματισμού • Ηλεκτρομαγνητικές παρεμβολές • Στατικός ηλεκτρισμός • Έκρηξη ηφαιστείου • Πυρηνικό ατύχημα • Κίνδυνος εκρήξεων • Έντομα/ τρωκτικά • Κίνδυνος δονήσεων • Καπνός / μικροσωματίδια • Μαγνήτες/ μαγνητικά εργαλεία
Νομικοί - Κοινωνικοί	• Αγωγές – Μηνύσεις • Απώλεια καλής φήμης • Κλοπή πνευματικής ιδιοκτησίας
Πολιτικοί	• Αλλαγή σχεδιασμού συστήματος ή ματαίωση κατασκευής του λόγω πολιτικών αποφάσεων • Κίνδυνος καταστροφής του πληροφοριακού συστήματος λόγω πολιτικής αστάθειας

Εξωτερικοί	• Κλοπή υλικού • Βανδαλισμοί • Εισβολείς (Hackers) – Υποκλοπή δεδομένων • Εισβολείς (Hackers) – Καταστροφή δεδομένων • Ηλεκτρονικοί Εγκληματίες(Μετάδοση κακόβουλου λογισμικού) • Πρώην εργαζόμενοι που εργάζονται για ανταγωνιστές • Κατασκοπεία • Τρομοκρατικές επιθέσεις

Πίνακας 3: Πίνακας κατηγοροποίησης κινδύνων του συστήματος Fleetbroadband Provisioning System

Με το πέρας των παραπάνω, δημιουργείται το Μητρώο Κινδύνων (Risk Register), δηλαδή ένα έγγραφο όπου καταγράφονται όλοι οι κίνδυνοι που εντοπίζονται κατά τη φάση του προσδιορισμού και το οποίο γίνεται λεπτομερέστερο όσο προχωρούν τα στάδια της ανάλυσης και της αντιμετώπισης αυτών. Το μητρώο κινδύνων παρακολουθείται και ενημερώνεται σε τακτική βάση με σκοπό να υπάρχουν οργανωμένα και συγκεντρωμένα οι πληροφορίες των κινδύνων, της ανάλυσης, του τρόπου αντιμετώπισης και της κατάστασής τους. Στο μητρώο αυτό στηρίζεται η εφαρμογή της διαδικασίας διαχείρισης κινδύνων. Στη φάση του ροσδιορισμού των κινδύνων, όπου το έγγραφο αυτό δημιουργείται, τα βασικά στοιχεία που πρέπει να αναγραφούν για τους κινδύνους φαίνονται στον παρακάτω πίνακα (Πίνακας 4).

Πιο αναλυτικά, στα παραπάνω πεδία συμπληρώνονται τα εξής στοιχεία:

- στο πεδίο «ονομασία» καταγράφεται η αντιπροσωπευτική ονομασία του κινδύνου που προσδιορίστηκε
- στο πεδίο «περιγραφή» καταγράφεται μία σύντομη περιγραφή του κινδύνου και της πιθανής συνέπειάς του
- στο πεδίο «κατηγορία» καταγράφεται η κατηγορία στην οποία ανήκει ο κίνδυνος
- στο πεδίο «ημερομηνία αναγνώρισης» καταγράφεται η ημερομηνία όπου πρωτοαναφέρθηκε ο κίνδυνος
- στο πεδίο «υπεύθυνος» καταγράφεται το όνομα του υπεύθυνου ή της υπεύθυνης ομάδας για τον κίνδυνο

#	Ονομασία	Περιγραφή	Κατηγορία	Ημερομηνία Αναγνώρισης	Υπεύθυνος
1	Ασυμβατότητα λογισμικού με τις απαιτήσεις	Το ήδη υπάρχον λογισμικό δεν ανταποκρίνεται στις απαιτήσεις του συστήματος	Τεχνολογικοί	17/02/2016	Δέλιος Ι.
2	Εξάντληση πόρων του συστήματος	Εξάντληση των πόρων του συστήματος από την αυξημένη κίνηση των χρηστών του	Τεχνολογικοί	17/02/2016	Δέλιος Ι.
3	Λανθασμένη βάση δεδομένων	Λάθος ή ελλιπής δημιουργία της βάσης δεδομένων	Τεχνολογικοί	17/02/2016	Δέλιος Ι.
4	Ελλιπής ασφάλειες των προσωπικών δεδομένων των πολιτών	Έλλειψη μεθόδων προστασίας των προσωπικών δεδομένων - έλλειψη πρωτοκόλλων ασφαλείας με αποτέλεσμα την πιθανή υποκλοπή των προσωπικών δεδομένων των χρηστών	Τεχνολογικοί	17/02/2016	Δέλιος Ι.
5	Δυσκολία σε αναβάθμιση-συντήρηση λογισμικού	Δημιουργία του κώδικα με μη δομημένο τρόπο με αποτέλεσμα την εμφάνιση δυσκολιών σε μελλοντικές αλλαγές και στην προσθήκη νέων λειτουργιών	Τεχνολογικοί	17/02/2016	Δέλιος Ι.
6	Έλλειψη διασυνδεσιμότητας των φορέων μέσω του συστήματος	Ελλιπής χρήση τεχνολογιών λογισμικού και πρωτοκόλλων για την διασυνδεσιμότητα μεταξύ των συσχετιζόμενων φορέων (π.χ. υπουργείο υγείας, ΓΓΚΑ, ΗΔΙΚΑ, Φ.Κ.Α)	Τεχνολογικοί	17/02/2016	Δέλιος Ι.
7	Λανθασμένος σχεδιασμός υλικού του συτήματος	Ανεπαρκής σχεδιασμός υλικού σε επίπεδο αρχιτεκτονικής συστήματος	Τεχνολογικοί	17/02/2016	Δέλιος Ι.
8	Λανθασμένος σχεδιασμός υλικού του συτήματος	Ανεπαρκής σχεδιασμός λογισμικού σε επίπεδο αρχιτεκτονικής συστήματος	Τεχνολογικοί	17/02/2016	Δέλιος Ι.
9	Ασυμβατότητα της τεχνολογίας του λογισμικού με τις υπάρχουσες κρατικές υποδομές ροής πληροφοριών	Επιλογή τεχνολογίας λογισμικού μη συμβατή με την υπάρχουσα δικτυακή υποδομή των συσχετιζόμενων φορέων	Τεχνολογικοί	17/02/2016	Δέλιος Ι.
10	Χρήση νέων και μη δοκιμασμένων τεχνολογιών ανάπτυξης λογισμικού	Επιλογή λογισμικού τελευταίας τεχνολογίας όπου δεν έχει ελεγχθεί εκτενώς όσον αφορά την ανάπτυξη αντίστοιχων εφαρμογών	Τεχνολογικοί	17/02/2016	Δέλιος Ι.
11	Μη αποδεκτή ποιότητα λογισμικού	Η ποιότητα της εφαρμογής είναι χαμηλότερη των αποδεκτών ορίων που έχουν τεθεί και προβληματική για τους χρήστες	Τεχνολογικοί	17/02/2016	Δέλιος Ι.
12	Ελλιπείς μηχανισμοί ελέγχου ασφάλειας του λογισμικού του πληροφοριακού συστήματος	Ελλιπής χρήσης λογισμικού ασφαλείας και αυστηρών μέτρων προστασίας για την αποφυγή κακόβουλων	Τεχνολογικοί	17/02/2016	Δέλιος Ι.

		ενεργειών και υποκλοπή προσωπικών δεδομένων			
13	Αδυναμία σύνδεσης με τον κεντρικό Η/Υ εξαιτίας υπερφόρτωσης των τηλεπικοινωνιακών δικτύων ή εξαιτίας της μειωμένης αξιοπιστείας του δικτύου	Ανεπαρκής διαδικτυακός εξοπλισμός για την αποτελεσματική εξυπηρέτηση του αριθμού των συνδεδεμένων χρηστών σε περιπτώσεις υψηλού φόρτου	Τεχνολογικοί	17/02/2016	Δέλιος Ι.
14	Ανεπαρκής προστασία κρυπτογραφικών κλειδιών	Λανθασμένη χρήση τεχνικών κρυπτογραφίας κλειδιών	Τεχνολογικοί	17/02/2016	Δέλιος Ι.
15	Ελλιπής επικύρωση της επεξεργασίας των δεδομένων	Λανθασμένος κώδικας για τον έλεγχό της επεξεργασίας των δεδομένων εισαγωγής	Τεχνολογικοί	17/02/2016	Δέλιος Ι.
16	Δυσλειτουργία του υλικού	Αστοχία του υλικού που είναι αποθηκευμένο το πληροφοριακό σύστημα	Τεχνολογικοί	17/02/2016	Δέλιος Ι.
17	Ανεπαρκήε έλεγχος λογισμικού	Ανεπαρκείς και ελλιπείς διαδικασίες ποιοτικού ελέγχου	Τεχνολογικοί	17/02/2016	Δέλιος Ι.
18	Σφάλματα λογισμικού	Εμφάνιση μεγάλου αριθμού λαθών στον κώδικα του πληροφοριακού συστήματος	Τεχνολογικοί	17/02/2016	Δέλιος Ι.
19	Πολυπλοκότητα λογισμικού	Μη τήρηση συγκεκριμένης μεθοδολογίας για τη συγγραφή κώδικα του πληροφοριακού συστήματος	Τεχνολογικοί	17/02/2016	Δέλιος Ι.
20	Μη ασφαλής αρχιτεκτονική δικτύου	Ανεπαρκής επιλογή επιπέδων ασφάλειας διαδικτύου	Τεχνολογικοί	17/02/2016	Δέλιος Ι.
21	Προβλήματα επικοινωνίας με την εταιρία ανάθεσης έργου	Αδυναμία αποτελεσματικής επικοινωνίας με την εταιρεία ανάθεσης με αποτέλεσμα την επιβράδυνση των εργασιών για την κατασκευή του έργου	Λειτουργικοί-Επιχειρησιακοί	17/02/2016	Δέλιος Ι.
22	Μη επαρκώς καθορισμένοι όροι του συμβολάιου μεταξύ του κράτους και του αναδόχου	Ασάφειες και κενά στους όρους του συμβολαίου οδηγούν στην ανεπαρκή εφαρμογή των συμφωνηθέντων στην περίπτωση εμφάνισης προβλήματος	Λειτουργικοί-Επιχειρησιακοί	17/02/2016	Δέλιος Ι.
23	Μη διαθεσιμότητα ομάδας υποστήριξης του συστήματος	Ανεπαρκής αριθμός ατόμων για την υποστήριξη του συστήματος λόγω κόστους σε ανθρώπινο δυναμικό	Λειτουργικοί-Επιχειρησιακοί	17/02/2016	Δέλιος Ι.
24	Έλλειψη συνεργασίας μεταξύ των ομάδων κατασκευής του έργου	Προβλήματα επικοινωνίας και καταμερισμού εργασιών των ομάδων ανάπτυξης λογισμικού με αποτέλεσμα τη δημιουργία εντάσεων μεταξύ των ατόμων και την διακοπή της ομαλής εξέλιξης του έργου	Λειτουργικοί-Επιχειρησιακοί	17/02/2016	Δέλιος Ι.
25	Ελλιπής φύλαξη του κτηρίου όπου στεγάζεται το πληροφοριακό σύστημα από εξειδικευμένα άτομα (φύλακες)	Η έλλειψη φύλαξης ενός κτηρίου από άτομο επιπλέον των τεχνικών μέσων μπορεί να έχει ως αποτέλεσμα την μη έγκαιρη αντιμετώπιση οποιασδήποτε πιθανή	Λειτουργικοί-Επιχειρησιακοί	17/02/2016	Δέλιος Ι.

		καταστροφής του κτηρίου όπου στεγάζεται το πληροφοριακό σύστημα			
26	Ελλιπής χρόνος προσαρμογής χρήσης του νέου πληροφοριακού συστήματος	Δεν έχει δοθεί αρκετό χρονικό διάστημα για την εξοικείωση των χρηστών (ιατροί, φαρμακοποιοί) με το νέο λογισμικό ώστε να υπάρχουν προβλήματα στη σύνταξη των συνταγών (χειρόγραφες, ηλεκτρονικές) με αποτέλεσμα την προβληματική εξυπηρέτηση των πολιτών	Λειτουργικοί-Επιχειρησιακοί	17/02/2016	Δέλιος Ι.
27	Ανεπαρκής ή λανθασμένος διαχωρισμός των καθηκόντων	Ελλιπής ή λανθασμένη επιλογή ατόμων για την υλοποίηση μερών του πληροφοριακού συστήματος	Λειτουργικοί-Επιχειρησιακοί	17/02/2016	Δέλιος Ι.
28	Ανεπαρκής επίβλεψη εργαζομένων	Ελλιπής επιλογή κατάλληλων ατόμων για επίβλεψη των εργαζομένων με αποτέλεσμα τη μη τήρηση του χρονοδιαγράμματος.	Λειτουργικοί-Επιχειρησιακοί	17/02/2016	Δέλιος Ι.
29	Ελλιπής διαδικασία για την αφαίρεση δικαιωμάτων πρόσβασης κατά τη λήξη της απασχόλησης	Η διαδικασία διακοπής συνεργασίας δεν πληροί όλες τις προϋποθέσεις που χρειάζονται για τη μη πρόσβαση των πρώην εργαζομένων στο πληροφοριακό σύστημα και στους χώρους του πληροφοριακού συστήματος	Λειτουργικοί-Επιχειρησιακοί	17/02/2016	Δέλιος Ι.
30	Ελλιπής σχεδιασμός τακτικών ελέγχων εύρυθμης λειτουργίας του λογισμικού	Ανεπαρκής διαδικασία τακτικού ελέγχου της λειτουργίας του λογισμικού	Λειτουργικοί-Επιχειρησιακοί	17/02/2016	Δέλιος Ι.
31	Κίνδυνος εσφαλμένης εγκατάστασης υλικού ή λογισμικού από το προσωπικό της αναδόχου εταιρίας	Εσφαλμένη εγκατάσταση υλικού ή λογισμικού λόγω έλλειψης τεχνικών γνώσεων ή εξαιτίας απλού ανθρώπινου σφάλματος του προσωπικού	Λειτουργικοί-Επιχειρησιακοί	17/02/2016	Δέλιος Ι.
32	Ανεπαρκής κάλυψη του κτηρίου από σύστημα συναγερμού	Μη εγκατεστημένο σύστημα ειδοποίησης σε περίπτωση εισβολής στο χώρο του πληροφοριακού συστήματος	Λειτουργικοί-Επιχειρησιακοί	17/02/2016	Δέλιος Ι.
33	Ανεπαρκής κάλυψη του κτηρίου από σύστημα πυρανίχνευσης	Μη εγκατεστημένο σύστημα ειδοποίησης σε περίπτωση πυρκαγιάς	Λειτουργικοί-Επιχειρησιακοί	17/02/2016	Δέλιος Ι.
34	Ανεπαρκής κάλυψη του κτηρίου από σύστημα αναγνώρισης και ελέγχου ταυτότητας	Μη εγκατεστημένο σύστημα αναγνώρισης και ελέγχου ταυτότητας για την είσοδο στους χώρους του πληροφοριακού συστήματος	Λειτουργικοί-Επιχειρησιακοί	17/02/2016	Δέλιος Ι.
35	Έλλειψη οικονομικών πόρων	Ανεπαρκείς οικονομικοί πόροι οδηγούν σε αδυναμία έναρξης ή ολοκλήρωσης του πληροφοριακού συστήματος	Χρηματο-οικονομικοί	17/02/2016	Δέλιος Ι.

36	Προβλήματα με τη χρηματοδότηση του έργου	Συνεχόμενες διακοπές κατά την υλοποίηση του έργου λόγω προβλημάτων στη χρηματοδότηση με αποτέλεσμα την χρονική καθυστέρηση και την αύξηση του κόστους	Χρηματο-οικονομικοί	17/02/2016	Δέλιος Ι.
37	Καταστροφή υλικού ή λογισμικού απο τους χειριστές του συτήματος	Καταστροφή υλικού ή λογισμικού του συστήματος λόγω κακής χρήσης του	Ανθρώπινοι	17/02/2016	Δέλιος Ι.
38	Κλοπή υλικού από τους εργαζομένους	Το υλικό ενδέχεται να κλαπεί από τους εργαζόμενους	Ανθρώπινοι	17/02/2016	Δέλιος Ι.
39	Απεργίες εργαζομένων που διαχειρίζονται το πληροφοριακό σύστημα	Καθυστέρηση στην υλοποίηση του έργου λόγω απεργιακών κινητοποιήσεων από τους εργαζόμενους	Ανθρώπινοι	17/02/2016	Δέλιος Ι.
40	Κίνδυνος απροθυμίας προσαρμογής στην αλλαγή	Απροθυμία των εργαζομένων του πληροφοριακού συστήματος να προσαρμοστούν στα νέα δεδομένα του εργασιακού τους περιβάλλοντος	Ανθρώπινοι	17/02/2016	Δέλιος Ι.
41	Καταστροφή εξοπλισμού από υγρά/τρόφιμα	Καταστροφή υλικού του πληροφοριακού συστήματος από επικίνδυνα υλικά που δεν επιτρέπονται κοντά στον εξοπλισμό (π.χ. τρόφιμα, υγρά)	Ανθρώπινοι	17/02/2016	Δέλιος Ι.
42	Διαρροή πληροφοριών	Διάδοση εμπιστευτικών πληροφοριών που αφορούν προσωπικά δεδομένα από εργαζόμενους σε μη εξουσιοδοτημένα άτομα	Ανθρώπινοι	17/02/2016	Δέλιος Ι.
43	Μη εξουσιοδοτημένη πρόσβαση στους χώρους του πληροφοριακού συστήματος	Ικανότητα μη εξουσιοδοτημένων ατόμων να έχουν πρόσβαση στους χώρους όπου βρίσκεται το πληροφοριακό σύστημα με αποτέλεσμα την πρόκληση φθοράς του εξοπλισμού	Ανθρώπινοι	17/02/2016	Δέλιος Ι.
44	Μη εξουσιοδοτημένη πρόσβαση στο πληρποφοριακό σύστημα από τους εργαζόμενους	Ικανότητα μη εξουσιοδοτημένων ατόμων να έχουν πρόσβαση στο πληροφοριακό σύστημα με αποτέλεσμα την πρόκληση καταστροφής του λογισμικού	Ανθρώπινοι	17/02/2016	Δέλιος Ι.
45	Διαρροή κωδικών εισόδου και διαχείρησης του πληροφοριακού συστήματος	Γνωστοποίηση των κωδικών εισόδου του πληροφοριακού συστήματος σε μη εξουσιοδοτημένα άτομα	Ανθρώπινοι	17/02/2016	Δέλιος Ι.
46	Μη εξουσιοδοτημένες αλλαγές αρχείων	Ελλιπή μηχανισμός κατανομής δικαιωμάτων διαχείρισης στους εργαζομένους του πληροφοριακού συστήματος με αποτέλεσμα τη δυνατότητα πρόσβαση όλων των εργαζομένων σε όλα τα μέρη του συστήματος	Ανθρώπινοι	17/02/2016	Δέλιος Ι.
47	Ακούσια αλλαγή των δεδομένων του	Μη εσκεμμένη αλλαγή των δεδομένων	Ανθρώπινοι	17/02/2016	Δέλιος Ι.

	πληροφοριακού συστήματος				
48	Έλλειψη κινήτρων για τους εργαζόμενους	Μη ύπαρξη διαδικασίας ανταμοιβής για τους εργαζόμενους	Ανθρώπινοι	17/02/2016	Δέλιος Ι.
49	Έλλειψη ευαισθητοποίησης σε θέματα ασφάλειας	Ελλιπής εκπαίδευση εργαζομένων σε θέματα ασφαλείας του πληροφοριακού συστήματος	Ανθρώπινοι	17/02/2016	Δέλιος Ι.
50	Σύνδεση προσοπικών συσκευών στο εταιρικό δίκτυο	Ο κάθε εργαζόμενος μπορεί να χρησιμοποιήσει δικές του συσκευές για να συνδεθεί στο δίκτυο της εταιρείας με αποτέλεσμα τη διάδοση κακόβουλου λογισμικού	Ανθρώπινοι	17/02/2016	Δέλιος Ι.
51	Εγκατάσταση μη εξουσιοδοτημένου λογισμικού και εφαρμογών	Εγκατάσταση επικίνδυνου για το πληροφοριακό σύστημα λογισμικού και εφαρμογών	Ανθρώπινοι	17/02/2016	Δέλιος Ι.
52	Ακούσια μεταφορά εμπιστευτικών δεδομένων του πληροφοριακού συστήματος εκτός γραφείου	Μη εσκεμμένη διάδοση προσωπικών δεδομένων μέσω συσκευών αποθήκευσης (π.χ. σκληρός δίσκος)	Ανθρώπινοι	17/02/2016	Δέλιος Ι.
53	Έλλειψη της απαιτούμενης εκπαίδευσης του προσωπικού	Μη επαρκής επιμόρφωση των εργαζομένων προκειμένου να ανταπεξέλθουν στις νέες απαιτήσεις	Ανθρώπινοι	17/02/2016	Δέλιος Ι.
54	Εσωτερικοί κίνδυνοι (δόλος)	Κίνδυνος δολιοφθορών του πληροφοριακού συστήματος από δυσαρεστημένα στελέχη ή υπαλλήλους που εργάζονται στον οργανισμό	Ανθρώπινοι	17/02/2016	Δέλιος Ι.
55	Λάθος κατανομή του κεφαλαίου	Λανθασμένη πρόβλεψη κοστολόγησης τμημάτων του πληροφοριακού συστήματος έτσι ώστε σε μερικά τμήματα του έργου να είναι αναγκαία η ανακοστολόγηση και αυτό να έχει ως αποτέλεσμα την καθυστέρηση του έργου	Στρατηγικοί-οργανωτικοί	17/02/2016	Δέλιος Ι.
56	Λανθασμένη κατανομή σημαντικότητας στις εφαρμογές του συστήματος	Λανθασμένη βαρύτητα κατά το σχεδιασμό των μερών του πληροφοριακού συστήματος μπορεί να οδηγήσει σε αναθεώρηση ορισμένων από αυτά και επανασχεδιασμού του έργου συνολικά	Στρατηγικοί-οργανωτικοί	17/02/2016	Δέλιος Ι.
57	Έλλειψη εφεδρικού σχεδίου απρόσκοπτης λειτουργίας του συστήματος	Έλλειψη εφεδρικού σχεδίου σε περίπτωση διακοπής ηλεκτροδότησης ή σε περίπτωση προβλημάτων λειτουργίας των διακομιστών που υποστηρίζουν το πληροφοριακό σύστημα	Στρατηγικοί-οργανωτικοί	17/02/2016	Δέλιος Ι.
58	Λανθασμένη πρόβλεψη απαιτούμενων πόρων υλικού	Έλλειψη υλικών πόρων (π.χ. διακομιστές, καλωδίωση κτιρίου κ.τ.λ.)χρήσιμων για την κατασκευή του έργου λόγω λανθασμένης αρχικής πρόβλεψης	Στρατηγικοί-οργανωτικοί	17/02/2016	Δέλιος Ι.

59	Αλλαγή του χρονοδιαγράμματος λόγω λανθασμένου αρχικού προγραμματισμού	Επιλογή ακολουθίας εργασιών διάφορη της βέλτιστης που έχει ως αποτέλεσμα την χρονική επιμήκυνση του έργου σε σχέση με τη βέλτιστη επιλογή	Στρατηγικοί-οργανωτικοί	17/02/2016	Δέλιος Ι.
60	Λανθασμένη κοστολόγηση του έργου	Το κόστος υλοποίησης του συστήματος αυξήθηκε, θέτοντας σε κίνδυνο την υπόσταση του έργου	Στρατηγικοί-οργανωτικοί	17/02/2016	Δέλιος Ι.
61	Κοινή χρήση εμπιστευτικών δεδομένων με τους συνεργάτες και τους προμηθευτές	Πρόσβαση σε εμπιστευτικά δεδομένα από συνεργάτες και προμηθευτές	Στρατηγικοί-οργανωτικοί	17/02/2016	Δέλιος Ι.
62	Έλλειψη εμπειρίας και τεχνογνωσίας των προσώπων που είναι υπεύθυνα για την παρακολούθηση της υλοποίησης του έργου	Παρακολούθηση της υλοποίησης του πληροφοριακού συστήματος από άτομα με καθόλου ή λίγη εμπειρία και με ελλιπής γνώσεις τεχνογνωσίας καθώς και ελλιπής γνώσεις τα οποία σε μελλοντικό χρόνο θα κληθούν να λάβουν σημαντικές αποφάσεις κάτω από πιθανές συνθήκες πίεσης ή έλλειψης χρόνου	Στρατηγικοί-οργανωτικοί	17/02/2016	Δέλιος Ι.
63	Λανθασμένες αποφάσεις διαχείρησης κινδύνων	Έλλειψη εμπειρίας των ατόμων που λαμβάνουν τις αποφάσεις διαχείρισης κινδύνων του έργου με αποτέλεσμα την ανεπαρκή αντιμετώπιση των κινδύνων	Στρατηγικοί-οργανωτικοί	17/02/2016	Δέλιος Ι.
64	Κίνδυνος σεισμού	Καταστροφή του κτιρίου που στεγάζεται το πληροφοριακό σύστημα λόγω σεισμού	Φυσικοί-Περιβαλλοντικοί	17/02/2016	Δέλιος Ι.
65	Κίνδυνος κεραυνού	Καταστροφή στην ηλεκτροδότηση του κτιρίου λόγω κεραυνού που προκλήθηκε από ακραία καιρικά φαινόμενα	Φυσικοί-Περιβαλλοντικοί	17/02/2016	Δέλιος Ι.
66	Κίνδυνος πλημμύρας	Καταστροφή του χώρου που στεγάζεται το σύστημα λόγω ακραίων καιρικών φαινομένων	Φυσικοί-Περιβαλλοντικοί	17/02/2016	Δέλιος Ι.
67	Κίνδυνος πυρκαγιάς	Κίνδυνος εκδήλωσης πυρκαγιάς στο χώρο της εγκατάστασης ή σε γειτονικά κτίρια από φυσικά αίτια ή τεχνητά	Φυσικοί-Περιβαλλοντικοί	17/02/2016	Δέλιος Ι.
68	Κίνδυνος διαρροής υδάτων	Καταστροφή του χώρου που στεγάζεται το σύστημα από πλημμύρα που οφείλεται σε διαρροή υδάτων λόγω παλαιότητας ή κακής κατασκευής του δικτύου υδροδότησης	Φυσικοί-Περιβαλλοντικοί	17/02/2016	Δέλιος Ι.
69	Κίνδυνος αδυναμίας ηλεκτροδότησης του συστήματος λόγω ελλείψεων στην ηλεκτρολογική εγκατάσταση	Αδυναμία ηλεκτροδότησης μέσω της εγκατάστασης του κτιρίου που στεγάζεται το σύστημα λόγω ελλιπούς υποστήριξης σε περιπτώσεις διακοπής της	Φυσικοί-Περιβαλλοντικοί	17/02/2016	Δέλιος Ι.

		ηλεκτροδότησης			
70	Κατολίσθηση – διάβρωση εδάφους	Καταστροφή κτιρίου που στεγάζεται το πληροφοριακό σύστημα λόγω κατολίσθησης ή διάβρωσης εδάφους	Φυσικοί-Περιβαλλοντικοί	17/02/2016	Δέλιος Ι.
71	Ηλιακές εκλάμψεις	Προβληματική λειτουργία του δικτύου λόγω ηλιακών εκλάμψεων	Φυσικοί-Περιβαλλοντικοί	17/02/2016	Δέλιος Ι.
72	Σκόνη	Βλάβες ή δυσλειτουργία υλικού λόγω σκόνης	Φυσικοί-Περιβαλλοντικοί	17/02/2016	Δέλιος Ι.
73	Βλάβη του συστήματος κλιματισμού	Καταστροφή από υπερθέρμανση του εξοπλισμού του πληροφοριακού συστήματος λόγω βλάβης του κλιματισμού	Φυσικοί-Περιβαλλοντικοί	17/02/2016	Δέλιος Ι.
74	Ηλεκτρομαγνητικές παρεμβολές	Προβληματική λειτουργία του δικτύου λόγω ηλεκτρομαγνητικών παρεμβολών	Φυσικοί-Περιβαλλοντικοί	17/02/2016	Δέλιος Ι.
75	Στατικός ηλεκτρισμός	Καταστροφή του εξοπλισμού του πληροφοριακού συστήματος λόγω διαρροής ρεύματος	Φυσικοί-Περιβαλλοντικοί	17/02/2016	Δέλιος Ι.
76	Έκρηξη ηφαιστείου	Εγκατάσταση του πληροφοριακού συστήματος ή του διακομιστή του πληροφοριακού συστήματος σε περιοχή που είναι επιρρεπής στις ηφαιστειακές εκρήξεις	Φυσικοί-Περιβαλλοντικοί	17/02/2016	Δέλιος Ι.
77	Πυρηνικό ατύχημα	Εγκατάσταση του πληροφοριακού συστήματος σε περιοχή όπου βρίσκονται πυρηνικά εργοστάσια	Φυσικοί-Περιβαλλοντικοί	17/02/2016	Δέλιος Ι.
78	Κίνδυνος εκρήξεων	Εγκατάσταση του πληροφοριακού συστήματος σε χώρο όπου βρίσκονται εύφλεκτα υλικά	Φυσικοί-Περιβαλλοντικοί	17/02/2016	Δέλιος Ι.
79	Έντομα –τρωκτικά	Εγκατάσταση του πληροφοριακού συστήματος σε κτίριο όπου δεν έχει την κατάλληλη υποδομή και την απαραίτητη προστασία με αποτέλεσμα να εισβάλλουν στο χώρο διάφορα έντομα και τρωκτικά και να προκαλέσουν ζημιά στο υλικό του συστήματος	Φυσικοί-Περιβαλλοντικοί	17/02/2016	Δέλιος Ι.
80	Κίνδυνος δονήσεων	Εγκατάσταση πληροφοριακού συστήματος σε περιοχή κοντά σε σιδηροδρομικό σταθμό ή σε εργοτάξιο	Φυσικοί-Περιβαλλοντικοί	17/02/2016	Δέλιος Ι.
81	Καπνός – Μικροσωματίδια	Εγκατάσταση πληροφοριακού συστήματος σε σημείο όπου υπάρχουν μεγάλες ποσότητες καπνού και μικροσωματιδίων οι οποίες μπορεί να προκαλέσουν ζημιά στον εξοπλισμό του συστήματος	Φυσικοί-Περιβαλλοντικοί	17/02/2016	Δέλιος Ι.

82	Μαγνήτες – μαγνητικά εργαλεία	Χρήση μαγνητών ή μαγνητικών εργαλείων μπορούν να προκαλέσουν βλάβη σε ευαίσθητο εξοπλισμό ή να διαγράψουν δεδομένα	Φυσικοί-Περιβαλλοντικοί	17/02/2016	Δέλιος Ι.
83	Αγωγές – Μηνύσεις	Παράβλεψη ή καταπάτηση νομοθετικών ρυθμίσεων ή υπάρχουσας νομοθεσίας όσον αφορά τις διαδικασίες μετάδοσης πληροφορίας και τήρησης αρχείων προσωπικών δεδομένων	Νομικοί-Κοινωνικοί	17/02/2016	Δέλιος Ι.
84	Απώλεια καλής φήμης	Μη αποτελεσματική λειτουργία του συστήματος λόγω λανθασμένου σχεδιασμού με αποτέλεσμα τη δυσαρέσκεια των τελικών χρηστών του συστήματος	Νομικοί-Κοινωνικοί	17/02/2016	Δέλιος Ι.
85	Κλοπή πνευματικής ιδιοκτησίας	Κλοπή μερών του λογισμικού του πληροφοριακού συστήματος από ανταγωνίστρια εταιρεία το οποίο υπόκειται σε καθεστώς πνευματικής ιδιοκτησίας	Νομικοί-Κοινωνικοί	17/02/2016	Δέλιος Ι.
86	Αλλαγή σχεδιασμού συστήματος ή ματαίωση κατασκευής του λόγω πολιτικών αποφάσεων	Αλλαγή πολιτικής ηγεσίας με αποτέλεσμα την αλλαγή ή ματαίωση κατασκευής του συστήματος και την ύπαρξη χρονικής καθυστέρησης ή κόστους	Πολιτικοί	17/02/2016	Δέλιος Ι.
87	Κίνδυνος καταστροφής του πληροφοριακού συστήματος λόγω πολιτικής αστάθειας	Εγκατάσταση του πληροφοριακού συστήματος σε περιοχή με πολιτικές αναταραχές / πολέμους	Πολιτικοί	17/02/2016	Δέλιος Ι.
88	Κλοπή υλικού	Εισβολή αγνώστων ατόμων στο κτίριο που στεγάζεται το πληροφοριακό σύστημα με αποτέλεσμα την κλοπή υλικού απαραίτητου για τη σωστή λειτουργία του	Εξωτερικοί	17/02/2016	Δέλιος Ι.
89	Βανδαλισμοί	Καταστροφή του εξοπλισμού από βανδαλισμούς αγνώστων ατόμων	Εξωτερικοί	17/02/2016	Δέλιος Ι.
90	Εισβολείς (Hackers) – Υποκλοπή δεδομένων	Προσβολή του συστήματος από την επιδρομή hackers με αποτέλεσμα την ύπαρξη κινδύνου υποκλοπής μεταδιδόμενων πληροφοριών	Εξωτερικοί	17/02/2016	Δέλιος Ι.
91	Εισβολείς (Hackers) – Καταστροφή δεδομένων	Προσβολή του συστήματος από την επιδρομή hackers με αποτέλεσμα την ύπαρξη κινδύνου καταστροφής δεδομένων	Εξωτερικοί	17/02/2016	Δέλιος Ι.
92	Ηλεκτρονικοί εγκληματίες (Μετάδοση κακόβουλου λογισμικού)	Προσβολή του συστήματος από ηλεκτρονικούς εγκληματίες με αποτέλεσμα την αλλοίωση ή καταστροφή των αποθηκευμένων δεδομένων του	Εξωτερικοί	17/02/2016	Δέλιος Ι.

		συστήματος			
93	Πρώην εργαζόμενοι που εργάζονται για ανταγωνιστές	Αντιγραφή μερών ή ολόκληρου του σχεδιασμού του πληροφοριακού συστήματος από πρών εργαζόμενους	Εξωτερικοί	17/02/2016	Δέλιος Ι.
94	Κατασκοπεία	Υποκλοπή ευαίσθητων προσωπικών δεδομένων του πληθυσμού από εχθρικά κράτη	Εξωτερικοί	17/02/2016	Δέλιος Ι.
95	Τρομοκρατικές ενέργειες	Καταστροφή των εγκαταστάσεων που στεγάζεται το πληροφοριακό σύστημα λόγω τρομοκρατικών επιθέσεων σε παραπλήσιο κτήριο ή και στο ίδιο κτήριο	Εξωτερικοί	17/02/2016	Δέλιος Ι.

Πίνακας 4 : Μητρώο κινδύνων - Προσδιορισμός κινδύνων συστήματος FleetBroadband Provisioning System

6.3 Ανάλυση κινδύνων

Στη φάση αυτή πρέπει να γίνει ποιοτική ανάλυση των κίνδυνων επομένως πρέπει να ομαδοποιηθούν οι κίνδυνοι με βάση τη σημαντικότητά τους και να αναπαρασταθούν σε έναν πίνακα κινδύνων.
Έστω ότι ο πίνακας κινδύνων της ποιοτικής ανάλυσης του συστήματος ορίζεται ως εξής:

Επίπεδο κινδύνου / Πιθανότητα	Πολύ χαμηλό (1)	Χαμηλό (2)	Μέτριο (3)	Υψηλό (4)	Πολύ υψηλό (5)
Πολύ χαμηλή (0.1)	0.10	0.20	0.30	0.40	0.50
Χαμηλή (0.3)	0.30	0.60	0.90	1.20	1.50
Μέση (0.5)	0.50	1.00	1.50	2.00	2.50
Υψηλή (0.7)	0.70	1.40	2.10	2.80	3.50
Πολύ Υψηλή (0.9)	0.90	1.80	2.70	3.60	4.50

Πίνακας 5: Risk matrix ποιοτικής ανάλυσης του συστήματος FleetBroadband Provisioning System

Y(2.50-4.50) : Υψηλός κίνδυνος, δηλαδή μη αποδεκτός ο οποίος χρειάζεται άμεση αντίδραση
M(0.90-2.10) : Μέσος κίνδυνος, δηλαδή μπορεί να χρειάζεται αντίδραση
X(0.10-0.70): Χαμηλός κίνδυνος, δηλαδή δε χρειάζεται αντίδραση αλλά απλή παρακολούθηση

Επίπεδο κινδύνου / Πιθανότητα	Πολύ χαμηλό (1)	Χαμηλό (2)	Μέτριο (3)	Υψηλό (4)	Πολύ υψηλό (5)
Πολύ χαμηλή (0.1)	X_7	X_6	X_5	X_4	X_3
Χαμηλή (0.3)	X_5	X_2	M_8	M_6	M_4
Μέση (0.5)	X_3	M_7	M_4	M_2	Y_6
Υψηλή (0.7)	X_1	M_5	M_1	Y_4	Y_3
Πολύ Υψηλή (0.9)	M_8	M_3	Y_5	Y_2	Y_1

Πίνακας 5.1: Risk matrix ποιοτικής ανάλυσης του συστήματος FleetBroadband Provisioning System

X1: 0.70 , X2:0.60 , X3:0.50, X4:0.40, X5:0.30, X6:0.20, X7:0.10
M1:2.10 , M2: 2.00, M3: 1.80, M4:1.50, M5:1.40, M6:1.20, M7:1.00, M8:0.90
Y1: 4.50, Y2: 360, Y3: 3.50 , Y4:2.80, Y5:2.70, Y6:2.50

Στον παραπάνω πίνακα 5.1 οι κίνδυνοι έχουν ομαδοποιηθεί σε υποκατηγορίες των υψηλών, μέσων και χαμηλών κινδύνων, ώστε να γίνεται περισσότερο αντιληπτός ο διαχωρισμός της επικινδυνότητας αυτών. Πιο συγκεκριμένα, ο κίνδυνος που ανήκει στην κατηγορία Υ1 είναι περισσότερο επικίνδυνος από τον κίνδυνο που ανήκει στην κατηγορία Υ2 και αυτός με τη σειρά του είναι περισσότερο επικίνδυνος από τον κίνδυνο που ανήκει στην κατηγορία Υ3 και ούτω καθεξής. Το ίδιο ισχύει και για τους μέσους και τους χαμηλούς κινδύνους. Έτσι ο βαθμός επικινδυνότητας των κινδύνων από τον πιο μεγάλο στον πιο μικρό, δηλαδή από τον πιο σοβαρό κίνδυνο στον πιο ακίνδυνο, ορίζεται ως εξής:

Υ1 →Υ2 →Υ3 →Υ4→Υ5→Υ6→Μ1 →Μ2 →Μ3 →Μ4→Μ5→Μ6→Μ7→Μ8→Χ1→Χ2 →Χ3→Χ4→Χ5→Χ6→Χ7

Στον παρακάτω πίνακα (Πίνακας 6) ορίζονται η πιθανότητα και το επίπεδο κινδύνου του κάθε κινδύνου που έχει προσδιοριστεί και με βάση τον πίνακα κινδύνων βρίσκεται η έκθεση του κάθε κινδύνου, ώστε να γίνει η ποιοτική ανάλυση.

Κίνδυνοι	Πιθανότητα	Επίπεδο	Έκθεση
Ασυμβατότητα λογισμικού με τις απαιτήσεις	0.5	5	Y_6
Εξάντληση πόρων του συστήματος	0.5	5	Y_6
Λανθασμένη βάση δεδομένων αποθήκευσης των στοιχείων	0.1	5	X_3
Ελλιπής ασφάλεια των προσωπικών δεδομένων των πολιτών	0.9	5	Y_1
Δυσκολία σε αναβάθμιση – συντήρηση λογισμικού	0.3	4	M_6
Έλλειψη διασυνδεσιμότητας του φορέων μέσω του συστήματος	0.5	3	M_4
Λανθασμένος σχεδιασμός υλικού του συστήματος	0.1	5	X_3
Λανθασμένος σχεδιασμός λογισμικού του συστήματος	0.1	5	X_3
Ασυμβατότητα της τεχνολογίας του λογισμικού με τις υπάρχουσες κρατικές υποδομές ροής πληροφοριών	0.3	5	M_4
Χρήση νέων και μη δοκιμασμένων τεχνολογιών ανάπτυξης λογισμικού	0.5	3	M_4
Μη αποδεκτή ποιότητα λογισμικού	0.5	3	X_3
Ελλιπείς μηχανισμοί ελέγχου ασφάλειας του πληροφοριακού συστήματος	0.1	5	M_2
Αδυναμία σύνδεσης με τον κεντρικό Η/Υ εξαιτίας υπερφόρτωσης των τηλεπικοινωνιακών δικτύων ή εξαιτίας της μειωμένης αξιοπιστίας του δικτύου	0.5	4	M_1
Ανεπαρκής προστασία κρυπτογραφικών κλειδιών	0.3	4	M_6
Ελλιπής επικύρωση της επεξεργασίας των δεδομένων	0.3	4	M_6
Δυσλειτουργία του υλικού	0.5	4	M_2
Ανεπαρκής έλεγχος λογισμικού	0.5	4	M_2
Σφάλματα λογισμικού	0.5	5	Y_6
Πολυπλοκότητα λογισμικού	0.5	3	M_4
Μη ασφαλής αρχιτεκτονική δικτύου	0.5	4	M_2
Προβλήματα επικοινωνίας με την εταιρεία ανάθεσης έργου	0.5	2	M_7
Μη επαρκώς καθορισμένοι όροι του συμβολαίου μεταξύ του κράτους και του αναδόχου	0.5	2	M_7
Μη διαθεσιμότητα ομάδας υποστήριξης του συστήματος	0.5	4	M_2
Έλλειψη συνεργασίας μεταξύ των ομάδων κατασκευής του έργου.	0.5	3	M_4
Ελλιπής φύλαξη του κτιρίου όπου στεγάζεται το πληροφοριακό σύστημα από εξειδικευμένα άτομα(φύλακες)	0.3	5	M_4
Ελλιπής χρόνος προσαρμογής χρήσης του νέου πληροφοριακού συστήματος	0.7	2	M_5
Ανεπαρκής ή λανθασμένος διαχωρισμός των καθηκόντων	0.7	3	M_1
Ανεπαρκής επίβλεψη εργαζομένων	0.5	4	M_2

Ελλιπής διαδικασία για την αφαίρεση δικαιωμάτων πρόσβασης κατά την λήξη της απασχόλησης	0.3	4	M_6
Ελλιπής σχεδιασμό τακτικών ελέγχων εύρυθμης λειτουργίας του λογισμικού	0.7	3	M_1
Κίνδυνος εσφαλμένης εγκατάστασης υλικού ή λογισμικού από το προσωπικό της αναδόχου εταιρείας	0.5	5	Y_6
Ανεπαρκής κάλυψη του κτιρίου από σύστημα συναγερμού	0.7	4	Y_4
Ανεπαρκής κάλυψη του κτιρίου από σύστημα πυρανίχνευσης	0.7	4	Y_4
Ανεπαρκής κάλυψη του κτιρίου από σύστημα αναγνώρισης και ελέγχου ταυτότητας	0.7	4	Y_4
Έλλειψη οικονομικών πόρων	0.5	3	M_4
Προβλήματα με την χρηματοδότηση του έργου	0.7	2	M_5
Καταστροφή υλικού ή λογισμικού από τους χειριστές του συστήματος	0.7	4	Y_4
Κλοπή υλικού από εργαζομένους	0.7	4	Y_4
Απεργίες εργαζομένων που διαχειρίζονται το πληροφοριακό σύστημα	0.5	4	M_2
Κίνδυνος απροθυμίας προσαρμογής στην αλλαγή	0.7	4	Y_4
Καταστροφή εξοπλισμού από υγρά/τρόφιμα	0.5	4	M_2
Διαρροή πληροφοριών	0.7	4	Y_4
Μη εξουσιοδοτημένη πρόσβαση στους χώρους του πληροφοριακού συστήματος	0.7	4	Y_4
Μη εξουσιοδοτημένη πρόσβαση στο πληροφοριακό σύστημα από τους εργαζόμενους	0.7	5	Y_3
Διαρροή κωδικών εισόδου και διαχείρισης του πληροφοριακού συστήματος	0.7	5	Y_3
Μη εξουσιοδοτημένες αλλαγές αρχείων	0.3	5	M_4
Ακούσια αλλαγή των δεδομένων του πληροφοριακού συστήματος	0.3	5	M_4
Έλλειψη κινήτρων για τους εργαζόμενους	0.5	4	M_2
Έλλειψη ευαισθητοποίησης σε θέματα ασφάλειας	0.7	4	Y_4
Σύνδεση προσωπικών συσκευών στο εταιρικό δίκτυο	0.7	4	Y_4
Εγκατάσταση μη εξουσιοδοτημένου λογισμικού και εφαρμογών	0.3	5	M_4
Ακούσια μεταφορά εμπιστευτικών δεδομένων του πληροφοριακού συστήματος εκτός γραφείου	0.5	4	M_2
Έλλειψη της απαιτούμενης εκπαίδευσης του προσωπικού	0.7	1	X_1
Εσωτερικοί κίνδυνοι (δόλος)	0.3	3	M_8
Λάθος κατανομή του κεφαλαίου	0.3	3	M_8
Λανθασμένη κατανομή σημαντικότητας στις εφαρμογές του συστήματος	0.3	4	M_6
Έλλειψη εφεδρικού σχεδίου απρόσκοπτης λειτουργίας του συστήματος	0.5	4	M_2
Λανθασμένη πρόβλεψη απαιτούμενων πόρων υλικού	0.5	3	M_4
Αλλαγή του χρονοδιαγράμματος λόγω λανθασμένου αρχικού προγραμματισμού	0.5	2	M_7

Λανθασμένη κοστολόγηση του έργου			
Κοινή χρήση εμπιστευτικών δεδομένων με τους συνεργάτες και τους προμηθευτές	0.3	3	M_8
Έλλειψη εμπειρίας και τεχνογνωσίας των προσώπων που είναι υπεύθυνα για την παρακολούθηση της υλοποίησης του έργου	0.3	4	M_6
Λανθασμένες αποφάσεις διαχείρισης κινδύνων	0.1	4	X_4
Κίνδυνος σεισμού	0.5	3	M_4
Κίνδυνος Κεραυνού	0.3	4	M_6
Κίνδυνος πλημμύρας	0.3	4	M_6
Κίνδυνος πυρκαγιάς	0.7	4	Y_4
Κίνδυνος διαρροής υδάτων	0.1	4	X_4
Κίνδυνος αδυναμίας ηλεκτροδότησης του συστήματος λόγω ελλείψεων στην ηλεκτρολογική εγκατάσταση	0.3	4	M_6
Κατολίσθηση – διάβρωση εδάφους	0.1	5	X_3
Ηλιακές εκλάμψεις	0.1	3	X_5
Σκόνη	0.5	2	M_7
Βλάβη του συστήματος κλιματισμού	0.3	4	M_6
Ηλεκτρομαγνητικές παρεμβολές	0.3	3	M_8
Στατικός ηλεκτρισμός	0.1	4	X_4
Έκρηξη ηφαιστείου	0.1	5	X_3
Πυρηνικό ατύχημα	0.1	5	X_3
Κίνδυνος εκρήξεων	0.3	5	M_4
Έντομα /τρωκτικά	0.5	4	M_2
Κίνδυνος δονήσεων	0.3	4	M_6
Καπνός / μικροσωματίδια	0.3	4	M_6
Μαγνήτες /μαγνητικά εργαλεία	0.5	5	Y_6
Αγωγές/ Μηνύσεις	0.1	2	X_6
Απώλεια καλής φήμης	0.1	3	X_5
Κλοπή πνευματικής ιδιοκτησίας	0.3	2	X_2
Αλλαγή σχεδιασμού συστήματος ή ματαίωση κατασκευής του λόγω πολιτικών αποφάσεων	0.1	3	X_5
Κίνδυνος καταστροφής του πληροφοριακού συστήματος λόγω πολιτικής αστάθειας	0.1	5	X_3
Κλοπή υλικού	0.3	4	M_6
Βανδαλισμοί	0.3	4	M_6

Εισβολείς (Hackers) – Υποκλοπή δεδομένων			
Εισβολείς (Hackers) – Καταστροφή δεδομένων	0.7	5	Y_3
Ηλεκτρονικοί Εγκληματίες(Μετάδοση κακόβουλου λογισμικού)	0.9	5	Y_1
Πρώην εργαζόμενοι που εργάζονται για ανταγωνιστές	0.5	3	M_4
Κατασκοπεία	0.3	4	M_6
Τρομοκρατικές ενέργειες	0.3	4	M_6

Πίνακας 6: Εκθέσεις κινδύνων συστήματος FleetBroadband Provisioning System

6.4 Αξιολόγηση κινδύνων

Στη φάση αυτή οι κίνδυνοι που έχουν προσδιοριστεί και αναλυθεί ταξινομούνται ανάλογα με την έκθεση κινδύνου που βρέθηκε προηγουμένως και ενημερώνεται το μητρώο κινδύνων.

Στον παρακάτω πίνακα φαίνεται η ταξινόμηση των κινδύνων σύμφωνα με την έκθεσή τους, με σειρά προτεραιότητας από τον σημαντικότερο στον πιο ασήμαντο.

Κίνδυνοι	Πιθανότητα	Επίπεδο	Έκθεση
Ελλιπής ασφάλεια των προσωπικών δεδομένων των πολιτών	0.9	5	Y_1
Ηλεκτρονικοί Εγκληματίες(Μετάδοση κακόβουλου λογισμικού)	0.9	5	Y_1
Μη εξουσιοδοτημένη πρόσβαση στο πληροφοριακό σύστημα από τους εργαζόμενους	0.7	5	Y_3
Διαρροή κωδικών εισόδου και διαχείρισης του πληροφοριακού συστήματος	0.7	5	Y_3
Εισβολείς (Hackers) – Υποκλοπή δεδομένων	0.7	5	Y_3
Εισβολείς (Hackers) – Καταστροφή δεδομένων	0.7	5	Y_3
Ανεπαρκής κάλυψη του κτιρίου από σύστημα συναγερμού	0.7	4	Y_4
Ανεπαρκής κάλυψη του κτιρίου από σύστημα πυρανίχνευσης	0.7	4	Y_4
Ανεπαρκής κάλυψη του κτιρίου από σύστημα αναγνώρισης και ελέγχου ταυτότητας	0.7	4	Y_4
Καταστροφή υλικού ή λογισμικού από τους χειριστές του συστήματος	0.7	4	Y_4
Κλοπή υλικού από εργαζομένους	0.7	4	Y_4
Κίνδυνος απροθυμίας προσαρμογής στην αλλαγή	0.7	4	Y_4
Διαρροή πληροφοριών	0.7	4	Y_4
Μη εξουσιοδοτημένη πρόσβαση στους χώρους του πληροφοριακού συστήματος	0.7	4	Y_4
Έλλειψη ευαισθητοποίησης σε θέματα ασφάλειας	0.7	4	Y_4
Σύνδεση προσωπικών συσκευών στο εταιρικό δίκτυο	0.7	4	Y_4
Κίνδυνος πυρκαγιάς	0.7	4	Y_4
Εξάντληση πόρων του συστήματος	0.5	5	Y_6
Σφάλματα λογισμικού	0.5	5	Y_6
Κίνδυνος εσφαλμένης εγκατάστασης υλικού ή λογισμικού από το προσωπικό της αναδόχου εταιρείας	0.5	5	Y_6
Μαγνήτες / μαγνητικά εργαλεία	0.5	5	Y_6
Ανεπαρκής ή λανθασμένος διαχωρισμός καθηκόντων	0.7	3	M_1
Ελλιπής σχεδιασμός τακτικών ελέγχων εύρυθμης λειτουργίας του λογισμικού	0.7	3	M_1
Αδυναμία Σύνδεσης με τον κεντρικό Η/Υ εξαιτίας υπερφόρτωσης των τηλεπικοινωνιακών δικτύων ή εξαιτίας της μειωμένης αξιοπιστίας του δικτύου	0.5	4	M_2
Δυσλειτουργία του υλικού	0.5	4	M_2
Ανεπαρκής έλεγχος του λογισμικού	0.5	4	M_2
Μη ασφαλής αρχιτεκτονική δικτύου	0.5	4	M_2
Μη διαθεσιμότητα ομάδας υποστήριξης του συστήματος	0.5	4	M_2
Ανεπαρκής επίβλεψη των εργαζομένων	0.5	4	M_2
Απεργίες εργαζομένων που διαχειρίζονται το πληροφοριακό σύστημα	0.5	4	M_2

Καταστροφή εξοπλισμού από υγρά/τρόφιμα			
Έλλειψη κινήτρων για τους εργαζόμενους	0.5	4	M_2
Ακούσια μεταφορά εμπιστευτικών δεδομένων του πληροφοριακού συστήματος εκτός γραφείου	0.5	4	M_2
Έλλειψη εφεδρικού σχεδίου απρόσκοπτης λειτουργίας του συστήματος	0.5	4	M_2
Έντομα / τρωκτικά	0.5	4	M_2
Έλλειψη διασυνδεσιμότητας των φορέων μέσω του συστήματος	0.5	3	M_4
Χρήση νέων και μη δοκιμασμένων τεχνολογιών ανάπτυξης λογισμικού	0.5	3	M_4
Μη αποδεκτή ποιότητα λογισμικού	0.5	3	M_4
Πολυπλοκότητα λογισμικού	0.5	3	M_4
Έλλειψη συνεργασίας μεταξύ των ομάδων κατασκευής του έργου	0.5	3	M_4
Έλλειψη οικονομικών πόρων	0.5	3	M_4
Λανθασμένη πρόβλεψη απαιτούμενων πόρων υλικού	0.5	3	M_4
Λανθασμένη κοστολόγηση του έργου	0.5	3	M_4
Κίνδυνος σεισμού	0.5	3	M_4
Πρώην εργαζόμενοι που εργάζονται για ανταγωνιστές	0.5	3	M_4
Ασυμβατότητα τις τεχνολογίας του λογισμικού με τις υπάρχουσες κρατικές υποδομές ροής πληροφοριών	0.3	5	M_4
Ελλιπής φύλαξη του κτιρίου όπου στεγάζεται το πληροφοριακό σύστημα από εξειδικευμένα άτομα (φύλακες)	0.3	5	M_4
Μη εξουσιοδοτημένες αλλαγές αρχείων	0.3	5	M_4
Ακούσια αλλαγή των δεδομένων του πληροφοριακού συστήματος	0.3	5	M_4
Εγκατάσταση μη εξουσιοδοτημένου λογισμικού και εφαρμογών	0.3	5	M_4
Κίνδυνος εκρήξεων	0.3	5	M_4
Ελλιπής χρόνος προσαρμογής χρήσης του νέου πληροφοριακού συστήματος	0.7	2	M_5
Προβλήματα με την χρηματοδότηση του έργου	0.7	2	M_5
Δυσκολία σε αναβάθμιση – συντήρηση λογισμικού	0.3	4	M_6
Ανεπαρκής προστασία κρυπτογραφικών κλειδιών	0.3	4	M_6
Ελλιπής επικύρωση της επεξεργασίας των δεδομένων	0.3	4	M_6
Ελλιπής διαδικασία για την αφαίρεση των δικαιωμάτων πρόσβασης κατά τη λήξη της απασχόλησης	0.3	4	M_6
Λανθασμένη κατανομή σημαντικότητας στις εφαρμογές του συστήματος	0.3	4	M_6
Έλλειψη εμπειρίας και τεχνογνωσίας των προσώπων που είναι υπεύθυνα για την παρακολούθηση της υλοποίησης του έργου.	0.3	4	M_6
Κίνδυνος Κεραυνού	0.3	4	M_6

Κίνδυνος πλημμύρας			
Κίνδυνος αδυναμίας ηλεκτροδότησης του συστήματος λόγω ελλείψεων στην ηλεκτρολογική εγκατάσταση	0.3	4	M_6
Βλάβη του συστήματος κλιματισμού	0.3	4	M_6
Κίνδυνος δονήσεων	0.3	4	M_6
Καπνός - Μικροσωματίδια	0.3	4	M_6
Κλοπή υλικού	0.3	4	M_6
Βανδαλισμοί	0.3	4	M_6
Κατασκοπεία	0.3	4	M_6
Τρομοκρατικές επιθέσεις	0.3	4	M_6
Προβλήματα επικοινωνίας με την εταιρεία ανάθεσης έργου	0.5	2	M_7
Μη επαρκώς καθορισμένοι όροι του συμβολαίου μεταξύ του κράτους και του αναδόχου	0.5	2	M_7
Αλλαγή του χρονοδιαγράμματος λόγω λανθασμένου αρχικού προγραμματισμού	0.5	2	M_7
Σκόνη	0.5	2	M_7
Εσωτερικοί κίνδυνοι (δόλος)	0.3	3	M_8
Λάθος κατανομή του κεφαλαίου	0.3	3	M_8
Κοινή χρήση εμπιστευτικών δεδομένων με τους συνεργάτες και τους προμηθευτές	0.3	3	M_8
Ηλεκτρομαγνητικές παρεμβολές	0.3	3	M_8
Έλλειψη της απαιτούμενης εκπαίδευσης του προσωπικού	0.7	1	X_1
Κλοπή πνευματικής ιδιοκτησίας	0.3	2	X_2
Ασυμβατότητα λογισμικού με τις απαιτήσεις	0.1	5	X_3
Λανθασμένη βάση δεδομένων αποθήκευσης των στοιχείων	0.1	5	X_3
Λανθασμένος σχεδιασμός υλικού (αρχιτεκτονική συστήματος)	0.1	5	X_3
Λανθασμένος σχεδιασμός λογισμικού(αρχιτεκτονική συστήματος)	0.1	5	X_3
Ελλιπείς μηχανισμοί ελέγχου ασφάλειας του λογισμικού του πληροφοριακού συστήματος	0.1	5	X_3
Κατολίσθηση – διάβρωση εδάφους	0.1	5	X_3
Έκρηξη ηφαιστείου	0.1	5	X_3
Πυρηνικό ατύχημα	0.1	5	X_3
Κίνδυνος καταστροφής του πληροφοριακού συστήματος λόγω πολιτικής αστάθειας	0.1	5	X_3
Λανθασμένες αποφάσεις διαχείρισης κινδύνων	0.1	4	X_4
Κίνδυνος διαρροής υδάτων	0.1	4	X_4
Στατικός ηλεκτρισμός	0.1	4	X_4
Ηλιακές εκλάμψεις	0.1	3	X_5

Απώλεια καλής φήμης			
Αλλαγή σχεδιασμού συστήματος ή ματαίωση κατασκευής του λόγω πολιτικών αποφάσεων	0.1	3	X_5
Αγωγές – Μηνύσεις	0.1	2	X_6

Πίνακας 7: Σειρά κατάταξης κινδύνων συστήματος Fleetbroadband Provisioning System

Στη συνέχεια ενημερώνεται το μητρώο κινδύνων

	Ονομασία	Πιθανότητα	Επίπεδο	Έκθεση	Προτεραιότητα	Ημ. Ενημέρωσης
1	Ασυμβατότητα λογισμικού με τις απαιτήσεις	0.5	5	Y_6	80	20/02/2016
2	Εξάντληση πόρων του συστήματος	0.5	5	Y_6	18	20/02/2016
3	Λανθασμένη βάση δεδομένων αποθήκευσης των στοιχείων	0.1	5	X_3	81	20/02/2016
4	Ελλιπής ασφάλεια των προσωπικών δεδομένων των πολιτών	0.9	5	Y_1	1	20/02/2016
5	Δυσκολία σε αναβάθμιση – συντήρηση λογισμικού	0.3	4	M_6	54	20/02/2016
6	Έλλειψη διασυνδεσιμότητας του φορέων μέσω του συστήματος	0.5	3	M_4	36	20/02/2016
7	Λανθασμένος σχεδιασμός υλικού του συστήματος	0.1	5	X_3	82	20/02/2016
8	Λανθασμένος σχεδιασμός λογισμικού του συστήματος	0.1	5	X_3	83	20/02/2016
9	Ασυμβατότητα της τεχνολογίας του λογισμικού με τις υπάρχουσες κρατικές υποδομές ροής πληροφοριών	0.3	5	M_4	46	20/02/2016
10	Χρήση νέων και μη δοκιμασμένων τεχνολογιών ανάπτυξης λογισμικού	0.5	3	M_4	37	20/02/2016
11	Μη αποδεκτή ποιότητα λογισμικού	0.5	3	M_4	38	20/02/2016
12	Ελλιπείς μηχανισμοί ελέγχου ασφάλειας του πληροφοριακού συστήματος	0.1	5	X_3	84	20/02/2016
13	Αδυναμία σύνδεσης με τον κεντρικό Η/Υ εξαιτίας υπερφόρτωσης των τηλεπικοινωνιακών δικτύων ή εξαιτίας της μειωμένης αξιοπιστίας του δικτύου	0.5	4	M_2	24	20/02/2016
14	Ανεπαρκής προστασία κρυπτογραφικών κλειδιών	0.3	4	M_6	55	20/02/2016
15	Ελλιπής επικύρωση της επεξεργασίας των δεδομένων	0.3	4	M_6	56	20/02/2016
16	Δυσλειτουργία του υλικού	0.5	4	M_2	25	20/02/2016
17	Ανεπαρκής έλεγχος λογισμικού	0.5	4	M_2	26	20/02/2016
18	Σφάλματα λογισμικού	0.5	5	Y_6	19	20/02/2016
19	Πολυπλοκότητα λογισμικού	0.5	3	M_4	39	20/02/2016
20	Μη ασφαλής αρχιτεκτονική δικτύου	0.5	4	M_2	27	20/02/2016
21	Προβλήματα επικοινωνίας με την εταιρεία ανάθεσης έργου	0.5	2	M_7	70	20/02/2016
22	Μη επαρκώς καθορισμένοι όροι του συμβολαίου μεταξύ του κράτους και του αναδόχου	0.5	2	M_7	71	20/02/2016
23	Μη διαθεσιμότητα ομάδας υποστήριξης του συστήματος	0.5	4	M_2	28	20/02/2016
24	Έλλειψη συνεργασίας μεταξύ των ομάδων κατασκευής του έργου.	0.5	3	M_4	40	20/02/2016
25	Ελλιπής φύλαξη του κτιρίου όπου στεγάζεται το πληροφοριακό σύστημα από εξειδικευμένα άτομα(φύλακες)	0.3	5	M_4	47	20/02/2016
26	Ελλιπής χρόνος προσαρμογής χρήσης του νέου πληροφοριακού συστήματος	0.7	2	M_5	52	20/02/2016
27	Ανεπαρκής ή λανθασμένος διαχωρισμός των καθηκόντων	0.7	3	M_1	22	20/02/2016

28	Ανεπαρκής επίβλεψη εργαζομένων	0.5	4	M_2	29	20/02/2016
29	Ελλιπής διαδικασία για την αφαίρεση δικαιωμάτων πρόσβασης κατά την λήξη της απασχόλησης	0.3	4	M_6	57	20/02/2016
30	Ελλιπής σχεδιασμό τακτικών ελέγχων εύρυθμης λειτουργίας του λογισμικού	0.7	3	M_1	23	20/02/2016
31	Κίνδυνος εσφαλμένης εγκατάστασης υλικού ή λογισμικού από το προσωπικό της αναδόχου εταιρείας	0.5	5	Y_6	20	20/02/2016
32	Ανεπαρκής κάλυψη του κτιρίου από σύστημα συναγερμού	0.7	4	Y_4	7	20/02/2016
33	Ανεπαρκής κάλυψη του κτιρίου από σύστημα πυρανίχνευσης	0.7	4	Y_4	8	20/02/2016
34	Ανεπαρκής κάλυψη του κτιρίου από σύστημα αναγνώρισης και ελέγχου ταυτότητας	0.7	4	Y_4	9	20/02/2016
35	Έλλειψη οικονομικών πόρων	0.5	3	M_4	41	20/02/2016
36	Προβλήματα με την χρηματοδότηση του έργου	0.7	2	M_5	53	20/02/2016
37	Καταστροφή υλικού ή λογισμικού από τους χειριστές του συστήματος	0.7	4	Y_4	10	20/02/2016
38	Κλοπή υλικού από εργαζομένους	0.7	4	Y_4	11	20/02/2016
39	Απεργίες εργαζομένων που διαχειρίζονται το πληροφοριακό σύστημα	0.5	4	M_2	30	20/02/2016
40	Κίνδυνος απροθυμίας προσαρμογής στην αλλαγή	0.7	4	Y_4	12	20/02/2016
41	Καταστροφή εξοπλισμού από υγρά/τρόφιμα	0.5	4	M_2	31	20/02/2016
42	Διαρροή πληροφοριών	0.7	4	Y_4	13	20/02/2016
43	Μη εξουσιοδοτημένη πρόσβαση στους χώρους του πληροφοριακού συστήματος	0.7	4	Y_4	14	20/02/2016
44	Μη εξουσιοδοτημένη πρόσβαση στο πληροφοριακό σύστημα από τους εργαζόμενους	0.7	5	Y_3	3	20/02/2016
45	Διαρροή κωδικών εισόδου και διαχείρισης του πληροφοριακού συστήματος	0.7	5	Y_3	4	20/02/2016
46	Μη εξουσιοδοτημένες αλλαγές αρχείων	0.3	5	M_4	48	20/02/2016
47	Ακούσια αλλαγή των δεδομένων του πληροφοριακού συστήματος	0.3	5	M_4	49	20/02/2016
48	Έλλειψη κινήτρων για τους εργαζόμενους	0.5	4	M_2	32	20/02/2016
49	Έλλειψη ευαισθητοποίησης σε θέματα ασφάλειας	0.7	4	Y_4	15	20/02/2016
50	Σύνδεση προσωπικών συσκευών στο εταιρικό δίκτυο	0.7	4	Y_4	16	20/02/2016
51	Εγκατάσταση μη εξουσιοδοτημένου λογισμικού και εφαρμογών	0.3	5	M_4	50	20/02/2016
52	Ακούσια μεταφορά εμπιστευτικών δεδομένων του πληροφοριακού συστήματος εκτός γραφείου	0.5	4	M_2	33	20/02/2016
53	Έλλειψη της απαιτούμενης εκπαίδευσης του προσωπικού	0.7	1	X_1	78	20/02/2016

54	Εσωτερικοί κίνδυνοι (δόλος)	0.3	3	M_8	74	20/02/2016
55	Λάθος κατανομή του κεφαλαίου	0.3	3	M_8	75	20/02/2016
56	Λανθασμένη κατανομή σημαντικότητας στις εφαρμογές του συστήματος	0.3	4	M_6	58	20/02/2016
57	Έλλειψη εφεδρικού σχεδίου απρόσκοπτης λειτουργίας του συστήματος	0.5	4	M_2	34	20/02/2016
58	Λανθασμένη πρόβλεψη απαιτούμενων πόρων υλικού	0.5	3	M_4	42	20/02/2016
59	Αλλαγή του χρονοδιαγράμματος λόγω λανθασμένου αρχικού προγραμματισμού	0.5	2	M_7	72	20/02/2016
60	Λανθασμένη κοστολόγηση του έργου	0.5	3	M_4	43	20/02/2016
61	Κοινή χρήση εμπιστευτικών δεδομένων με τους συνεργάτες και τους προμηθευτές	0.3	3	M_8	76	20/02/2016
62	Έλλειψη εμπειρίας και τεχνογνωσίας των προσώπων που είναι υπεύθυνα για την παρακολούθηση της υλοποίησης του έργου	0.3	4	M_6	59	20/02/2016
63	Λανθασμένες αποφάσεις διαχείρησης κινδύνων	0.1	4	X_4	89	20/02/2016
64	Κίνδυνος σεισμού	0.5	3	M_4	44	20/02/2016
65	Κίνδυνος κεραυνού	0.3	4	M_6	60	20/02/2016
66	Κίνδυνος πλημμύρας	0.3	4	M_6	61	20/02/2016
67	Κίνδυνος πυρκαγιάς	0.7	4	Y_4	17	20/02/2016
68	Κίνδυνος διαρροής υδάτων	0.1	4	X_4	90	20/02/2016
69	Κίνδυνος αδυναμίας ηλεκτροδότησης του συστήματος λόγω ελλείψεων στην ηλεκτρολογική εγκατάσταση	0.3	4	M_6	62	20/02/2016
70	Κατολίσθηση – διάβρωση εδάφους	0.1	5	X_3	85	20/02/2016
71	Ηλιακές εκλάμψεις	0.1	3	X_5	92	20/02/2016
72	Σκόνη	0.5	2	M_7	73	20/02/2016
73	Βλάβη του συστήματος κλιματισμού	0.3	4	M_6	63	20/02/2016
74	Ηλεκτρομαγνητικές παρεμβολές	0.3	3	M_8	77	20/02/2016
75	Στατικός ηλεκτρισμός	0.1	4	X_4	91	20/02/2016
76	Έκρηξη ηφαιστείου	0.1	5	X_3	86	20/02/2016
77	Πυρηνικό ατύχημα	0.1	5	X_3	87	20/02/2016
78	Κίνδυνος εκρήξεων	0.3	5	M_4	51	20/02/2016
79	Έντομα –τρωκτικά	0.5	4	M_2	35	20/02/2016
80	Κίνδυνος δονήσεων	0.3	4	M_6	64	20/02/2016
81	Καπνός – Μικροσωματίδια	0.3	4	M_6	65	20/02/2016
82	Μαγνήτες – μαγνητικά εργαλεία	0.5	5	Y_6	21	20/02/2016

83	Αγωγές – Μηνύσεις	0.1	2	X_6	95	20/02/2016
84	Απώλεια καλής φήμης	0.1	3	X_5	93	20/02/2016
85	Κλοπή πνευματικής ιδιοκτησίας	0.3	2	X_2	79	20/02/2016
86	Αλλαγή σχεδιασμού συστήματος ή ματαίωση κατασκευής του λόγω πολιτικών αποφάσεων	0.1	3	X_5	94	20/02/2016
87	Κίνδυνος καταστροφής του πληροφοριακού συστήματος λόγω πολιτικής αστάθειας	0.1	5	X_3	88	20/02/2016
88	Κλοπή υλικού	0.3	4	M_6	66	20/02/2016
89	Βανδαλισμοί	0.3	4	M_6	67	20/02/2016
90	Εισβολείς (Hackers) – Υποκλοπή δεδομένων	0.7	5	Y_3	5	20/02/2016
91	Εισβολείς (Hackers) – Καταστροφή δεδομένων	0.7	5	Y_3	6	20/02/2016
92	Ηλεκτρονικοί εγκληματίες (Μετάδοση κακόβουλου λογισμικού)	0.9	5	Y_1	2	20/02/2016
93	Πρώην εργαζόμενοι που εργάζονται για ανταγωνιστές	0.5	3	M_4	45	20/02/2016
94	Κατασκοπεία	0.3	4	M_6	68	20/02/2016
95	Τρομοκρατικές ενέργειες	0.3	4	M_6	69	20/02/2016

Πίνακας 8: Μητρώο κινδύνων–Ανάλυση/Αξιολόγηση κινδύνων συστήματος Fleetbroadband Provisioning System

6.5 Σχέδια αντιμετώπισης κινδύνων

Στη φάση αυτή η ομάδα που ασχολείται με τη διαδικασία διαχείρισης των κινδύνων, έχει το μητρώο κινδύνων με τους κινδύνους που έχουν προσδιοριστεί, ιεραρχημένους ανάλογα με τη σοβαρότητά τους από την ανάλυση και την αξιολόγηση που έχει γίνει. Στη συνέχεια πρέπει να βρει την κατάλληλη μέθοδο αντιμετώπισης του κάθε κινδύνου. Οι μέθοδοι αντιμετώπισης των απειλών είναι η αποφυγή (avoidance), η μεταφορά (transfer), ο μετριασμός (mitigation) και η αποδοχή (acceptance). Στον παρακάτω πίνακα θα αναφερθούν οι κίνδυνοι και η μέθοδος αντιμετώπισης του καθενός.

Κίνδυνος	Μέθοδος Αντιμετώπισης
Ασυμβατότητα λογισμικού με τις απαιτήσεις	Μεταφορά
Εξάντληση πόρων του συστήματος	Αποφυγή
Λανθασμένη βάση δεδομένων αποθήκευσης των στοιχείων	Μεταφορά
Ελλιπής ασφάλεια των προσωπικών δεδομένων των πολιτών	Μεταφορά
Δυσκολία σε αναβάθμιση – συντήρηση λογισμικού	Μεταφορά
Έλλειψη διασυνδεσιμότητας του φορέων μέσω του συστήματος	Μεταφορά
Λανθασμένος σχεδιασμός υλικού του συστήματος	Μεταφορά
Λανθασμένος σχεδιασμός λογισμικού του συστήματος	Μεταφορά
Ασυμβατότητα της τεχνολογίας του λογισμικού με τις υπάρχουσες κρατικές υποδομές ροής πληροφοριών	Μεταφορά
Χρήση νέων και μη δοκιμασμένων τεχνολογιών ανάπτυξης λογισμικού	Μεταφορά
Μη αποδεκτή ποιότητα λογισμικού	Μεταφορά
Ελλιπείς μηχανισμοί ελέγχου ασφάλειας του πληροφοριακού συστήματος	Μεταφορά
Αδυναμία σύνδεσης με τον κεντρικό Η/Υ εξαιτίας υπερφόρτωσης των τηλεπικοινωνιακών δικτύων ή εξαιτίας της μειωμένης αξιοπιστίας του δικτύου	Αποφυγή
Ανεπαρκής προστασία κρυπτογραφικών κλειδιών	Μεταφορά
Ελλιπής επικύρωση της επεξεργασίας των δεδομένων	Μεταφορά
Δυσλειτουργία του υλικού	Αποδοχή
Ανεπαρκής έλεγχος λογισμικού	Μεταφορά
Σφάλματα λογισμικού	Μεταφορά
Πολυπλοκότητα λογισμικού	Μεταφορά
Μη ασφαλής αρχιτεκτονική δικτύου	Μεταφορά
Προβλήματα επικοινωνίας με την εταιρεία ανάθεσης έργου	Μετριασμός
Μη επαρκώς καθορισμένοι όροι του συμβολαίου μεταξύ του κράτους και του αναδόχου	Αποφυγή
Μη διαθεσιμότητα ομάδας υποστήριξης του συστήματος	Μεταφορά
Έλλειψη συνεργασίας μεταξύ των ομάδων κατασκευής του έργου.	Μετριασμός
Ελλιπής φύλαξη του κτιρίου όπου στεγάζεται το πληροφοριακό σύστημα από εξειδικευμένα άτομα(φύλακες)	Μετριασμός
Ελλιπής χρόνος προσαρμογής χρήσης του νέου πληροφοριακού συστήματος	Αποδοχή
Ανεπαρκής ή λανθασμένος διαχωρισμός των καθηκόντων	Μεταφορά
Ανεπαρκής επίβλεψη εργαζομένων	Μεταφορά
Ελλιπής διαδικασία για την αφαίρεση δικαιωμάτων πρόσβασης κατά την λήξη της απασχόλησης	Αποφυγή
Ελλιπής σχεδιασμό τακτικών ελέγχων εύρυθμης λειτουργίας του λογισμικού	Μεταφορά

Κίνδυνος εσφαλμένης εγκατάστασης υλικού ή λογισμικού από το προσωπικό της αναδόχου εταιρείας	Μεταφορά
Ανεπαρκής κάλυψη του κτιρίου από σύστημα συναγερμού	Μετριασμός
Ανεπαρκής κάλυψη του κτιρίου από σύστημα πυρανίχνευσης	Μετριασμός
Ανεπαρκής κάλυψη του κτιρίου από σύστημα αναγνώρισης και ελέγχου ταυτότητας	Μετριασμός
Έλλειψη οικονομικών πόρων	Αποφυγή
Προβλήματα με την χρηματοδότηση του έργου	Αποφυγή
Καταστροφή υλικού ή λογισμικού από τους χειριστές του συστήματος	Μετριασμός
Κλοπή υλικού από εργαζομένους	Αποφυγή
Απεργίες εργαζομένων που διαχειρίζονται το πληροφοριακό σύστημα	Μετριασμός
Κίνδυνος απροθυμίας προσαρμογής στην αλλαγή	Μετριασμός
Καταστροφή εξοπλισμού από υγρά/τρόφιμα	Αποφυγή
Διαρροή πληροφοριών	Μετριασμός
Μη εξουσιοδοτημένη πρόσβαση στους χώρους του πληροφοριακού συστήματος	Μετριασμός
Μη εξουσιοδοτημένη πρόσβαση στο πληροφοριακό σύστημα από τους εργαζόμενους	Μεταφορά
Διαρροή κωδικών εισόδου και διαχείρισης του πληροφοριακού συστήματος	Μετριασμός
Μη εξουσιοδοτημένες αλλαγές αρχείων	Μεταφορά
Ακούσια αλλαγή των δεδομένων του πληροφοριακού συστήματος	Αποδοχή
Έλλειψη κινήτρων για τους εργαζόμενους	Μετριασμός
Έλλειψη ευαισθητοποίησης σε θέματα ασφάλειας	Μετριασμός
Σύνδεση προσωπικών συσκευών στο εταιρικό δίκτυο	Αποδοχή
Εγκατάσταση μη εξουσιοδοτημένου λογισμικού και εφαρμογών	Μετριασμός
Ακούσια μεταφορά εμπιστευτικών δεδομένων του πληροφοριακού συστήματος εκτός γραφείου	Μετριασμός
Έλλειψη της απαιτούμενης εκπαίδευσης του προσωπικού	Μετριασμός
Εσωτερικοί κίνδυνοι (δόλος)	Μετριασμός
Λάθος κατανομή του κεφαλαίου	Μεταφορά
Λανθασμένη κατανομή σημαντικότητας στις εφαρμογές του συστήματος	Μεταφορά
Έλλειψη εφεδρικού σχεδίου απρόσκοπτης λειτουργίας του συστήματος	Μεταφορά
Λανθασμένη πρόβλεψη απαιτούμενων πόρων υλικού	Αποφυγή
Αλλαγή του χρονοδιαγράμματος λόγω λανθασμένου αρχικού προγραμματισμού	Μεταφορά
Λανθασμένη κοστολόγηση του έργου	Μεταφορά
Κοινή χρήση εμπιστευτικών δεδομένων με τους συνεργάτες και τους προμηθευτές	Μεταφορά
Έλλειψη εμπειρίας και τεχνογνωσίας των προσώπων που είναι υπεύθυνα για την παρακολούθηση της υλοποίησης του έργου	Μετριασμός

Λανθασμένες αποφάσεις διαχείρησης κινδύνων	Μετριασμός
Κίνδυνος σεισμού	Μετριασμός
Κίνδυνος κεραυνού	Αποφυγή
Κίνδυνος πλημμύρας	Μετριασμός
Κίνδυνος πυρκαγιάς	Μετριασμός
Κίνδυνος διαρροής υδάτων	Μετριασμός
Κίνδυνος αδυναμίας ηλεκτροδότησης του συστήματος λόγω ελλείψεων στην ηλεκτρολογική εγκατάσταση	Μετριασμός
Κατολίσθηση – διάβρωση εδάφους	Αποδοχή
Ηλιακές εκλάμψεις	Αποδοχή
Σκόνη	Μετριασμός
Βλάβη του συστήματος κλιματισμού	Μετριασμός
Ηλεκτρομαγνητικές παρεμβολές	Αποδοχή
Στατικός ηλεκτρισμός	Μετριασμός
Έκρηξη ηφαιστείου	Αποφυγή
Πυρηνικό ατύχημα	Αποφυγή
Κίνδυνος εκρήξεων	Μετριασμός
Έντομα –τρωκτικά	Μετριασμός
Κίνδυνος δονήσεων	Μετριασμός
Καπνός – Μικροσωματίδια	Μετριασμός
Μαγνήτες – μαγνητικά εργαλεία	Μετριασμός
Αγωγές – Μηνύσεις	Μεταφορά
Απώλεια καλής φήμης	Μεταφορά
Κλοπή πνευματικής ιδιοκτησίας	Μεταφορά
Αλλαγή σχεδιασμού συστήματος ή ματαίωση κατασκευής του λόγω πολιτικών αποφάσεων	Αποδοχή
Κίνδυνος καταστροφής του πληροφοριακού συστήματος λόγω πολιτικής αστάθειας	Αποδοχή
Κλοπή υλικού	Μετριασμός
Βανδαλισμοί	Μετριασμός
Εισβολείς (Hackers) – Υποκλοπή δεδομένων	Μεταφορά

Εισβολείς (Hackers) – Καταστροφή δεδομένων	Μεταφορά
Ηλεκτρονικοί εγκληματίες (Μετάδοση κακόβουλου λογισμικού)	Μεταφορά
Πρώην εργαζόμενοι που εργάζονται για ανταγωνιστές	Αποδοχή
Κατασκοπεία	Μεταφορά
Τρομοκρατικές ενέργειες	Μετριασμός

Πίνακας 9: Σχέδια αντιμετώπισης κινδύνων συστήματος Fleetbroadband Provisioning System

Οι κίνδυνοι οι οποίοι είναι αποδεκτοί, πρέπει να παρακολουθούνται ώστε να ελέγχεται η κατάστασή τους κατά τη διάρκεια της υλοποίησης του συστήματος. Οι κίνδυνοι οι οποίοι πρέπει να μεταφερθούν σε κάποιο εμπλεκόμενο μέρος πρέπει να καλύπτονται από τις ρήτρες του συμβολαίου μεταξύ του εργολάβου και του ανάδοχου του έργου.

Στους κινδύνους τους οποίους πρέπει να μειωθεί είτε η πιθανότητα εμφάνισής τους είτε η συνέπεια που μπορεί να επιφέρουν, πρέπει να βρεθούν κάποια εναλλακτικά σχέδια που θα τεθούν σε εφαρμογή είτε πριν την εμφάνισή τους είτε μετά από αυτή. Τέλος, οι κίνδυνοι που πρέπει να αποφευχθούν είναι αυτοί που μπορούν να έχουν το μεγαλύτερο αντίκτυπο στην υλοποίηση και λειτουργία του συστήματος και πρέπει να βρεθούν εναλλακτικοί τρόποι ώστε να εκλείψουν.

Στη συνέχεια ενημερώνεται το μητρώο κινδύνων με τη μέθοδο (στρατηγική) αντιμετώπισης, το δείκτη παρακολούθησης και τον προπομπό του κάθε κινδύνου (Πίνακας 9).

Πιο αναλυτικά, στα παρακάτω πεδία συμπληρώνονται τα εξής στοιχεία:

- στο πεδίο «δείκτης παρακολούθησης» καταγράφονται οι παράμετροι ή τα γεγονότα τα οποία χαρακτηρίζουν τον κίνδυνο και τα οποία θα παρακολουθεί η ομάδα διαχείρισης.
- στο πεδίο «προπομπός κινδύνου» (risk trigger), καταγράφεται το γεγονός που μπορεί να υποδηλώσει την έναρξη υλοποίησης του κάθε κινδύνου, ώστε η ομάδα διαχείρισης να ενεργήσει έγκαιρα και σωστά για την αντιμετώπισή του.
- στο πεδίο «στρατηγική αντιμετώπισης» καταγράφεται η μέθοδος με την οποία θα αντιμετωπιστεί ο κάθε κίνδυνος.
- στο πεδίο «ημερομηνία ενημέρωσης» καταγράφεται η ημερομηνία όπου έγινε το σχέδιο αντιμετώπισης του κάθε κινδύνου.

#	Κίνδυνοι	Δείκτης Παρακολούθησης	Προπομπός Κινδύνου	Στρατηγική Αντιμετώπισης	Ημερομηνία Ενημέρωσης
1	Ασυμβατότητα λογισμικού με τις απαιτήσεις	Έλεγχος του τρόπου λειτουργίας των εκδόσεων του συστήματος	Κάποια έκδοση δεν λειτουργεί σωστά	Μεταφορά	20/02/2016
2	Εξάντληση πόρων του συστήματος	Στατιστικά χρήσης του συστήματος	Η χρήση του συστήματος έχει ανέλθει στο ανώτατο κατώφλι ασφαλείας που έχει τεθεί από τον εργολάβο (π.χ. το 80% των πόρων του συστήματος)	Αποφυγή	20/02/2016
3	Λανθασμένη βάση δεδομένων αποθήκευσης των στοιχείων	Έλεγχος του τρόπου λειτουργίας των εκδόσεων του συστήματος	Σε κάποια έκδοση η βάση δεδομένων δε λειτουργεί σωστά	Μεταφορά	20/02/2016
4	Ελλιπής ασφάλεια των προσωπικών δεδομένων των πολιτών	Έλεγχος στις εκδόσεις των λογισμικών ασφαλείας	Υπάρχει ενδεχόμενο υποκλοπής κάποιων στοιχείων	Μεταφορά	20/02/2016
5	Δυσκολία σε αναβάθμιση – συντήρηση λογισμικού	Παρακολούθηση του σχεδιασμού και των τεχνικών προδιαγραφών υλοποίησης του συστήματος	Εμφάνιση αυξημένης πολυπλοκότητας στην αρχιτεκτονική σχεδιασμού και δυσκολία εισαγωγής νέων χαρακτηριστικών	Μεταφορά	20/02/2016
6	Έλλειψη διασυνδεσιμότητας του φορέων μέσω του συστήματος	Πρωτόκολλα επικοινωνίας	Αδυναμία διασύνδεσης με τα συστήματα των άλλων φορέων	Μεταφορά	20/02/2016
7	Λανθασμένος σχεδιασμός υλικού του συστήματος	Παρακολούθηση των απαιτήσεων σχεδιασμού	Λανθασμένη υλοποίηση των απαιτήσεων σχεδιασμού	Μεταφορά	20/02/2016
8	Λανθασμένος σχεδιασμός λογισμικού του συστήματος	Παρακολούθηση των απαιτήσεων σχεδιασμού	Λανθασμένη υλοποίηση των απαιτήσεων σχεδιασμού	Μεταφορά	20/02/2016
9	Ασυμβατότητα της τεχνολογίας του λογισμικού με τις υπάρχουσες κρατικές υποδομές ροής πληροφοριών	Παρακολούθηση τεχνολογίας ανάπτυξης λογισμικού	Αδυναμία αξιοποίησης στο μέγιστο των υποδομών ροής πληροφοριών	Μεταφορά	20/02/2016
10	Χρήση νέων και μη δοκιμασμένων τεχνολογιών ανάπτυξης λογισμικού	Παρακολούθηση τεχνολογίας ανάπτυξης λογισμικού	Αδυναμία κάλυψης των λειτουργικών απαιτήσεων του συστήματος	Μεταφορά	20/02/2016
11	Μη αποδεκτή ποιότητα λογισμικού	Παρακολούθηση των ποιοτικών χαρακτηριστικών του συστήματος	Απόκλιση από τα αποδεκτά όρια ποιότητας	Μεταφορά	20/02/2016
12	Ελλιπείς μηχανισμοί ελέγχου ασφάλειας του πληροφοριακού συστήματος	Έλεγχος του τρόπου λειτουργίας των εκδόσεων του λογισμικού ασφαλείας	Κάποια έκδοση του λογισμικού ασφαλείας δεν λειτουργεί σωστά με αποτέλεσμα την μετάδοση κακόβουλου λογισμικού	Μεταφορά	20/02/2016

13	Αδυναμία σύνδεσης με τον κεντρικό Η/Υ εξαιτίας υπερφόρτωσης των τηλεπικοινωνιακών δικτύων ή εξαιτίας της μειωμένης αξιοπιστίας του δικτύου	Παρακολούθηση χαρακτηριστικών του τηλεπικοινωνιακού δικτύου	Συνεχής υπερφόρτωση του δικτύου	Αποφυγή	20/02/2016
14	Ανεπαρκής προστασία κρυπτογραφικών κλειδιών	Παρακολούθηση των απαιτήσεων ασφάλειας στο σχεδιασμό του λογισμικού	Λανθασμένη υλοποίηση των απαιτήσεων ασφάλειας	Μεταφορά	20/02/2016
15	Ελλιπής επικύρωση της επεξεργασίας των δεδομένων	Παρακολούθηση του τρόπου επεξεργασίας των δεδομένων	Λανθασμένη επεξεργασία των δεδομένων	Μεταφορά	20/02/2016
16	Δυσλειτουργία του υλικού	Παρακολούθηση του τρόπου λειτουργίας του υλικού	Συνεχής υπερθέρμανση του συστήματος/ έντονος ήχος κατά τη λειτουργία του	Αποδοχή	20/02/2016
17	Ανεπαρκής έλεγχος λογισμικού	Παρακολούθηση των απαιτήσεων ελέγχου του λογισμικού	Λανθασμένη υλοποίηση των απαιτήσεων ελέγχου	Μεταφορά	20/02/2016
18	Σφάλματα λογισμικού	Έλεγχος του τρόπου λειτουργίας των εκδόσεων του λογισμικού	Κάποια έκδοση του λογισμικού δεν παράγει τα αναμενόμενα αποτελέσματα	Μεταφορά	20/02/2016
19	Πολυπλοκότητα λογισμικού	Έλεγχος στον σχεδιασμό του λογισμικού	Δυσκολία στην αναβάθμιση του λογισμικού	Μεταφορά	20/02/2016
20	Μη ασφαλής αρχιτεκτονική δικτύου	Παρακολούθηση των απαιτήσεων ασφάλειας για το σχεδιασμό του δικτύου	Λανθασμένη υλοποίηση των απαιτήσεων ασφάλειας	Μεταφορά	20/02/2016
21	Προβλήματα επικοινωνίας με την εταιρεία ανάθεσης έργου	Έλεγχος της επικοινωνίας με την εταιρεία ανάθεσης έργου	Έλλειψη επικοινωνίας με την εταιρεία ανάθεσης έργου	Μετριασμός	20/02/2016
22	Μη επαρκώς καθορισμένοι όροι του συμβολαίου μεταξύ του κράτους και του αναδόχου	Παρακολούθηση της διαδικασίας καθορισμού των όρων του συμβολαίου	Ύπαρξη ασαφειών μεταξύ των όρων του συμβολαίου	Αποφυγή	20/02/2016
23	Μη διαθεσιμότητα ομάδας υποστήριξης του συστήματος	Παρακολούθηση ανταπόκρισης της ομάδα υποστήριξης του συστήματος σε περίπτωση ανάγκης	Προβληματική υποστήριξη του συστήματος	Μεταφορά	20/02/2016
24	Έλλειψη συνεργασίας μεταξύ των ομάδων κατασκευής του έργου.	Παρακολούθηση της επικοινωνίας μεταξύ των ομάδων	Προβληματική συνεργασία μεταξύ των ομάδων	Μετριασμός	20/02/2016

25	Ελλιπής φύλαξη του κτιρίου όπου στεγάζεται το πληροφοριακό σύστημα από εξειδικευμένα άτομα(φύλακες)	Παρακολούθηση της ασφάλειας του κτιρίου	Εμφάνιση φαινομένων εισβολής	Μετριασμός	20/02/2016
26	Ελλιπής χρόνος προσαρμογής χρήσης του νέου πληροφοριακού συστήματος	Έλεγχος του χρόνου προσαρμογής των χρηστών	Απόκλιση από τον προβλεπόμενο χρόνο προσαρμογής	Αποδοχή	20/02/2016
27	Ανεπαρκής ή λανθασμένος διαχωρισμός των καθηκόντων	Έλεγχος και αξιολόγηση των εργαζομένων του συστήματος σύμφωνα με τα προσόντα και τις γνώσεις τους	Λανθασμένη υλοποίηση του συστήματος και μη σωστή λειτουργία των ομάδων που συνεργάζονται για την υλοποίηση του συστήματος	Μεταφορά	20/02/2016
28	Ανεπαρκής επίβλεψη εργαζομένων	Μη ύπαρξη προσωπικού για την επίβλεψη εργαζομένων	Καθυστέρηση στην υλοποίηση του έργου /Υπαρξη λαθών κατά την υλοποίηση του	Μεταφορά	20/02/2016
29	Ελλιπής διαδικασία για την αφαίρεση δικαιωμάτων πρόσβασης κατά την λήξη της απασχόλησης	Έλεγχος των ατόμων που συνδέονται καθημερινά στο σύστημα	Ανίχνευση πρόσβασης στο σύστημα από πρώην εργαζόμενο στην εταιρεία	Αποφυγή	20/02/2016
30	Ελλιπής σχεδιασμό τακτικών ελέγχων εύρυθμης λειτουργίας του λογισμικού	Έλεγχος της λειτουργίας του λογισμικού	Μη αναμενόμενη συμπεριφορά του λογισμικού	Μεταφορά	20/02/2016
31	Κίνδυνος εσφαλμένης εγκατάστασης υλικού ή λογισμικού από το προσωπικό της αναδόχου εταιρείας	Έλεγχος των όρων που υπάρχουν στο συμβόλαιο με την εταιρεία ανάθεσης έργου	Μη ύπαρξη του όρου για την αποφυγή του κινδύνου	Μεταφορά	20/02/2016
32	Ανεπαρκής κάλυψη του κτιρίου από σύστημα συναγερμού	Επιθεώρηση του υλικού και του χώρου στον οποίο βρίσκεται αυτό	Μη αναμενόμενη συμπεριφορά του υλικού, μη τακτική συντήρηση του υλικού	Μετριασμός	20/02/2016
33	Ανεπαρκής κάλυψη του κτιρίου από σύστημα πυρανίχνευσης	Επιθεώρηση του υλικού και του χώρου στον οποίο βρίσκεται αυτό	Μη αναμενόμενη συμπεριφορά του υλικού, ύπαρξη εύφλεκτων υλικών στο χώρο, μη τακτική συντήρηση του υλικού	Μετριασμός	20/02/2016
34	Ανεπαρκής κάλυψη του κτιρίου από σύστημα αναγνώρισης και ελέγχου ταυτότητας	Επιθεώρηση του υλικού και του χώρου στον οποίο βρίσκεται αυτό	Μη αναμενόμενη συμπεριφορά του υλικού, μη τακτική συντήρηση του υλικού	Μετριασμός	20/02/2016
35	Έλλειψη οικονομικών πόρων	Οικονομικοί δείκτες ρευστότητας και χρηματοδότησης του έργου	Περικοπή κάποιου προϋπολογισμού	Αποφυγή	20/02/2016
36	Προβλήματα με την χρηματοδότηση του έργου	Ανακοινώσεις της κυβέρνησης σχετικά με τη χρηματοδότηση	Ύπαρξη γενικότερων οικονομικών προβλημάτων και έλλειψη	Αποφυγή	20/02/2016

		του έργου	ρευστότητας του κράτους		
37	Καταστροφή υλικού ή λογισμικού από τους χειριστές του συστήματος	Επιθεώρηση του υλικού και του χώρου στον οποίο βρίσκεται αυτό	Μη αναμενόμενη συμπεριφορά του υλικού, μη τακτική συντήρηση του υλικού	Μετριασμός	20/02/2016
38	Κλοπή υλικού από εργαζομένους	Έλεγχος του εξοπλισμού σε τακτά χρονικά διαστήματα	Μη ταύτιση καταγεγραμμένου και υπάρχοντος εξοπλισμού	Αποφυγή	20/02/2016
39	Απεργίες εργαζομένων που διαχειρίζονται το πληροφοριακό σύστημα	Παρακολούθηση της συμπεριφοράς των εργαζομένων ως προς τα εργασιακά ζητήματα	Εμφάνιση αντιδράσεων σε εργασιακές αλλαγές	Μετριασμός	20/02/2016
40	Κίνδυνος απροθυμίας προσαρμογής στην αλλαγή	Παρακολούθηση των στατιστικών χρήσης του συστήματος	Τα στατιστικά χρήσης του συστήματος είναι στο κατώτατο όριο από αυτό που έχει οριστεί από την εταιρεία ανάθεσης του έργου	Μετριασμός	20/02/2016
41	Καταστροφή εξοπλισμού από υγρά/τρόφιμα	Έλεγχος αν υπάρχει σήμανση για την απαγόρευση των τροφίμων και των ποτών στου χώρους που βρίσκεται το πληροφοριακό σύστημα	Εργαζόμενοι που εισέρχονται με τρόφιμα και ποτά στους χώρους του πληροφοριακού συστήματος	Αποφυγή	20/02/2016
42	Διαρροή πληροφοριών	Έλεγχος για την ύπαρξη ειδικού λογισμικού που να καταγράφει τις κινήσεις του κάθε εργαζομένου κατά τη διάρκεια της χρήσης του πληροφοριακού συστήματος	Μη ύπαρξη του λογισμικού που να καταγράφει τις κινήσεις του κάθε εργαζομένου κατά τη διάρκεια της χρήσης του πληροφοριακού συστήματος	Μετριασμός	20/02/2016
43	Μη εξουσιοδοτημένη πρόσβαση στους χώρους του πληροφοριακού συστήματος	Έλεγχος για την ύπαρξη συσκευών αναγνώρισης των ειδικών καρτών των εργαζομένων	Μη ύπαρξη των συσκευών αναγνώρισης στις εισόδους του κτιρίου που στεγάζεται το σύστημα	Μετριασμός	20/02/2016
44	Μη εξουσιοδοτημένη πρόσβαση στο πληροφοριακό σύστημα από τους εργαζόμενους	Έλεγχος των όρων που υπάρχουν στο συμβόλαιο με την εταιρεία ανάθεσης έργου	Μη ύπαρξη του όρου για την αποφυγή του κινδύνου	Μεταφορά	20/02/2016
45	Διαρροή κωδικών εισόδου και διαχείρισης του πληροφοριακού συστήματος	Έλεγχος για την ύπαρξη ειδικού λογισμικού που να καταγράφει την ηλεκτρονική διεύθυνση που	Μη ύπαρξη του ειδικού λογισμικού	Μετριασμός	20/02/2016

		αντιστοιχεί σε κάθε εργαζόμενο			
46	Μη εξουσιοδοτημένες αλλαγές αρχείων	Έλεγχος των όρων που υπάρχουν στο συμβόλαιο με την εταιρεία ανάθεσης έργου	Μη ύπαρξη του όρου για την αποφυγή του κινδύνου	Μεταφορά	20/02/2016
47	Ακούσια αλλαγή των δεδομένων του πληροφοριακού συστήματος	Περιοδική ταυτοποίηση ενός δείγματος δεδομένων και έλεγχος των αποτελεσμάτων	Εμφάνιση σφαλμάτων κατά την ταυτοποίηση	Αποδοχή	20/02/2016
48	Έλλειψη κινήτρων για τους εργαζόμενους	Παρακολούθηση δεικτών παραγωγικότητας	Μείωση παραγωγικότητας των εργαζομένων	Μετριασμός	20/02/2016
49	Έλλειψη ευαισθητοποίησης σε θέματα ασφάλειας	Παρακολούθηση της τήρησης των κανόνων ασφαλείας	Εμφάνισης συχνής παραβατικότητας	Μετριασμός	20/02/2016
50	Σύνδεση προσωπικών συσκευών στο εταιρικό δίκτυο	Τακτικός έλεγχος του δικτύου μέσω λογισμικού ασφαλείας (Antivirus)	Εμφάνιση και διόρθωση ιού κατά τη διαδικασία του τακτικού ελέγχου	Αποδοχή	20/02/2016
51	Εγκατάσταση μη εξουσιοδοτημένου λογισμικού και εφαρμογών	Τακτικός έλεγχος για την αυθεντικότητα του λογισμικού και των εφαρμογών	Εμφάνιση μη εξουσιοδοτημένου λογισμικού και εφαρμογών	Μετριασμός	20/02/2016
52	Ακούσια μεταφορά εμπιστευτικών δεδομένων του πληροφοριακού συστήματος εκτός γραφείου	Έλεγχος για την ύπαρξη ειδικού λογισμικού που να καταγράφει τις κινήσεις του κάθε εργαζομένου κατά τη διάρκεια της χρήσης του πληροφοριακού συστήματος	Μη ύπαρξη του λογισμικού που να καταγράφει τις κινήσεις του κάθε εργαζομένου κατά τη διάρκεια της χρήσης του πληροφοριακού συστήματος	Μετριασμός	20/02/2016
53	Έλλειψη της απαιτούμενης εκπαίδευσης του προσωπικού	Παρακολούθηση του αρχείου εκπαίδευσης των υπαλλήλων	Ύπαρξη προβλημάτων κατά τη χρήση του συστήματος	Μετριασμός	20/02/2016
54	Εσωτερικοί κίνδυνοι (δόλος)	Παρακολούθηση συμπεριφοράς εργαζομένων	Ύποπτες κινήσεις εργαζομένων	Μετριασμός	20/02/2016
55	Λάθος κατανομή του κεφαλαίου	Παρακολούθηση της προσυμφωνημένης κατανομής του κεφαλαίου	Ανομοιόμορφη κατανομή του κεφαλαίου	Μεταφορά	20/02/2016
56	Λανθασμένη κατανομή σημαντικότητας στις εφαρμογές του συστήματος	Έλεγχος στις εκδόσεις του συστήματος	Το σύστημα δεν καλύπτει κάποια σημαντικά σημεία που έπρεπε να έχουν ληφθεί πολύ σοβαρά υπ' όψιν	Μεταφορά	20/02/2016

57	Έλλειψη εφεδρικού σχεδίου απρόσκοπτης λειτουργίας του συστήματος	Παρακολούθηση του σχεδιασμού του έργου	Ανεπαρκής ή ελλιπής ύπαρξη εφεδρικού σχεδίου κατά το στάδιο ολοκλήρωσης του έργου	Μεταφορά	20/02/2016
58	Λανθασμένη πρόβλεψη απαιτούμενων πόρων υλικού	Έλεγχος του προγραμματισμού των απαιτούμενων πόρων υλικού	Απόκλιση από τον αρχικό προγραμματισμό των απαιτούμενων πόρων	Αποφυγή	20/02/2016
59	Αλλαγή του χρονοδιαγράμματος λόγω λανθασμένου αρχικού προγραμματισμού	Παρακολούθηση και σύγκριση του πραγματικού χρονοδιαγράμματος με το εκτιμώμενο	Παρατήρηση καθυστερήσεων κατά τα επιμέρους στάδια ολοκλήρωσης του έργου	Μεταφορά	20/02/2016
60	Λανθασμένη κοστολόγηση του έργου	Παρακολούθηση οικονομικών δεικτών	Τα πρώτα στάδια της υλοποίησης του έργου βγαίνουν εκτός του αρχικού προϋπολογισμού	Μεταφορά	20/02/2016
61	Κοινή χρήση εμπιστευτικών δεδομένων με τους συνεργάτες και τους προμηθευτές	Έλεγχος των όρων που υπάρχουν στο συμβόλαιο με την εταιρεία ανάθεσης έργου	Μη ύπαρξη του όρου για την αποφυγή του κινδύνου	Μεταφορά	20/02/2016
62	Έλλειψη εμπειρίας και τεχνογνωσίας των προσώπων που είναι υπεύθυνα για την παρακολούθηση της υλοποίησης του έργου	Ελλιπής έλεγχος των απαραίτητων διαδικασιών για την διεξαγωγή του έργου	Εμφάνιση πολλών λαθών κατά τη διάρκεια του προγραμματισμού και της διαχείρισης του έργου	Μετριασμός	20/02/2016
63	Λανθασμένες αποφάσεις διαχείρησης κινδύνων	Τακτική παρακολούθηση του σχεδιασμού διαχείρισης κινδύνου	Απόκλιση αποφάσεων από τον αρχικό σχεδιασμό διαχείρισης κινδύνου	Μετριασμός	20/02/2016
64	Κίνδυνος σεισμού	Έλεγχος στατικότητας του κτιρίου όπου στεγάζεται το πληροφοριακό σύστημα	Ενδείξεις προβληματικής στατικότητας του κτιρίου	Μετριασμός	20/02/2016
65	Κίνδυνος κεραυνού	Έλεγχος των καιρικών φαινομένων	Έντονες βροχοπτώσεις	Αποφυγή	20/02/2016
66	Κίνδυνος πλημμύρας	Έλεγχος των καιρικών φαινομένων	Παρατήρηση πλημμυρικών φαινομένων σε ορισμένα τμήματα του κτιρίου	Μετριασμός	20/02/2016
67	Κίνδυνος πυρκαγιάς	Έλεγχος του χώρου εγκατάστασης ως προς τα μέτρα πυρασφάλειας	Ελλιπής ή ανύπαρκτη συντήρηση του εξοπλισμού πυρασφάλειας	Μετριασμός	20/02/2016
68	Κίνδυνος διαρροής υδάτων	Έλεγχος του δικτύου υδροδότησης του κτιρίου	Ελλιπής ή ανύπαρκτη συντήρηση του δικτύου υδροδότησης	Μετριασμός	20/02/2016

69	Κίνδυνος αδυναμίας ηλεκτροδότησης του συστήματος λόγω ελλείψεων στην ηλεκτρολογική εγκατάσταση	Έλεγχος του δικτύου ηλεκτροδότησης του κτιρίου	Ελλιπής ή ανύπαρκτη συντήρηση του δικτύου ηλεκτροδότησης	Μετριασμός	20/02/2016
70	Κατολίσθηση – διάβρωση εδάφους	Περιοδικοί έλεγχοι του εδάφους περιμετρικά του κτιρίου όπου βρίσκεται το πληροφοριακό σύστημα	Εμφάνιση φαινομένων διάβρωσης	Αποδοχή	20/02/2016
71	Ηλιακές εκλάμψεις	Περιοδικός έλεγχος της σωστής λειτουργίας του δικτύου από ηλεκτρομαγνητικές παρεμβολές	Μη σωστή λειτουργία του δικτύου λόγω ηλεκτρομαγνητικών παρεμβολών	Αποδοχή	20/02/2016
72	Σκόνη	Τακτικός έλεγχος της κατάστασης του εξοπλισμού	Παρατήρηση δυσλειτουργιών λόγω σκόνης	Μετριασμός	20/02/2016
73	Βλάβη του συστήματος κλιματισμού	Τακτική παρακολούθηση του συστήματος κλιματισμού	Παρατήρηση δυσλειτουργιών του συστήματος λόγω υπερθέρμανσης	Μετριασμός	20/02/2016
74	Ηλεκτρομαγνητικές παρεμβολές	Περιοδικός έλεγχος της σωστής λειτουργίας του δικτύου από ηλεκτρομαγνητικές παρεμβολές	Μη σωστή λειτουργία του δικτύου λόγω ηλεκτρομαγνητικών παρεμβολών	Αποδοχή	20/02/2016
75	Στατικός ηλεκτρισμός	Περιοδικός έλεγχος του κτιρίου που στεγάζεται το πληροφοριακό σύστημα για διαρροή ρεύματος	Εμφάνιση σημείων του κτιρίου όπου μπορεί να προκληθεί διαρροή ρεύματος - βραχυκύκλωμα	Μετριασμός	20/02/2016
76	Έκρηξη ηφαιστείου	Παρακολούθηση των μετρήσεων που γίνονται από το ηφαιστειολογικό παρατηρητήριο της περιοχής όπου στεγάζεται το πληροφοριακό σύστημα	Όταν οι μετρήσεις αποκλίνουν από τα επιτρεπτά όρια που έχουν ορισθεί	Αποφυγή	20/02/2016
77	Πυρηνικό ατύχημα	Παρακολούθηση των μετρήσεων που γίνονται από τα πυρηνικά εργοστάσια της περιοχής όπου στεγάζεται το πληροφοριακό σύστημα	Όταν οι μετρήσεις αποκλίνουν από τα επιτρεπτά όρια που έχουν ορισθεί	Αποφυγή	20/02/2016
78	Κίνδυνος εκρήξεων	Έλεγχος για την ύπαρξη εύφλεκτων υλικών στο χώρο όπου στεγάζεται το	Εμφάνιση αποθηκευμένων υλικών που μπορεί να προκαλέσουν εκρήξεις	Μετριασμός	20/02/2016

		πληροφοριακό σύστημα			
79	Έντομα –τρωκτικά	Τακτικός έλεγχος του κτιρίου για εμφάνιση τρωκτικών	Εμφάνιση καταστροφών στο υλικό του συστήματος από τρωκτικά	Μετριασμός	20/02/2016
80	Κίνδυνος δονήσεων	Έλεγχος του κτιρίου όπου στεγάζεται το πληροφοριακό σύστημα για την ύπαρξη ιδιοτήτων αντικραδασμικής λειτουργίας	Μη ύπαρξη ιδιοτήτων αντικραδασμικής λειτουργίας	Μετριασμός	20/02/2016
81	Καπνός – Μικροσωματίδια	Έλεγχος της καθαρότητας του αέρα	Εμφάνιση καπνού στο χώρο του πληροφοριακού συστήματος	Μετριασμός	20/02/2016
82	Μαγνήτες – μαγνητικά εργαλεία	Τακτικός έλεγχος της βάσης δεδομένων και καταμέτρηση των αποθηκευμένων δεδομένων στη βάση	Απώλεια δεδομένων/μη σωστή αποθήκευση των δεδομένων	Μετριασμός	20/02/2016
83	Αγωγές – Μηνύσεις	Παρακολούθηση ορθής λειτουργίας του συστήματος και αποδοχής του από τα εμπλεκόμενα μέρη	Ύπαρξη σοβαρών αντιδράσεων	Μεταφορά	20/02/2016
84	Απώλεια καλής φήμης	Έλεγχος της αποδοχής και της χρήσης του συστήματος από τα εμπλεκόμενα μέλη	Μη χρήση της εφαρμογής από τους χρήστες λόγω ύπαρξης λαθών / μη εύχρηστη εφαρμογή για τους τελικούς χρήστες του συστήματος	Μεταφορά	20/02/2016
85	Κλοπή πνευματικής ιδιοκτησίας	Παρακολούθηση των εφαρμογών που χρησιμοποιούν ανταγωνίστριες εταιρείες	Χρήση εφαρμογής από ανταγωνίστρια εταιρεία με ίδια χαρακτηριστικά	Μεταφορά	20/02/2016
86	Αλλαγή σχεδιασμού συστήματος ή ματαίωση κατασκευής του λόγω πολιτικών αποφάσεων	Παρακολούθηση των πολιτικών αποφάσεων και δραστηριοτήτων της κυβέρνησης	Αποφάσεις μείωσης λειτουργικότητας και περιορισμού χρήσης του πληροφοριακού στο σύστημα υγείας	Αποδοχή	20/02/2016
87	Κίνδυνος καταστροφής του πληροφοριακού συστήματος λόγω πολιτικής αστάθειας	Παρακολούθηση των πολιτικών αποφάσεων και δραστηριοτήτων της κυβέρνησης	Πολεμικές αναταραχές	Αποδοχή	20/02/2016
88	Κλοπή υλικού	Έλεγχος του εξοπλισμού και επιθεώρηση του χώρου όπου βρίσκεται ο εξοπλισμός σε τακτά	Μη ταύτιση καταγεγραμμένου και υπάρχοντος εξοπλισμού	Μετριασμός	20/02/2016

		χρονικά διαστήματα			
89	Βανδαλισμοί	Έλεγχος των κτιριακών εγκαταστάσεων όπου στεγάζεται το πληροφοριακό σύστημα καθώς και του εξοπλισμού του πληροφοριακού συστήματος	Καταστροφή του κτιρίου και του εξοπλισμού	Μετριασμός	20/02/2016
90	Εισβολείς (Hackers) – Υποκλοπή δεδομένων	Έλεγχος του λογισμικού ασφαλείας	Υποκλοπή μεταδιδόμενων πληροφοριών	Μεταφορά	20/02/2016
91	Εισβολείς (Hackers) – Καταστροφή δεδομένων	Έλεγχος του λογισμικού ασφαλείας	Καταστροφή/ διαγραφή δεδομένων	Μεταφορά	20/02/2016
92	Ηλεκτρονικοί εγκληματίες (Μετάδοση κακόβουλου λογισμικού)	Έλεγχος του λογισμικού ασφαλείας	Μετάδοση κακόβουλου λογισμικού	Μεταφορά	20/02/2016
93	Πρώην εργαζόμενοι που εργάζονται για ανταγωνιστές	Παρακολούθηση των εφαρμογών που χρησιμοποιούν ανταγωνίστριες εταιρείες	Χρήση εφαρμογής από ανταγωνίστρια εταιρεία με ίδια χαρακτηριστικά	Αποδοχή	20/02/2016
94	Κατασκοπεία	Έλεγχος του λογισμικού ασφαλείας	Υποκλοπή ευαίσθητων προσωπικών δεδομένων	Μεταφορά	20/02/2016
95	Τρομοκρατικές ενέργειες	Έλεγχος του χώρου εγκατάστασης του πληροφοριακού συστήματος και της συμπεριφοράς των εργαζομένων	Ύποπτες ενέργειες των εργαζομένων/ εύρεση ύποπτου εξοπλισμού στο χώρο	Μετριασμός	20/02/2016

Πίνακας 10: Μητρώο κινδύνων–Σχέδια αντιμετώπισης κινδύνων συστήματος Fleetbroadband Provisioning System

Έπειτα, αν η μέθοδος αντιμετώπισης είναι ο μετριασμός αναγράφονται σε αυτό τα προληπτικά ή και διορθωτικά σχέδια αντιμετώπισης του κάθε κινδύνου, το εναλλακτικό σχέδιο ή και το σχέδιο μετάπτωσης (Πίνακας 11) και στις άλλες στρατηγικές τα σχέδια αποφυγής, μεταφοράς, ή αποδοχής (Πίνακας 11).

Πιο αναλυτικά, στα παρακάτω πεδία συμπληρώνονται τα εξής στοιχεία:

- στο πεδίο «προληπτικά μέτρα» καταγράφονται οι ενέργειες που πρέπει να γίνουν και αφορούν την αλλαγή της πιθανότητας εμφάνισης του κάθε κινδύνου και τα οποία θα παρθούν πριν εμφανιστεί ο κίνδυνος
- στο πεδίο «διορθωτικά μέτρα» καταγράφονται οι ενέργειες που πρέπει να γίνουν και αφορούν τη συνέπεια που μπορεί να έχει η εμφάνιση του κάθε κινδύνου και τα οποία θα παρθούν πριν εμφανιστεί ο κίνδυνος
- στο πεδίο «εναλλακτικό σχέδιο» καταγράφονται οι ενέργειες που πρέπει να γίνουν και αφορούν τη συνέπεια που μπορεί να έχει η εμφάνιση του κάθε κινδύνου και τα οποία θα παρθούν αφού εμφανιστεί ο κίνδυνος
- στο πεδίο «σχέδιο μετάπτωσης» καταγράφονται οι ενέργειες που πρέπει να γίνουν σε περίπτωση που αποτύχει το εναλλακτικό σχέδιο

#	Κίνδυνοι	Προληπτικά μέτρα	Διορθωτικά μέτρα	Ενναλακτικό σχέδιο	Σχέδιο μετάπτωσης
21	Προβλήματα επικοινωνίας με την εταιρεία ανάθεσης έργου	Συναντήσεις με την εταιρεία ανάθεσης έργου για επίτευξη καλύτερης επικοινωνίας	Ύπαρξη έγγραφων αναφορών για την αποφυγή παρερμηνεύσεων	Εφαρμογή των κυρώσεων που αναγράφονται στο συμβόλαιο	Ακύρωση του συμβολαίου με την εταιρεία ανάθεσης έργου και ανάθεση ανάθεση του έργου στον επόμενο μειοδότη
24	Έλλειψη συνεργασίας μεταξύ των ομάδων κατασκευής του έργου.	Συνεχής επικοινωνία μεταξύ των ομάδων κατασκευής του έργου		Συγκέντρωση των ομάδων κατασκευής στον ίδιο χώρο	
25	Ελλιπής φύλαξη του κτιρίου όπου στεγάζεται το πληροφοριακό σύστημα από εξειδικευμένα άτομα (φύλακες)	Πρόσληψη προσωπικού για τη φύλαξη του κτιρίου όπου στεγάζεται το πληροφοριακό σύστημα	Πρόσληψη ειδικά εκπαιδευμένου προσωπικού	Χρήση ειδικού εξοπλισμού παρακολούθησης του κτιρίου όπου στεγάζεται το πληροφοριακό σύστημα (κάμερες ασφαλείας)	
32	Ανεπαρκής κάλυψη του κτιρίου από σύστημα συναγερμού	Εγκατάσταση συστήματος συναγερμού			
33	Ανεπαρκής κάλυψη του κτιρίου από σύστημα πυρανίχνευσης	Εγκατάσταση συστήματος πυρανίχνευσης			
34	Ανεπαρκής κάλυψη του κτιρίου από σύστημα αναγνώρισης και ελέγχου ταυτότητας	Εγκατάσταση μηχανημάτων ελέγχου ταυτότητας στις εσωτερικές εισόδους που οδηγούν σε κάθε όροφο			
37	Καταστροφή υλικού ή λογισμικού από τους χειριστές του συστήματος	Εκπαίδευση των εργαζομένων σχετικά με τον τρόπο χρήσης του εξοπλισμού		Επίπληξη εργαζομένου που δεν συμβαδίζει με τους κανονισμούς ασφαλής χρήσης του εξοπλισμού	Επιβολή ποινών σε όποιον δεν ακολουθεί τους κανονισμούς ασφαλής χρήσης του εξοπλισμού
39	Απεργίες εργαζομένων που διαχειρίζονται το πληροφοριακό σύστημα	Επικοινωνία με τους εργαζόμενους για την κατανόηση των αναγκών τους και συζήτηση μαζί	Ύπαρξη εγγράφων που να γίνεται η καταγραφή των αναγκών των εργαζομένων με στόχο την κάλυψη τους	Αλλαγή αρμοδιοτήτων	

		τους για την εύρεση της βέλτιστης λύσης			
40	Κίνδυνος απροθυμίας προσαρμογής στην αλλαγή	Μελέτη των αναγκών των χρηστών για την κατανόηση των αναγκών τους όσον αφορά τη χρήση της εφαρμογής	Καταγραφή των αναγκών των χρηστών και υλοποίηση τυχόν αλλαγές στην εφαρμογής για να είναι πιο φιλικοί προς τους χρήστες		
42	Διαρροή πληροφοριών	Εγκατάσταση ειδικού λογισμικού το οποίο ελέγχει τις ενέργειες των εργαζομένων	Ενημέρωση των εργαζομένων σχετικά με τους κανονισμούς της εταιρείας όσον αφορά την ασφάλεια των πληροφοριών και των δεδομένων	Επίπληξη εργαζομένου που δεν συμβαδίζει με τους κανονισμούς της εταιρείας	Επιβολή ποινών σε όποιον δεν ακολουθεί τους κανονισμούς της εταιρείας
43	Μη εξουσιοδοτημένη πρόσβαση στους χώρους του πληροφοριακού συστήματος	Συνεχής έλεγχος των εγκαταστάσεων όπου βρίσκεται ο εξοπλισμός	Χρήση ειδικού εξοπλισμού όπου απαγορεύει την πρόσβαση μη εξουσιοδοτημένου προσωπικού στους χώρους εγκατάστασης του εξοπλισμού		
45	Διαρροή κωδικών εισόδου και διαχείρισης του πληροφοριακού συστήματος	Ενημέρωση των εργαζομένων για τη διαφύλαξη των κωδικών που έχουν για τη χρήση του πληροφοριακού συστήματος	Δυνατότητα αλλαγής των κωδικών περιοδικά		
48	Έλλειψη κινήτρων για τους εργαζόμενους	Επικοινωνία με τους εργαζόμενους για την κατανόηση των αναγκών τους και συζήτηση μαζί τους για την εύρεση της βέλτιστης λύσης	Δημιουργία περισσότερων κινήτρων για τους εργαζόμενους με βάση τις ανάγκες που έχουν		
49	Έλλειψη ευαισθητοποίησης σε θέματα ασφάλειας	Εκπαίδευση των εργαζομένων σε θέματα ασφάλειας του εξοπλισμού και του λογισμικού	Καταγραφή και ενημέρωση των εργαζομένων με τους κανόνες που πρέπει να ακολουθούν για την ασφάλεια του	Επίπληξη εργαζομένου που δεν συμβαδίζει με του κανονισμούς της ασφάλειας του	Επιβολή ποινών σε όποιον δεν ακολουθεί τους κανονισμούς της ασφάλειας του πληροφοριακού

			πληροφοριακού συστήματος	πληροφοριακού συστήματος	συστήματος
51	Εγκατάσταση μη εξουσιοδοτημένου λογισμικού και εφαρμογών	Ύπαρξη ειδικού λογισμικού ασφαλείας όπου ανιχνεύει την εγκατάσταση μη εξουσιοδοτημένου λογισμικού στο σύστημα	Τακτικός έλεγχος του λογισμικού και των εφαρμογών που χρησιμοποιούνται		
52	Ακούσια μεταφορά εμπιστευτικών δεδομένων του πληροφοριακού συστήματος εκτός γραφείου	Μη δυνατή αποθήκευση των προσωπικών δεδομένων σε αποθηκευτικά μέσα καθώς μη ύπαρξη δυνατότητας μεταφορά δεδομένων μέσω διαδικτύου			
53	Έλλειψη της απαιτούμενης εκπαίδευσης του προσωπικού	Εκπαίδευση του προσωπικού για την ανταπόκρισή του στις απαιτήσεις του συστήματος		Αλλαγή αρμοδιοτήτων	
54	Εσωτερικοί κίνδυνοι (δόλος)	Χρήση κωδικών ασφαλείας έτσι ώστε ο κάθε χρήστης να έχει δικαιώματα στο σύστημα ανάλογα με την ιδιότητά του	Χρήση εξειδικευμένου λογισμικού έτσι ώστε να ελέγχονται όλες οι ενέργειες των χρηστών		
62	Έλλειψη εμπειρίας και τεχνογνωσίας των προσώπων που είναι υπεύθυνα για την παρακολούθηση της υλοποίησης του έργου	Έλεγχος των εργαζομένων που προσλαμβάνονται για να αναλάβουν την παρακολούθηση του έργου σύμφωνα με την εμπειρία τους και τις γνώσεις που έχουν για τη συγκεκριμένη θέση με τη βοήθεια συνεντεύξεων και γραπτού διαγωνισμού όπου οι υποψήφιοι θα εξετάζονται σε θέματα που αφορούν τη διαχείριση ενός έργου	Ύπαρξη συνεχών ενημερώσεων από τα πρόσωπα που έχουν αναλάβει την παρακολούθηση του έργου καθώς και καταγραφή των δραστηριοτήτων τους και των ελέγχων που έχουν πραγματοποιήσει καθ’ όλη τη διάρκεια έργου	Συνεχής κατάρτιση των εργαζομένων σε θέματα διαχείρισης έργου και νέων τεχνολογιών με διεξαγωγή σεμιναρίων	Αλλαγή αρμοδιοτήτων
63	Λανθασμένες αποφάσεις διαχείρησης κινδύνων	Τακτικός έλεγχος των		Συνεχής κατάρτιση	Αλλαγή αρμοδιοτήτων

		εργαζομένων που έχουν αναλάβει τις αποφάσεις διαχείρισης κινδύνων		των εργαζομένων σε θέματα διαχείρισης κινδύνων με διεξαγωγή σεμιναρίων	
64	Κίνδυνος σεισμού	Συνεχής έλεγχος των κτιριακών εγκαταστάσεων	Μετεγκατάσταση του εξοπλισμού σε πιο σύγχρονες κτιριακές εγκαταστάσεις	Εγκατάσταση του εξοπλισμού σε χώρο αντισεισμικών προδιαγραφών	
66	Κίνδυνος πλημμύρας	Δημιουργία αντιπλημμυρικών έργων στο χώρο εγκατάστασης του εξοπλισμού	Τοποθέτηση του συστήματος σε σημείο υψηλότερο της επιφάνειας του εδάφους		
67	Κίνδυνος πυρκαγιάς	Ύπαρξη και συνεχής έλεγχος λειτουργικών πυροσβεστήρων σε όλους τους ορόφους του κτιρίου	Χρήση εξοπλισμού πυρανίχνευσης		
68	Κίνδυνος διαρροής υδάτων	Συνεχής έλεγχος και συντήρηση του δικτύου υδροδότησης	Μετεγκατάσταση του εξοπλισμού σε πιο σύγχρονες κτιριακές εγκαταστάσεις		
69	Κίνδυνος αδυναμίας ηλεκτροδότησης του συστήματος λόγω ελλείψεων στην ηλεκτρολογική εγκατάσταση	Συνεχής έλεγχος και συντήρηση του συστήματος ηλεκτροδότησης	Χρήση γεννητριών	Μετεγκατάσταση του εξοπλισμού σε πιο σύγχρονες κτιριακές εγκαταστάσεις	
72	Σκόνη	Τακτικός καθαρισμός του χώρου όπου βρίσκεται ο εξοπλισμό του συστήματος	Τοποθέτηση του εξοπλισμού σε ειδικό χώρο		
73	Βλάβη του συστήματος κλιματισμού	Τακτικός έλεγχος και συντήρηση του συστήματος κλιματισμού	Ύπαρξη εφεδρικού συστήματος κλιματισμού στους χώρους όπου βρίσκεται ο εξοπλισμός του συστήματος	Αλλαγή του συστήματος κλιματισμού	
75	Στατικός ηλεκτρισμός	Τακτικός έλεγχος του δικτύου ηλεκτροδότησης όπου στεγάζεται το πληροφοριακό σύστημα	Ύπαρξη πινάκων ασφαλείας όπου θα διακόπτουν την παροχή ρεύματος σε περίπτωση διαρροής ρεύματος και θα		

			γίνεται η ρευματοδότηση του συστήματος από γεννήτριες		
78	Κίνδυνος εκρήξεων	Έλεγχος των κτιριακών εγκαταστάσεων και του περιβάλλοντα χώρου για τυχόν εύφλεκτα υλικά όπου μπορεί να προκαλέσουν εκρήξεις και απομάκρυνση αυτών από το χώρο	Αποθήκευση των δεδομένων του συστήματος και σε άλλους servers σε άλλες περιοχές	Μετεγκατάσταση του εξοπλισμού σε άλλες κτιριακές εγκαταστάσεις	
79	Έντομα –τρωκτικά	Τακτικός έλεγχος των κτιριακών εγκαταστάσεων και συχνή απολύμανση του χώρου όπου στεγάζεται το πληροφοριακό για τυχόν έντομα και τρωκτικά	Εγκατάσταση ειδικού εξοπλισμού όπου αποτρέπει τα έντομα και τρωκτικά να εισχωρήσουν στο χώρο	Ύπαρξη εφεδρικού εξοπλισμού σε περίπτωση φθοράς του υπάρχοντος	
80	Κίνδυνος δονήσεων	Εγκατάσταση του πληροφοριακού συστήματος σε κτίριο όπου έχει αντικραδασμική λειτουργία		Μετεγκατάσταση του εξοπλισμού σε άλλες κτιριακές εγκαταστάσεις όπου βρίσκονται σε περιοχή με μειωμένη κραδασμική δραστηριότητα	
81	Καπνός – Μικροσωματίδια	Τακτικός έλεγχος και συντήρηση του συστήματος εξαερισμού καθώς και τοποθέτηση του εξοπλισμού σε ειδικό χώρο		Μετεγκατάσταση του εξοπλισμού σε άλλες κτιριακές εγκαταστάσεις όπου βρίσκονται σε περιοχή με λιγότερο καπνό και ρύπους	
82	Μαγνήτες – μαγνητικά εργαλεία	Τοποθέτηση πινακίδας απαγόρευσης όπου δεν θα επιτρέπει την είσοδο μαγνητών και μαγνητικών εργαλείων στο χώρο όπου βρίσκονται οι servers του συστήματος	Τοποθέτηση αισθητήρων ανίχνευσης μαγνητικών εργαλείων στην είσοδο του χώρου όπου βρίσκονται οι servers του συστήματος	Επιβολή ποινών σε όποιον δεν συμμορφώνεται με τους κανονισμούς	

88	Κλοπή υλικού	Εγκατάσταση καμερών στους χώρους όπου βρίσκεται ο εξοπλισμός	Συνεχής παρακολούθηση του χώρου όλο το 24ώρο	Ύπαρξη εφεδρικού εξοπλισμού	
89	Βανδαλισμοί	Εγκατάσταση καμερών και συνεχή παρακολούθηση των εισόδων του κτιρίου όπου στεγάζεται το πληροφοριακό σύστημα	Έλεγχος των ατόμων που εισέρχονται στο κτίριο επιδεικνύοντας κάποιο αποδεικτικό στοιχείο (π.χ. ΑΔΤ)	Μετεγκατάσταση του εξοπλισμού σε άλλες κτιριακές εγκαταστάσεις	
95	Τρομοκρατικές ενέργειες	Συνεχής έλεγχος των εγκαταστάσεων όπου βρίσκεται ο εξοπλισμός για τυχόν εύρεση ύποπτων αντικειμένων εντός και εκτός του χώρου καθώς και ύποπτων συμπεριφορών των εργαζομένων	Χρήση ειδικού εξοπλισμού ανίχνευσης μετάλλων στην είσοδο του κτιρίου	Μετεγκατάσταση του εξοπλισμού σε άλλες κτιριακές εγκαταστάσεις	

Πίνακας 11: Μητρώο κινδύνων–Μείωση/Μετριασμός κινδύνων συστήματος Fleetbroadband Provisioning System

Πιο αναλυτικά, στα παραπάνω πεδία συμπληρώνονται τα εξής στοιχεία:

- στο πεδίο «σχέδιο αποφυγής» καταγράφονται οι ενέργειες που πρέπει να γίνουν εφ’ όσον ο η στρατηγική του κινδύνου είναι η αποφυγή
- στο πεδίο «σχέδιο μεταφοράς» καταγράφονται οι ενέργειες που πρέπει να γίνουν εφ’ όσον ο η στρατηγική του κινδύνου είναι η μεταφορά
- στο πεδίο «σχέδιο αποδοχής» καταγράφονται οι ενέργειες που πρέπει να γίνουν εφ’ όσον ο η στρατηγική του κινδύνου είναι η αποδοχή

#	Κίνδυνοι	Σχέδιο Αποφυγής	Σχέδιο Μεταφοράς	Σχέδιο Αποδοχής
1	Ασυμβατότητα λογισμικού με τις απαιτήσεις		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
2	Εξάντληση πόρων του συστήματος	Συνεχής έλεγχος για έγκαιρη διάγνωση του κινδύνου, άμεσες κινήσεις για την αύξηση των πόρων του συστήματος		
3	Λανθασμένη βάση δεδομένων αποθήκευσης των στοιχείων		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
4	Ελλιπής ασφάλεια των προσωπικών δεδομένων των πολιτών		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
5	Δυσκολία σε αναβάθμιση – συντήρηση λογισμικού		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
6	Έλλειψη διασυνδεσιμότητας του φορέων μέσω του συστήματος		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
7	Λανθασμένος σχεδιασμός υλικού του συστήματος		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
8	Λανθασμένος σχεδιασμός λογισμικού του συστήματος		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
9	Ασυμβατότητα της τεχνολογίας του λογισμικού με τις υπάρχουσες κρατικές υποδομές ροής πληροφοριών		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
10	Χρήση νέων και μη δοκιμασμένων τεχνολογιών ανάπτυξης λογισμικού		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
11	Μη αποδεκτή ποιότητα λογισμικού		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
12	Ελλιπείς μηχανισμοί ελέγχου ασφάλειας του πληροφοριακού συστήματος		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
13	Αδυναμία σύνδεσης με τον κεντρικό Η/Υ εξαιτίας υπερφόρτωσης των τηλεπικοινωνιακών δικτύων ή εξαιτίας της μειωμένης αξιοπιστίας του δικτύου	Αποθήκευσης των δεδομένων και των προγραμμάτων του πληροφοριακού συστήματος σε περιβάλλον cloud		
14	Ανεπαρκής προστασία κρυπτογραφικών κλειδιών		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
15	Ελλιπής επικύρωση της επεξεργασίας των δεδομένων		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
16	Δυσλειτουργία του υλικού			Τακτικός έλεγχος και συντήρηση του υλικού καθώς και ύπαρξη εφεδρικού

				υλικού ώστε να αποφευχθεί ο κίνδυνος
17	Ανεπαρκής έλεγχος λογισμικού		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
18	Σφάλματα λογισμικού		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
19	Πολυπλοκότητα λογισμικού		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
20	Μη ασφαλής αρχιτεκτονική δικτύου		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
22	Μη επαρκώς καθορισμένοι όροι του συμβολαίου μεταξύ του κράτους και του αναδόχου	Σύνταξη του συμβολαίου από έμπειρα στελέχη		
23	Μη διαθεσιμότητα ομάδας υποστήριξης του συστήματος		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
26	Ελλιπής χρόνος προσαρμογής χρήσης του νέου πληροφοριακού συστήματος			Έλεγχος της απόδοσης των χρηστών και συνεχής εκπαίδευση σε νέες τεχνολογίες
27	Ανεπαρκής ή λανθασμένος διαχωρισμός των καθηκόντων		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
28	Ανεπαρκής επίβλεψη εργαζομένων		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
29	Ελλιπής διαδικασία για την αφαίρεση δικαιωμάτων πρόσβασης κατά την λήξη της απασχόλησης	Έλεγχος των ατόμων που συνδέονται καθημερινά στο σύστημα και είναι εν ενεργεία		
30	Ελλιπής σχεδιασμό τακτικών ελέγχων εύρυθμης λειτουργίας του λογισμικού		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
31	Κίνδυνος εσφαλμένης εγκατάστασης υλικού ή λογισμικού από το προσωπικό της αναδόχου εταιρείας		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
35	Έλλειψη οικονομικών πόρων	Δέσμευση κεφαλαίων για την κατασκευή του έργου		
36	Προβλήματα με την χρηματοδότηση του έργου	Δέσμευση κεφαλαίων για την κατασκευή του έργου		
38	Κλοπή υλικού από εργαζομένους	Τακτικός έλεγχος του καταγεγραμμένου υλικού για τυχόν απώλειες		
41	Καταστροφή εξοπλισμού από υγρά/τρόφιμα	Ενημέρωση όλων των εργαζομένων για την απαγόρευση		

		ποτών και τροφίμων στους χώρους όπου βρίσκεται ο εξοπλισμός		
44	Μη εξουσιοδοτημένη πρόσβαση στο πληροφοριακό σύστημα από τους εργαζόμενους		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
46	Μη εξουσιοδοτημένες αλλαγές αρχείων		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
47	Ακούσια αλλαγή των δεδομένων του πληροφοριακού συστήματος			Περιοδική ταυτοποίηση ενός δείγματος δεδομένων και έλεγχος των αποτελεσμάτων
50	Σύνδεση προσωπικών συσκευών στο εταιρικό δίκτυο			Ενημέρωση των εργαζομένων να ελέγχουν πρώτα κάθε συσκευή που πρόκειται να συνδέσουν στο εταιρικό δίκτυο για τυχόν κακόβουλο λογισμικό
51	Εγκατάσταση μη εξουσιοδοτημένου λογισμικού και εφαρμογών		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
55	Λάθος κατανομή του κεφαλαίου		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
56	Λανθασμένη κατανομή σημαντικότητας στις εφαρμογές του συστήματος		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
57	Έλλειψη εφεδρικού σχεδίου απρόσκοπτης λειτουργίας του συστήματος		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
58	Λανθασμένη πρόβλεψη απαιτούμενων πόρων υλικού	Συνεχής έλεγχος του σχεδιασμού του συστήματος για έγκαιρη διάγνωση του κινδύνου, άμεσες κινήσεις για την αύξηση των πόρων υλικού		
59	Αλλαγή του χρονοδιαγράμματος λόγω λανθασμένου αρχικού προγραμματισμού		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
60	Λανθασμένη κοστολόγηση του έργου		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
61	Κοινή χρήση εμπιστευτικών δεδομένων με τους συνεργάτες και τους προμηθευτές		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
65	Κίνδυνος κεραυνού	Χρήση ειδικού εξοπλισμού για την αποφυγή κεραυνών		

		(αλεξικέραυνο)		
70	Κατολίσθηση – διάβρωση εδάφους			Εύρεση νέων κτιριακών εγκαταστάσεων για τη στέγαση του πληροφοριακού συστήματος
71	Ηλιακές εκλάμψεις			Αποθήκευσης των δεδομένων και των προγραμμάτων του πληροφοριακού συστήματος σε περιβάλλον cloud
74	Ηλεκτρομαγνητικές παρεμβολές			Αποθήκευσης των δεδομένων και των προγραμμάτων του πληροφοριακού συστήματος σε περιβάλλον cloud
76	Έκρηξη ηφαιστείου	Εγκατάσταση του πληροφοριακού συστήματος σε περιοχή που δεν είναι ηφαιστειογενής		
77	Πυρηνικό ατύχημα	Εγκατάσταση του πληροφοριακού συστήματος σε περιοχή όπου δεν υπάρχουν πυρηνικά εργοστάσια		
83	Αγωγές – Μηνύσεις		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
84	Απώλεια καλής φήμης		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
85	Κλοπή πνευματικής ιδιοκτησίας		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
86	Αλλαγή σχεδιασμού συστήματος ή ματαίωση κατασκευής του λόγω πολιτικών αποφάσεων			Συμμετοχή των πολιτικών δυνάμεων στην απόφαση κατασκευής του συστήματος
87	Κίνδυνος καταστροφής του πληροφοριακού συστήματος λόγω πολιτικής αστάθειας			Συμμετοχή των πολιτικών δυνάμεων στην απόφαση να μην

				επηρεαστεί το έργο
90	Εισβολείς (Hackers) – Υποκλοπή δεδομένων		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
91	Εισβολείς (Hackers) – Καταστροφή δεδομένων		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
92	Ηλεκτρονικοί εγκληματίες (Μετάδοση κακόβουλου λογισμικού)		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
93	Πρώην εργαζόμενοι που εργάζονται για ανταγωνιστές			Όρος στο συμβόλαιο με τον εργαζόμενο για τη μη γνωστοποίηση σε τρίτους των εφαρμογών που κατασκευάζονται στην εταιρεία
94	Κατασκοπεία		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	

Πίνακας 12: Μητρώο κινδύνων–Αποφυγή, Μεταφορά, Αποδοχή κινδύνων συστήματος Fleetbroadband Provisioning System

6.6 Έλεγχος και παρακολούθηση κινδύνων

Στη φάση αυτή η ομάδα διαχείρισης κινδύνων πρέπει να παρακολουθεί τους κινδύνους που έχει προσδιορίσει, αναλύσει και αξιολογήσει ώστε να δει αν κάποιος κίνδυνος έχει αλλάξει μορφή και πρέπει να αλλάξει τη στρατηγική αντιμετώπισης που είχε ορίσει αρχικά. Επίσης, πρέπει να ελέγχει και να επαναλαμβάνει τη διαδικασία διαχείρισης των κινδύνων ώστε να είναι σε θέσει να εντοπίσει πιθανούς νέους κινδύνους που μπορεί να έχουν προκύψει.

Τέλος, ενημερώνει το μητρώο κινδύνων με τη συχνότητα που πρέπει να παρακολουθείται ο κάθε κίνδυνος, με την κατάσταση στην οποία βρίσκεται αυτός και με την ημερομηνία κλεισίματος, εφ' όσον κάποιος κίνδυνος θεωρείται ότι είτε έχει επέλθει και έχει περάσει είτε ότι δεν πρόκειται να συμβεί.

Πιο αναλυτικά, στα παραπάνω πεδία συμπληρώνονται τα εξής στοιχεία:

- στο πεδίο «παρακολούθηση» καταγράφεται η συχνότητα με την οποία πρέπει να παρακολουθείται ο κάθε κίνδυνος
- στο πεδίο «κατάσταση» καταγράφεται η κατάσταση του κινδύνου, αν δηλαδή είναι ανοιχτή (δεν έχει ακόμα συμβεί ο κίνδυνος), αν είναι κλειστή (έχει συμβεί ο κίνδυνος) ή αν είναι τελειωμένη (έχει ξεπεραστεί ο κίνδυνος).
- στο πεδίο «ημερομηνία κλεισίματος» καταγράφεται η ημερομηνία που έκλεισε ο κίνδυνος, εφ' όσον η κατάστασή του είναι κλειστή
- στο πεδίο «ημερομηνία ελέγχου» καταγράφεται η ημερομηνία που έγινε ο έλεγχος και η παρακολούθηση του κάθε κινδύνου

#	Κίνδυνοι	Παρακολούθηση	Κατάσταση	Ημερομηνία κλεισίματος	Ημερομηνία ελέγχου
1	Ασυμβατότητα λογισμικού με τις απαιτήσεις	1 φορά στον αρχικό σχεδιασμό	Τελειωμένη		24/02/2016
2	Εξάντληση πόρων του συστήματος	Μηνιαία	Ανοιχτή		24/02/ 2016
3	Λανθασμένη βάση δεδομένων αποθήκευσης των στοιχείων	1 φορά στον αρχικό σχεδιασμό	Τελειωμένη		24/02/2016
4	Ελλιπής ασφάλεια των προσωπικών δεδομένων των πολιτών	Κάθε μέρα	Ανοιχτή		24/02/2016
5	Δυσκολία σε αναβάθμιση – συντήρηση λογισμικού	Εφόσον προκύψει	Ανοιχτή		24/02/2016
6	Έλλειψη διασυνδεσιμότητας του φορέων μέσω του συστήματος	Κάθε μέρα	Ανοιχτή		24/02/2016
7	Λανθασμένος σχεδιασμός υλικού του συστήματος	1 φορά στον αρχικό σχεδιασμό	Τελειωμένη		24/02/2016
8	Λανθασμένος σχεδιασμός λογισμικού του συστήματος	1 φορά στον αρχικό σχεδιασμό	Τελειωμένη		24/02/2016
9	Ασυμβατότητα της τεχνολογίας του λογισμικού με τις υπάρχουσες κρατικές υποδομές ροής πληροφοριών	Εφόσον προκύψει	Κλειστή	2015	24/02/2016
10	Χρήση νέων και μη δοκιμασμένων τεχνολογιών ανάπτυξης λογισμικού	1 φορά στον αρχικό σχεδιασμό	Τελειωμένη		24/02/2016
11	Μη αποδεκτή ποιότητα λογισμικού	1 φορά στον αρχικό σχεδιασμό	Τελειωμένη		24/02/2016
12	Ελλιπείς μηχανισμοί ελέγχου ασφάλειας του πληροφοριακού συστήματος	Μηνιαία	Ανοιχτή		24/02/2016
13	Αδυναμία σύνδεσης με τον κεντρικό Η/Υ εξαιτίας υπερφόρτωσης των τηλεπικοινωνιακών δικτύων ή εξαιτίας της μειωμένης αξιοπιστίας του δικτύου	Κάθε μέρα	Ανοιχτή		24/02/2016
14	Ανεπαρκής προστασία κρυπτογραφικών κλειδιών	Μηνιαία	Ανοιχτή		24/02/2016
15	Ελλιπής επικύρωση της επεξεργασίας των δεδομένων	1 φορά στον αρχικό σχεδιασμό	Τελειωμένη		24/02/2016
16	Δυσλειτουργία του υλικού	Κάθε 2 μήνες έλεγχος και συντήρηση του υλικού	Κλειστή	2015	24/02/2016
17	Ανεπαρκής έλεγχος λογισμικού	Εφόσον προκύψει	Κλειστή	2015	24/02/2016
18	Σφάλματα λογισμικού	Εφόσον προκύψει	Κλειστή	2015	24/02/2016

19	Πολυπλοκότητα λογισμικού	Εφόσον προκύψει	Κλειστή	2015	24/02/2016
20	Μη ασφαλής αρχιτεκτονική δικτύου	1 φορά στον αρχικό σχεδιασμό	Τελειωμένη		24/02/2016
21	Προβλήματα επικοινωνίας με την εταιρεία ανάθεσης έργου	Εφόσον προκύψει	Κλειστή	2015	24/02/2016
22	Μη επαρκώς καθορισμένοι όροι του συμβολαίου μεταξύ του κράτους και του αναδόχου	1 φορά στην αρχική σύναψη του έργου	Τελειωμένη		24/02/2016
23	Μη διαθεσιμότητα ομάδας υποστήριξης του συστήματος	1 φορά στην αρχική σύναψη του έργου	Τελειωμένη		24/02/2016
24	Έλλειψη συνεργασίας μεταξύ των ομάδων κατασκευής του έργου.	Έλεγχος κάθε μήνα για τη συνεργασία που υπάρχει μεταξύ των ομάδων	Κλειστή	2015	24/02/2016
25	Ελλιπής φύλαξη του κτιρίου όπου στεγάζεται το πληροφοριακό σύστημα από εξειδικευμένα άτομα(φύλακες)	Κάθε μέρα	Ανοιχτή		24/02/2016
26	Ελλιπής χρόνος προσαρμογής χρήσης του νέου πληροφοριακού συστήματος	Εφόσον προκύψει	Κλειστή	2015	24/02/2016
27	Ανεπαρκής ή λανθασμένος διαχωρισμός των καθηκόντων	Εξαμηνιαίος έλεγχος στις αναφορές που θα υπάρχουν από κάθε εργαζόμενο για το έργο που έχει υλοποιήσει	Κλειστή	2015	24/02/2016
28	Ανεπαρκής επίβλεψη εργαζομένων	Μηνιαίος έλεγχος για το αν έχουν υλοποιηθεί οι στόχοι του προηγούμενου μήνα	Ανοιχτή		24/02/2016
29	Ελλιπής διαδικασία για την αφαίρεση δικαιωμάτων πρόσβασης κατά την λήξη της απασχόλησης	1 φορά στον αρχικό σχεδιασμό	Τελειωμένη		24/02/2016
30	Ελλιπής σχεδιασμό τακτικών ελέγχων εύρυθμης λειτουργίας του λογισμικού	1 φορά στον αρχικό σχεδιασμό	Τελειωμένη		24/02/2016
31	Κίνδυνος εσφαλμένης εγκατάστασης υλικού ή λογισμικού από το προσωπικό της αναδόχου εταιρείας	1 φορά στον αρχικό σχεδιασμό	Τελειωμένη		24/02/2016
32	Ανεπαρκής κάλυψη του κτιρίου από σύστημα συναγερμού	Κάθε μέρα	Ανοιχτή		24/02/2016
33	Ανεπαρκής κάλυψη του κτιρίου από σύστημα πυρανίχνευσης	Μηνιαία	Ανοιχτή		24/02/2016
34	Ανεπαρκής κάλυψη του κτιρίου από σύστημα αναγνώρισης και ελέγχου ταυτότητας	Κάθε μέρα	Ανοιχτή		24/02/2016

35	Έλλειψη οικονομικών πόρων	Εφόσον προκύψει	Ανοιχτή		24/02/2016
36	Προβλήματα με την χρηματοδότηση του έργου	Εφόσον προκύψει	Ανοιχτή		24/02/2016
37	Καταστροφή υλικού ή λογισμικού από τους χειριστές του συστήματος	Κάθε μέρα	Ανοιχτή		24/02/2016
38	Κλοπή υλικού από εργαζομένους	Κάθε μέρα	Ανοιχτή		24/02/2016
39	Απεργίες εργαζομένων που διαχειρίζονται το πληροφοριακό σύστημα	Εφόσον προκύψει	Κλειστή	2015	24/02/2016
40	Κίνδυνος απροθυμίας προσαρμογής στην αλλαγή	Εφόσον προκύψει	Κλειστή	2015	24/02/2016
41	Καταστροφή εξοπλισμού από υγρά/τρόφιμα	Κάθε μέρα	Ανοιχτή		24/02/2016
42	Διαρροή πληροφοριών	Κάθε μέρα	Ανοιχτή		24/02/2016
43	Μη εξουσιοδοτημένη πρόσβαση στους χώρους του πληροφοριακού συστήματος	Κάθε μέρα	Ανοιχτή		24/02/2016
44	Μη εξουσιοδοτημένη πρόσβαση στο πληροφοριακό σύστημα από τους εργαζόμενους	Κάθε μέρα	Ανοιχτή		24/02/2016
45	Διαρροή κωδικών εισόδου και διαχείρισης του πληροφοριακού συστήματος	Κάθε μέρα	Ανοιχτή		24/02/2016
46	Μη εξουσιοδοτημένες αλλαγές αρχείων	1 φορά στον αρχικό σχεδιασμό	Τελειωμένη		24/02/2016
47	Ακούσια αλλαγή των δεδομένων του πληροφοριακού συστήματος	Μηνιαία	Ανοιχτή		24/02/2016
48	Έλλειψη κινήτρων για τους εργαζόμενους	Εφόσον προκύψει	Ανοιχτή		24/02/2016
49	Έλλειψη ευαισθητοποίησης σε θέματα ασφάλειας	Εφόσον προκύψει	Ανοιχτή		24/02/2016
50	Σύνδεση προσωπικών συσκευών στο εταιρικό δίκτυο	Κάθε μέρα	Ανοιχτή		24/02/2016
51	Εγκατάσταση μη εξουσιοδοτημένου λογισμικού και εφαρμογών	1 φορά στον αρχικό σχεδιασμό	Τελειωμένη		24/02/2016
52	Ακούσια μεταφορά εμπιστευτικών δεδομένων του πληροφοριακού συστήματος εκτός γραφείου	Κάθε μέρα	Ανοιχτή		24/02/2016
53	Έλλειψη της απαιτούμενης εκπαίδευσης του προσωπικού	Ετήσια	Ανοιχτή		24/02/2016
54	Εσωτερικοί κίνδυνοι (δόλος)	Κάθε μέρα	Ανοιχτή		24/02/2016
55	Λάθος κατανομή του κεφαλαίου	1 φορά στον αρχικό σχεδιασμό	Τελειωμένη		24/02/2016
56	Λανθασμένη κατανομή σημαντικότητας στις εφαρμογές του συστήματος	1 φορά στον αρχικό σχεδιασμό	Τελειωμένη		24/02/2016

57	Έλλειψη εφεδρικού σχεδίου απρόσκοπτης λειτουργίας του συστήματος	1 φορά στον αρχικό σχεδιασμό	Τελειωμένη		24/02/2016
58	Λανθασμένη πρόβλεψη απαιτούμενων πόρων υλικού	1 φορά στον αρχικό σχεδιασμό	Τελειωμένη		24/02/2016
59	Αλλαγή του χρονοδιαγράμματος λόγω λανθασμένου αρχικού προγραμματισμού	Μηνιαία μέχρι την ολοκλήρωση του έργου	Ανοιχτή		24/02/2016
60	Λανθασμένη κοστολόγηση του έργου	Μηνιαία μέχρι την ολοκλήρωση του έργου	Ανοιχτή		24/02/2016
61	Κοινή χρήση εμπιστευτικών δεδομένων με τους συνεργάτες και τους προμηθευτές	1 φορά στον αρχικό σχεδιασμό	Ανοιχτή		24/02/2016
62	Έλλειψη εμπειρίας και τεχνογνωσίας των προσώπων που είναι υπεύθυνα για την παρακολούθηση της υλοποίησης του έργου	Εφόσον προκύψει	Ανοιχτή		24/02/2016
63	Λανθασμένες αποφάσεις διαχείρησης κινδύνων	Εφόσον προκύψει	Ανοιχτή		24/02/2016
64	Κίνδυνος σεισμού	Εφόσον προκύψει	Ανοιχτή		24/02/2016
65	Κίνδυνος κεραυνού	Εφόσον προκύψει	Ανοιχτή		24/02/2016
66	Κίνδυνος πλημμύρας	Εφόσον προκύψει	Ανοιχτή		24/02/2016
67	Κίνδυνος πυρκαγιάς	Εφόσον προκύψει	Ανοιχτή		24/02/2016
68	Κίνδυνος διαρροής υδάτων	Εφόσον προκύψει	Ανοιχτή		24/02/2016
69	Κίνδυνος αδυναμίας ηλεκτροδότησης του συστήματος λόγω ελλείψεων στην ηλεκτρολογική εγκατάσταση	Μηνιαία	Ανοιχτή		24/02/2016
70	Κατολίσθηση – διάβρωση εδάφους	Εφόσον προκύψει	Ανοιχτή		24/02/2016
71	Ηλιακές εκλάμψεις	Εφόσον προκύψει	Ανοιχτή		24/02/2016
72	Σκόνη	Εβδομαδιαία	Ανοιχτή		24/02/2016
73	Βλάβη του συστήματος κλιματισμού	Μηνιαία	Ανοιχτή		20/02/2016
74	Ηλεκτρομαγνητικές παρεμβολές	Εφόσον προκύψει	Ανοιχτή		24/02/2016
75	Στατικός ηλεκτρισμός	Μηνιαία	Ανοιχτή		24/02/2016
76	Έκρηξη ηφαιστείου	Εφόσον προκύψει	Ανοιχτή		24/02/2016
77	Πυρηνικό ατύχημα	Εφόσον προκύψει	Ανοιχτή		24/02/2016
78	Κίνδυνος εκρήξεων	Εφόσον προκύψει	Ανοιχτή		24/02/2016
79	Έντομα –τρωκτικά	Εξαμηνιαία	Ανοιχτή		24/02/2016
80	Κίνδυνος δονήσεων	Εφόσον προκύψει	Ανοιχτή		24/02/2016
81	Καπνός – Μικροσωματίδια	Εφόσον προκύψει	Ανοιχτή		24/02/2016
82	Μαγνήτες – μαγνητικά εργαλεία	Εφόσον προκύψει	Ανοιχτή		24/02/2016
83	Αγωγές – Μηνύσεις	Εφόσον προκύψει	Ανοιχτή		24/02/2016
84	Απώλεια καλής φήμης	Εφόσον προκύψει	Ανοιχτή		24/02/2016
85	Κλοπή πνευματικής ιδιοκτησίας	Εφόσον προκύψει	Ανοιχτή		24/02/2016

86	Αλλαγή σχεδιασμού συστήματος ή ματαίωση κατασκευής του λόγω πολιτικών αποφάσεων	Εφόσον προκύψει	Ανοιχτή		24/02/2016
87	Κίνδυνος καταστροφής του πληροφοριακού συστήματος λόγω πολιτικής αστάθειας	Εφόσον προκύψει	Ανοιχτή		24/02/2016
88	Κλοπή υλικού	Κάθε 2 μήνες	Ανοιχτή		24/02/2016
89	Βανδαλισμοί	Κάθε μέρα	Ανοιχτή		24/02/2016
90	Εισβολείς (Hackers) – Υποκλοπή δεδομένων	Κάθε μέρα	Ανοιχτή		24/02/2016
91	Εισβολείς (Hackers) – Καταστροφή δεδομένων	Κάθε μέρα	Ανοιχτή		24/02/2016
92	Ηλεκτρονικοί εγκληματίες (Μετάδοση κακόβουλου λογισμικού)	Κάθε μέρα	Ανοιχτή		24/02/2016
93	Πρώην εργαζόμενοι που εργάζονται για ανταγωνιστές	Εφόσον προκύψει	Ανοιχτή		24/02/2016
94	Κατασκοπεία	Κάθε μέρα	Ανοιχτή		24/02/2016
95	Τρομοκρατικές ενέργειες	Κάθε μέρα	Ανοιχτή		24/02/2016

Πίνακας 13: Μητρώο κινδύνων–Παρακολούθηση κινδύνων συστήματος Fleetbroadband Provisioning System

Κατά τη φάση του εντοπισμού των κινδύνων δημιουργούνται τα φύλλα κινδύνων (risk sheet). Το φύλλο κινδύνου είναι ουσιαστικά η ταυτότητα του κάθε κινδύνου, δημιουργείται κατά τον εντοπισμό του και αρχειοθετείται όταν ο κίνδυνος έχει παρέλθει ή εκλείψει. Το φύλλο κινδύνου περιέχει στοιχεία από όλες τις φάσεις διαχείρισης κινδύνων.

Στη συνέχεια παρουσιάζονται τα φύλλα των κινδύνων (Πίνακες 14- 108)

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #1				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Εξάντληση πόρων συστήματος			
Σύντομη Περιγραφή:	Εξάντληση των πόρων του συστήματος από την αυξημένη κίνηση των χρηστών του			
Κατηγορία Κινδύνου:	Τεχνολογικός			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.5	5	Y_6	18	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Στατιστικά χρήσης του συστήματος			
Προπομπός Κινδύνου:	Η χρήση του συστήματος έχει ανέλθει στο ανώτερο κατώφλι ασφάλειας που έχει τεθεί από τον εργολάβο (π.χ το 80% των πόρων του συστήματος)			
Στρατηγική Αντιμετώπισης:	Αποφυγή			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:	Συνεχής έλεγχος για έγκαιρη διάγνωση του κινδύνου, άμεσες κινήσεις για την αύξηση των πόρων του συστήματος			
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Μηνιαία			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 14: Φύλλο κινδύνου #1 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #2				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Ασυμβατότητα λογισμικού με τις απαιτήσεις			
Σύντομη Περιγραφή:	Το ήδη υπάρχον λογισμικό δεν ανταποκρίνεται στις απαιτήσεις του συστήματος			
Κατηγορία Κινδύνου:	Τεχνολογικός			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.5	5	Y_6	80	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος του τρόπου λειτουργίας των εκδόσεων του συστήματος			
Προπομπός Κινδύνου:	Κάποια έκδοση δεν λειτουργεί σωστά			
Στρατηγική Αντιμετώπισης:	Μεταφορά			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	1 φορά στον αρχικό σχεδιασμό			
Κατάσταση:	Τελειωμένη			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 15: Φύλλο κινδύνου #2 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #3				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Λανθασμένη βάση δεδομένων αποθήκευσης των στοιχείων			
Σύντομη Περιγραφή:	Λάθος ή ελλιπής δημιουργία της βάσης δεδομένων			
Κατηγορία Κινδύνου:	Τεχνολογικός			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.1	5	X_3	81	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος του τρόπου λειτουργίας των εκδόσεων του συστήματος			
Προπομπός Κινδύνου:	Κάποια έκδοση η βάση δεδομένων δεν λειτουργεί σωστά			
Στρατηγική Αντιμετώπισης:	Μεταφορά			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	1 φορά στον αρχικό σχεδιασμό			
Κατάσταση:	Τελειωμένη			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 16: Φύλλο κινδύνου #3 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #4				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Ελλιπής ασφάλεια προσωπικών δεδομένων των πολιτών			
Σύντομη Περιγραφή:	Έλλειψη μεθόδων προστασίας των προσωπικών δεδομένων - έλλειψη πρωτοκόλλων ασφαλείας με αποτέλεσμα την πιθανή υποκλοπή των προσωπικών δεδομένων των χρηστών			
Κατηγορία Κινδύνου:	Τεχνολογικός			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.9	5	Y_1	1	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος στις εκδόσεις των λογισμικών ασφαλείας			
Προπομπός Κινδύνου:	Υπάρχει ενδεχόμενο υποκλοπής κάποιων στοιχείων			
Στρατηγική Αντιμετώπισης:	Μεταφορά			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Κάθε μέρα			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 17: Φύλλο κινδύνου #4 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #5				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Δυσκολία σε αναβάθμιση – συντήρηση λογισμικού			
Σύντομη Περιγραφή:	Δημιουργία του κώδικα με μη δομημένο τρόπο με αποτέλεσμα την εμφάνιση δυσκολιών σε μελλοντικές αλλαγές και στην προσθήκη νέων λειτουργιών			
Κατηγορία Κινδύνου:	Τεχνολογικός			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.3	4	M_6	54	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση του σχεδιασμού και των τεχνικών προδιαγραφών υλοποίησης του συστήματος			
Προπομπός Κινδύνου:	Εμφάνιση αυξημένης πολυπλοκότητας στην αρχιτεκτονική σχεδιασμού και δυσκολία εισαγωγής νέων χαρακτηριστικών			
Στρατηγική Αντιμετώπισης:	Μεταφορά			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 18: Φύλλο κινδύνου #5 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #6				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Έλλειψη διασυνδεσιμότητας των φορέων μέσω του συστήματος			
Σύντομη Περιγραφή:	Ελλιπής χρήση τεχνολογιών λογισμικού και πρωτοκόλλων για την διασυνδεσιμότητα μεταξύ των συσχετιζόμενων φορέων			
Κατηγορία Κινδύνου:	Τεχνολογικός			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.5	3	M_4	36	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Πρωτόκολλα επικοινωνίας			
Προπομπός Κινδύνου:	Αδυναμία διασύνδεσης με τα συστήματα των άλλων φορέων			
Στρατηγική Αντιμετώπισης:	Μεταφορά			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Κάθε μέρα			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 19: Φύλλο κινδύνου #6 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #7				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Λανθασμένος σχεδιασμός υλικού (αρχιτεκτονική συστήματος)			
Σύντομη Περιγραφή:	Ανεπαρκής σχεδιασμός υλικού σε επίπεδο αρχιτεκτονικής συστήματος			
Κατηγορία Κινδύνου:	Τεχνολογικός			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.1	5	X_3	82	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση των απαιτήσεων σχεδιασμού			
Προπομπός Κινδύνου:	Λανθασμένη υλοποίηση των απαιτήσεων σχεδιασμού			
Στρατηγική Αντιμετώπισης:	Μεταφορά			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	1 φορά στον αρχικό σχεδιασμό			
Κατάσταση:	Τελειωμένη			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 20: Φύλλο κινδύνου #7 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #8				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Λανθασμένος σχεδιασμός υλικού (αρχιτεκτονική συστήματος)			
Σύντομη Περιγραφή:	Ανεπαρκής σχεδιασμός υλικού σε επίπεδο αρχιτεκτονικής συστήματος			
Κατηγορία Κινδύνου:	Τεχνολογικός			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.1	5	X_3	82	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση των απαιτήσεων σχεδιασμού			
Προπομπός Κινδύνου:	Λανθασμένη υλοποίηση των απαιτήσεων σχεδιασμού			
Στρατηγική Αντιμετώπισης:	Μεταφορά			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	1 φορά στον αρχικό σχεδιασμό			
Κατάσταση:	Τελειωμένη			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 21: Φύλλο κινδύνου #8 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #9				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Ασυμβατότητα της τεχνολογίας του λογισμικού με τις υπάρχουσες κρατικές υποδομές ροής πληροφοριών			
Σύντομη Περιγραφή:	Επιλογή τεχνολογίας λογισμικού μη συμβατή με την υπάρχουσα δικτυακή υποδομή των συσχετιζόμενων φορέων			
Κατηγορία Κινδύνου:	Τεχνολογικός			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.3	5	M_4	46	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση τεχνολογίας ανάπτυξης λογισμικού			
Προπομπός Κινδύνου:	Αδυναμία αξιοποίησης στο μέγιστο των υποδομών ροής πληροφοριών			
Στρατηγική Αντιμετώπισης:	Μεταφορά			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Κλειστή			
Ημερομηνία Κλεισίματος:	2015			
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 22: Φύλλο κινδύνου #9 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #10				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Χρήση νέων και μη δοκιμασμένων τεχνολογιών ανάπτυξης λογισμικού			
Σύντομη Περιγραφή:	Επιλογή λογισμικού τελευταίας τεχνολογίας όπου δεν έχει ελεγχθεί εκτενώς όσον αφορά την ανάπτυξη αντίστοιχων εφαρμογών			
Κατηγορία Κινδύνου:	Τεχνολογικός			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.5	3	M_4	37	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση τεχνολογίας ανάπτυξης λογισμικού			
Προπομπός Κινδύνου:	Αδυναμία κάλυψης των λειτουργικών απαιτήσεων του συστήματος			
Στρατηγική Αντιμετώπισης:	Μεταφορά			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	1 φορά στον αρχικό σχεδιασμό			
Κατάσταση:	Τελειωμένη			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 23: Φύλλο κινδύνου #10 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #11				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Μη αποδεκτή ποιότητα λογισμικού			
Σύντομη Περιγραφή:	Η ποιότητα της εφαρμογής είναι χαμηλότερη των αποδεκτών ορίων που έχουν τεθεί και προβληματική για τους χρήστες			
Κατηγορία Κινδύνου:	Τεχνολογικός			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.5	3	M_4	38	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση των ποιοτικών χαρακτηριστικών του συστήματος			
Προπομπός Κινδύνου:	Απόκλιση από τα αποδεκτά όρια			
Στρατηγική Αντιμετώπισης:	Μεταφορά			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	1 φορά στον αρχικό σχεδιασμό			
Κατάσταση:	Τελειωμένη			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 24: Φύλλο κινδύνου #11 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #12				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Ελλιπείς μηχανισμοί ελέγχου ασφάλειας του λογισμικού του πληροφοριακού συστήματος			
Σύντομη Περιγραφή:	Ελλιπής χρήσης λογισμικού ασφαλείας και αυστηρών μέτρων προστασίας για την αποφυγή κακόβουλων ενεργειών και υποκλοπή προσωπικών δεδομένων			
Κατηγορία Κινδύνου:	Τεχνολογικός			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.1	5	X_3	84	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος του τρόπου λειτουργίας των εκδόσεων του λογισμικού ασφαλείας			
Προπομπός Κινδύνου:	Κάποια έκδοση του λογισμικού ασφαλείας δεν λειτουργεί σωστά με αποτέλεσμα την μετάδοση κακόβουλου λογισμικού			
Στρατηγική Αντιμετώπισης:	Μεταφορά			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Μηνιαία			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 25: Φύλλο κινδύνου #12 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #13				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Αδυναμία Σύνδεσης με τον κεντρικό Η/Υ εξαιτίας υπερφόρτωσης των τηλεπικοινωνιακών δικτύων ή εξαιτίας της μειωμένης αξιοπιστίας του δικτύου			
Σύντομη Περιγραφή:	Ανεπαρκής διαδικτυακός εξοπλισμός για την αποτελεσματική εξυπηρέτηση του αριθμού των συνδεδεμένων χρηστών σε περιπτώσεις υψηλού φόρτου			
Κατηγορία Κινδύνου:	Τεχνολογικός			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.5	4	M_2	24	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση χαρακτηριστικών του τηλεπικοινωνιακού δικτύου			
Προπομπός Κινδύνου:	Συνεχής υπερφόρτωση του δικτύου			
Στρατηγική Αντιμετώπισης:	Αποφυγή			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:	Αποθήκευσης των δεδομένων και των προγραμμάτων του πληροφοριακού συστήματος σε περιβάλλον cloud			
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Κάθε μέρα			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 26: Φύλλο κινδύνου #13 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #14				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Ανεπαρκής προστασία κρυπτογραφικών κλειδιών			
Σύντομη Περιγραφή:	Λανθασμένη χρήση τεχνικών κρυπτογραφίας κλειδιών			
Κατηγορία Κινδύνου:	Τεχνολογικός			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.3	4	M_6	55	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση των απαιτήσεων ασφάλειας στο σχεδιασμό του λογισμικού			
Προπομπός Κινδύνου:	Λανθασμένη υλοποίηση των απαιτήσεων ασφάλειας			
Στρατηγική Αντιμετώπισης:	Μεταφορά			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Μηνιαία			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 27: Φύλλο κινδύνου #14 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #15				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Ελλιπής επικύρωση της επεξεργασίας των δεδομένων			
Σύντομη Περιγραφή:	Λανθασμένος κώδικας για τον έλεγχό της επεξεργασίας των δεδομένων εισαγωγής			
Κατηγορία Κινδύνου:	Τεχνολογικός			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.3	4	M_6	56	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση του τρόπου επεξεργασίας των δεδομένων			
Προπομπός Κινδύνου:	Λανθασμένη επεξεργασία των δεδομένων			
Στρατηγική Αντιμετώπισης:	Μεταφορά			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	1 φορά στον αρχικό σχεδιασμό			
Κατάσταση:	Τελειωμένη			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 28: Φύλλο κινδύνου #15 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #16				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Δυσλειτουργία του υλικού			
Σύντομη Περιγραφή:	Αστοχία του υλικού που είναι αποθηκευμένο το πληροφοριακό σύστημα			
Κατηγορία Κινδύνου:	Τεχνολογικός			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.5	4	M_2	25	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση του τρόπου λειτουργίας του υλικού			
Προπομπός Κινδύνου:	Συνεχής υπερθέρμανση του συστήματος/ έντονος ήχος κατά τη λειτουργία του			
Στρατηγική Αντιμετώπισης:				
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:	Τακτικός έλεγχος και συντήρηση του υλικού καθώς και ύπαρξη εφεδρικού υλικού ώστε να αποφευχθεί ο κίνδυνος			
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Κάθε 2 μήνες έλεγχος και συντήρηση του υλικού			
Κατάσταση:	Κλειστή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 29: Φύλλο κινδύνου #16 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #17				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Ανεπαρκής έλεγχος λογισμικού			
Σύντομη Περιγραφή:	Ανεπαρκείς και ελλιπείς διαδικασίες ποιοτικού ελέγχου			
Κατηγορία Κινδύνου:	Τεχνολογικός			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.5	4	M_2	26	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση των απαιτήσεων ελέγχου του λογισμικού			
Προπομπός Κινδύνου:	Λανθασμένη υλοποίηση των απαιτήσεων ελέγχου			
Στρατηγική Αντιμετώπισης:	Μεταφορά			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Κλειστή			
Ημερομηνία Κλεισίματος:	2015			
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 30: Φύλλο κινδύνου #17 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #18				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Σφάλματα λογισμικού			
Σύντομη Περιγραφή:	Εμφάνιση μεγάλου αριθμού λαθών στον κώδικα του πληροφοριακού συστήματος			
Κατηγορία Κινδύνου:	Τεχνολογικός			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.5	5	Y_6	6	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος του τρόπου λειτουργίας των εκδόσεων του λογισμικού			
Προπομπός Κινδύνου:	Κάποια έκδοση του λογισμικού δεν παράγει τα αναμενόμενα αποτελέσματα			
Στρατηγική Αντιμετώπισης:	Μεταφορά			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψουν			
Κατάσταση:	Κλειστή			
Ημερομηνία Κλεισίματος:	2015			
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 31: Φύλλο κινδύνου #18 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #19				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Πολυπλοκότητα λογισμικού			
Σύντομη Περιγραφή:	Μη τήρηση συγκεκριμένης μεθοδολογίας για τη συγγραφή κώδικα του πληροφοριακού συστήματος			
Κατηγορία Κινδύνου:	Τεχνολογικός			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.5	3	M_4	39	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος στον σχεδιασμό του λογισμικού			
Προπομπός Κινδύνου:	Δυσκολία στην αναβάθμιση του λογισμικού			
Στρατηγική Αντιμετώπισης:	Μεταφορά			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Κλειστή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 32: Φύλλο κινδύνου #19 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #20				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Μη ασφαλής αρχιτεκτονική δικτύου			
Σύντομη Περιγραφή:	Ανεπαρκής επιλογή επιπέδων ασφάλειας διαδικτύου			
Κατηγορία Κινδύνου:	Τεχνολογικός			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.5	4	M_2	27	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση των απαιτήσεων ασφάλειας για το σχεδιασμό του δικτύου			
Προπομπός Κινδύνου:	Λανθασμένη υλοποίηση των απαιτήσεων ασφάλειας			
Στρατηγική Αντιμετώπισης:	Μεταφορά			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	1 φορά στον αρχικό σχεδιασμό			
Κατάσταση:	Τελειωμένη			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 33: Φύλλο κινδύνου #20 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #21				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Προβλήματα επικοινωνίας με την εταιρεία ανάθεσης έργου			
Σύντομη Περιγραφή:	Αδυναμία αποτελεσματικής επικοινωνίας με την εταιρεία ανάθεσης με αποτέλεσμα την επιβράδυνση των εργασιών για την κατασκευή του έργου			
Κατηγορία Κινδύνου:	Λειτουργικοί – Επιχειρησιακοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.5	2	M_7	25	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος της επικοινωνίας με την εταιρεία ανάθεσης έργου			
Προπομπός Κινδύνου:	Έλλειψη επικοινωνίας με την εταιρεία ανάθεσης έργου			
Στρατηγική Αντιμετώπισης:	Μετριασμός			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Συναντήσεις με την εταιρεία ανάθεσης έργου για επίτευξη καλύτερης επικοινωνίας			
Διορθωτικά μέτρα:	Ύπαρξη έγγραφων αναφορών για την αποφυγή παρερμηνεύσεων			
Εναλλακτικό σχέδιο:	Εφαρμογή των κυρώσεων που αναγράφονται στο συμβόλαιο			
Σχέδιο μετάπτωσης:	Ακύρωση του συμβολαίου με την εταιρεία ανάθεσης έργου και ανάθεση του έργου στον επόμενο μειοδότη			
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψουν			
Κατάσταση:	Κλειστή			
Ημερομηνία Κλεισίματος:	2015			
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 34: Φύλλο κινδύνου #21 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #22				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Μη επαρκώς καθορισμένοι όροι του συμβολαίου μεταξύ του κράτους και του αναδόχου			
Σύντομη Περιγραφή:	Ασάφειες και κενά στους όρους του συμβολαίου οδηγούν στην ανεπαρκή εφαρμογή των συμφωνηθέντων στην περίπτωση εμφάνισης προβλήματος			
Κατηγορία Κινδύνου:	Λειτουργικοί – Επιχειρησιακοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.5	2	M_7	71	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση της διαδικασίας καθορισμού των όρων του συμβολαίου			
Προπομπός Κινδύνου:	Ύπαρξη ασαφειών μεταξύ των όρων του συμβολαίου			
Στρατηγική Αντιμετώπισης:	Αποφυγή			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:	Σύνταξη του συμβολαίου από έμπειρα στελέχη			
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	1 φορά στην αρχική σύναψη του συμβολαίου			
Κατάσταση:	Τελειωμένη			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 35: Φύλλο κινδύνου #22 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #23				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Μη διαθεσιμότητα ομάδας υποστήριξης του συστήματος			
Σύντομη Περιγραφή:	Ανεπαρκής αριθμός ατόμων για την υποστήριξη του συστήματος λόγω κόστους σε ανθρώπινο δυναμικό			
Κατηγορία Κινδύνου:	Λειτουργικοί – Επιχειρησιακοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.5	4	M_2	28	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση ανταπόκρισης της ομάδα υποστήριξης του συστήματος σε περίπτωση ανάγκης			
Προπομπός Κινδύνου:	Προβληματική υποστήριξη του συστήματος			
Στρατηγική Αντιμετώπισης:	Μεταφορά			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	1 φορά στην αρχική σύναψη του συμβολαίου			
Κατάσταση:	Τελειωμένη			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 36: Φύλλο κινδύνου #23 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #24				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Έλλειψη συνεργασίας μεταξύ των ομάδων κατασκευής του έργου			
Σύντομη Περιγραφή:	Προβλήματα επικοινωνίας και καταμερισμού εργασιών των ομάδων ανάπτυξης λογισμικού με αποτέλεσμα τη δημιουργία εντάσεων μεταξύ των ατόμων και την διακοπή της ομαλής εξέλιξης του έργου			
Κατηγορία Κινδύνου:	Λειτουργικοί – Επιχειρησιακοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.5	3	M_4	40	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση της επικοινωνίας μεταξύ των ομάδων			
Προπομπός Κινδύνου:	Προβληματική συνεργασία μεταξύ των ομάδων			
Στρατηγική Αντιμετώπισης:	Μετριασμός			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Συνεχής επικοινωνία μεταξύ των ομάδων κατασκευής του έργου			
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:	Συγκέντρωση των ομάδων κατασκευής στον ίδιο χώρο			
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Έλεγχος κάθε μήνα για τη συνεργασία που υπάρχει μεταξύ των ομάδων			
Κατάσταση:	Κλειστή			
Ημερομηνία Κλεισίματος:	2015			
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 37: Φύλλο κινδύνου #24 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #25				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Ελλιπής φύλαξη του κτιρίου όπου στεγάζεται το πληροφοριακό σύστημα από εξειδικευμένα άτομα(φύλακες)			
Σύντομη Περιγραφή:	Η έλλειψη φύλαξης ενός κτηρίου από άτομο επιπλέον των τεχνικών μέσων μπορεί να έχει ως αποτέλεσμα την μη έγκαιρη αντιμετώπιση οποιασδήποτε πιθανή καταστροφής του κτηρίου όπου στεγάζεται το πληροφοριακό σύστημα			
Κατηγορία Κινδύνου:	Λειτουργικοί – Επιχειρησιακοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.3	5	M_4	47	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση της ασφάλειας του κτιρίου			
Προπομπός Κινδύνου:	Εμφάνιση φαινομένων εισβολής			
Στρατηγική Αντιμετώπισης:	Μετριασμός			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Πρόσληψη προσωπικού για τη φύλαξη του κτιρίου όπου στεγάζεται το πληροφοριακό σύστημα			
Διορθωτικά μέτρα:	Πρόσληψη ειδικά εκπαιδευμένου προσωπικού			
Εναλλακτικό σχέδιο:	Χρήση ειδικού εξοπλισμού παρακολούθησης του κτιρίου όπου στεγάζεται το πληροφοριακό σύστημα (κάμερες ασφαλείας)			
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Κάθε μέρα			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 38: Φύλλο κινδύνου #25 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #26				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Ελλιπής χρόνος προσαρμογής χρήσης του νέου πληροφοριακού συστήματος			
Σύντομη Περιγραφή:	Δεν έχει δοθεί αρκετό χρονικό διάστημα για την εξοικείωση των χρηστών με το νέο λογισμικό με αποτέλεσμα την προβληματική εξυπηρέτηση των πελατών			
Κατηγορία Κινδύνου:	Λειτουργικοί – Επιχειρησιακοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.7	2	M_5	52	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος του χρόνου προσαρμογής των χρηστών			
Προπομπός Κινδύνου:	Απόκλιση από τον προβλεπόμενο χρόνο Προσαρμογής			
Στρατηγική Αντιμετώπισης:	Αποδοχή			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:	Έλεγχος της απόδοσης των χρηστών και συνεχής εκπαίδευση σε νέες τεχνολογίες			
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Κλειστή			
Ημερομηνία Κλεισίματος:	2015			
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 39: Φύλλο κινδύνου #26 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #27				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Ανεπαρκής ή λανθασμένος διαχωρισμός των καθηκόντων			
Σύντομη Περιγραφή:	Ελλιπής ή λανθασμένη επιλογή ατόμων για την υλοποίηση μερών του πληροφοριακού συστήματος			
Κατηγορία Κινδύνου:	Λειτουργικοί – Επιχειρησιακοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.7	3	M_1	22	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος και αξιολόγηση των εργαζομένων του συστήματος σύμφωνα με τα προσόντα και τις γνώσεις τους			
Προπομπός Κινδύνου:	Λανθασμένη υλοποίηση του συστήματος και μη σωστή λειτουργία των ομάδων που συνεργάζονται για την υλοποίηση του συστήματος			
Στρατηγική Αντιμετώπισης:	Μεταφορά			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εξαμηνιαίος έλεγχος στις αναφορές που θα υπάρχουν από κάθε εργαζόμενο για το έργο που έχει υλοποιήσει			
Κατάσταση:	Κλειστή			
Ημερομηνία Κλεισίματος:	2015			
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 40: Φύλλο κινδύνου #27 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #28				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Ανεπαρκής επίβλεψη εργαζομένων			
Σύντομη Περιγραφή:	Ελλιπής επιλογή κατάλληλων ατόμων για επίβλεψη των εργαζομένων με αποτέλεσμα τη μη τήρηση του χρονοδιαγράμματος			
Κατηγορία Κινδύνου:	Λειτουργικοί – Επιχειρησιακοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.5	4	M_2	29	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Μη ύπαρξη προσωπικού για την επίβλεψη εργαζομένων			
Προπομπός Κινδύνου:	Καθυστέρηση στην υλοποίηση του έργου/Υπαρξη λαθών κατά την υλοποίηση του έργου			
Στρατηγική Αντιμετώπισης:	Μεταφορά			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Μηνιαίος έλεγχος για το αν έχουν υλοποιηθεί οι στόχοι του προηγούμενου μήνα			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 41: Φύλλο κινδύνου #28 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #29				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Ελλιπής διαδικασία για την αφαίρεση δικαιωμάτων πρόσβασης κατά την λήξη της απασχόλησης			
Σύντομη Περιγραφή:	Η διαδικασία διακοπής συνεργασίας δεν πληροί όλες τις προϋποθέσεις που χρειάζονται για τη μη πρόσβαση των πρώην εργαζομένων στο πληροφοριακό σύστημα και στους χώρους του πληροφοριακού συστήματος			
Κατηγορία Κινδύνου:	Λειτουργικοί – Επιχειρησιακοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.3	4	M_6	57	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος των ατόμων που συνδέονται καθημερινά στο σύστημα			
Προπομπός Κινδύνου:	Ανίχνευση πρόσβασης στο σύστημα από πρώην εργαζόμενο στην εταιρεία			
Στρατηγική Αντιμετώπισης:	Αποφυγή			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:	Έλεγχος των ατόμων που συνδέονται καθημερινά στο σύστημα και είναι εν ενεργεία			
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	1 φορά στον αρχικό σχεδιασμό			
Κατάσταση:	Τελειωμένη			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 42: Φύλλο κινδύνου #29 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #30				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Ελλιπής σχεδιασμός τακτικών ελέγχων εύρυθμης λειτουργίας του λογισμικού			
Σύντομη Περιγραφή:	Ανεπαρκής διαδικασία τακτικού ελέγχου της λειτουργίας του λογισμικού			
Κατηγορία Κινδύνου:	Λειτουργικοί – Επιχειρησιακοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.7	3	M_1	23	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος της λειτουργίας του λογισμικού			
Προπομπός Κινδύνου:	Μη αναμενόμενη συμπεριφορά του λογισμικού			
Στρατηγική Αντιμετώπισης:	Μεταφορά			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	1 φορά στον αρχικό σχεδιασμό			
Κατάσταση:	Τελειωμένη			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 43: Φύλλο κινδύνου #30 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #31				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κίνδυνος εσφαλμένης εγκατάστασης υλικού ή λογισμικού από το προσωπικό της αναδόχου εταιρείας			
Σύντομη Περιγραφή:	Εσφαλμένη εγκατάσταση υλικού ή λογισμικού λόγω έλλειψης τεχνικών γνώσεων ή εξαιτίας απλού ανθρώπινου σφάλματος του προσωπικού			
Κατηγορία Κινδύνου:	Λειτουργικοί – Επιχειρησιακοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.5	5	Y_6	20	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος των όρων που υπάρχουν στο συμβόλαιο με την εταιρεία ανάθεσης έργου			
Προπομπός Κινδύνου:	Μη ύπαρξη του όρου για την αποφυγή του κινδύνου			
Στρατηγική Αντιμετώπισης:	Μεταφορά			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	1 φορά στον αρχικό σχεδιασμό			
Κατάσταση:	Τελειωμένη			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 44: Φύλλο κινδύνου #31 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #32				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Ανεπαρκής κάλυψη του κτιρίου από σύστημα συναγερμού			
Σύντομη Περιγραφή:	Μη εγκατεστημένο σύστημα ειδοποίησης σε περίπτωση εισβολής στο χώρο του πληροφοριακού συστήματος			
Κατηγορία Κινδύνου:	Λειτουργικοί – Επιχειρησιακοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.7	4	Y_4	7	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Επιθεώρηση του υλικού και του χώρου στον οποίο βρίσκεται αυτό			
Προπομπός Κινδύνου:	Μη αναμενόμενη συμπεριφορά του υλικού, μη τακτική συντήρηση του υλικού			
Στρατηγική Αντιμετώπισης:	Μετριασμός			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Εγκατάσταση συστήματος συναγερμού			
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Κάθε μέρα			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 45: Φύλλο κινδύνου #32 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #33				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Ανεπαρκής κάλυψη του κτιρίου από σύστημα πυρανίχνευσης			
Σύντομη Περιγραφή:	Μη εγκατεστημένο σύστημα ειδοποίησης σε περίπτωση πυρκαγιάς			
Κατηγορία Κινδύνου:	Λειτουργικοί – Επιχειρησιακοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.7	4	Y_4	8	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Επιθεώρηση του υλικού και του χώρου στον οποίο βρίσκεται αυτό			
Προπομπός Κινδύνου:	Μη αναμενόμενη συμπεριφορά του υλικού, ύπαρξη εύφλεκτων υλικών στο χώρο, μη τακτική συντήρηση του υλικού			
Στρατηγική Αντιμετώπισης:	Μετριασμός			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Εγκατάσταση συστήματος πυρανίχνευσης			
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Μηνιαία			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 46: Φύλλο κινδύνου #33 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #34				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Ανεπαρκής κάλυψη του κτιρίου από σύστημα αναγνώρισης και ελέγχου ταυτότητας			
Σύντομη Περιγραφή:	Μη εγκατεστημένο σύστημα αναγνώρισης και ελέγχου ταυτότητας για την είσοδο στους χώρους του πληροφοριακού συστήματος			
Κατηγορία Κινδύνου:	Λειτουργικοί – Επιχειρησιακοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.7	4	Y_4	9	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Επιθεώρηση του υλικού και του χώρου στον οποίο βρίσκεται αυτό			
Προπομπός Κινδύνου:	Μη αναμενόμενη συμπεριφορά του υλικού, μη τακτική συντήρηση του υλικού			
Στρατηγική Αντιμετώπισης:	Μετριασμός			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Εγκατάσταση μηχανημάτων ελέγχου ταυτότητας στις εσωτερικές εισόδους που οδηγούν σε κάθε όροφο			
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Κάθε μέρα			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 47: Φύλλο κινδύνου #34 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #35				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Έλλειψη οικονομικών πόρων			
Σύντομη Περιγραφή:	Ανεπαρκείς οικονομικοί πόροι οδηγούν σε αδυναμία έναρξης ανάπτυξης του πληροφοριακού συστήματος			
Κατηγορία Κινδύνου:	Χρηματοοικονομικοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.5	5	M_4	41	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Οικονομικοί δείκτες ρευστότητας και χρηματοδότησης του έργου			
Προπομπός Κινδύνου:	Περικοπή κάποιου προϋπολογισμού			
Στρατηγική Αντιμετώπισης:	Αποφυγή			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:	Δέσμευση κεφαλαίων για την κατασκευή του έργου			
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 48: Φύλλο κινδύνου #35 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #36				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Προβλήματα με την χρηματοδότηση του έργου			
Σύντομη Περιγραφή:	Συνεχόμενες διακοπές κατά την υλοποίηση του έργου λόγω προβλημάτων στη χρηματοδότηση με αποτέλεσμα την χρονική καθυστέρηση και την αύξηση του κόστους.			
Κατηγορία Κινδύνου:	Χρηματοοικονομικοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.7	2	M_5	53	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Ανακοινώσεις της κυβέρνησης σχετικά με τη χρηματοδότηση του έργου			
Προπομπός Κινδύνου:	Ύπαρξη γενικότερων οικονομικών προβλημάτων και έλλειψη ρευστότητας			
Στρατηγική Αντιμετώπισης:	Αποφυγή			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:	Δέσμευση κεφαλαίων για την κατασκευή του έργου			
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 49: Φύλλο κινδύνου #36 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #37				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Καταστροφή υλικού ή λογισμικού από τους χειριστές του συστήματος			
Σύντομη Περιγραφή:	Καταστροφή υλικού ή λογισμικού του συστήματος λόγω κακής χρήσης			
Κατηγορία Κινδύνου:	Ανθρώπινοι			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.7	4	Y_4	10	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Επιθεώρηση του υλικού και του χώρου στον οποίο βρίσκεται αυτό			
Προπομπός Κινδύνου:	Μη αναμενόμενη συμπεριφορά του υλικού, μη τακτική συντήρηση του υλικού			
Στρατηγική Αντιμετώπισης:	Μετριασμός			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Εκπαίδευση των εργαζομένων σχετικά με τον τρόπο χρήσης του εξοπλισμού			
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:	Επίπληξη εργαζομένου που δεν συμβαδίζει με τους κανονισμούς ασφαλής χρήσης του εξοπλισμού			
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Κάθε μέρα			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 50: Φύλλο κινδύνου #37 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #38				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κλοπή υλικού από εργαζομένους			
Σύντομη Περιγραφή:	Το υλικό ενδέχεται να κλαπεί από τους εργαζόμενους			
Κατηγορία Κινδύνου:	Ανθρώπινοι			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.7	4	Y_4	11	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος του εξοπλισμού σε τακτά χρονικά διαστήματα			
Προπομπός Κινδύνου:	Μη ταύτιση καταγεγραμμένου και υπάρχοντος εξοπλισμού			
Στρατηγική Αντιμετώπισης:	Αποφυγή			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:	Τακτικός έλεγχος του καταγεγραμμένου υλικού για τυχόν απώλειες			
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Κάθε μέρα			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 51: Φύλλο κινδύνου #38 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #39				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Απεργίες εργαζομένων που διαχειρίζονται το πληροφοριακό σύστημα			
Σύντομη Περιγραφή:	Καθυστέρηση στην υλοποίηση του έργου λόγω απεργιακών κινητοποιήσεων από τους εργαζόμενους.			
Κατηγορία Κινδύνου:	Ανθρώπινοι			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.5	4	M_2	30	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση της συμπεριφοράς των εργαζομένων ως προς τα εργασιακά ζητήματα			
Προπομπός Κινδύνου:	Εμφάνιση αντιδράσεων σε εργασιακές αλλαγές			
Στρατηγική Αντιμετώπισης:	Μετριασμός			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Επικοινωνία με τους εργαζόμενους για την κατανόηση των αναγκών τους και συζήτηση μαζί τους για την εύρεση της βέλτιστης λύσης			
Διορθωτικά μέτρα:	Ύπαρξη εγγράφων που να γίνεται η καταγραφή των αναγκών των εργαζομένων με στόχο την κάλυψη των περισσότερων αναγκών			
Εναλλακτικό σχέδιο:	Αλλαγή αρμοδιοτήτων			
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Κλειστή			
Ημερομηνία Κλεισίματος:	2015			
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 52: Φύλλο κινδύνου #39 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #40				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κίνδυνος απροθυμίας προσαρμογής στην αλλαγή			
Σύντομη Περιγραφή:	Απροθυμία των εργαζομένων του πληροφοριακού συστήματος να προσαρμοστούν στα νέα δεδομένα του εργασιακού τους περιβάλλοντος			
Κατηγορία Κινδύνου:	Ανθρώπινοι			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.7	4	Y_4	12	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση των στατιστικών χρήσης του συστήματος			
Προπομπός Κινδύνου:	Τα στατιστικά χρήσης του συστήματος είναι στο κατώτατο όριο από αυτό που έχει οριστεί από την εταιρεία ανάθεσης του έργου			
	Μετριασμός			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Μελέτη των αναγκών των χρηστών για την κατανόηση των αναγκών τους όσον αφορά τη χρήση της εφαρμογής			
Διορθωτικά μέτρα:	Καταγραφή των αναγκών των χρηστών και υλοποίηση τυχόν αλλαγές στην εφαρμογής για να είναι πιο φιλικοί προς τους χρήστες			
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Κλειστή			
Ημερομηνία Κλεισίματος:	2015			
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 53: Φύλλο κινδύνου #40 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #41				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Καταστροφή εξοπλισμού από υγρά/τρόφιμα			
Σύντομη Περιγραφή:	Καταστροφή υλικού του πληροφοριακού συστήματος από επικίνδυνα υλικά που δεν επιτρέπονται κοντά στον εξοπλισμό (π.χ. τρόφιμα, υγρά)			
Κατηγορία Κινδύνου:	Ανθρώπινοι			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.5	4	M_2	31	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος αν υπάρχει σήμανση για την απαγόρευση των τροφίμων και των ποτών στου χώρους που βρίσκεται το πληροφοριακό σύστημα			
Προπομπός Κινδύνου:	Εργαζόμενοι που εισέρχονται με τρόφιμα και ποτά στους χώρους του πληροφοριακού συστήματος			
Στρατηγική Αντιμετώπισης:	Αποφυγή			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:	Ενημέρωση όλων των εργαζομένων για την απαγόρευση ποτών και τροφίμων στους χώρους όπου βρίσκεται ο εξοπλισμός			
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Κάθε μέρα			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 54: Φύλλο κινδύνου #41 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #42				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Διαρροή πληροφοριών			
Σύντομη Περιγραφή:	Διάδοση εμπιστευτικών πληροφοριών που αφορούν προσωπικά δεδομένα από εργαζόμενους σε μη εξουσιοδοτημένα άτομα			
Κατηγορία Κινδύνου:	Ανθρώπινοι			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.7	4	Y_4	13	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος για την ύπαρξη ειδικού λογισμικού που να καταγράφει τις κινήσεις του κάθε εργαζομένου κατά τη διάρκεια της χρήσης του πληροφοριακού συστήματος			
Προπομπός Κινδύνου:	Μη ύπαρξη του λογισμικού που να καταγράφει τις κινήσεις του κάθε εργαζομένου κατά τη διάρκεια της χρήσης του πληροφοριακού συστήματος			
Στρατηγική Αντιμετώπισης:	Μετριασμός			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Εγκατάσταση ειδικού λογισμικού το οποίο ελέγχει τις ενέργειες των εργαζομένων			
Διορθωτικά μέτρα:	Ενημέρωση των εργαζομένων σχετικά με τους κανονισμούς της εταιρείας όσον αφορά την ασφάλεια των πληροφοριών και των δεδομένων			
Εναλλακτικό σχέδιο:	Επίπληξη εργαζομένου που δεν συμβαδίζει με του κανονισμούς της εταιρείας			
Σχέδιο μετάπτωσης:	Επιβολή ποινών σε όποιον δεν ακολουθεί τους κανονισμούς της εταιρείας			
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Κάθε μέρα			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 55: Φύλλο κινδύνου #42 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #43				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Μη εξουσιοδοτημένη πρόσβαση στους χώρους του πληροφοριακού συστήματος			
Σύντομη Περιγραφή:	Ικανότητα μη εξουσιοδοτημένων ατόμων να έχουν πρόσβαση στους χώρους όπου βρίσκεται το πληροφοριακό σύστημα με αποτέλεσμα την πρόκληση φθοράς του εξοπλισμού			
Κατηγορία Κινδύνου:	Ανθρώπινοι			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
4	4	Y_3	17	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος για την ύπαρξη συσκευών αναγνώρισης των ειδικών καρτών των εργαζομένων			
Προπομπός Κινδύνου:	Μη ύπαρξη των συσκευών αναγνώρισης στις εισόδους του κτιρίου που στεγάζεται το σύστημα			
Στρατηγική Αντιμετώπισης:	Μετριασμός			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Συνεχής έλεγχος των εγκαταστάσεων όπου βρίσκεται ο εξοπλισμός			
Διορθωτικά μέτρα:	Χρήση ειδικού εξοπλισμού όπου απαγορεύει την πρόσβαση μη εξουσιοδοτημένου προσωπικού στους χώρους εγκατάστασης του εξοπλισμού			
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Κάθε μέρα			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 56: Φύλλο κινδύνου #43 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #44				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Μη εξουσιοδοτημένη πρόσβαση στο πληροφοριακό σύστημα από τους εργαζόμενους			
Σύντομη Περιγραφή:	Ικανότητα μη εξουσιοδοτημένων ατόμων να έχουν πρόσβαση στο πληροφοριακό σύστημα με αποτέλεσμα την πρόκληση καταστροφής του λογισμικού			
Κατηγορία Κινδύνου:	Ανθρώπινοι			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.7	5	Y_3	3	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος των όρων που υπάρχουν στο συμβόλαιο με την εταιρεία ανάθεσης έργου			
Προπομπός Κινδύνου:	Μη ύπαρξη του όρου για την αποφυγή του κινδύνου			
Στρατηγική Αντιμετώπισης:	Μεταφορά			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Κάθε μέρα			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 57: Φύλλο κινδύνου #44 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #45				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Διαρροή κωδικών εισόδου και διαχείρισης του πληροφοριακού συστήματος			
Σύντομη Περιγραφή:	Γνωστοποίηση των κωδικών εισόδου του πληροφοριακού συστήματος σε μη εξουσιοδοτημένα άτομα			
Κατηγορία Κινδύνου:	Ανθρώπινοι			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.7	5	Y_3	4	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος για την ύπαρξη ειδικού λογισμικού που να καταγράφει την ηλεκτρονική διεύθυνση που αντιστοιχεί σε κάθε εργαζόμενο			
Προπομπός Κινδύνου:	Μη ύπαρξη του ειδικού λογισμικού			
Στρατηγική Αντιμετώπισης:	Μετριασμός			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Ενημέρωση των εργαζομένων για τη διαφύλαξη των κωδικών που έχουν για τη χρήση του πληροφοριακού συστήματος			
Διορθωτικά μέτρα:	Δυνατότητα αλλαγής των κωδικών περιοδικά			
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Κάθε μέρα			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 58: Φύλλο κινδύνου #45 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #46				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Μη εξουσιοδοτημένες αλλαγές αρχείων			
Σύντομη Περιγραφή:	Ελλιπής μηχανισμός κατανομής δικαιωμάτων διαχείρισης στους εργαζομένους του πληροφοριακού συστήματος με αποτέλεσμα τη δυνατότητα πρόσβαση όλων των εργαζομένων σε όλα τα μέρη του συστήματος			
Κατηγορία Κινδύνου:	Ανθρώπινοι			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.3	5	M_4	48	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος των όρων που υπάρχουν στο συμβόλαιο με την εταιρεία ανάθεσης έργου			
Προπομπός Κινδύνου:	Μη ύπαρξη του όρου για την αποφυγή του κινδύνου			
Στρατηγική Αντιμετώπισης:	Μεταφορά			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	1 φορά στον αρχικό σχεδιασμό			
Κατάσταση:	Τελειωμένη			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 59: Φύλλο κινδύνου #46 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #47				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Ακούσια αλλαγή των δεδομένων του πληροφοριακού συστήματος			
Σύντομη Περιγραφή:	Μη εσκεμμένη αλλαγή των δεδομένων			
Κατηγορία Κινδύνου:	Ανθρώπινοι			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.3	5	M_4	49	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Περιοδική ταυτοποίηση ενός δείγματος δεδομένων και έλεγχος των αποτελεσμάτων			
Προπομπός Κινδύνου:	Εμφάνιση σφαλμάτων κατά την ταυτοποίηση			
Στρατηγική Αντιμετώπισης:	Αποδοχή			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:	Περιοδική ταυτοποίηση ενός δείγματος δεδομένων και έλεγχος των αποτελεσμάτων			
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Μηνιαία			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 60: Φύλλο κινδύνου #47 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #48				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Έλλειψη κινήτρων για τους εργαζόμενους			
Σύντομη Περιγραφή:	Μη ύπαρξη διαδικασίας ανταμοιβής για τους εργαζόμενους			
Κατηγορία Κινδύνου:	Ανθρώπινοι			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.5	4	M_2	32	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση δεικτών παραγωγικότητας			
Προπομπός Κινδύνου:	Μείωση παραγωγικότητας των εργαζομένων			
Στρατηγική Αντιμετώπισης:	Μετριασμός			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Επικοινωνία με τους εργαζόμενους για την κατανόηση των αναγκών τους και συζήτηση μαζί τους για την εύρεση της βέλτιστης λύσης			
Διορθωτικά μέτρα:	Δημιουργία περισσότερων κινήτρων για τους εργαζόμενους με βάση τις ανάγκες που έχουν			
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 61: Φύλλο κινδύνου #48 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #49				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Έλλειψη ευαισθητοποίησης σε θέματα ασφάλειας			
Σύντομη Περιγραφή:	Ελλιπής εκπαίδευση εργαζομένων σε θέματα ασφαλείας του πληροφοριακού συστήματος			
Κατηγορία Κινδύνου:	Ανθρώπινοι			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.7	4	Y_4	15	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση της τήρησης των κανόνων ασφαλείας			
Προπομπός Κινδύνου:	Εμφάνιση συχνής παραβατικότητας			
Στρατηγική Αντιμετώπισης:	Μετριασμός			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Εκπαίδευση των εργαζομένων σε θέματα ασφάλειας του εξοπλισμού και του λογισμικού			
Διορθωτικά μέτρα:	Καταγραφή και ενημέρωση των εργαζομένων με του κανόνες που πρέπει να ακολουθούν για την ασφάλεια του πληροφοριακού συστήματος			
Εναλλακτικό σχέδιο:	Επίπληξη εργαζομένου που δεν συμβαδίζει με του κανονισμούς της ασφάλειας του πληροφοριακού συστήματος			
Σχέδιο μετάπτωσης:	Επιβολή ποινών σε όποιον δεν ακολουθεί τους κανονισμούς της ασφάλειας του πληροφοριακού συστήματος			
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 62: Φύλλο κινδύνου #49 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #50				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Σύνδεση προσωπικών συσκευών στο εταιρικό δίκτυο			
Σύντομη Περιγραφή:	Ο κάθε εργαζόμενος μπορεί να χρησιμοποιήσει δικές του συσκευές για να συνδεθεί στο δίκτυο της εταιρείας με αποτέλεσμα τη μετάδοση κακόβουλου λογισμικού			
Κατηγορία Κινδύνου:	Ανθρώπινοι			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.7	4	Y_4	16	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Τακτικός έλεγχος του δικτύου μέσω λογισμικού ασφαλείας (Antivirus)			
Προπομπός Κινδύνου:	Εμφάνιση και διόρθωση ιού κατά τη διαδικασία του τακτικού ελέγχου			
Στρατηγική Αντιμετώπισης:	Αποδοχή			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:	Ενημέρωση των εργαζομένων να ελέγχουν πρώτα κάθε συσκευή που πρόκειται να συνδέσουν στο εταιρικό δίκτυο για τυχόν κακόβουλο λογισμικό			
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Κάθε μέρα			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 63: Φύλλο κινδύνου #50 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #51				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Εγκατάσταση μη εξουσιοδοτημένου λογισμικού και εφαρμογών			
Σύντομη Περιγραφή:	Εγκατάσταση επικίνδυνου για το πληροφοριακό σύστημα λογισμικού και εφαρμογών			
Κατηγορία Κινδύνου:	Ανθρώπινοι			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.3	5	M_4	50	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Τακτικός έλεγχος για την αυθεντικότητα του λογισμικού και των εφαρμογών			
Προπομπός Κινδύνου:	Εμφάνιση μη εξουσιοδοτημένου λογισμικού και εφαρμογών			
Στρατηγική Αντιμετώπισης:	Μετριασμός			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Ύπαρξη ειδικού λογισμικού ασφαλείας όπου ανιχνεύει την εγκατάσταση μη εξουσιοδοτημένου λογισμικού στο σύστημα			
Διορθωτικά μέτρα:	Τακτικός έλεγχος του λογισμικού και των εφαρμογών που χρησιμοποιούνται			
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	1 φορά στον αρχικό σχεδιασμό			
Κατάσταση:	Τελειωμένη			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 64: Φύλλο κινδύνου #51 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #52				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Ακούσια μεταφορά εμπιστευτικών δεδομένων του πληροφοριακού συστήματος εκτός γραφείου			
Σύντομη Περιγραφή:	Μη εσκεμμένη διάδοση προσωπικών δεδομένων μέσω συσκευών αποθήκευσης (π.χ. σκληρός δίσκος)			
Κατηγορία Κινδύνου:	Ανθρώπινοι			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.5	4	M_2	33	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος για την ύπαρξη ειδικού λογισμικού που να καταγράφει τις κινήσεις του κάθε εργαζομένου κατά τη διάρκεια της χρήσης του πληροφοριακού συστήματος			
Προπομπός Κινδύνου:	Μη ύπαρξη του λογισμικού που να καταγράφει τις κινήσεις του κάθε εργαζομένου κατά τη διάρκεια της χρήσης του πληροφοριακού συστήματος			
Στρατηγική Αντιμετώπισης:	Μετριασμός			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Μη εφικτή αποθήκευση των προσωπικών δεδομένων σε αποθηκευτικά μέσα καθώς μη ύπαρξη δυνατότητας μεταφορά δεδομένων μέσω διαδικτύου			
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Κάθε μέρα			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 65: Φύλλο κινδύνου #52 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #53				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Έλλειψη της απαιτούμενης εκπαίδευσης του προσωπικού			
Σύντομη Περιγραφή:	Μη επαρκής επιμόρφωση των εργαζομένων προκειμένου να ανταπεξέλθουν στις νέες απαιτήσεις			
Κατηγορία Κινδύνου:	Ανθρώπινοι			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.7	1	X_1	78	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση του αρχείου εκπαίδευσης των υπαλλήλων			
Προπομπός Κινδύνου:	Ύπαρξη προβλημάτων κατά τη χρήση του συστήματος			
Στρατηγική Αντιμετώπισης:	Μετριασμός			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Εκπαίδευση του προσωπικού για την ανταπόκρισή του στις απαιτήσεις του συστήματος			
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:	Αλλαγή αρμοδιοτήτων			
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Ετήσια			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 66: Φύλλο κινδύνου #53 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #54				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Εσωτερικοί κίνδυνοι (δόλος)			
Σύντομη Περιγραφή:	Κίνδυνος δολιοφθορών του πληροφοριακού συστήματος από δυσαρεστημένα στελέχη ή υπαλλήλους που εργάζονται στον οργανισμό			
Κατηγορία Κινδύνου:	Ανθρώπινοι			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.3	3	M_3	74	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση συμπεριφοράς εργαζομένων			
Προπομπός Κινδύνου:	Ύποπτες κινήσεις εργαζομένων			
Στρατηγική Αντιμετώπισης:	Μετριασμός			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Χρήση κωδικών ασφαλείας έτσι ώστε ο κάθε χρήστης να έχει δικαιώματα στο σύστημα ανάλογα με την ιδιότητά του			
Διορθωτικά μέτρα:	Χρήση εξειδικευμένου λογισμικού έτσι ώστε να ελέγχονται όλες οι ενέργειες των χρηστών			
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Κάθε μέρα			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 67: Φύλλο κινδύνου #54 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #55				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Λάθος κατανομή του κεφαλαίου			
Σύντομη Περιγραφή:	Λανθασμένη πρόβλεψη κοστολόγησης τμημάτων του πληροφοριακού συστήματος έτσι ώστε σε μερικά τμήματα του έργου να είναι αναγκαία η ανακοστολόγηση και αυτό να έχει ως αποτέλεσμα την καθυστέρηση του έργου			
Κατηγορία Κινδύνου:	Στρατηγικοί - Οργανωτικοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.3	3	M_8	75	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση της προσυμφωνημένης κατανομής του κεφαλαίου			
Προπομπός Κινδύνου:	Ανομοιόμορφη κατανομή του κεφαλαίου			
Στρατηγική Αντιμετώπισης:	Μεταφορά			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	1 φορά πριν την έναρξη του έργου			
Κατάσταση:	Τελειωμένη			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 68: Φύλλο κινδύνου #55 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #56				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Λανθασμένη κατανομή σημαντικότητας στις εφαρμογές του συστήματος			
Σύντομη Περιγραφή:	Λανθασμένη βαρύτητα κατά το σχεδιασμό των μερών του πληροφοριακού συστήματος μπορεί να οδηγήσει σε αναθεώρηση ορισμένων από αυτά και επανασχεδιασμού του έργου συνολικά			
Κατηγορία Κινδύνου:	Στρατηγικοί - Οργανωτικοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.3	4	M_6	58	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος στις εκδόσεις του συστήματος			
Προπομπός Κινδύνου:	Το σύστημα δεν καλύπτει κάποια σημαντικά σημεία που έπρεπε να έχουν ληφθεί πολύ σοβαρά υπ' όψιν			
Στρατηγική Αντιμετώπισης:	Μεταφορά			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	1 φορά πριν την έναρξη του έργου			
Κατάσταση:	Τελειωμένη			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 69: Φύλλο κινδύνου #56 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #57				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Έλλειψη εφεδρικού σχεδίου απρόσκοπτης λειτουργίας του συστήματος			
Σύντομη Περιγραφή:	Έλλειψη εφεδρικού σχεδίου σε περίπτωση διακοπής ηλεκτροδότησης ή σε περίπτωση προβλημάτων λειτουργίας των διακομιστών που υποστηρίζουν το πληροφοριακό σύστημα			
Κατηγορία Κινδύνου:	Στρατηγικοί - Οργανωτικοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.5	4	M_2	34	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση του σχεδιασμού του έργου			
Προπομπός Κινδύνου:	Ανεπαρκής ή ελλιπής ύπαρξη εφεδρικού σχεδίου κατά το στάδιο ολοκλήρωσης του έργου			
Στρατηγική Αντιμετώπισης:	Μεταφορά			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Προκήρυξη διαγωνισμού για την ανάθεση του εφεδρικού σχεδίου με τη μέθοδο outsourcing σε εξειδικευμένες εταιρίες			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	1 φορά πριν την έναρξη του έργου			
Κατάσταση:	Τελειωμένη			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 70: Φύλλο κινδύνου #57 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #58				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Λανθασμένη πρόβλεψη απαιτούμενων πόρων υλικού			
Σύντομη Περιγραφή:	Έλλειψη υλικών πόρων (π.χ. διακομιστές, καλωδίωση κτιρίου κ.τ.λ.)χρήσιμων για την κατασκευή του έργου λόγω λανθασμένης αρχικής πρόβλεψης			
Κατηγορία Κινδύνου:	Στρατηγικοί - Οργανωτικοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.5	3	M_4	42	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος του προγραμματισμού των απαιτούμενων πόρων υλικού			
Προπομπός Κινδύνου:	Απόκλιση από τον αρχικό προγραμματισμό των απαιτούμενων πόρων			
Στρατηγική Αντιμετώπισης:	Αποφυγή			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:	Συνεχής έλεγχος του σχεδιασμού του συστήματος για έγκαιρη διάγνωση του κινδύνου, άμεσες κινήσεις για την αύξηση των πόρων υλικού			
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	1 φορά πριν την έναρξη του έργου			
Κατάσταση:	Τελειωμένη			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 71: Φύλλο κινδύνου #58 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #59				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Αλλαγή του χρονοδιαγράμματος λόγω λανθασμένου αρχικού προγραμματισμού			
Σύντομη Περιγραφή:	Επιλογή ακολουθίας εργασιών διάφορη της βέλτιστης που έχει ως αποτέλεσμα την χρονική επιμήκυνση του έργου σε σχέση με τη βέλτιστη επιλογή			
Κατηγορία Κινδύνου:	Στρατηγικοί - Οργανωτικοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.5	2	M_7	72	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση και σύγκριση του πραγματικού χρονοδιαγράμματος με το εκτιμώμενο			
Προπομπός Κινδύνου:	Παρατήρηση καθυστερήσεων κατά τα επιμέρους στάδια ολοκλήρωσης του έργου			
Στρατηγική Αντιμετώπισης:	Μεταφορά			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Μηνιαία μέχρι την ολοκλήρωση του έργου			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 72: Φύλλο κινδύνου #59 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #60				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Λανθασμένη κοστολόγηση του έργου			
Σύντομη Περιγραφή:	Το κόστος υλοποίησης του συστήματος αυξήθηκε, θέτοντας σε κίνδυνο την υπόσταση του έργου			
Κατηγορία Κινδύνου:	Στρατηγικοί - Οργανωτικοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.5	3	M_4	43	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση οικονομικών δεικτών			
Προπομπός Κινδύνου:	Τα πρώτα στάδια της υλοποίησης του έργου βγαίνουν εκτός του αρχικού προϋπολογισμού			
Στρατηγική Αντιμετώπισης:	Μεταφορά			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Μηνιαία μέχρι την ολοκλήρωση του έργου			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 73: Φύλλο κινδύνου #60 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #61				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κοινή χρήση εμπιστευτικών δεδομένων με τους συνεργάτες και τους προμηθευτές			
Σύντομη Περιγραφή:	Πρόσβαση σε εμπιστευτικά δεδομένα από συνεργάτες και προμηθευτές			
Κατηγορία Κινδύνου:	Στρατηγικοί - Οργανωτικοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.3	3	M_8	76	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος των όρων που υπάρχουν στο συμβόλαιο με την εταιρεία ανάθεσης έργου			
Προπομπός Κινδύνου:	Μη ύπαρξη του όρου για την αποφυγή του κινδύνου			
Στρατηγική Αντιμετώπισης:	Μεταφορά			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	1 φορά στην αρχική σύναψη του συμβολαίου			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 74: Φύλλο κινδύνου #61 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #62				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Έλλειψη εμπειρίας και τεχνογνωσίας των προσώπων που είναι υπεύθυνα για την παρακολούθηση της υλοποίησης του έργου			
Σύντομη Περιγραφή:	Παρακολούθηση της υλοποίησης του πληροφοριακού συστήματος από άτομα με καθόλου ή λίγη εμπειρία και με ελλιπής γνώσεις τεχνογνωσίας καθώς και ελλιπής γνώσεις τα οποία σε μελλοντικό χρόνο θα κληθούν να λάβουν σημαντικές αποφάσεις κάτω από πιθανές συνθήκες πίεσης ή έλλειψης χρόνου			
Κατηγορία Κινδύνου:	Στρατηγικοί - Οργανωτικοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.3	4	M_6	59	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Ελλιπής έλεγχος των απαραίτητων διαδικασιών για την διεξαγωγή του έργου			
Προπομπός Κινδύνου:	Εμφάνιση πολλών λαθών κατά τη διάρκεια του προγραμματισμού και της διαχείρισης του έργου			
Στρατηγική Αντιμετώπισης:	Μετριασμός			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Έλεγχος των εργαζομένων που προσλαμβάνονται για να αναλάβουν την παρακολούθηση του έργου σύμφωνα με την εμπειρία τους και τις γνώσεις που έχουν για τη συγκεκριμένη θέση με τη βοήθεια συνεντεύξεων και γραπτού διαγωνισμού όπου οι υποψήφιοι θα εξετάζονται σε θέματα που αφορούν τη διαχείριση ενός έργου			
Διορθωτικά μέτρα:	Ύπαρξη συνεχών ενημερώσεων από τα πρόσωπα που έχουν αναλάβει την παρακολούθηση του έργου καθώς και καταγραφή των δραστηριοτήτων τους και των ελέγχων που έχουν πραγματοποιήσει καθ' όλη τη διάρκεια έργου			
Εναλλακτικό σχέδιο:	Συνεχής κατάρτιση των εργαζομένων σε θέματα διαχείρισης έργου και νέων τεχνολογιών με διεξαγωγή σεμιναρίων			
Σχέδιο μετάπτωσης:	Αλλαγή αρμοδιοτήτων			
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 75: Φύλλο κινδύνου #62 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #63				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Λανθασμένες αποφάσεις διαχείρισης κινδύνων			
Σύντομη Περιγραφή:	Έλλειψη εμπειρίας των ατόμων που λαμβάνουν τις αποφάσεις διαχείρισης κινδύνων του έργου με αποτέλεσμα την ανεπαρκή αντιμετώπιση των κινδύνων			
Κατηγορία Κινδύνου:	Ανθρώπινοι			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.1	4	X_4	89	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Τακτική παρακολούθηση του σχεδιασμού διαχείρισης κινδύνου			
Προπομπός Κινδύνου:	Απόκλιση αποφάσεων από τον αρχικό σχεδιασμό διαχείρισης κινδύνου			
Στρατηγική Αντιμετώπισης:	Μετριασμός			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Τακτικός έλεγχος των εργαζομένων που έχουν αναλάβει τις αποφάσεις διαχείρισης κινδύνων			
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:	Συνεχής κατάρτιση των εργαζομένων σε θέματα διαχείρισης κινδύνων με διεξαγωγή σεμιναρίων.			
Σχέδιο μετάπτωσης:	Αλλαγή αρμοδιοτήτων			
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 76: Φύλλο κινδύνου #63 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #64				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κίνδυνος σεισμού			
Σύντομη Περιγραφή:	Καταστροφή του κτιρίου που στεγάζεται το πληροφοριακό σύστημα λόγω σεισμού			
Κατηγορία Κινδύνου:	Φυσικοί - Περιβαλλοντικοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.5	3	M_4	44	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος στατικότητας του κτιρίου όπου στεγάζεται το πληροφοριακό σύστημα			
Προπομπός Κινδύνου:	Ενδείξεις προβληματικής στατικότητας του κτιρίου			
Στρατηγική Αντιμετώπισης:	Μετριασμός			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Συνεχής έλεγχος των κτιριακών εγκαταστάσεων			
Διορθωτικά μέτρα:	Μετεγκατάσταση του εξοπλισμού σε πιο σύγχρονες κτιριακές εγκαταστάσεις			
Εναλλακτικό σχέδιο:	Εγκατάσταση του εξοπλισμού σε χώρο αντισεισμικών προδιαγραφών			
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 77: Φύλλο κινδύνου #64 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #65				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κίνδυνος Κεραυνού			
Σύντομη Περιγραφή:	Καταστροφή στην ηλεκτροδότηση του κτιρίου λόγω κεραυνού που προκλήθηκε από ακραία καιρικά φαινόμενα			
Κατηγορία Κινδύνου:	Φυσικοί - Περιβαλλοντικοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.3	4	M_6	60	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος των καιρικών φαινομένων			
Προπομπός Κινδύνου:	Έντονες βροχοπτώσεις			
Στρατηγική Αντιμετώπισης:	Αποφυγή			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:	Χρήση ειδικού εξοπλισμού για την αποφυγή κεραυνών (αλεξικέραυνο)			
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 78: Φύλλο κινδύνου #65 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #66				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κίνδυνος πλημμύρας			
Σύντομη Περιγραφή:	Καταστροφή του χώρου που στεγάζεται το σύστημα λόγω ακραίων καιρικών φαινομένων			
Κατηγορία Κινδύνου:	Φυσικοί - Περιβαλλοντικοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.3	4	M_6	61	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος των καιρικών φαινομένων			
Προπομπός Κινδύνου:	Παρατήρηση πλημμυρικών φαινομένων σε ορισμένα τμήματα του κτιρίου			
Στρατηγική Αντιμετώπισης:				
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Μετριασμός			
Διορθωτικά μέτρα:	Δημιουργία αντιπλημμυρικών έργων στο χώρο εγκατάστασης του εξοπλισμού			
Εναλλακτικό σχέδιο:	Τοποθέτηση του συστήματος σε σημείο υψηλότερο της επιφάνειας του εδάφους			
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 79: Φύλλο κινδύνου #66 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #67				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κίνδυνος πυρκαγιάς			
Σύντομη Περιγραφή:	Κίνδυνος εκδήλωσης πυρκαγιάς στο χώρο της εγκατάστασης ή σε γειτονικά κτίρια από φυσικά αίτια ή τεχνητά			
Κατηγορία Κινδύνου:	Φυσικοί - Περιβαλλοντικοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.7	4	Y_4	17	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος του χώρου εγκατάστασης ως προς τα μέτρα πυρασφάλειας			
Προπομπός Κινδύνου:	Ελλιπής ή ανύπαρκτη συντήρηση του εξοπλισμού πυρασφάλειας			
Στρατηγική Αντιμετώπισης:	Μετριασμός			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Ύπαρξη και συνεχής έλεγχος λειτουργικών πυροσβεστήρων σε όλους τους ορόφους του κτιρίου			
Διορθωτικά μέτρα:	Χρήση εξοπλισμού πυρανίχνευσης			
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 80: Φύλλο κινδύνου #67 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #68				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κίνδυνος διαρροής υδάτων			
Σύντομη Περιγραφή:	Καταστροφή του χώρου που στεγάζεται το σύστημα από πλημμύρα που οφείλεται σε διαρροή υδάτων λόγω παλαιότητας ή κακής κατασκευής του δικτύου υδροδότησης			
Κατηγορία Κινδύνου:	Φυσικοί - Περιβαλλοντικοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.3	4	X_4	90	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος του δικτύου υδροδότησης του κτιρίου			
Προπομπός Κινδύνου:	Ελλιπής ή ανύπαρκτη συντήρηση του δικτύου υδροδότησης			
Στρατηγική Αντιμετώπισης:	Μετριασμός			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Συνεχής έλεγχος και συντήρηση του δικτύου υδροδότησης			
Διορθωτικά μέτρα:	Μετεγκατάσταση του εξοπλισμού σε πιο σύγχρονες κτιριακές εγκαταστάσεις			
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 81: Φύλλο κινδύνου #68 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #69				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κίνδυνος αδυναμίας ηλεκτροδότησης του συστήματος λόγω ελλείψεων στην ηλεκτρολογική εγκατάσταση			
Σύντομη Περιγραφή:	Αδυναμία ηλεκτροδότησης μέσω της εγκατάστασης του κτιρίου που στεγάζεται το σύστημα λόγω ελλιπούς υποστήριξης σε περιπτώσεις διακοπής της ηλεκτροδότησης			
Κατηγορία Κινδύνου:	Φυσικοί - Περιβαλλοντικοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.3	4	M_6	62	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος του δικτύου ηλεκτροδότησης του κτιρίου			
Προπομπός Κινδύνου:	Ελλιπής ή ανύπαρκτη συντήρηση του δικτύου ηλεκτροδότησης			
Στρατηγική Αντιμετώπισης:	Μετριασμός			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Συνεχής έλεγχος και συντήρηση του συστήματος ηλεκτροδότησης			
Διορθωτικά μέτρα:	Χρήση γεννητριών			
Εναλλακτικό σχέδιο:	Μετεγκατάσταση του εξοπλισμού σε πιο σύγχρονες κτιριακές εγκαταστάσεις			
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Μηνιαία			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 82: Φύλλο κινδύνου #69 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #70				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κατολίσθηση – διάβρωση εδάφους			
Σύντομη Περιγραφή:	Καταστροφή κτιρίου που στεγάζεται το πληροφοριακό σύστημα λόγω κατολίσθησης ή διάβρωσης εδάφους.			
Κατηγορία Κινδύνου:	Φυσικοί - Περιβαλλοντικοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.1	5	X_3	85	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Περιοδικοί έλεγχοι του εδάφους περιμετρικά του κτιρίου όπου βρίσκεται το πληροφοριακό σύστημα			
Προπομπός Κινδύνου:	Εμφάνιση φαινομένων διάβρωσης			
Στρατηγική Αντιμετώπισης:	Αποδοχή			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:	Εύρεση νέων κτιριακών εγκαταστάσεων για τη στέγαση του πληροφοριακού συστήματος			
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 83: Φύλλο κινδύνου #70 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #71				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Ηλιακές εκλάμψεις			
Σύντομη Περιγραφή:	Προβληματική λειτουργία του δικτύου λόγω ηλιακών εκλάμψεων			
Κατηγορία Κινδύνου:	Φυσικοί - Περιβαλλοντικοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.1	3	X_5	92	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Περιοδικός έλεγχος της σωστής λειτουργίας του δικτύου από ηλεκτρομαγνητικές παρεμβολές			
Προπομπός Κινδύνου:	Μη σωστή λειτουργία του δικτύου λόγω ηλεκτρομαγνητικών παρεμβολών			
Στρατηγική Αντιμετώπισης:	Αποδοχή			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:	Αποθήκευσης των δεδομένων και των προγραμμάτων του πληροφοριακού συστήματος σε περιβάλλον cloud			
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 84: Φύλλο κινδύνου #71 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #72				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Σκόνη			
Σύντομη Περιγραφή:	Βλάβες ή δυσλειτουργία υλικού λόγω σκόνης			
Κατηγορία Κινδύνου:	Φυσικοί - Περιβαλλοντικοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.5	2	M_7	73	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Τακτικός έλεγχος της κατάστασης του εξοπλισμού			
Προπομπός Κινδύνου:	Παρατήρηση δυσλειτουργιών λόγω σκόνης			
Στρατηγική Αντιμετώπισης:	Μετριασμός			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Τακτικός καθαρισμός του χώρου όπου βρίσκεται ο εξοπλισμό του συστήματος			
Διορθωτικά μέτρα:	Τοποθέτηση του εξοπλισμού σε ειδικό χώρο			
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εβδομαδιαία			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 85: Φύλλο κινδύνου #72 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #73				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Βλάβη του συστήματος κλιματισμού			
Σύντομη Περιγραφή:	Καταστροφή από υπερθέρμανση του εξοπλισμού του πληροφοριακού συστήματος λόγω βλάβης του κλιματισμού			
Κατηγορία Κινδύνου:	Φυσικοί - Περιβαλλοντικοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.3	4	M_6	63	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Τακτική παρακολούθηση του συστήματος κλιματισμού			
Προπομπός Κινδύνου:	Παρατήρηση δυσλειτουργιών του συστήματος λόγω υπερθέρμανσης			
Στρατηγική Αντιμετώπισης:	Μετριασμός			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Τακτικός έλεγχος και συντήρηση του συστήματος κλιματισμού			
Διορθωτικά μέτρα:	Ύπαρξη εφεδρικού συστήματος κλιματισμού στους χώρους όπου βρίσκεται ο εξοπλισμός του συστήματος			
Εναλλακτικό σχέδιο:	Αλλαγή του συστήματος κλιματισμού			
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Μηνιαία			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 86: Φύλλο κινδύνου #73 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #74				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Ηλεκτρομαγνητικές παρεμβολές			
Σύντομη Περιγραφή:	Προβληματική λειτουργία του δικτύου λόγω ηλεκτρομαγνητικών παρεμβολών			
Κατηγορία Κινδύνου:	Φυσικοί - Περιβαλλοντικοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.3	3	M_8	77	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Περιοδικός έλεγχος της σωστής λειτουργίας του δικτύου από ηλεκτρομαγνητικές παρεμβολές			
Προπομπός Κινδύνου:	Μη σωστή λειτουργία του δικτύου λόγω ηλεκτρομαγνητικών παρεμβολών			
Στρατηγική Αντιμετώπισης:	Αποδοχή			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:	Αποθήκευσης των δεδομένων και των προγραμμάτων του πληροφοριακού συστήματος σε περιβάλλον cloud			
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 87: Φύλλο κινδύνου #74 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #75				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Στατικός ηλεκτρισμός			
Σύντομη Περιγραφή:	Καταστροφή του εξοπλισμού του πληροφοριακού συστήματος λόγω διαρροής ρεύματος			
Κατηγορία Κινδύνου:	Φυσικοί - Περιβαλλοντικοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.1	4	X_4	91	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Περιοδικός έλεγχος του κτιρίου που στεγάζεται το πληροφοριακό σύστημα για διαρροή ρεύματος			
Προπομπός Κινδύνου:	Εμφάνιση σημείων του κτιρίου όπου μπορεί να προκληθεί διαρροή ρεύματος - βραχυκύκλωμα			
Στρατηγική Αντιμετώπισης:	Μετριασμός			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Τακτικός έλεγχος του δικτύου ηλεκτροδότησης όπου στεγάζεται το πληροφοριακό σύστημα			
Διορθωτικά μέτρα:	Ύπαρξη πινάκων ασφαλείας όπου θα διακόπτουν την παροχή ρεύματος σε περίπτωση διαρροής ρεύματος και θα γίνεται η ρευματοδότηση του συστήματος από γεννήτριες			
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Μηνιαία			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 88: Φύλλο κινδύνου #75 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #76				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Έκρηξη ηφαιστείου			
Σύντομη Περιγραφή:	Εγκατάσταση του πληροφοριακού συστήματος ή του διακομιστή του πληροφοριακού συστήματος σε περιοχή που είναι επιρρεπείς στις ηφαιστειακές εκρήξεις			
Κατηγορία Κινδύνου:	Φυσικοί - Περιβαλλοντικοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.1	5	X_3	86	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση των μετρήσεων που γίνονται από το ηφαιστειολογικό παρατηρητήριο της περιοχής όπου στεγάζεται το πληροφοριακό σύστημα			
Προπομπός Κινδύνου:	Όταν οι μετρήσεις αποκλίνουν από τα επιτρεπτά όρια που έχουν ορισθεί			
Στρατηγική Αντιμετώπισης:	Αποφυγή			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:	Εγκατάσταση του πληροφοριακού συστήματος σε περιοχή που δεν είναι ηφαιστειογενής			
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 89: Φύλλο κινδύνου #76 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #77				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Πυρηνικό ατύχημα			
Σύντομη Περιγραφή:	Εγκατάσταση του πληροφοριακού συστήματος σε περιοχή όπου βρίσκονται πυρηνικά εργοστάσια			
Κατηγορία Κινδύνου:	Φυσικοί - Περιβαλλοντικοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.1	5	X_3	81	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση των μετρήσεων που γίνονται από τα πυρηνικά εργοστάσια της περιοχής όπου στεγάζεται το πληροφοριακό σύστημα			
Προπομπός Κινδύνου:	Όταν οι μετρήσεις αποκλίνουν από τα επιτρεπτά όρια που έχουν ορισθεί			
Στρατηγική Αντιμετώπισης:	Αποφυγή			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:	Εγκατάσταση του πληροφοριακού συστήματος σε περιοχή όπου δεν υπάρχουν πυρηνικά εργοστάσια			
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 90: Φύλλο κινδύνου #77 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #78				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κίνδυνος εκρήξεων			
Σύντομη Περιγραφή:	Εγκατάσταση του πληροφοριακού συστήματος σε χώρο όπου βρίσκονται εύφλεκτα υλικά			
Κατηγορία Κινδύνου:	Φυσικοί - Περιβαλλοντικοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.3	5	M_4	51	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος για την ύπαρξη εύφλεκτων υλικών στο χώρο όπου στεγάζεται το πληροφοριακό σύστημα			
Προπομπός Κινδύνου:	Εμφάνιση αποθηκευμένων υλικών που μπορεί να προκαλέσουν εκρήξεις			
Στρατηγική Αντιμετώπισης:	Μετριασμός			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Έλεγχος των κτιριακών εγκαταστάσεων και του περιβάλλοντα χώρου για τυχόν εύφλεκτα υλικά όπου μπορεί να προκαλέσουν εκρήξεις και απομάκρυνση αυτών από το χώρο			
Διορθωτικά μέτρα:	Αποθήκευση των δεδομένων του συστήματος και σε άλλους servers σε άλλες περιοχές			
Εναλλακτικό σχέδιο:	Μετεγκατάσταση του εξοπλισμού σε άλλες κτιριακές εγκαταστάσεις			
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 91: Φύλλο κινδύνου #78 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #79				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Έντομα – τρωκτικά			
Σύντομη Περιγραφή:	Εγκατάσταση του πληροφοριακού συστήματος σε κτίριο όπου δεν έχει την κατάλληλη υποδομή και την απαραίτητη προστασία με αποτέλεσμα να εισβάλλουν στο χώρο διάφορα έντομα και τρωκτικά και να προκαλέσουν ζημιά στο υλικό του συστήματος			
Κατηγορία Κινδύνου:	Φυσικοί - Περιβαλλοντικοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.5	4	M_2	35	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Τακτικός έλεγχος του κτιρίου για εμφάνιση εντόμων και τρωκτικών			
Προπομπός Κινδύνου:	Εμφάνιση καταστροφών στο υλικό του συστήματος από τρωκτικά			
Στρατηγική Αντιμετώπισης:	Μετριασμός			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Τακτικός έλεγχος των κτιριακών εγκαταστάσεων και συχνή απολύμανση του χώρου όπου στεγάζεται το πληροφοριακό για τυχόν έντομα και τρωκτικά			
Διορθωτικά μέτρα:	Εγκατάσταση ειδικού εξοπλισμού όπου αποτρέπει τα έντομα και τρωκτικά να εισχωρήσουν στο χώρο			
Εναλλακτικό σχέδιο:	Ύπαρξη εφεδρικού εξοπλισμού σε περίπτωση φθοράς του υπάρχοντος			
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εξαμινιαία			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 92: Φύλλο κινδύνου #79 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #80				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κίνδυνος δονήσεων			
Σύντομη Περιγραφή:	Εγκατάσταση πληροφοριακού συστήματος σε περιοχή κοντά σε σιδηροδρομικό σταθμό ή σε εργοτάξιο			
Κατηγορία Κινδύνου:	Φυσικοί - Περιβαλλοντικοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.3	4	M_6	64	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος του κτιρίου όπου στεγάζεται το πληροφοριακό σύστημα για την ύπαρξη ιδιοτήτων αντικραδασμικής λειτουργίας			
Προπομπός Κινδύνου:	Μη ύπαρξη ιδιοτήτων αντικραδασμικής λειτουργίας			
Στρατηγική Αντιμετώπισης:	Μετριασμός			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Εγκατάσταση του πληροφοριακού συστήματος σε κτίριο όπου έχει αντικραδασμική λειτουργία			
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:	Μετεγκατάσταση του εξοπλισμού σε άλλες κτιριακές εγκαταστάσεις όπου βρίσκονται σε περιοχή με μειωμένη κραδασμική δραστηριότητα			
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 93: Φύλλο κινδύνου #80 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #81				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Καπνός - Μικροσωματίδια			
Σύντομη Περιγραφή:	Εγκατάσταση πληροφοριακού συστήματος σε σημείο όπου υπάρχουν μεγάλες ποσότητες καπνού και μικροσωματιδίων οι οποίες μπορεί να προκαλέσουν ζημιά στον εξοπλισμό του συστήματος			
Κατηγορία Κινδύνου:	Φυσικοί - Περιβαλλοντικοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.3	4	M_6	65	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος της καθαρότητας του αέρα			
Προπομπός Κινδύνου:	Εμφάνιση καπνού στο χώρο του πληροφοριακού συστήματος			
Στρατηγική Αντιμετώπισης:	Μετριασμός			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Τακτικός έλεγχος και συντήρηση του συστήματος εξαερισμού καθώς και τοποθέτηση του εξοπλισμού σε ειδικό χώρο			
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:	Μετεγκατάσταση του εξοπλισμού σε άλλες κτιριακές εγκαταστάσεις όπου βρίσκονται σε περιοχή με λιγότερο καπνό και ρύπους			
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 94: Φύλλο κινδύνου #81 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #82				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Μαγνήτες – μαγνητικά εργαλεία			
Σύντομη Περιγραφή:	Χρήση μαγνητών ή μαγνητικών εργαλείων μπορούν να προκαλέσουν βλάβη σε ευαίσθητο εξοπλισμό ή να διαγράψουν δεδομένα			
Κατηγορία Κινδύνου:	Φυσικοί - Περιβαλλοντικοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.5	5	Y_6	21	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Τακτικός έλεγχος της βάσης δεδομένων και καταμέτρηση των αποθηκευμένων δεδομένων στη βάση			
Προπομπός Κινδύνου:	Απώλεια δεδομένων/μη σωστή αποθήκευση των δεδομένων			
Στρατηγική Αντιμετώπισης:	Μετριασμός			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Τοποθέτηση πινακίδας απαγόρευσης όπου δεν θα επιτρέπει την είσοδο μαγνητών και μαγνητικών εργαλείων στο χώρο όπου βρίσκονται οι servers του συστήματος			
Διορθωτικά μέτρα:	Τοποθέτηση αισθητήρων ανίχνευσης μαγνητικών εργαλείων στην είσοδο του χώρου όπου βρίσκονται οι servers του συστήματος			
Εναλλακτικό σχέδιο:	Επιβολή ποινών σε όποιον δεν συμμορφώνεται με τους κανονισμούς			
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 95: Φύλλο κινδύνου #82 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #83				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Αγωγές – Μηνύσεις			
Σύντομη Περιγραφή:	Παράβλεψη ή καταπάτηση νομοθετικών ρυθμίσεων ή υπάρχουσας νομοθεσίας όσον αφορά τις διαδικασίες μετάδοσης πληροφορίας και τήρησης αρχείων προσωπικών δεδομένων			
Κατηγορία Κινδύνου:	Νομικοί - Κοινωνικοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.1	2	X_6	95	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση ορθής λειτουργίας του συστήματος και αποδοχής του από τα εμπλεκόμενα μέρη			
Προπομπός Κινδύνου:	Ύπαρξη σοβαρών αντιδράσεων			
Στρατηγική Αντιμετώπισης:	Μεταφορά			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 96: Φύλλο κινδύνου #83 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #84				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Απώλεια καλής φήμης			
Σύντομη Περιγραφή:	Μη αποτελεσματική λειτουργία του συστήματος λόγω λανθασμένου σχεδιασμού με αποτέλεσμα τη δυσαρέσκεια των τελικών χρηστών του συστήματος			
Κατηγορία Κινδύνου:	Νομικοί - Κοινωνικοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.1	3	X_5	93	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος της αποδοχής και της χρήσης του συστήματος από τα εμπλεκόμενα μέλη			
Προπομπός Κινδύνου:	Μη χρήση της εφαρμογής από τους χρήστες λόγω ύπαρξης λαθών / μη εύχρηστη εφαρμογή για τους τελικούς χρήστες του συστήματος			
Στρατηγική Αντιμετώπισης:	Μεταφορά			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 97: Φύλλο κινδύνου #84 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #85				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κλοπή πνευματικής ιδιοκτησίας			
Σύντομη Περιγραφή:	Κλοπή μέρων του λογισμικού του πληροφοριακού συστήματος από ανταγωνίστρια εταιρεία το οποίο υπόκειται σε καθεστώς πνευματικής ιδιοκτησίας			
Κατηγορία Κινδύνου:	Νομικοί - Κοινωνικοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.3	2	X_2	79	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση των εφαρμογών που χρησιμοποιούν ανταγωνίστριες εταιρείες			
Προπομπός Κινδύνου:	Χρήση εφαρμογής από ανταγωνίστρια εταιρεία με ίδια χαρακτηριστικά			
Στρατηγική Αντιμετώπισης:	Μεταφορά			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 98: Φύλλο κινδύνου #85 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #86				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Αλλαγή σχεδιασμού συστήματος ή ματαίωση κατασκευής του λόγω πολιτικών αποφάσεων			
Σύντομη Περιγραφή:	Αλλαγή πολιτικής ηγεσίας με αποτέλεσμα την αλλαγή ή ματαίωση κατασκευής του συστήματος και την ύπαρξη χρονικής καθυστέρησης ή κόστους			
Κατηγορία Κινδύνου:	Πολιτικοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.1	3	X_5	94	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση των πολιτικών αποφάσεων και δραστηριοτήτων της κυβέρνησης			
Προπομπός Κινδύνου:	Αποφάσεις μείωσης λειτουργικότητας και περιορισμού χρήσης του πληροφοριακού συστήματος			
Στρατηγική Αντιμετώπισης:	Αποδοχή			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:	Συμμετοχή των πολιτικών δυνάμεων στην απόφαση κατασκευής του συστήματος			
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 99: Φύλλο κινδύνου #86 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #87				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κίνδυνος καταστροφής του πληροφοριακού συστήματος λόγω πολιτικής αστάθειας			
Σύντομη Περιγραφή:	Εγκατάσταση του πληροφοριακού συστήματος σε περιοχή με πολιτικές αναταραχές / πολέμους			
Κατηγορία Κινδύνου:	Πολιτικοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.1	5	X_3	88	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση των πολιτικών αποφάσεων και δραστηριοτήτων της κυβέρνησης			
Προπομπός Κινδύνου:	Πολεμικές αναταραχές			
Στρατηγική Αντιμετώπισης:	Αποδοχή			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:	Συμμετοχή των πολιτικών δυνάμεων στην απόφαση να μην επηρεαστεί το έργο			
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 100: Φύλλο κινδύνου #87 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #88				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κλοπή υλικού			
Σύντομη Περιγραφή:	Εισβολή αγνώστων στο κτίριο που στεγάζεται το πληροφοριακό σύστημα με αποτέλεσμα την κλοπή υλικού απαραίτητου για τη σωστή λειτουργία του			
Κατηγορία Κινδύνου:	Εξωτερικοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.3	4	M_6	66	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος του εξοπλισμού και επιθεώρηση του χώρου όπου βρίσκεται ο εξοπλισμός σε τακτά χρονικά διαστήματα			
Προπομπός Κινδύνου:	Μη ταύτιση καταγεγραμμένου και υπάρχοντος εξοπλισμού			
Στρατηγική Αντιμετώπισης:	Μετριασμός			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Εγκατάσταση καμερών καθώς και συναγερμού στους χώρους όπου βρίσκεται ο εξοπλισμός			
Διορθωτικά μέτρα:	Συνεχής παρακολούθηση του χώρου όλο το 24ώρο			
Εναλλακτικό σχέδιο:	Ύπαρξη εφεδρικού εξοπλισμού			
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Κάθε μήνα			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 101: Φύλλο κινδύνου #88 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #89				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Βανδαλισμοί			
Σύντομη Περιγραφή:	Καταστροφή του εξοπλισμού από βανδαλισμούς αγνώστων ατόμων			
Κατηγορία Κινδύνου:	Εξωτερικοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.3	4	M_6	67	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος των κτιριακών εγκαταστάσεων όπου στεγάζεται το πληροφοριακό σύστημα καθώς και του εξοπλισμού του πληροφοριακού συστήματος			
Προπομπός Κινδύνου:	Καταστροφή του κτιρίου και του εξοπλισμού			
Στρατηγική Αντιμετώπισης:	Μετριασμός			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Εγκατάσταση καμερών και συνεχή παρακολούθηση των εισόδων του κτιρίου όπου στεγάζεται το πληροφοριακό σύστημα			
Διορθωτικά μέτρα:	Έλεγχος των ατόμων που εισέρχονται στο κτίριο επιδεικνύοντας κάποιο αποδεικτικό στοιχείο (π.χ. ΑΔΤ) και έκδοση καρτών με την ιδιότητα εισόδου τους στο κτήριο			
Εναλλακτικό σχέδιο:	Μετεγκατάσταση του εξοπλισμού σε άλλες κτιριακές εγκαταστάσεις			
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Κάθε μέρα			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 102: Φύλλο κινδύνου #89 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #90				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Εισβολείς (Hackers) – Υποκλοπή δεδομένων			
Σύντομη Περιγραφή:	Προσβολή του συστήματος από την επιδρομή hackers με αποτέλεσμα την ύπαρξη κινδύνου υποκλοπής μεταδιδόμενων πληροφοριών			
Κατηγορία Κινδύνου:	Εξωτερικοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.7	5	Y_3	5	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος του λογισμικού ασφαλείας			
Προπομπός Κινδύνου:	Υποκλοπή μεταδιδόμενων πληροφοριών			
Στρατηγική Αντιμετώπισης:	Μεταφορά			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Παρακολούθηση εισβολέων (hackers) με τη βοήθεια ειδικού λογισμικού			
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Κάθε μέρα			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 103: Φύλλο κινδύνου #90 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #91				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Εισβολείς (Hackers) – Καταστροφή δεδομένων			
Σύντομη Περιγραφή:	Προσβολή του συστήματος από την επιδρομή hackers με αποτέλεσμα την ύπαρξη κινδύνου καταστροφής δεδομένων			
Κατηγορία Κινδύνου:	Εξωτερικοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.7	5	Y_3	6	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος του λογισμικού ασφαλείας			
Προπομπός Κινδύνου:	Καταστροφή/ διαγραφή δεδομένων			
Στρατηγική Αντιμετώπισης:	Μεταφορά			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Κάθε μέρα			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 104: Φύλλο κινδύνου #91 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #92				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Ηλεκτρονικοί Εγκληματίες(Μετάδοση κακόβουλου λογισμικού)			
Σύντομη Περιγραφή:	Προσβολή του συστήματος από ηλεκτρονικούς εγκληματίες με αποτέλεσμα την αλλοίωση ή καταστροφή των αποθηκευμένων δεδομένων του συστήματος			
Κατηγορία Κινδύνου:	Εξωτερικοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.9	5	Y_1	2	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος του λογισμικού ασφαλείας			
Προπομπός Κινδύνου:	Μετάδοση κακόβουλου λογισμικού			
Στρατηγική Αντιμετώπισης:	Μεταφορά			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:	Ελεγχος σε καθημερινή βάση του Firewall και του antivirus			
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Κάθε μέρα			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 105: Φύλλο κινδύνου #92 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #93				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Πρώην εργαζόμενοι που εργάζονται για ανταγωνιστές			
Σύντομη Περιγραφή:	Αντιγραφή μερών ή ολόκληρου του σχεδιασμού του πληροφοριακού συστήματος από πρώην εργαζόμενους			
Κατηγορία Κινδύνου:	Εξωτερικοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.5	3	M_4	45	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση των εφαρμογών που χρησιμοποιούν ανταγωνίστριες εταιρείες			
Προπομπός Κινδύνου:	Χρήση εφαρμογής από ανταγωνίστρια εταιρεία με ίδια χαρακτηριστικά			
Στρατηγική Αντιμετώπισης:	Αποδοχή			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:	Όρος στο συμβόλαιο με τον εργαζόμενο για τη μη γνωστοποίηση σε τρίτους των εφαρμογών που κατασκευάζονται στην εταιρεία (ρήτρα επιστευτικότητας)			
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 106: Φύλλο κινδύνου #93 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #94				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κατασκοπεία			
Σύντομη Περιγραφή:	Υποκλοπή ευαίσθητων προσωπικών δεδομένων του πληθυσμού από εχθρικά κράτη			
Κατηγορία Κινδύνου:	Εξωτερικοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.3	4	M_6	68	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος του λογισμικού ασφαλείας			
Προπομπός Κινδύνου:	Υποκλοπή ευαίσθητων προσωπικών δεδομένων			
Στρατηγική Αντιμετώπισης:	Μεταφορά			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Κάθε μέρα			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 107: Φύλλο κινδύνου #94 του Fleetbroadband Provisioning System

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #95				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Τρομοκρατικές ενέργειες			
Σύντομη Περιγραφή:	Καταστροφή των εγκαταστάσεων που στεγάζεται το πληροφοριακό σύστημα λόγω τρομοκρατικών επιθέσεων σε διπλανό κτίριο ή και στο ίδιο κτίριο.			
Κατηγορία Κινδύνου:	Εξωτερικοί			
Ημερομηνία Αναγνώρισης:	17/02/2016			
Υπεύθυνος:	Δέλιος Ι.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία Ενημέρωσης**
0.3	4	M_6	69	20/02/2016
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος του χώρου εγκατάστασης του πληροφοριακού συστήματος και της συμπεριφοράς των εργαζομένων			
Προπομπός Κινδύνου:	Ύποπτες ενέργειες των εργαζομένων/ εύρεση ύποπτου εξοπλισμού στο χώρο			
Στρατηγική Αντιμετώπισης:	Μετριασμός			
Ημερομηνία Ενημέρωσης:	20/02/2016			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Συνεχής έλεγχος των εγκαταστάσεων όπου βρίσκεται ο εξοπλισμός για τυχόν εύρεση ύποπτων αντικειμένων εντός και εκτός του χώρου καθώς και ύποπτων συμπεριφορών των εργαζομένων			
Διορθωτικά μέτρα:	Χρήση ειδικού εξοπλισμού ανίχνευσης μετάλλων στην είσοδο του κτιρίου			
Εναλλακτικό σχέδιο:	Μετεγκατάσταση του εξοπλισμού σε άλλες κτιριακές εγκαταστάσεις			
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Κάθε μέρα			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	24/02/2016			

Πίνακας 108: Φύλλο κινδύνου #95 του Fleetbroadband Provisioning System

Εκτός από τα φύλλα κινδύνων, πρέπει να υπάρχει και μια συγκεντρωτική αναφορά των κινδύνων που θα ενημερώνει περιληπτικά τη Διοίκηση για την κατάσταση του κάθε κινδύνου.

# Φύλλο Κινδύνου	Ονομασία Κινδύνου	Έκθεση Κινδύνου	Κατάσταση Κινδύνου	Ημερομηνία Τελευταίας Ενημέρωσης	Υπεύθυνος
1	Ασυμβατότητα λογισμικού με τις απαιτήσεις	Y_6	Τελειωμένη	24/02/2016	Δέλιος Ι.
2	Εξάντληση πόρων του συστήματος	Y_6	Ανοιχτή	24/02/2016	Δέλιος Ι.
3	Λανθασμένη βάση δεδομένων αποθήκευσης των στοιχείων	X_3	Τελειωμένη	24/02/2016	Δέλιος Ι.
4	Ελλιπής ασφάλεια των προσωπικών δεδομένων των πολιτών	Y_1	Ανοιχτή	24/02/2016	Δέλιος Ι.
5	Δυσκολία σε αναβάθμιση – συντήρηση λογισμικού	M_6	Ανοιχτή	24/02/2016	Δέλιος Ι.
6	Έλλειψη διασυνδεσιμότητας του φορέων μέσω του συστήματος	M_4	Ανοιχτή	24/02/2016	Δέλιος Ι.
7	Λανθασμένος σχεδιασμός υλικού του συστήματος	X_3	Τελειωμένη	24/02/2016	Δέλιος Ι.
8	Λανθασμένος σχεδιασμός λογισμικού του συστήματος	X_3	Τελειωμένη	24/02/2016	Δέλιος Ι.
9	Ασυμβατότητα της τεχνολογίας του λογισμικού με τις υπάρχουσες κρατικές υποδομές ροής πληροφοριών	M_4	Κλειστή	24/02/2016	Δέλιος Ι.
10	Χρήση νέων και μη δοκιμασμένων τεχνολογιών ανάπτυξης λογισμικού	M_4	Τελειωμένη	24/02/2016	Δέλιος Ι.
11	Μη αποδεκτή ποιότητα λογισμικού	M_4	Τελειωμένη	24/02/2016	Δέλιος Ι.
12	Ελλιπείς μηχανισμοί ελέγχου ασφάλειας του πληροφοριακού συστήματος	X_3	Ανοιχτή	24/02/2016	Δέλιος Ι.
13	Αδυναμία σύνδεσης με τον κεντρικό Η/Υ εξαιτίας υπερφόρτωσης των τηλεπικοινωνιακών δικτύων ή εξαιτίας της μειωμένης αξιοπιστίας του δικτύου	M_2	Ανοιχτή	24/02/2016	Δέλιος Ι.
14	Ανεπαρκής προστασία κρυπτογραφικών κλειδιών	M_6	Ανοιχτή	24/02/2016	Δέλιος Ι.
15	Ελλιπής επικύρωση της επεξεργασίας των δεδομένων	M_6	Τελειωμένη	24/02/2016	Δέλιος Ι.
16	Δυσλειτουργία του υλικού	M_2	Κλειστή	24/02/2016	Δέλιος Ι.
17	Ανεπαρκής έλεγχος λογισμικού	M_2	Κλειστή	24/02/2016	Δέλιος Ι.
18	Σφάλματα λογισμικού	Y_6	Κλειστή	24/02/2016	Δέλιος Ι.
19	Πολυπλοκότητα λογισμικού	M_4	Κλειστή	24/02/2016	Δέλιος Ι.
20	Μη ασφαλής αρχιτεκτονική δικτύου	M_2	Τελειωμένη	24/02/2016	Δέλιος Ι.
21	Προβλήματα επικοινωνίας με την εταιρεία ανάθεσης έργου	M_7	Κλειστή	24/02/2016	Δέλιος Ι.
22	Μη επαρκώς καθορισμένοι όροι του συμβολαίου μεταξύ του κράτους και του αναδόχου	M_7	Τελειωμένη	24/02/2016	Δέλιος Ι.
23	Μη διαθεσιμότητα ομάδας υποστήριξης του συστήματος	M_2	Τελειωμένη	24/02/2016	Δέλιος Ι.
24	Έλλειψη συνεργασίας μεταξύ των ομάδων κατασκευής του έργου.	M_4	Κλειστή	24/02/2016	Δέλιος Ι.
25	Ελλιπής φύλαξη του κτιρίου όπου στεγάζεται το πληροφοριακό σύστημα από εξειδικευμένα άτομα(φύλακες)	M_4	Ανοιχτή	24/02/2016	Δέλιος Ι.
26	Ελλιπής χρόνος προσαρμογής χρήσης του νέου πληροφοριακού συστήματος	M_5	Κλειστή	24/02/2016	Δέλιος Ι.
27	Ανεπαρκής ή λανθασμένος διαχωρισμός των καθηκόντων	M_1	Κλειστή	24/02/2016	Δέλιος Ι.
28	Ανεπαρκής επίβλεψη εργαζομένων	M_2	Ανοιχτή	24/02/2016	Δέλιος Ι.

29	Ελλιπής διαδικασία για την αφαίρεση δικαιωμάτων πρόσβασης κατά την λήξη της απασχόλησης	M_6	Τελειωμένη	24/02/2016	Δέλιος Ι.
30	Ελλιπής σχεδιασμό τακτικών ελέγχων εύρυθμης λειτουργίας του λογισμικού	M_1	Τελειωμένη	24/02/2016	Δέλιος Ι.
31	Κίνδυνος εσφαλμένης εγκατάστασης υλικού ή λογισμικού από το προσωπικό της αναδόχου εταιρείας	Y_6	Τελειωμένη	24/02/2016	Δέλιος Ι.
32	Ανεπαρκής κάλυψη του κτιρίου από σύστημα συναγερμού	Y_4	Ανοιχτή	24/02/2016	Δέλιος Ι.
33	Ανεπαρκής κάλυψη του κτιρίου από σύστημα πυρανίχνευσης	Y_4	Ανοιχτή	24/02/2016	Δέλιος Ι.
34	Ανεπαρκής κάλυψη του κτιρίου από σύστημα αναγνώρισης και ελέγχου ταυτότητας	Y_4	Ανοιχτή	24/02/2016	Δέλιος Ι.
35	Έλλειψη οικονομικών πόρων	M_4	Ανοιχτή	24/02/2016	Δέλιος Ι.
36	Προβλήματα με την χρηματοδότηση του έργου	M_5	Ανοιχτή	24/02/2016	Δέλιος Ι.
37	Καταστροφή υλικού ή λογισμικού από τους χειριστές του συστήματος	Y_4	Ανοιχτή	24/02/2016	Δέλιος Ι.
38	Κλοπή υλικού από εργαζομένους	Y_4	Ανοιχτή	24/02/2016	Δέλιος Ι.
39	Απεργίες εργαζομένων που διαχειρίζονται το πληροφοριακό σύστημα	M_2	Ανοιχτή	24/02/2016	Δέλιος Ι.
40	Κίνδυνος απροθυμίας προσαρμογής στην αλλαγή	Y_4	Ανοιχτή	24/02/2016	Δέλιος Ι.
41	Καταστροφή εξοπλισμού από υγρά/τρόφιμα	M_2	Ανοιχτή	24/02/2016	Δέλιος Ι.
42	Διαρροή πληροφοριών	Y_4	Ανοιχτή	24/02/2016	Δέλιος Ι.
43	Μη εξουσιοδοτημένη πρόσβαση στους χώρους του πληροφοριακού συστήματος	Y_4	Ανοιχτή	24/02/2016	Δέλιος Ι.
44	Μη εξουσιοδοτημένη πρόσβαση στο πληροφοριακό σύστημα από τους εργαζόμενους	Y_3	Ανοιχτή	24/02/2016	Δέλιος Ι.
45	Διαρροή κωδικών εισόδου και διαχείρισης του πληροφοριακού συστήματος	Y_3	Ανοιχτή	24/02/2016	Δέλιος Ι.
46	Μη εξουσιοδοτημένες αλλαγές αρχείων	M_4	Τελειωμένη	24/02/2016	Δέλιος Ι.
47	Ακούσια αλλαγή των δεδομένων του πληροφοριακού συστήματος	M_4	Ανοιχτή	24/02/2016	Δέλιος Ι.
48	Έλλειψη κινήτρων για τους εργαζόμενους	M_2	Ανοιχτή	24/02/2016	Δέλιος Ι.
49	Έλλειψη ευαισθητοποίησης σε θέματα ασφάλειας	Y_4	Ανοιχτή	24/02/2016	Δέλιος Ι.
50	Σύνδεση προσωπικών συσκευών στο εταιρικό δίκτυο	Y_4	Ανοιχτή	24/02/2016	Δέλιος Ι.
51	Εγκατάσταση μη εξουσιοδοτημένου λογισμικού και εφαρμογών	M_4	Τελειωμένη	24/02/2016	Δέλιος Ι.
52	Ακούσια μεταφορά εμπιστευτικών δεδομένων του πληροφοριακού συστήματος εκτός γραφείου	M_2	Ανοιχτή	24/02/2016	Δέλιος Ι.
53	Έλλειψη της απαιτούμενης εκπαίδευσης του προσωπικού	X_1	Ανοιχτή	24/02/2016	Δέλιος Ι.
54	Εσωτερικοί κίνδυνοι (δόλος)	M_8	Ανοιχτή	24/02/2016	Δέλιος Ι.
55	Λάθος κατανομή του κεφαλαίου	M_8	Τελειωμένη	24/02/2016	Δέλιος Ι.
56	Λανθασμένη κατανομή σημαντικότητας στις εφαρμογές του συστήματος	M_6	Τελειωμένη	24/02/2016	Δέλιος Ι.
57	Έλλειψη εφεδρικού σχεδίου απρόσκοπτης λειτουργίας του συστήματος	M_2	Τελειωμένη	24/02/2016	Δέλιος Ι.
58	Λανθασμένη πρόβλεψη απαιτούμενων πόρων υλικού	M_4	Τελειωμένη	24/02/2016	Δέλιος Ι.

59	Αλλαγή του χρονοδιαγράμματος λόγω λανθασμένου αρχικού προγραμματισμού	M_7	Ανοιχτή	24/02/2016	Δέλιος Ι.
60	Λανθασμένη κοστολόγηση του έργου	M_4	Ανοιχτή	24/02/2016	Δέλιος Ι.
61	Κοινή χρήση εμπιστευτικών δεδομένων με τους συνεργάτες και τους προμηθευτές	M_8	Ανοιχτή	24/02/2016	Δέλιος Ι.
62	Έλλειψη εμπειρίας και τεχνογνωσίας των προσώπων που είναι υπεύθυνα για την παρακολούθηση της υλοποίησης του έργου	M_6	Ανοιχτή	24/02/2016	Δέλιος Ι.
63	Λανθασμένες αποφάσεις διαχείρησης κινδύνων	X_4	Ανοιχτή	24/02/2016	Δέλιος Ι.
64	Κίνδυνος σεισμού	M_4	Ανοιχτή	24/02/2016	Δέλιος Ι.
65	Κίνδυνος κεραυνού	M_6	Ανοιχτή	24/02/2016	Δέλιος Ι.
66	Κίνδυνος πλημμύρας	M_6	Ανοιχτή	24/02/2016	Δέλιος Ι.
67	Κίνδυνος πυρκαγιάς	Y_4	Ανοιχτή	24/02/2016	Δέλιος Ι.
68	Κίνδυνος διαρροής υδάτων	X_4	Ανοιχτή	24/02/2016	Δέλιος Ι.
69	Κίνδυνος αδυναμίας ηλεκτροδότησης του συστήματος λόγω ελλείψεων στην ηλεκτρολογική εγκατάσταση	M_6	Ανοιχτή	24/02/2016	Δέλιος Ι.
70	Κατολίσθηση – διάβρωση εδάφους	X_3	Ανοιχτή	24/02/2016	Δέλιος Ι.
71	Ηλιακές εκλάμψεις	X_5	Ανοιχτή	24/02/2016	Δέλιος Ι.
72	Σκόνη	M_7	Ανοιχτή	24/02/2016	Δέλιος Ι.
73	Βλάβη του συστήματος κλιματισμού	M_6	Ανοιχτή	24/02/2016	Δέλιος Ι.
74	Ηλεκτρομαγνητικές παρεμβολές	M_8	Ανοιχτή	24/02/2016	Δέλιος Ι.
75	Στατικός ηλεκτρισμός	X_4	Ανοιχτή	24/02/2016	Δέλιος Ι.
76	Έκρηξη ηφαιστείου	X_3	Ανοιχτή	24/02/2016	Δέλιος Ι.
77	Πυρηνικό ατύχημα	X_3	Ανοιχτή	24/02/2016	Δέλιος Ι.
78	Κίνδυνος εκρήξεων	M_4	Ανοιχτή	24/02/2016	Δέλιος Ι.
79	Έντομα –τρωκτικά	M_2	Ανοιχτή	24/02/2016	Δέλιος Ι.
80	Κίνδυνος δονήσεων	M_6	Ανοιχτή	24/02/2016	Δέλιος Ι.
81	Καπνός – Μικροσωματίδια	M_6	Ανοιχτή	24/02/2016	Δέλιος Ι.
82	Μαγνήτες – μαγνητικά εργαλεία	Y_6	Ανοιχτή	24/02/2016	Δέλιος Ι.
83	Αγωγές – Μηνύσεις	X_6	Ανοιχτή	24/02/2016	Δέλιος Ι.
84	Απώλεια καλής φήμης	X_5	Ανοιχτή	24/02/2016	Δέλιος Ι.
85	Κλοπή πνευματικής ιδιοκτησίας	X_2	Ανοιχτή	24/02/2016	Δέλιος Ι.
86	Αλλαγή σχεδιασμού συστήματος ή ματαίωση κατασκευής του λόγω πολιτικών αποφάσεων	X_5	Ανοιχτή	24/02/2016	Δέλιος Ι.
87	Κίνδυνος καταστροφής του πληροφοριακού συστήματος λόγω πολιτικής αστάθειας	X_3	Ανοιχτή	24/02/2016	Δέλιος Ι.
88	Κλοπή υλικού	M_6	Ανοιχτή	24/02/2016	Δέλιος Ι.
89	Βανδαλισμοί	M_6	Ανοιχτή	24/02/2016	Δέλιος Ι.

90	Εισβολείς (Hackers) – Υποκλοπή δεδομένων	Y_3	Ανοιχτή	24/02/2016	Δέλιος Ι.
91	Εισβολείς (Hackers) – Καταστροφή δεδομένων	Y_3	Ανοιχτή	24/02/2016	Δέλιος Ι.
92	Ηλεκτρονικοί εγκληματίες (Μετάδοση κακόβουλου λογισμικού)	Y_1	Ανοιχτή	24/02/2016	Δέλιος Ι.
93	Πρώην εργαζόμενοι που εργάζονται για ανταγωνιστές	M_4	Ανοιχτή	24/02/2016	Δέλιος Ι.
94	Κατασκοπεία	M_6	Ανοιχτή	24/02/2016	Δέλιος Ι.
95	Τρομοκρατικές ενέργειες	M_6	Ανοιχτή	24/02/2016	Δέλιος Ι.

Πίνακας 109: Μητρώο Κινδύνων – Παρακολούθηση κινδύνων του Fleetbroadband Provisioning System

ΚΕΦΑΛΑΙΟ 7

Συμπεράσματα

Σύμφωνα με όλα τα παραπάνω έγινε σαφής η αξία και η επιτακτικότητα της εφαρμογής των διαδικασιών διαχείρισης κινδύνων σε μεγάλα πληροφοριακά έργα. Όσο μεγαλύτερο είναι το κόστος των έργων αυτών, η πολυπλοκότητά τους και η αξία τους για τη λειτουργία ενός οργανισμού τόσο σημαντικότερο εργαλείο για την εξασφάλιση της επιτυχημένης υλοποίησης τους αποτελεί η διαχείριση κινδύνων. Μέσα από αυτή μπορούν να προβλεφθούν τα προβλήματα που ενδέχεται να εμφανιστούν κατά την πορεία υλοποίησης του έργου και να προκαλέσουν σημαντικές απώλειες είτε από πλευράς κόστους, είτε από πλευράς χρόνου ολοκλήρωσης των εργασιών, είτε στην ποιότητα και την αξιοπιστία του. Η ευθύνη της διαχείρισης κινδύνων δεν τελειώνει εδώ καθώς καλείται να παρουσιάσει και τον τρόπο με τον οποίο θα μειωθεί η έκθεση του έργου στον κάθε κίνδυνο, να παρακολουθεί την εφαρμογή των μέτρων που συνέστησε αλλά και τον κίνδυνο που απομένει και μετά την εφαρμογή των μέτρων αυτών.

Η διαχείριση κινδύνων είναι μια αυστηρά δομημένη διαδικασία της οποίας τα βήματα θα πρέπει να εκτελούνται με επιμέλεια και σύνεση, καθώς μόνο έτσι θα καταφέρει να επιτύχει τους στόχους της.

Στην παρούσα εργασία εξετάστηκε η εφαρμογή της διαδικασίας διαχείρισης κινδύνων στο έργο: «Fleetbroadband Provisioning System». Αφού πραγματοποιήθηκε η ανάλυση του έργου και καθορίστηκαν οι στόχοι του, εισήχθησαν οι κίνδυνοι που μπορεί να επηρεάσουν την ποιότητα, την αξιοπιστία, το κόστος και το χρονοδιάγραμμα του έργου. Στη συνέχεια πραγματοποιήθηκε ποιοτική ανάλυση των κινδύνων αυτών και παρουσιάστηκαν κάποιες μετρήσεις όσον αφορά την πιθανότητα εμφάνισης των κινδύνων, το επίπεδο των επιπτώσεων τους και το συνολικό επίπεδο έκθεσης σε κάθε κίνδυνο. Από τα αποτελέσματα που εξήχθησαν έγινε αντιληπτό ποιοι κίνδυνοι μπορεί να επηρεάσουν το έργο. Γι’ αυτό το λόγο, προτάθηκαν και τρόποι αντιμετώπισης των κινδύνων αυτών.

Πιο συγκεκριμένα :

- Οι περισσότεροι κίνδυνοι ανήκουν στην κατηγορία των τεχνολογικών κινδύνων εφόσον πρόκειται για έργο πληροφορικής.
- Σύμφωνα με την έκθεση των κινδύνων σημαντικότεροι θεωρούνται οι κίνδυνοι που είναι σχετικοί με την ασφάλεια προσωπικών δεδομένων.
- Λόγω της φύσης του έργου η συνήθης στρατηγική αντιμετώπισης είναι η μεταφορά.
- Όσον αφορά την κατάσταση του κάθε κινδύνου οι περισσότεροι κίνδυνοι έχουν κατάσταση ανοιχτή με δεδομένο ότι δεν έχουν εμφανιστεί.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1) A guide to the project management body of knowledge (PMBOK GUIDE) Fourth Edition.
2) Inmarsat PSA. Ενεργοποίηση καρτών Inmarsat. Ανάκτηση 2016 από http://www.otesat-maritel.com/Support/article/151/psa.html
3) Inmarsat Fleetbroad features. Ανάκτηση 2016 από http://www.inmarsat.com/service-collection/fleetbroadband/
4) Stoneburner, G., Goguen A. & Feringa, A. (2002).*Risk Management Guide for Information Tecnology Systems*. Ανάκτηση 2015 από http://dl.acm.org/citation.cfm?id=2206240
5) Wallumer, E. *Risk Management for It and Software Projects.* Ανάκτηση 2015 από http://www.itq.ch/pdf/RM__ITProjekteV211.pdf
6) Kyriazoglou, J., Kyriazoglou, C., Sygkouna, I. (2007). *Πρότυπο Διαχείρισης Κινδύνου.* Ανάκτηση 2015 από http://www.theirm.org/media/886331/Risk_Management_Standard_Greek_000.pdf
7) Configuring the Fleetbroadband terminal for static IP. Ανάκτηση 2015 από http://www.groundcontrol.com/fleetbroadband/Configuring_the_FleetBroadband_terminal_for_static_IP.pdf
8) Θεμιστοκλέους Μαρίνος, Risk Managemnet, Σημειώσεις Πανεπιστημίου Πειραιώς, Τμήμα Ψηφιακών Συστημάτων.
9) FleetBroadband Best Practices Manual. Ανάκτηση 2015 από http://www.inmarsat.com/wp-content/uploads/2013/10/Inmarsat_FleetBroadband_Best_Practices_Manual.pdf
10) *An onymous*, Introduction: Conducting risk assessments, online, Διαθέσιμο από: http://toolboxes.flexiblelearning.net.au/demosites/series9/904/toolbox904/u2_cond_risk_ass/u210_estab_conte/u210_estab_conte.htm
11) *Gardner C*, Cloud Computing Risk Management Begins With Proper Vendor Selection, online, 2015, © ClearRisk™ Inc., Διαθέσιμο από: http://articles.clearrisk.com/risk-management-blog-0/bid/28305/Cloud-Computing-Risk-Management-Begins-With-Proper-Vendor-Selection
12) *Anonymous*, Risk Assessment Template, online, © ER Technical Inc. 2015, Διαθέσιμο από: http://internationalbusinessphd.com/