ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΤΜΗΜΑ ΟΡΓΑΝΩΣΗΣ & ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΕΥΡΩΠΑΙΚΟ ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΤΗ ΔΙΟΙΚΗΣΗ ΕΠΙΧΕΙΡΗΣΕΩΝ-ΟΛΙΚΗ ΠΟΙΟΤΗΤΑ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΕΦΑΡΜΟΓΗ ΤΟΥ ΠΡΟΤΥΠΟΥ ISO/IEC 27001:2005 ΣΤΗ ΔΙΑΧΕΙΡΙΣΗ ΚΡΙΣΙΜΩΝ ΠΛΗΡΟΦΟΡΙΩΝ ΤΗΣ ΥΠΗΡΕΣΙΑΣ ΠΟΛΙΤΙΚΗΣ ΑΕΡΟΠΟΡΙΑΣ

ΒΑΣΙΛΙΚΗ Μ. ΚΑΡΔΑΡΗ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ

ΑΘΑΝΑΣΙΟΣ. Γ. ΛΑΓΟΔΗΜΟΣ
ΚΑΘΗΓΗΤΗΣ ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΠΕΙΡΑΙΑ

2011

ΕΦΑΡΜΟΓΗ ΤΟΥ ΠΡΟΤΥΠΟΥ ISO/IEC 27001:2005
ΣΤΗ ΔΙΑΧΕΙΡΙΣΗ ΚΡΙΣΙΜΩΝ ΠΛΗΡΟΦΟΡΙΩΝ ΤΗΣ ΥΠΗΡΕΣΙΑΣ ΠΟΛΙΤΙΚΗΣ ΑΕΡΟΠΟΡΙΑΣ

ΠΕΡΙΛΗΨΗ

Η ασφάλεια των πληροφοριών αποτελεί αναμφισβήτητα σήμερα ένα από τα κεντρικά αντικείμενα ενδιαφέροντος των οργανισμών. Δίχως αυτήν ο εκάστοτε οργανισμός βρίσκεται αντιμέτωπος με πληθώρα κινδύνων που ενδέχεται να οδηγήσουν σε δυσλειτουργία, απώλεια φήμης ή ακόμα και σε νομικές κυρώσεις.

Οι οργανισμοί στην προσπάθειά τους να εξαλείψουν τους κινδύνους που απειλούν την ασφάλεια των πληροφοριών τους δαπανούν ενίοτε σημαντικά ποσά προκειμένου να εγκαταστήσουν διάφορες τεχνολογικές λύσεις. Η διαχείριση όμως της ασφάλειας των πληροφοριών είναι πολλά περισσότερα από την απλή εγκατάσταση ορισμένων εξειδικευμένων τεχνικών λύσεων, περιλαμβάνει και άλλες συνιστώσες, όπως τα άτομα και τις διαδικασίες.

Το πρότυπο ISO/IEC 2001:2005 «Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών-Απαιτήσεις» προέκυψε από την ανάγκη να ληφθούν υπόψη αυτές οι συνιστώσες. Το εν λόγω πρότυπο πραγματεύεται την ασφάλεια των πληροφοριών και προσεγγίζει τα άτομα, τις διαδικασίες και την τεχνολογία ενός οργανισμού συνολικά μέσα από ένα «Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών» - ISMS (Information Security Management System). Ο σχεδιασμός, η υλοποίηση, ο έλεγχος και η συνεχής βελτίωση ενός ISMS με βάση τις οδηγίες και τις απαιτήσεις του προτύπου θα βοηθήσει τον οργανισμό να διασφαλίσει την ασφάλεια των πληροφοριών του.

Το πρότυπο είναι σχετικά καινούριο και η παρούσα διπλωματική εργασία θέλοντας να συνεισφέρει σε επίπεδο εμπειρικής έρευνας παρουσιάζει μια εμπειρική μελέτη του προτύπου σε ένα υπαρκτό οργανισμό σε ένα εν λειτουργία «Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών», εκείνο της Υπηρεσίας Πολιτικής Αεροπορίας.

Ο λόγος που επιλέχτηκε ο συγκεκριμένος οργανισμός είναι επειδή η ποιότητα των αεροναυτικών πληροφοριών που είναι υποχρεωμένος σύμφωνα με το Διεθνή Οργανισμό Πολιτικής Αεροπορίας, να παρέχει στους αεροναυτιλωμένους, όπως πιλότους και αεροπορικές εταιρείες είναι ζωτικής σημασίας για την ασφαλή πλοήγηση των αεροσκαφών.

Συγκεκριμένα, το υπάρχον «Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών» που εφαρμόζει η Υπηρεσία Πολιτικής Αεροπορίας στη βασική διεργασία έκδοσης και διανομής ενός από τα σημαντικότερα εγγράφα αεροναυτιλίας, του «Εγχειριδίου Αεροναυτικών Πληροφοριών AIP (Aeronutical Information Publication», εξετάστηκε ως προς το σχεδιασμό, την υλοποίηση, τον έλεγχο και τη συνεχή βελτίωσή του ώστε να προκύψει ο βαθμός κατά τον οποίο πληροί τις απαιτήσεις του προτύπου ISO/IEC 27001:2005 και όπου υπήρξε απόκλιση προτάθηκαν εναλλακτικοί τρόποι προσέγγισης.

Ευχής έργον θα είναι η παρούσα εργασία να συνεισφέρει στη βαθύτερη κατανόηση του προτύπου μέσα από τη θεωρητική παρουσίαση και ανάλυσή του, αλλά και να

συμβάλλει στη βελτίωση της υφιστάμενης διεργασίας που ισχύει σήμερα στην Υπηρεσία Πολιτικής Αεροπορίας.

Περιεχόμενα

ΕΥΧΑΡΙΣΤΙΕΣ

Η παρούσα εργασία αποτελεί τη Διπλωματική μου Εργασία στα πλαίσια των σπουδών μου στο μεταπτυχιακό πρόγραμμα στη Διοίκηση επιχειρήσεων-Ολική ποιότητα (MBA-TQM) του Πανεπιστημίου Πειραιώς υπό την επίβλεψη του καθηγητή κ. Αθανάσιου Λαγοδήμου, στον οποίο οφείλω ιδιαίτερες ευχαριστίες τόσο για την ανάθεση της εργασίας όσο και για τη γενικότερη συμβολή του στην ολοκλήρωσή της. Με την ευκαιρία αυτή θα ήθελα να ευχαριστήσω θερμά τον κ. Παναγιώτη Χουντάλα, για τη βοήθεια, τις πολύτιμες συμβουλές, την υποστήριξη και την καθοδήγηση που μου παρείχε καθ' όλη τη διάρκεια εκπόνησης της εργασίας.

1. ΕΙΣΑΓΩΓΗ

1.1. Αντικείμενο

Το αντικείμενο της παρούσας εργασίας είναι η θεωρητική ανάλυση ενός σχετικά πρόσφατου προτύπου, του ISO/IEC 27001:2005 «*Συστήματα διαχείρισης ασφάλειας πληροφοριών- Απαιτήσεις*», αλλά παράλληλα και η εμπειρική μελέτη του σε έναν οργανισμό που διαχειρίζεται πληροφορίες, η ασφάλεια των οποίων θεωρείται κρίσιμη.

Η «Ασφάλεια» ως μια από τις βασικές αρχές της Διοίκησης Ολικής Ποιότητας (αξιοπιστία, ανταποκρισιμότητα, πάθος, απτά στοιχεία, ασφάλεια) και οριζόμενη ως « η ικανότητα δημιουργίας αισθήματος εμπιστοσύνης», (Parasuraman,1990) αποτελεί πλέον το επίκεντρο της ποιότητας των διαδικασιών (Coulson,1997). Οργανισμοί ανεξαρτήτου είδους εργασιών ή μεγέθους, που επιθυμούν να λειτουργούν σύμφωνα με τις αρχές της Διοίκησης Ολικής Ποιότητας, οφείλουν να τη λαμβάνουν σοβαρά υπ'οψιν (Khosrow-Pour,2004).

Συγκεκριμένα, η ασφάλεια των πληροφοριών, αποτελεί αναμφισβήτητα σήμερα ένα από τα κεντρικά αντικείμενα ενδιαφέροντος των επιστημόνων τόσο σε τεχνικό όσο και σε οικονομικό και διοικητικό επίπεδο. Σύμφωνα με την κλασσική προσέγγιση ασφάλεια νοείται η διατήρηση τριών βασικών ιδιοτήτων της πληροφορίας : της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας (Κάτσικας,2001).

Δίχως ασφάλεια πληροφοριών, ο εκάστοτε οργανισμός βρίσκεται αντιμέτωπος με τις διάφορες αρνητικές επιπτώσεις συμπεριλαμβανομένων των οικονομικών συνεπειών, της μη προστασίας της πνευματικής του ιδιοκτησίας, της απώλειας μεριδίου αγοράς, της μειωμένης αποδοτικότητας,της μη συμμόρφωσης με τους νόμους και τους κανονισμούς και της απώλειας φήμης.

Για τον σκοπό αυτό κρίνεται απαραίτητη η ανάπτυξη και ενσωμάτωση στην λειτουργία του οργανισμού, ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών. Το εν λόγω Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (Information Security Management System–ISMS) συνιστά μια συνολική και συστηματική προσέγγιση του οργανισμού στην ορθή διαχείριση της ευαίσθητης πληροφορίας του και των κινδύνων που την απειλούν, έτσι ώστε η πληροφορία να παραμένει ασφαλής.

Μετά την ανάπτυξη και εφαρμογή στον οργανισμό ενός τέτοιου Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών, η πιστοποίηση του κατά το πρότυπο ISO/IEC 27001:2005 είναι ένας τρόπος διαβεβαίωσης ότι ο πιστοποιημένος οργανισμός έχει

εφαρμόσει ένα σύστημα για τη διαχείριση της ασφάλειας των πληροφοριών του σύμφωνα με τις απαιτήσεις του προτύπου.

1.2. Βασικός Σκοπός

Αυτός είναι και ο κεντρικός σκοπός της παρούσας διπλωματικής εργασίας, να μελετηθεί ο βαθμός κατά τον οποίο το «Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών» ενός οργανισμού που διαχειρίζεται κρίσιμες πληροφορίες, όπως η Υ.Π.Α (Υπηρεσία Πολιτικής Αεροπορίας), πληροί τις απαιτήσεις του προτύπου ISO/IEC 27001:2005.

Ο λόγος που επιλέχτηκε ο συγκεκριμένος οργανισμός είναι ότι η ποιότητα των αεροναυτικών πληροφοριών που είναι υποχρεωμένος, σύμφωνα με το Διεθνή Οργανισμό Πολιτικής Αεροπορίας, να παρέχει στους αεροναυτιλομένους, όπως πιλότους και αεροπορικές εταιρείες, είναι ζωτικής σημασίας για την ασφαλή πλοήγηση των αεροσκαφών.

Οι πληροφορίες αυτές είναι μέρος ενός ευρύτερου δικτύου παροχής αεροναυτικών υπηρεσιών που παρέχει η ΥΠΑ. Μερικές από αυτές είναι το «Εγχειρίδιο Αεροναυτικών Πληροφοριών AIP (Aeronautical Information Publication)», οι «Αεροναυτικές Αγγελίες NOTAM», τα «Δελτία Αεροναυτικών Πληροφοριών AIC (Aeronautical Information Circulars)» και τα «Δελτία Διαδρομής προ πτήσεως PIB (Pre-flight Information Bulleting)».

Λόγω όμως του τεράστιου όγκου δεδομένων, στη συγκεκριμένη εργασία πρόκειται να μελετηθεί η δυνατότητα εφαρμογής του προτύπου μόνο στη διεργασία έκδοσης και ενημέρωσης του «Εγχειριδίου Αεροναυτικών Πληροφοριών-AIP (Aeronautical Information Publication)».

Οι πληροφορίες που εμπεριέχονται σε αυτό το εγχειρίδιο αφορούν διαδικασίες που πρέπει να ακολουθούν τα αεροσκάφη κατά τη φάση προσέγγισης ή αναχώρησης, προς ή από ένα αεροδρόμιο και συνεπώς είναι απολύτως αναγκαίο να έχουν αξιοπιστία, ακεραιότητα, εμπιστευτικότητα, διαθεσιμότητα. Αυτός είναι και ο λόγος που τα τελευταία χρόνια σε όλο και περισσότερες χώρες υπάρχει η απαίτηση οι πληροφορίες αυτές να είναι και πιστοποιημένες.

Τα οφέλη λοιπόν για έναν οργανισμό όπως η Υπηρεσία Πολιτικής Αεροπορίας από την υιοθέτηση ενός «Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών» το οποίο θα είναι πιστοποιήσιμο κατά ISO/IEC 27001:2005 προβλέπονται να είναι πολλαπλά και πολυσήμαντα.

Παράλληλα όμως, υπάρχουν και επιμέρους στόχοι, όπως να γίνει επιπρόσθετα κατανοητό το πρότυπο ISO/IEC 27001:2005 μέσα από την θεωρητική παρουσίαση και ανάλυση του, αλλά και να παρουσιαστούν προτάσεις και τρόποι οι οποίοι θα συμβάλλουν στη βελτίωση της υφιστάμενης διεργασίας που ισχύει στην Υ.Π.Α.

1.3. Μεθοδολογία

Η μεθοδολογία που ακολουθήθηκε για να υλοποιηθούν οι παραπάνω στόχοι, συνοψίζεται σε τέσσερα βήματα. Αρχικά, αποτυπώθηκε η βασική διεργασία «Έκδοση & Ενημέρωση του Εγχειριδίου Αεροναυτικών Πληροφοριών AIP (Aeronautical Information Publication)». Έπειτα, παρουσιάστηκαν οι απαιτήσεις του προτύπου. Στη συνέχεια, πραγματοποιήθηκε σύγκριση ανάμεσα στις απαιτήσεις και στην υπάρχουσα διεργασία. Τέλος, όπου υπήρξε απόκλιση μεταξύ των δύο προτάθηκαν εναλλακτικοί τρόποι προσέγγισης.

Όλες οι πληροφορίες που χρησιμοποιήθηκαν στην παρούσα εργασία ήταν αποτέλεσμα επιτόπιων ερευνών, οι οποίες διεξήχθηκαν στην Υ.Π.Α. Ειδικότερα, αναζητήθηκε το οργανόγραμμα, πραγματοποιήθηκαν συνεντεύξεις με στελέχη και αρμόδιους υπαλλήλους των εμπλεκόμενων διευθύνσεων και των αντίστοιχων τμημάτων τους. Επίσης, ελέγχθηκαν έγγραφα, έντυπα, αρχεία, εγχειρίδια, οδηγίες, μελετήθηκαν σχετικές εταιρικές παρουσιάσεις, παρακολουθήθηκε εν λειτουργία η ηλεκτρονική εφαρμογή **eAIP.wiz@rd**, ενώ δεν θα μπορούσε να παραληφθεί η ουσιαστική μελέτη ενός πρόσφατου «Εγχειριδίου Αεροναυτικών Πληροφοριών AIP».

1.4. Δομή

Εφαλτήριο της εργασίας είναι το κεφάλαιο 2, το οποίο περιλαμβάνει τη βιβλιογραφική ανασκόπηση. Η εξέλιξη του προτύπου από έναν κώδικα ορθής πρακτικής στο πρότυπο ISO/IEC 27001:2005 που είναι σήμερα παρουσιάζεται αναλυτικά μέσα από μια ιστορική αναδρομή. Ενώ, το κεφάλαιο συμπληρώνεται με μια ανασκόπηση του προτύπου αρχικά σε θεωρητικό και στη συνέχεια σε εμπειρικό επίπεδο.

Η μεθοδολογία παρουσιάζεται στο τρίτο κεφάλαιο. Όπου γίνεται αναφορά στην έρευνα η οποία διεξήχθη στον οργανισμό, προκειμένου να συγκεντρωθούν όλες εκείνες οι απαραίτητες πληροφορίες για τη μελέτη του συστήματος διαχείρισης ασφάλειας αεροναυτικών πληροφοριών που εφαρμόζει η Υ.Π.Α. Ενώ, συγχρόνως παρουσιάζεται και η μεθοδολογία που ακολουθήθηκε, ούτος ώστε να προκύψει ο βαθμός κατά τον οποίο το σύστημα διαχείρισης αεροναυτικών πληροφοριών που εφαρμόζει η Υ.Π.Α πληροί τις απαιτήσεις του προτύπου ISO/IEC 27001:2005.

Στο τέταρτο κεφάλαιο αποτυπώνεται η βασική διεργασία έκδοσης και ενημέρωσης του «Εγχειριδίου Αεροναυτικών Πληροφοριών-AIP» καθώς και οι τρείς υποδιεργασίες στις οποίες αναλύεται, «Συλλογή & καταγραφή αεροναυτικών πληροφοριών», «Επεξεργασία αεροναυτικών πληροφοριών» και «Έκδοση & διανομή «Εγχειριδίου Αεροναυτικών Πληροφοριών-AIP».

Στη συνέχεια, στο πέμπτο κεφάλαιο αναφέρονται αναλυτικά οι απαιτήσεις του προτύπου ISO/IEC 27001:2005 όπως και το «Παράρτημα Α-*Στόχοι ελέγχων & έλεγχοι*». Συγχρόνως, πραγματοποιείται μια σύγκριση μεταξύ της βασικής διεργασίας έκδοσης και ενημέρωσης του Εγχειριδίου AIP και των απαιτήσεων του προτύπου, ώστε να προκύψει ο βαθμός ικανοποίησής τους. Επιπρόσθετα, η παρουσίαση κάθε απαίτησης ακολουθείται από προτάσεις και εναλλακτικούς τρόπους διενέργειας κάποιων σταδίων της υπάρχουσας διεργασίας έχοντας ως στόχο τη περαιτέρω σύγκλισή της στις απαιτήσεις του προτύπου.

Εν κατακλείδι, στο τελευταίο έκτο κεφάλαιο, παραθέτονται τα συμπεράσματα που προέκυψαν από τα προαναφερθείσα κεφάλαια σχετικά με το βαθμό κατά τον οποίο το «Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών» της Υ.Π.Α (Υπηρεσία Πολιτικής Αεροπορίας), πληροί τις απαιτήσεις του προτύπου ISO/IEC 27001:2005, μέσα από την οπτική της θεωρίας του κύκλου του Deming «Σχεδιασμός-Υλοποίηση-Έλεγχος-Συνεχής Βελτίωση».

2. ΒΙΒΛΙΟΓΡΑΦΙΚΗ ΑΝΑΣΚΟΠΗΣΗ

2.1. Εισαγωγή

Το πρότυπο ISO/IEC 27001:2005 εκδόθηκε όπως αναγράφεται και στον τίτλο του σχετικά πρόσφατα, η ιδέα όμως σύνταξής του και οι προσπάθειες ολοκλήρωσής του χρονολογούνται σχεδόν είκοσι χρόνια πρίν.Προκειμένου να μελετηθεί το πρότυπο σε βάθος θα παρουσιαστεί στο παρόν κεφάλαιο η πορεία του μέσα από το πρίσμα μιας βιβλιογραφικής ανασκόπησης.

Συγκεκριμένα, θα αναφερθεί μέσα από μια ιστορική αναδρομή η πρωταρχική μορφή του προτύπου, η οποία ήταν ένας *«Κώδικας ορθής πρακτικής»*, η εξέλιξη του κώδικα σε πρότυπο, το οποίο αποτελούνταν από δύο μέρη και η εξέλιξη του καθενός ξεχωριστού μέρους στα σημερινά πρότυπα ISO/IEC 27001:2005-*«Τεχνολογία πληροφοριών- Τεχνικές ασφάλειας- Συστήματα διαχείρισης ασφάλειας πληροφοριών-Απαιτήσεις»* και ISO/IEC 27002:2005-*«Τεχνολογία Πληροφοριών-Τεχνικές ασφάλειας- Κώδικας πρακτικής για διαχείριση ασφάλειας πληροφοριών»*.

Υπήρξαν όμως και εξειδικεύσεις του προτύπου με αποτέλεσμα να δημιουργηθεί μια ολόκληρη σειρά προτύπων ασφάλειας πληροφοριών ISO/IEC 27000, επίσης γνωστή και ως «Οικογένεια Προτύπων ISMS».

Τέλος, θα πραγματοποιηθεί και μια ανασκόπηση του προτύπου. Ειδικότερα, παρατηρήθηκε ότι ορισμένοι συγγραφείς έχουν αναπτύξει το πρότυπο σε θεωρητικό επίπεδο, ενώ κάποιοι άλλοι σε εμπειρικό. Στη συνέχεια θα αναφερθούν αναλυτικά και οι δύο προσεγγίσεις.

2.2. ISO/IEC 27001:2005 – Ιστορική αναδρομή

Το πρότυπο διαχείρισης ασφάλειας πληροφοριών ISO/IEC 27001:2005, που αφορά την προστασία της πληροφορίας, ως σημαντικό περιουσιακό στοιχείο κάθε οργανισμού, εκδόθηκε τον Ιούλιο του 2005 και έχει διακλαδική μορφή (Δερβιτσιώτης & Λαγοδήμος, 2007).

Οι ρίζες όμως του προτύπου μπορούν να αναζητηθούν στο πρώτο πλαίσιο αναφοράς για την ασφάλεια των πληροφοριών.Το Υπουργείο Εμπορίου και Βιομηχανίας του Ηνωμένου Βασιλείου (UK Department of Trade and Industry-DTI) σύστησε μια ομάδα εργασίας προκειμένου να συντάξει έναν κώδικα ορθής πρακτικής όσον αφορά την ασφάλεια. Το DTI εξέδωσε το πρότυπο *«Κώδικα ορθής πρακτικής (User Code of*

Practice)» το 1989. Το πρότυπο αυτό ήταν κυρίως ένα σύνολο ελέγχων ασφαλείας, που εκείνη την περίοδο θεωρούνταν κατάλληλοι για την τεχνολογία και το περιβάλλον της εποχής.

Η ομάδα ξεκίνησε πάλι εργασίες το 1992 και το Φεβρουάριο του 1995 το Βρετανικό Ινστιτούτο Πιστοποίησης (BSI-British Standard Institute) εξέδωσε τον«DTI-*Κώδικα ορθής πρακτικής (*DTI-*User Code of Practice)»* ως το πρώτο εθνικό Βρετανικό Πρότυπο (BS-British Standard) με την ονομασία BS7799:1995-*«Κώδικας πρακτικής για διαχείριση ασφάλειας πληροφοριών (Code of Practice for Information Security Management)»*. Οργανισμοί οι οποίοι ανέπτυσσαν ένα «Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών-ISMS (Information Security Management System)» το οποίο συμμορφωνόταν με αυτόν τον κώδικα πρακτικής μπορούσαν να επιθεωρηθούν από ανεξάρτητο φορέα, εφόσον όμως δεν υπήρχε κάποιο επίσημο καθεστώς πιστοποίησης δεν ήταν εφικτό επίσημα να πιστοποιηθούν (Bon & Verheijen, 2006).

2.2.1. BS 7799:1999 (BS 7799-1:1999, BS 7799-2:1999)

Οι εξελίξεις της τεχνολογίας δικτύων και επικοινωνίας και η συνεχώς αυξανόμενη συμμετοχή των επιχειρήσεων στην ασφάλεια των πληροφοριών είχε ως αποτέλεσμα το 1998 να πραγματοποιηθεί μια σημαντική αναθεώρηση του BS 7799:1995 και τον Απρίλιο του 1999 το Βρετανικό Ινστιτούτο Πιστοποίησης (BSI-British Standard Institute) να εκδώσει ένα νέο πρότυπο, το BS 7799:1999, που αφορούσε την Ασφάλεια των Πληροφοριών και αποτελείτο από δύο μέρη (BS 7799-1:1999, BS 7799-2:1999).

Ο παλαιότερος κώδικας πρακτικής οBS7799:1995-*«Κώδικας πρακτικής για διαχείριση ασφάλειας πληροφοριών»* που προαναφέρθηκε αναθεωρήθηκε σημαντικά και αποτέλεσε το Μέρος I του νέου προτύπου (BS 7799-1:1999) και ένα νέο Μέρος II (BS 7799-2:1999) συντάχθηκε και προστέθηκε. Ο σκοπός του Μέρους II ήταν να αποτελέσει ένα μέσο μέτρησης και παρακολούθησης του Μέρους I καθώς παράλληλα και ένα σημείο αναφοράς για την πιστοποίηση.

Το Μέρος I - (BS7799-1:1999) είχε τον τίτλο *«Κώδικας πρακτικής για διαχείριση ασφάλειας πληροφοριών-Οδηγίες & Συστάσεις (Code of Practice for Information Security Management- Guidance & Recommendations)»* και παρείχε καθοδήγηση σχετικά με τις βέλτιστες πρακτικές στη διαχείριση της ασφάλειας των πληροφοριών. Στον πρόλογό του καθιστούσε σαφές ότι δεν πρέπει να αντιμετωπίζεται ως απαίτηση. Το Μέρος II-(BS7799-2:1999) είχε τον τίτλο *«Συστήματα διαχείρισης ασφάλειας πληροφοριών-Προδιαγραφές με οδηγίες χρήσης (Information Security Management Systems-Specifications with Guidance for Use)»*, συντάχθηκε ως οι απαιτήσεις έναντι των οποίων το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ISMS-Information

Security Management System) ενός οργανισμού θα μπορούσε να αξιολογηθεί και να πιστοποιηθεί.

Η σύνδεση μεταξύ των δυο προτύπων ήταν εξ αρχής το γεγονός ότι η λίστα των ελέγχων της ασφάλειας των πληροφοριών του BS 7799-2 ευθυγραμμίζεται με τη λίστα των ελέγχων του BS 7799-1 και το BS 7799-2 απαιτεί από το χρήστη να αναζητήσει πιο λεπτομερή καθοδήγηση όσον αφορά την εφαρμογή των απαριθμημένων ελέγχων στο BS 7799-1 (Calder & Watkins,2006).

2.2.2. Πρώτη πιστοποίηση

Ο πρώτος οργανισμός στον κόσμο που πιστοποιήθηκε ότι το «Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ISMS-Information Security Management System)» το οποίο διέθετε συμμορφωνόταν με τις απαιτήσεις του προτύπου BS 7799-2:1999 ήταν ο «Business Link London City Partners». Από τότε υπήρξε μια αυξητική τάση των πιστοποιήσεων. Το 2007 οι πιστοποιήσεις ξεπερνούσαν τις 3,000 (Calder & Haren,2006).

2.2.3. Κοινή τεχνική επιτροπή JTC 1 & Υποεπιτροπή SC 27

Ο Διεθνής Οργανισμός Τυποποίησης -ISO(International Organization of Standardization) και η Διεθνής Ηλεκτροτεχνική Επιτροπή -IEC (International Electrotechnical Commission) σύστησαν μια κοινή τεχνική επιτροπή, τηνJTC 1 (Joint Technical Committee) προκειμένου να ενασχοληθούν από κοινού με τα διεθνή πρότυπα και τις οδηγίες.

Η επιτροπή αυτή έχει πλήθος υπό-επιτροπών, μια εκ των οποίων είναι η Υποεπιτροπή 27 (Subcommittee 27 ή SC 27), η οποία είναι υπεύθυνη για το σχεδιασμό προτύπων για την ασφάλεια. Η επιτροπή περιλαμβάνει με τη σειρά της άλλες ομάδες εργασίας (workinggroups), τις«WG 1», «WG 2», «WG 3». Το πεδίο της «WG 1» είναι τα πρότυπα διαχείρισης ασφάλειας αλλά και η ανάπτυξη νέων προτύπων για τη διαχείριση της ασφάλειας των πληροφοριών (Calder & Haren,2006). Αυτή εξάλλου είναι υπεύθυνη για την έκδοση του προτύπου ISO/IEC 27001:2005, το οποίο θα αναλυθεί παρακάτω πώς προέκυψε.

2.2.4. Εξέλιξη BS 7799-1:1999 σε ISO/IEC 27002:2005

Το πρότυπο BS 7799-1:1999 έπειτα από πολλές αναθεωρήσεις προτάθηκε για διεθνές πρότυπο. Η ανάγκη για δημιουργία ενός αντίστοιχου διεθνούς κώδικα κοινής

πρακτικής οδήγησε τελικά το Διεθνή Οργανισμό Τυποποίησης να υιοθετήσει το Δεκέμβριο του 2000 αυτούσιο το αναθεωρημένο βρετανικό πρότυπο ως διεθνές πρώιμο πρότυπο με τον τίτλο ISO/IEC 17799:2000-*«Τεχνολογία πληροφοριών-Κώδικας πρακτικής για διαχείριση ασφάλειας πληροφοριών (Information Technology-Code of Practice for Information Security Management)»* (Δερβιτσιώτης & Λαγοδήμος,2007).

Τον Ιούνιο του 2005 πραγματοποιήθηκε μια ουσιαστική αναθεώρηση και ενημέρωση του ISO/IEC 17799:2000 και η νέα έκδοση ISO/IEC 17799:2005 δημοσιεύτηκε τον Ιούλιο του 2005.

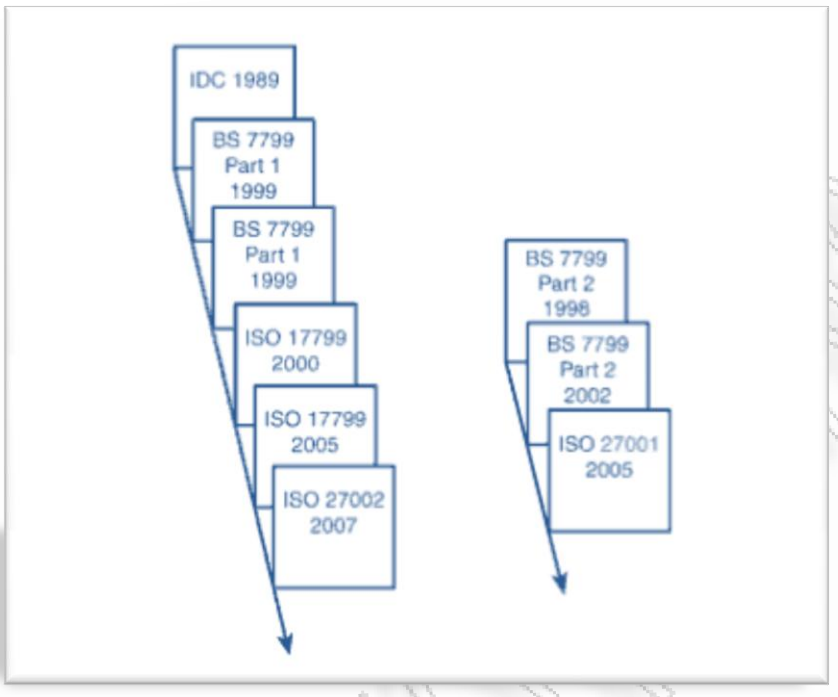
Τελευταία αναθεώρηση έγινε τον Ιούλιο του 2007 όπου μετονομάστηκε σε ISO/IEC 27002:2005-*«Τεχνολογία Πληροφοριών-Τεχνικές ασφάλειας- Κώδικας πρακτικής για διαχείριση ασφάλειας πληροφοριών (Information technology-Security techniques-Code of practice for information security management)»* και αποτελεί έναν κώδικα πρακτικής που εμπεριέχει συμβουλές που αφορούν όσους είναι υπεύθυνοι για την ανάπτυξη, την εφαρμογή και τη διατήρηση ενός «Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ISMS)» (Calder & Haren,2006).

2.2.5. Εξέλιξη BS 7799-2:1999 σε ISO/IEC 27001:2005

Το πρότυπο BS 7799-2:1999 το 2002 εισήγαγε το «Μοντέλο Διασφάλισης Ποιότητας» του Deming «PDCA» (PLAN-DO-CHECK-ACT) και έγινε BS 7799-2:2002. Με αυτόν τον τρόπο κατάφερε να συσχετιστεί άμεσα με πρότυπα όπως το ISO 9000.

Το Νοέμβριο του 2005 το BS 7799-2:2002 υιοθετήθηκε από τον ISO ως ένα διεθνές πρότυπο με τον τίτλο ISO/IEC27001:2005-*«Τεχνολογία πληροφοριών-Τεχνικές ασφάλειας-Συστήματα διαχείρισης ασφάλειας πληροφοριών- Απαιτήσεις (Information technology- Security techniques- Information security management systems-Requirements)»*. Αποτελεί το σύνολο των κριτηρίων για την αξιολόγηση του «Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ISMS)» ενός οργανισμού καθώς και τη βάση για ένα επίσημο σύστημα πιστοποίησης (Dey,2007).

Στο παρακάτω διάγραμμα παρουσιάζεται η ιστορική εξέλιξη του προτύπου από τονIDC:1989-«*Κώδικα ορθής πρακτικής για την ασφάλεια των πληροφοριών*» έως το ISO/IEC 27001:2005-*«Τεχνολογία πληροφοριών- Τεχνικές ασφάλειας - Συστήματα διαχείρισης ασφάλειας πληροφοριών- Απαιτήσεις»*.



Σχήμα 2.1

2.2.6. Συνδυαστική χρήση προτύπων ISO/IEC 27001 & ISO/IEC 27002

Το ISO/IEC 27001 χρησιμοποιείται σε συνδυασμό με το ISO/IEC 27002, διότι το τελευταίο θέτει στόχους όσον αφορά τον έλεγχο της ασφάλειας και προτείνει ένα μεγάλο εύρος συγκεκριμένων ελέγχων της ασφάλειας των πληροφοριών.

Το αντίστροφο όμως δε συμβαίνει. Οργανισμοί οι οποίοι εγκαθιστούν ένα ISMS σύμφωνα με τις συμβουλές ορθής πρακτικής που περιλαμβάνονται στο ISO/IEC 27002 είναι πιθανό ταυτόχρονα να ικανοποιούν τις απαιτήσεις του ISO/IEC 27001, αλλά η πιστοποίηση είναι απολύτως προαιρετική, εκτός εάν εξουσιοδοτηθεί από τους ενδιαφερόμενους (stakeholders)του οργανισμού (Harris,2007).

2.2.7. Σειρά ISO/IEC 27000 «Οικογένεια προτύπων ISMS»

Παρότι υπήρχαν τα πρότυπα ISO/IEC 27001:2005 και ISO/IEC 27002:2005 και η συνδυαστική χρήση αυτών, προέκυψε η ανάγκη για τη δημιουργία μιας σειράς προτύπων αναφορικά με τη διαχείριση της ασφάλειας των πληροφοριών.

Πρώτο βήμα για τη δημιουργία της σειράς ήταν η ανάπτυξη ενός προτύπου ISO/IEC 27000.Το ISO/IEC 27000, όπως συμβαίνει και με το ISO 9000 και το ISO 14000, το

βασικό «000» πρότυπο παρέχει μια γενική επισκόπηση των προτύπων που ανήκουν στην οικογένεια των προτύπων «27000» καθώς και επεξήγηση των θεμελιωδών όρων και ορισμών (vocabulary) που χρησιμοποιούνται σε αυτά τα πρότυπα.

Το αποτέλεσμα ήταν να αναπτυχθεί από μια υπό-επιτροπή της κοινής τεχνικής επιτροπής JTC 1 το ISO/IEC 27000:2009 -*«Τεχνολογία πληροφοριών- Τεχνικές ασφάλειας- Συστήματα διαχείρισης ασφάλειας πληροφοριών-Επισκόπηση & ορισμοί (Information technology - Security techniques - Information security management systems - Overview and vocabulary)»*,το οποίο αποτελεί το νέο διεθνές πρότυπο που έρχεται να προστεθεί στα πρότυπα ISO/IECISMS.

Στη συνέχεια, προέκυψε η ανάγκη για τη δημιουργία ενός προτύπου που να παρέχει κατευθυντήριες γραμμές για τη διαπίστευση των φορέων που αναλαμβάνουν την πιστοποίηση των «Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών (ISMS)» των οργανισμών.

Έτσι, το 2007 δημοσιεύτηκε το ISO/IEC 27006:2007 -*«Τεχνολογία πληροφοριών- Τεχνικές ασφάλειας- Απαιτήσεις για τους φορείς που παρέχουν υπηρεσίες ελέγχου και πιστοποίησης των συστημάτων διαχείρισης ασφάλειας πληροφοριών (Information technology - Security techniques -Requirements for bodies providing audit and certification of information security management systems)»*, το οποίο αποτελεί έναν οδηγό για τη διαπίστευση της διαδικασίας των φορέων πιστοποίησης.

Ακολούθησαν και άλλα πιο εξειδικευμένα πρότυπα με συνέπεια η σειρά **ISO/IEC 27000** (επίσης γνωστή ως «Οικογένεια Προτύπων ISMS (ISMS Family of Standards)»να περιλαμβάνει πλέον πρότυπα ασφάλειας πληροφοριών δημοσιευμένα από κοινού από τον Διεθνή Οργανισμό Τυποποίησης-ISO (International Organization of Standardization) και τη Διεθνή Ηλεκτροτεχνική Επιτροπή-IEC (International Electrotechnical Commission), παρόμοια στο σχεδιασμό με τα διαχειριστικά συστήματα διασφάλισης ποιότητας ISO 9000 και της προστασίας του περιβάλλοντος ISO 14000.

Η σειρά έχει σκόπιμα ένα ευρύ πεδίο εφαρμογής. Είναι εφαρμόσιμη σε οργανισμούς όλων των σχημάτων και μεγεθών. Όλοι οι οργανισμοί καλούνται να αξιολογήσουν τους κινδύνους ασφάλειας των πληροφοριών τους, στη συνέχεια, να εφαρμόσουν κατάλληλους ελέγχους ασφάλειας των πληροφοριών σύμφωνα με τις ανάγκες τους, χρησιμοποιώντας τις κατευθύνσεις και τις προτάσεις των προτύπων κατά περίπτωση.

Η σειρά ISO/IEC 27000,η οποία περιλαμβάνει και ορισμένα πρότυπα τα οποία είναι υπό κατασκευή, παρουσιάζεται αναλυτικά στον παρακάτω πίνακα.(Διεθνής Οργανισμός Τυποποίησης-ISO-International Organization of Standardization).

ISO/IEC Πρότυπο	Περιγραφή
ISO/IEC 27000:2009	Τεχνολογία πληροφοριών Τεχνικές ασφάλειας Συστήματα διαχείρισης ασφάλειας πληροφοριών Επισκόπηση & ορισμοί
ISO/IEC 27001:2005	Τεχνολογία πληροφοριών Τεχνικές ασφάλειας Συστήματα διαχείρισης ασφάλειας πληροφοριών Απαιτήσεις
ISO/IEC 27002:2005	Τεχνολογία πληροφοριών Τεχνικές ασφάλειας Κώδικας πρακτικής για διαχείριση ασφάλειας πληροφοριών
ISO/IEC 27003 (υπό κατασκευή)	Τεχνολογία πληροφοριών Τεχνικές ασφάλειας Οδηγός υλοποίησης συστημάτων διαχείρισης ασφάλειας πληροφοριών
ISO/IEC 27004 (υπό κατασκευή)	Τεχνολογία πληροφοριών Τεχνικές ασφάλειας Διαχείριση ασφάλειας πληροφοριών Μετρήσεις
ISO/IEC 27005:2008	Τεχνολογία πληροφοριών Τεχνικές ασφάλειας *Διαχείριση των κινδύνων ασφάλειας πληροφοριών*
ISO/IEC 27006:2007	Τεχνολογία πληροφοριών Τεχνικές ασφάλειας Απαιτήσεις για τους φορείς που παρέχουν υπηρεσίες ελέγχου και πιστοποίησης των συστημάτων διαχείρισης ασφάλειας πληροφοριών
ISO/IEC 27007 (υπό κατασκευή)	Οδηγίες για έλεγχο του ISMS (για διάφορους λόγους εκτός της πιστοποίησης πχ εσωτερικές επιθεωρήσεις, εξωτερικές επιθεωρήσεις, ανασκοπήσεις Διοίκησης)
ISO/IEC 27008 (υπό κατασκευή)	Οδηγίες για έλεγχο των ελέγχων ασφάλειας του ISMS (που παρουσιάζονται στη «Δήλωση Εφαρμοσιμότητας» του οργανισμού)
ISO/IEC 27011:2008	Τεχνολογία πληροφοριών Τεχνικές ασφάλειας Οδηγίες για διαχείριση ασφάλειας πληροφοριών σε οργανισμούς τηλεπικοινωνιών βασισμένες σ το ISO/IEC 27002

Πηγή:*Διεθνής Οργανισμός Τυποποίησης - ISO (International Organization of Standardization)*

2.3. ISO/IEC 27001:2005 – Ανασκόπηση

Από τα παραπάνω διαπιστώνεται ότι το πρότυπο ISO/IEC 27001:2005 είναι σχετικά καινούριο. Αυτός είναι και ο κύριος λόγος, που αν και θεωρείται ένα από τα πιο σημαντικά πρότυπα, οι περισσότεροι συγγραφείς το έχουν αναπτύξει σε θεωρητικό μόνο επίπεδο και δεν υπάρχει στη βιβλιογραφία πληθώρα αναφορών σε επίπεδο εμπειρικής έρευνας. Με την πάροδο βέβαια του χρόνου αναμένεται να παρατηρηθεί μια αύξηση του αριθμού των συγγραμμάτων που θα έχουν ως αντικείμενό τους την ανάλυση του συγκεκριμένου προτύπου μέσω της εφαρμογής του.

Όταν γίνεται λοιπόν αναφορά στην ανασκόπηση του προτύπου, νοείται κυρίως η θεωρητική ανασκόπηση. Αρκετοί συγγραφείς ασχολήθηκαν με τη θεωρητική ανάλυση του προτύπου ISO 27001. Συγκεκριμένα, μελέτησαν ποιό είναι το αντικείμενό του, ποιό σύστημα διαχείρισης εφαρμόζει, ποιά μέθοδο χρησιμοποιεί για να αναπτύξει ένα τέτοιο σύστημα, ποιά η σχέση του με άλλα πρότυπα διαχείρισης όπως το ISO 9001 και το ISO 14001, ποιά τα οφέλη και οι αδυναμίες του αλλά και ποιοί οι μύθοι που σχετίζονται με το συγκεκριμένο πρότυπο.

Ωστόσο, υπάρχουν και κάποιες έρευνες που έχουν ασχοληθεί σε εμπειρικό επίπεδο με το αντικείμενο του εν λόγω προτύπου, που είναι η ασφάλεια των πληροφοριών.

2.3.1. Ασφάλεια πληροφοριών

Το πρότυπο ISO/IEC 27001:2005 πραγματεύεται την ασφάλεια των πληροφοριών. Στο παρελθόν την «ασφάλειά» του ένας οργανισμός έτεινε να την αντιλαμβάνεται μόνο ως την ασφάλεια των τυπικών και απτών περιουσιακών του στοιχείων, τα οποία δεν ήταν άλλα από τον εξοπλισμό, τα κτίρια, τα γραφεία, τα χρήματα. Σήμερα, τόσο η έννοια της «ασφάλειας», όσο και η έννοια του «περιουσιακού στοιχείου» ενός οργανισμού έχει διευρυνθεί.

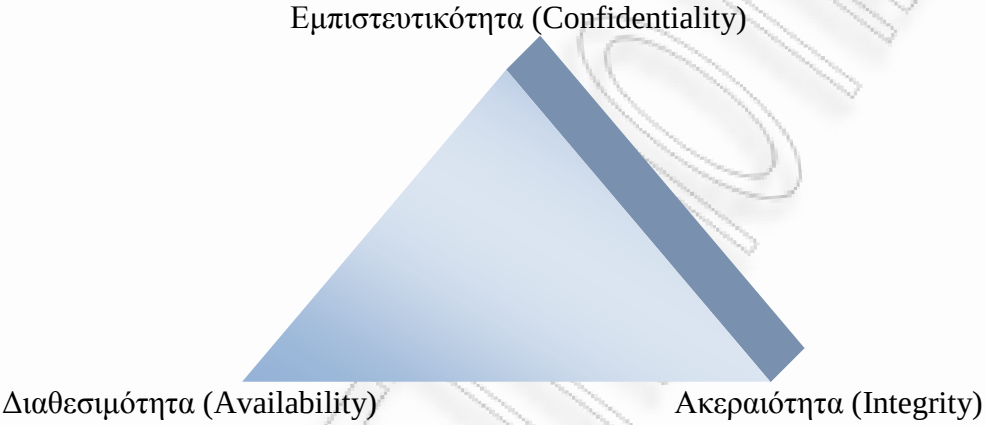
Το ISO/IEC 27001:2005 ορίζει στο εξής ως περιουσιακό στοιχείο «οτιδήποτε έχει αξία για τον οργανισμό».Αυτό επηρέασε τη λειτουργία των οργανισμών, οι οποίοι πλέον ενδιαφέρονται και για τη διαφύλαξη των μη απτών περιουσιακών τους στοιχείων,όπως είναι οι πληροφορίες που παράγουν με τη μορφή εγγράφων, δεδομένων, ηχογραφήσεων, εικόνων και διαχειρίζονται με τη βοήθεια πληροφοριακών συστημάτων και ηλεκτρονικών υπολογιστών.Η πληροφορία μετατράπηκε σε ένα περιουσιακό στοιχείο ζωτικής σημασίας για τον εκάστοτε οργανισμό και αποτελεί πλέον «πνευματική ιδιοκτησία» του (Arnason&Willett,2007).

Σήμερα, όλο και περισσότεροι οργανισμοί που διαχειρίζονται κρίσιμες πληροφορίες ενδιαφέρονται για την ασφάλειά τους.

Η ασφάλεια πληροφοριών ορίζεται από το πρότυπο ISO/IEC 27001:2005 ως «η διατήρηση και προστασία των τριών βασικών ιδιοτήτων της πληροφορίας, της Εμπιστευτικότητας, της Ακεραιότητας και της Διαθεσιμότητας. Επιπρόσθετες όμως ιδιότητες μπορούν να συμπεριληφθούν όπως η αυθεντικότητα, η αναγνωρισιμότητα, η κυριότητα, η μη-άρνηση, η αξιοπιστία»

Η προστασία των τριών αυτών ιδιοτήτων αποβλέπει στο να είναι η κατάλληλη πληροφορία διαθέσιμη στους κατάλληλους ανθρώπους, στο κατάλληλο μέρος και την κατάλληλη χρονική στιγμή (Dey,2007).

Γνωστό στη βιβλιογραφία και ως *" Τρίγωνο C-I-A (C-I-A triad) "*(Stewartetal.,2005).



Σχήμα 2.2 | **Πηγή** : Endorf, 2002

Οι τρείς αυτές ιδιότητες ορίζονται στο ISO/IEC 27001:2005 ως εξής :

- Εμπιστευτικότητα (*Confidentiality*): η πληροφορία να μην είναι διαθέσιμη ή να γνωστοποιείται σε μη εξουσιοδοτημένα πρόσωπα, φορείς ή διεργασίες.
- Ακεραιότητα (*Integrity*): η διαφύλαξη της ακρίβειας και πληρότητας πληροφορίας της πληροφορίας.
- Διαθεσιμότητα (*Availability*): η πληροφορία να είναι προσβάσιμη και εύχρηστη κατόπιν

αιτήματος οποιουδήποτε εξουσιοδοτημένου φορέα.

Σχήμα 2.3 | Πηγή :Calder & Haren, 2006

Όπως διακρίνουμε και από το σχήμα, οι πιο κρίσιμες πληροφορίες ενός οργανισμού είναι εκείνες για τις οποίες και οι τρείς αυτές ιδιότητες είναι σημαντικές (Calder & Haren, 2006).

Ο Endorf (2002) αλλά και ο Hill (2009) καθώς και πολλοί άλλοι συγγραφείς συμπληρώνουν το τρίπτυχο αυτό με επιπρόσθετες έννοιες:

- Αυθεντικότητα : η διασφάλιση ότι η πληροφορία είναι γνήσια και όχι πλαστή
- Αναγνωρισιμότητα: η πληροφορία να έχει μια ταυτότητα μέσα σε ένα σύστημα, ούτος ώστε να μπορεί να ελεγχτεί η ταυτότητά της, αλλά και να μπορεί να εντοπιστεί εύκολα μέσα στο σύστημα.
- Κυριότητα: να έχει οριστεί κάποιος αρμόδιος και

υπεύθυνος για τη συγκεκριμένη πληροφορία.

- Μη-άρνηση: τα αποδεικτικά στοιχεία που επιβεβαιώνουν τη γνησιότητα και την προέλευση των πληροφοριών.
- Αξιοπιστία : η απόλυτη ακρίβεια και πληρότητα της πληροφορίας.Η έλλειψη ατελειών και ανακριβειών.

Ο Dey (2007) θεωρεί πως οτιδήποτε θα μπορούσε να προξενήσει ζημιά σε κάποια από τις παραπάνω ιδιότητες της πληροφορίας αποτελεί κίνδυνο. Οι πληροφορίες ως περιουσιακό στοιχείο είναι εκτεθειμένες σε μια πληθώρα κινδύνων, τόσο εξωτερικούς όσο και εσωτερικούς, τυχαίους ή μη.

Οι κίνδυνοι αυτοί με την πάροδο του χρόνου εξελίσσονταν και άλλαζαν μορφή. Αρχικά, οι κίνδυνοι που απειλούσαν την πληροφορία ήταν εκείνοι της κλοπής και της παράνομης πρόσβασης, οι οποίοι αντιμετωπίστηκαν με κωδικούς, κλειδαριές, φρουρούς, κάρτες ταυτοποίησης και συναγερμούς.

Έπειτα, εμφανίστηκαν οι κίνδυνοι που σχετίζονταν με τη λειτουργία του Διαδικτύου, αλλά και αυτοί αντιμετωπίστηκαν με «πυρότοιχους» (firewalls) και με το διαχωρισμό των διαδικτύου (Internet), εσωτερικού δικτύου (Intranet) και εξωτερικού δικτύου (Extranet).

Οι πιο πρόσφατοι όμως και οι πιο απειλητικοί είναι οι κίνδυνοι από ιούς και μηνύματα που μεταφέρουν ιούς. Η εξέλιξη της τεχνολογίας και τα ασύρματα δίκτυα ήρθαν να προσθέσουν επιπρόσθετες ανησυχίες ενώ οι σοβαρότεροι κίνδυνοι συνήθως προέρχονται από τους εσωτερικούς χρήστες.

Στην πραγματικότητα σήμερα αντιμετωπίζουμε όλους αυτούς τους πολυδιάστατους κινδύνους ασφάλειας πληροφοριών ταυτόχρονα. Οι Calder και Watkins (2006) παρατηρούν ότι η πληροφορία απειλείται καθημερινά από απώλεια, κλοπή, παράνομη πρόσβαση και καταστροφή από ανθρώπινα λάθη, ιούς , φυσικά φαινόμενα (σεισμοί, πλημμύρα, πυρκαγιά), τρομοκρατικές ενέργειες (επίθεση 9/11), ξαφνικές καταστροφές (μπλάκ-αουτ στις ΗΠΑ το 2003) ή αποτυχίες του ίδιου του συστήματος. Ο Κάτσικας (2001) ομαδοποιεί τους εν λόγω κινδύνους στις εξής κατηγορίες:

- Ζημιά (Security Flaw): η μερική ή ολική απώλεια μίας ή περισσότερων από τις ιδιότητες της πληροφορίας που χρήζουν προστασίας.

- Απειλή (Security Risk): μια πιθανή πράξη ή γεγονός που μπορεί να προκαλέσει Ζημιά στην πληροφορία.
- Περιστατικό (Security Incident): ένα γεγονός που ενδεχομένως συνέβη εξαιτίας της υλοποίησης μιας απειλής.

Οι κίνδυνοι εάν δεν αποφευχθούν ενδέχεται να έχουν σοβαρές επιπτώσεις σε μία ή και σε περισσότερες από τις τρείς βασικές ιδιότητες της πληροφορίας. Σε αυτήν την περίπτωση, το αποτέλεσμα θα είναι ένα ελλιπές σύστημα ασφάλειας πληροφοριών, το οποίο θα εκθέσει τον οργανισμό σε τρία άλλα είδη κινδύνων :

- Κακή λειτουργία
- Απώλεια φήμης
- Νομικές κυρώσεις

Ένας οργανισμός, λοιπόν, οφείλει να εντοπίσει τους πιθανούς κινδύνους και να λάβει διορθωτικά μέτρα με απώτερο σκοπό να ελαχιστοποιήσει αυτές τις απειλές, μέσα από ένα πρότυπο σύστημα διαχείρισης. Η σημασία της ύπαρξης ενός «Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών» αναλύεται ακολούθως.

2.3.2. Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών-ISMS με βάση το μοντέλο PDCA

Οι οργανισμοί στην προσπάθειά τους να εξαλείψουν τους κινδύνους που απειλούν την ασφάλεια των πληροφοριών τους δαπανούν ενίοτε σημαντικά ποσά προκειμένου να εγκαταστήσουν διάφορες τεχνολογικές λύσεις. Ορισμένες από αυτές που επιλέγουν είναι μηχανισμοί ανίχνευσης, ειδικές συσκευές δικτύου, πρωτόκολλα, ψηφιακές υπογραφές, πυρότοιχοι (firewalls), ειδικά λογισμικά κατά των ιών (anti-virus software), υποθέτοντας ότι με αυτόν τον τρόπο μπορεί να εξασφαλιστεί η ασφάλεια των πληροφοριών τους. Αυτή όμως είναι μία λανθασμένη αντίληψη, διότι η διαχείριση της ασφάλειας των πληροφοριών είναι πολλά περισσότερα από την απλή εγκατάσταση ορισμένων εξειδικευμένων τεχνικών λύσεων, περιλαμβάνει και άλλες συνιστώσες, όπως τα άτομα και τις διαδικασίες (Dey,2007).

Άτομα, διαδικασίες και τεχνολογία προσεγγίζονται συνολικά μέσα σε ένα «Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών-ISMS (Information Security Management System)». Η ανάπτυξη και η υλοποίηση ενός αποτελεσματικού ISMS, το οποίο ο οργανισμός θα σχεδιάσει με βάση τις οδηγίες και τις απαιτήσεις της σειράς διεθνών

προτύπων ασφάλειας πληροφοριών ISO/IEC 27000, θα τον βοηθήσει να επιτύχει την ασφάλεια των πληροφοριών του (Dey,2007).

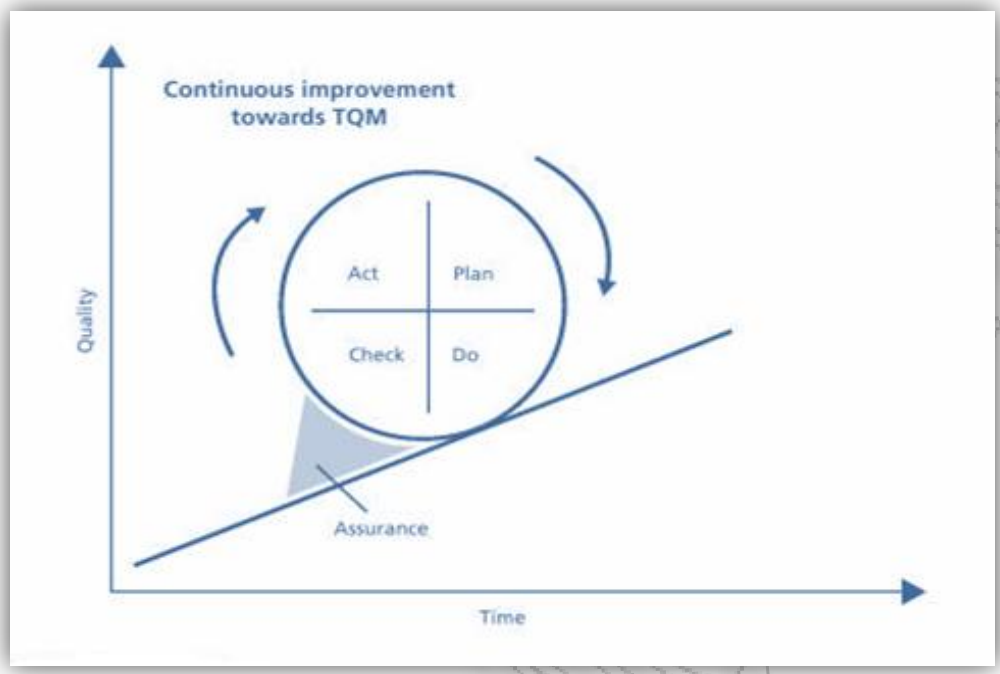
Το πρότυπο ISO/IEC 27001:2005 ορίζει ως ISMS -"το τμήμα εκείνο του συνολικού συστήματος διαχείρισης, το οποίο βασίζεται σε μια επιχειρηματική προσέγγιση του κινδύνου, προκειμένου να σχεδιάσει, να εφαρμόσει, να λειτουργήσει, να παρακολουθήσει, να ελέγξει, να διατηρήσει και να βελτιώσει την ασφάλεια των πληροφοριών. Το ISMS περιλαμβάνει οργανωτική δομή, πολιτικές, προγραμματισμό δραστηριοτήτων, αρμοδιότητες, πρακτικές, διαδικασίες, διεργασίες και πόρους."(Calder & Haren, 2006).

Η βασική ιδέα του ISMS είναι ένας οργανισμός να σχεδιάσει, να εγκαταστήσει και να διατηρήσει ένα σύστημα διεργασιών, το οποίο θα εξασφαλίζει την αποτελεσματική αλληλεπίδραση χρηστών, τεχνολογίας και διαδικασιών και κατά συνέπεια θα επιτυγχάνει την ορθή διαχείριση της προσβασιμότητας στην πληροφορία. Αυτό σημαίνει ότι θα διαφυλάξει την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα των πληροφοριακών δεδομένων και θα ελαχιστοποιήσει τους κινδύνους που απειλούν την ασφάλειά τους.

Πρέπει όμως να ληφθεί υπόψη ότι η ανάπτυξη ενός ISMS δεν είναι μια απλή διαδικασία. Ομοίως με όλα τα διαχειριστικά συστήματα, έτσι και ένα ISMS δεν αποτελεί μια ενιαία, στατική λύση, η οποία μπορεί να εφαρμοστεί δίχως τροποποιήσεις σε κάθε επιχείρηση.

Το πρότυπο ISO/IEC 27001:2005 αναγνωρίζει ρητά ότι ο σχεδιασμός και η υλοποίηση ενός ISMS πρέπει να είναι σύμφωνα με τις ανάγκες, τους στόχους, τις απαιτήσεις ασφάλειας, τις μεθόδους, το μέγεθος και τη διάρθρωση του κάθε οργανισμού. Επίσης, το πρότυπο αναφέρει ότι εάν πρόκειται για μια απλή διεργασία τότε χρειάζεται ένα απλό ISMS. Τέλος, το ISMS πρέπει να παραμένει αποτελεσματικό και αποδοτικό μακροπρόθεσμα. Αυτό μπορεί να επιτευχθεί μόνο εάν αλλάζει με την πάροδο του χρόνου. Συγκεκριμένα, πρέπει να προσαρμόζεται στις αλλαγές τόσο του εσωτερικού περιβάλλοντος (οργανισμός) όσο και του εξωτερικού (Calder&Haren,2006).Παρότι όμως, η ανάπτυξη ενός ISMSθεωρείται δύσκολη, η μελέτη άλλων προτύπων έδωσε λύση σε αυτό το πρόβλημα.

Το πρότυπο ISO/IEC 9001:2000 «Συστήματα Διαχείρισης Ποιότητας-Απαιτήσεις» εισήγαγε τον *«Κύκλο του Deming-PDCA (Plan-Do-Check-Act)»* για την διαχείριση της ποιότητας σε συστήματα διοίκησης. Αντίστοιχα, τα σημαντικότερα πρότυπα συστήματα διαχείρισης που ακολούθησαν (π.χ. ISO 14001:2004) υιοθέτησαν το ίδιο μοντέλο (Arnason & Willett, 2007). Το ISO/IEC 27001:2005 ακολουθώντας αυτήν την τάση, βασίστηκε επίσης στο μοντέλο PDCA, το οποίο παρουσιάζεται στο ακόλουθο σχήμα.



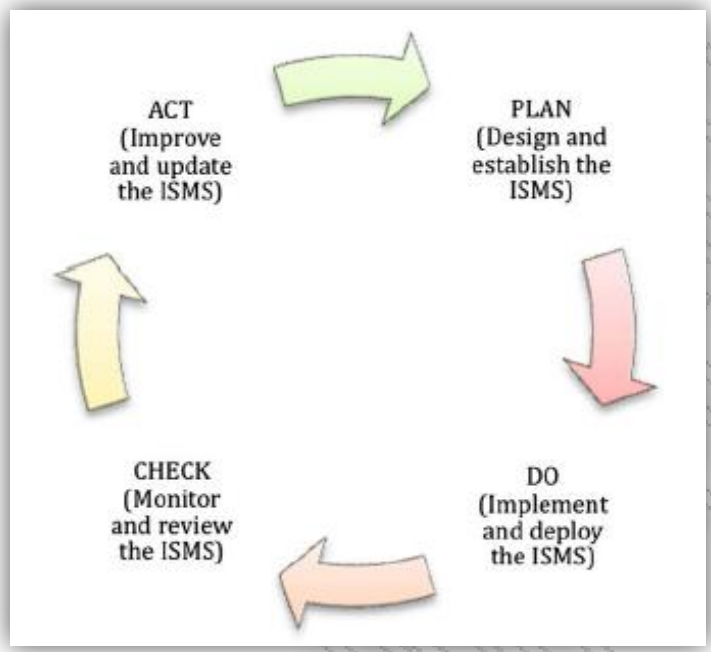
Σχήμα 2.4 | **Πηγή :**Bon & Verheijen,2006

Σύμφωνα με τους Bon και Verheijen, (2006), ο Deming με τον *«Κύκλο PDCA»* πρότεινε τέσσερα στάδια:

- Σχεδιασμό *(Plan)* τον ενδελεχή σχεδιασμό της παραγωγής ενός προϊόντος
- Υλοποίηση *(Do)* την ίδια την παραγωγή
- Έλεγχο *(Check)* τον έλεγχο αν η παραγωγή του προϊόντος εξακολουθεί να συμφωνεί με το σχέδιο
- Δράση *(Act)* την ανάληψη δράσης, όταν υπάρχει ανάγκη προσαρμογής του προϊόντος, εφόσον ο έλεγχος δείχνει ότι η παραγωγή δεν είναι σύμφωνη με το σχέδιο

Το ISO/IEC 27001:2005 χρησιμοποιεί τον παραπάνω *«Κύκλο του Deming-PDCA»*, με στόχο την αποτελεσματική ανάπτυξη ενός «Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών-ISMS (Information Security Management System)». Με τον όρο ανάπτυξη νοείται ο σχεδιασμός, η υλοποίηση, ο έλεγχος και τέλος η συνεχής βελτίωση ενός συστήματος ISMS. Αυτός είναι και ο λόγος που πολλές φορές αναφέρεται στη βιβλιογραφία και ως *«Κύκλος ISMS»*.

Ο *«Κύκλος ISMS»* αποτελείται επίσης από τέσσερα στάδια, όπως αναλύονται παρακάτω.



Σχήμα 2.5 | Πηγή : Humphreys,2008

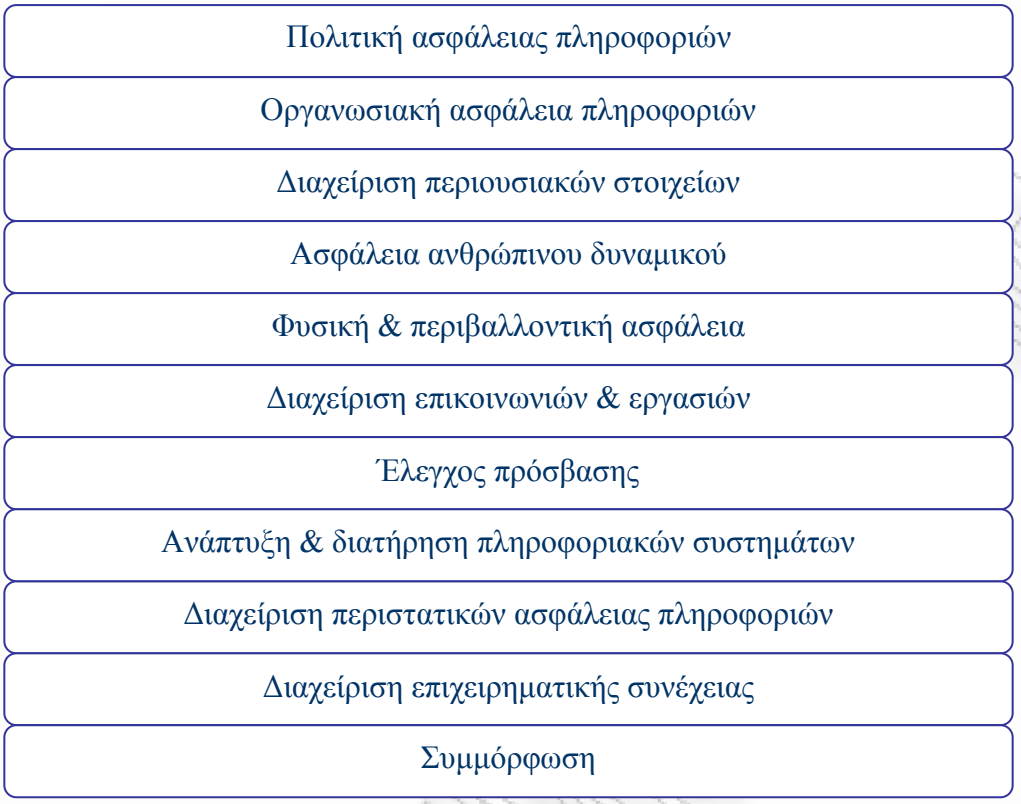
- Σχεδιασμός του ISMS *(Plan)* — τον καθορισμό των προδιαγραφών του συστήματος. Τον προσδιορισμό του αντικειμένου και των ορίων του συστήματος, τη διατύπωση μιας πολιτικής ασφάλειας πληροφοριών («πολιτική ISMS»),τον εντοπισμό των κινδύνων, την αξιολόγησή τους, την αντιμετώπισή τους και τέλος την επιλογή των κατάλληλων ελέγχων

- Υλοποίηση του ISMS *(Do)* — η εφαρμογή των προδιαγραφών που ορίστηκαν κατά το σχεδιασμό. Η διατύπωση ενός «Σχεδίου Μείωσης Κινδύνου», η εφαρμογή του, η εφαρμογή των προεπιλεγμένων ελέγχων και η καθιέρωση μιας μεθόδου μέτρησης της αποτελεσματικότητάς τους

▪ Έλεγχο του ISMS *(Check)*	ο έλεγχος σε επίπεδο διεργασίας, σε επίπεδο Εσωτερικών Επιθεωρήσεων και τέλος σε επίπεδο Ανασκοπήσεων, τόσο στο στάδιο της υλοποίησης όσο και στο στάδιο του σχεδιασμού, έχοντας ως ρόλο να εξασφαλίσει στον οργανισμό την αποτελεσματικότητα και την καταλληλότητα του συστήματος
▪ Βελτίωση ISMS*(Act)*	η ανάληψη δράσης όταν υπάρχει ανάγκη. Όλες εκείνες οι απαραίτητες ενέργειες, διορθωτικές και προληπτικές, που γίνονται εκ μέρους του οργανισμού προκειμένου να βελτιωθεί το επίπεδο ασφάλειας των πληροφοριών του

Όπως θα αναφερθεί σε επόμενο κεφάλαιο, το κάθε ένα από αυτά τα τέσσερα στάδια του *«Κύκλου ISMS»* αποτελεί και μια ενότητα του προτύπου ISO/IEC 27001:2005. Στην παρούσα διπλωματική εργασία, κάθε ενότητα του προτύπου αναλύθηκε λεπτομερώς μέσα από το πρίσμα της μεθοδολογίας του *«Κύκλου PDCA»*.

Επίσης, ο Freeman (2007) σημειώνει ότι το ISO/IEC 27001 εκτός από διεργασίες βασισμένες στον παραπάνω *«Κύκλο PDCA»* περιέχει και ελέγχους. Συγκεκριμένα, στο Παράρτημα Α του προτύπου ISO 27001 αναφέρονται 11 περιοχές ελέγχου, 39 στόχοι ελέγχων και 133 έλεγχοι συνολικά. Οι έλεγχοι αυτοί είναι σχετικά ευέλικτοι και προσαρμόσιμοι στις ανάγκες του οργανισμού, στο αντικείμενο του συστήματος και στο επίπεδο της απαιτούμενης ασφάλειάς του. Τα θέματα που καλύπτουν οι έλεγχοι είναι τα εξής :



Σχήμα 2.6 |**Πηγή:** Humphreys,2008

Οι έλεγχοι αυτοί συνδυαστικά με διεργασίες βασισμένες στον *«Κύκλο PDCA»* μπορούν να συντελέσουν στην αντιμετώπιση των κινδύνων ασφάλειας πληροφοριών.

Συμπερασματικά, ο *«Κύκλος PDCA»* παρέχει τη μεθοδολογία για την ανάπτυξη ενός «Συστήματος ISMS», ενώ το πρότυπο ISO 27001 παρέχει οδηγίες ως προς το πώς πρέπει να εφαρμοστεί ένα «Σύστημα ISMS» μέσω της διαδικασίας PDCA, ώστε να είναι πιστοποιήσιμο.

Ο Humphreys (2008) αναφέρει ότι πρόκειται για μια διαδικασία συνεχούς βελτίωσης, αφού το σύστημα διαχείρισης επιθεωρείται και ανασκοπείται τακτικά ούτως ώστε να ελεγχθεί εάν οι έλεγχοι ασφάλειας παραμένουν αποτελεσματικοί και εάν όχι, βελτιωμένοι έλεγχοι να εισαχθούν.

Το γεγονός αυτό συνδέει άμεσα το «Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών-ISMS» με τη φιλοσοφία της Διοίκησης Ολικής Ποιότητας (TQM). Και κατά συνέπεια συνδέει και το πρότυπο ISO 27001 με τα άλλα πρότυπα, που επίσης έχουν υιοθετήσει το ίδιο μοντέλο.

2.3.3. Ολοκλήρωση Συστημάτων

Στη παρούσα ενότητα θα εξεταστεί η ολοκλήρωση συστημάτων διαχείρισης διαφορετικών προτύπων.

Το ISO 9001 αφορά τη διαχείριση της ποιότητας, το ISO 14001 τη διαχείριση του περιβάλλοντος, ενώ το ISO 27001, που μελετάται στην παρούσα εργασία, τη διαχείριση της ασφάλειας πληροφοριών.

Παρότι, τα πρότυπα αυτά εστιάζουν σε διαφορετικούς τομείς και ορισμένα από αυτά έχουν εξειδικευμένες απαιτήσεις, υπάρχουν ορισμένα κοινά χαρακτηριστικά που τα συνδέουν.

Οι Arnason και Willett (2007) παραθέτουν τα κυριότερα κοινά χαρακτηριστικά μεταξύ των συστημάτων διαχείρισης είναι τα εξής :

- Βασική προϋπόθεση η δέσμευση της Διοίκησης
- Αλλαγή οργανωσιακής κουλτούρας
- Καθορισμός αρμοδιοτήτων και ευθυνών
- Έλεγχος εγγράφων
- Εκπαίδευση
- Έγγραφη Τεκμηρίωση
- Ανασκόπηση της Διοίκησης
- Εσωτερικές επιθεωρήσεις
- Διορθωτικές και προληπτικές ενέργειες
- Χρήση κοινού μοντέλου PDCA
- Διαδικασίες ελέγχου
- Παρόμοιες απαιτήσεις
- Ο φορέας πιστοποίησης είναι αρμόδιος για την πιστοποίηση των προσόντων των επιθεωρητών

Παρακάτω αναλύονται δύο από τα πιο σημαντικά.

ΚΟΙΝΗ ΧΡΗΣΗ «ΚΥΚΛΟΥ PDCA»

Το πρότυπο ISO/IEC 9001:2000 -«Συστήματα Διαχείρισης Ποιότητας – Απαιτήσεις (*Quality management systems - Requirements)*», χρησιμοποίησε το Μοντέλο Διασφάλισης Ποιότητας του Deming *«Κύκλο PDCA» (Plan-Do-Check-Act)*, για την υλοποίηση αποτελεσματικών συστημάτων διαχείρισης της ποιότητας. Πρότυπα συστήματα διαχείρισης που ακολούθησαν επίσης χρησιμοποίησαν το ίδιο μοντέλο.

Το BS7799-2:1999 το 2002 εισήγαγε τον *«Κύκλο PDCA»* στο ανανεωμένο πια BS7799-2:2002, το οποίο μετονομάστηκε αργότερα σε ISO/IEC 27001 (JanVanBon, Tieneke Verheijen, 2006).Το πρότυπο ασφάλειας πληροφοριών ISO/IEC 27001 εξακολουθεί να χρησιμοποιεί το μοντέλο PDCA για το σχεδιασμό, την υλοποίηση, παρακολούθηση και βελτίωση ενός «Συστήματος ISMS» (Sigurjon Thor Arnason, KeithD. Willett, 2007).
Συνεπώς, το ISO/IEC 27001 δεν θα μπορούσε παρά να συσχετίζεται άμεσα τόσο με το ISO/IEC 9001, όσο και με τα άλλα πρότυπα που χρησιμοποιούν το ίδιο μοντέλο.

ΚΟΙΝΑ ΒΑΣΙΚΑ ΔΟΜΙΚΑ ΣΤΟΙΧΕΙΑ

Τα βασικά δομικά στοιχεία του ISO/IEC 27001 είναι όπως σε κάθε σύστημαISO, η διεργασία και η έγγραφη τεκμηρίωση (Timothy P.Layton,2006).

Σύμφωνα με τους Κώστα.Ν.Δερβιτσιώτη και Αθανάσιο.Γ.Λαγοδήμο (2007) η θεώρηση του οργανισμού ως πλέγματος αλληλεπιδρώντων διεργασιών αποτελεί ιδιαίτερα χρήσιμο εργαλείο για την κατανόηση της έννοιας των απαιτήσεων εξειδικευμένων πρότυπων συστημάτων διαχείρισης (ΠΣΔ), όπως είναι το ISO 27001, τα οποία στη πλειονότητά τους καθορίζουν :

- Προδιαγραφές σχεδιασμού επιμέρους διεργασιών του οργανισμού, κρίσιμων για τη σχετική εκροή-στόχο του ΠΣΔ.

- Τύπο και εύρος των διεργασιών του οργανισμού που αφορούν άμεσα την εκροή-στόχο του ΠΣΔ.

Μία επιχείρηση που εφαρμόζει το πρότυπο ISO 9001 θα μπορούσε να συμμορφωθεί και στις απαιτήσεις ενός εξειδικευμένου προτύπου, όπως είναι το ISO 27001, μόνο μέσω επανασχεδιασμού κάποιων συγκεκριμένων διεργασιών, έτσι ώστε να καλύψει τις εξειδικευμένες απαιτήσεις του προτύπου αυτού.

Ένα δεύτερο δομικό στοιχείο όπως προαναφέρθηκε είναι η συστηματική έγγραφη τεκμηρίωση (documentation). Σκοπός της τεκμηρίωσης είναι η δημιουργία ενός σταθερού πλαισίου αναφοράς τόσο για την ομαλή υλοποίηση των δραστηριοτήτων όσο και για την άσκηση αποτελεσματικού ελέγχου. Μέσω της τεκμηρίωσης, ο οργανισμός τυποποιεί την καθημερινή του λειτουργία, παρέχοντας έτσι τη δυνατότητα στα στελέχη να ασκήσουν ουσιαστική διοίκηση.

Η στρατηγική διαχείρισης ασφάλειας πληροφοριών του οργανισμού, για να είναι αποτελεσματική και για να καλύπτει τις απαιτήσεις του προτύπου ISO 27001, πρέπει να είναι συνδεδεμένη με ένα τεκμηριωμένο πρόγραμμα το οποίο θα είναι μετρήσιμο και ανακοινώσιμο (Layton,2006).

Από τα παραπάνω διαπιστώθηκε ότι το πρότυπο ISO 27001 διαθέτει πολλά κοινά χαρακτηριστικά με τα πρότυπαISO 9001 και ISO 14001. Το ερώτημα όμως που προκύπτει είναι εάν θα μπορούσε να ενσωματωθεί σε κάποιο από τα δύο πρότυπα, με την προϋπόθεση βέβαια ο οργανισμός διαθέτει τουλάχιστον ένα από αυτά.

Πράγματι, οργανισμοί που έχουν ήδη εγκαταστημένο ένα σύστημα βασισμένο σε ένα άλλο πρότυπο ISO (ISO 9001, ISO 14001), τότε μπορούν απλά να το επεκτείνουν για να συμπεριλάβουν και τους ειδικούς μηχανισμούς ενός «Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών-ISMS», που θα είναι ικανό να πιστοποιηθεί με το πρότυπο ISO27001.

Η ρήτρα 1, 2 αναγνωρίζει ότι:
"Αν ένας οργανισμός έχει ήδη ένα σύστημα διαχείρισης επιχειρησιακών διεργασιών, είναι προτιμότερο στις περισσότερες περιπτώσεις να ικανοποιήσει τις απαιτήσεις του παρόντος διεθνούς προτύπου ISO27001 στο πλαίσιο αυτού του υφιστάμενου συστήματος διαχείρισης." (Calder & Haren,2006).

Σε αυτήν την περίπτωση, η ενσωμάτωση του ISO 27001 θα είναι πολύ απλή και η Διοίκηση θα είναι ήδη εξοικειωμένη με τις απαιτήσεις του προτύπου.

Αλλά και η ενσωμάτωση άλλων προτύπων σε ένα ήδη εγκατεστημένο ISO 27001 είναι εφικτή. Το ISO 27001 προτίθεται να εναρμονιστεί με τα άλλα πρότυπα συστήματα διαχείρισης προκειμένου να παρέχει συνεκτική και ολοκληρωμένη εφαρμογή και λειτουργία ενός συστήματος διαχείρισης της επιχείρησης.

Όταν παρουσιαστεί η ανάγκη ένας οργανισμός να εφαρμόσει και να διαχειριστεί περισσότερα από ένα πρότυπα διαχείρισης, τότε μπορεί απλά να επεκτείνει το υφιστάμενο «Σύστημα ISMS» του προκειμένου να καλύψει τις επιπρόσθετες απαιτήσεις των υπολοίπων προτύπων διαχείρισης.

Η χρήση του «Συστήματος ISMS» μέσω πολλών προτύπων διαχείρισης ονομάζεται και πρόγραμμα διαχείρισης συμμόρφωσης (CMP-compliance management programme).

Τα οφέλη από ένα τέτοιο ενιαίο σύστημα διαχείρισης είναι η επένδυση σε ένα ενιαίο σύστημα διαχείρισης σε όλον τον οργανισμό, ένα μοναδικό σημείο εστίασης για τους ελεγκτές, καθώς και για τον φορέα πιστοποίησης, και τελικά μικρότερο κόστος για τον οργανισμό (Arnason & Willett,2007).

Περαιτέρω, όσο περισσότερο συγκρίνουμε το πρόσφατα δημοσιευμένο πρότυπο που αφορά την ασφάλεια πληροφοριών ISO 27001 με το πρότυπο ISO 9001, το οποίο

είναι ένα παρόμοιο πρότυπο με ιστορία είκοσι χρόνων, μπορούμε να προβλέψουμε πώς θα εξελιχθεί η μελλοντική υιοθέτηση του πρόσφατου προτύπου ISO 27001. Μεταξύ άλλων, το νομοθετικό περιβάλλον μπορεί να διαδραματίσει ζωτικό ρόλο για την περαιτέρω υιοθέτηση των προτύπων ασφαλείας (Fominetal, 2008).

2.3.4. Οφέλη & Αδυναμίες προτύπου ISO 27001

Η πιστοποίηση κατά ISO/IEC 27001:2005 δεν είναι υποχρεωτική βάσει κάποιας νομοθετικής ή κανονιστικής απαίτησης. Παρόλα αυτά υπάρχει μια σειρά άμεσων, πρακτικών λόγων για την εφαρμογή μιας πολιτικής για την ασφάλεια των πληροφοριών και ενός συστήματος διαχείρισης ασφάλειας πληροφοριών (ISMS) το οποίο θα είναι δυνατόν να πιστοποιηθεί ότι συμμορφώνεται με το πρότυπο ISO 27001.

Οι Calder και Watkins (2006) αναφέρουν ορισμένους από αυτούς. Αρχικά, μια πιστοποίηση λέει στους υφιστάμενους και στους δυνητικούς πελάτες ότι ο οργανισμός έχει προσδιορίσει και καθιερώσει αποτελεσματικές διαδικασίες ασφάλειας των πληροφοριών του, συμβάλλοντας έτσι στην δημιουργία μιας σχέσης εμπιστοσύνης.

Ένας άλλος λόγος είναι ότι τόσο η πιστοποίηση, όσο και η τακτική εξωτερική αξιολόγηση από την οποία εξαρτάται η πιστοποίηση, εξασφαλίζουν ότι ο οργανισμός διατηρεί το σύστημα διαχείρισης ασφάλειας των πληροφοριών του ενημερωμένο και ότι θα συνεχίσει να διαβεβαιώνεται η ικανότητά του να λειτουργεί. Συνεπώς, η διαδικασία πιστοποίησης βοηθάει τον οργανισμό να επικεντρωθεί στη συνεχή βελτίωση του συστήματός του.

Ενώ, οι Arnason και Willett (2007), συμπλήρωσαν ορισμένα επιπρόσθετα οφέλη της πιστοποίησης. Επισημαίνουν ότι η πιστοποίηση παρέχει μια ανεξάρτητη επικύρωση ότι ο οργανισμός έχει εφαρμόσει αποτελεσματικά τις απαιτήσεις του προτύπου και αποδεικνύει τη δέουσα επιμέλεια εκ μέρους των στελεχών και της διοίκησης στον εντοπισμό των αναγκών ασφαλείας.

Επίσης, τονίζουν ότι η παρακολούθηση και η υποβολή αναφορών, έχοντας ως βάση το πρότυπο ISO 27001, διευκολύνουν τους ελέγχους. Αυτό συνεπάγεται λιγότερο κόστος του ελέγχου και υψηλότερη πιθανότητα της επιτυχίας σε έναν έλεγχο.

Πιο σημαντικό όμως θεωρούν το γεγονός ότι η πιστοποίηση ενός οργανισμού με ISO 27001 επικυρώνει ότι η επένδυση που έκανε ο οργανισμός σε ελέγχους ασφάλειας πληροί τους αρχικούς του στόχους και του αποφέρει επιχειρηματική αξία. Η επιχειρηματική αξία βρίσκεται στη διαχείριση του επιχειρηματικού κινδύνου, στην

επίτευξη υψηλών επιπέδων νομοθετικής και κανονιστικής συμμόρφωσης καθώς και στη διαχείριση των απειλών.

Συγκεκριμένα, ο Boehmer (2009) αναφέρει στο σύγγραμμά του ότι η επένδυση στην εφαρμογή ενός συστήματος ISMS με βάση το ISO / IEC 27001:2005, πρέπει να είναι συγκρίσιμη προς το όφελος που αποφέρει στον οργανισμό. Στο έγγραφο αυτό προτείνει, για τη διεξαγωγή μιας τέτοιας σύγκρισης, τη χρήση «Βασικών Δεικτών Απόδοσης-KPI (Key Performance Indicators)», οι οποίοι μετρούν την αποτελεσματικότητα και την οικονομική αποδοτικότητα ενός συστήματος ISMS.Ωστόσο, πολλές φορές οι δείκτες KPI είναι αντιφατικοί. Ως, εναλλακτική λύση προτείνει τη «Συνδυαστική βελτιστοποίηση» όπου ο οργανισμός πρέπει να σταθμίσει τα οφέλη μιας πολιτικής από την άποψη του κινδύνου για κάθε έλεγχο, έναντι του κόστους του κάθε ελέγχου όσον αφορά την αποφυγή, τον μετριασμό ή τη μεταφορά του κινδύνου στα πλαίσια ενός προκαθορισμένου ορίου επενδύσεων.

Η πιστοποίηση λοιπόν του συστήματος διαχείρισης ασφάλειας πληροφοριών ενός οργανισμού κατά ISO 27001, παρότι δεν είναι υποχρεωτική, παρέχει μια συστηματική προσέγγιση για τον εντοπισμό και την καταπολέμηση των δυνητικών κινδύνων που απειλούν τις κρίσιμες πληροφορίες του, του εξοικονομεί χρήματα και του εξασφαλίζει την εμπιστοσύνη των πελατών του. Το πρότυπο όμως έχει και αδυναμίες.

Ο Bon (2006) αναφέρει δύο βασικές αδυναμίες του προτύπου. Ένα από τα κύρια προβλήματα που εντοπίζει κατά τη διάρκεια υλοποίησης ενός ISMS είναι ο μεγάλος αριθμός των περιουσιακών στοιχείων που διαθέτει ένας οργανισμός. Ακόμα και στη σπάνια περίπτωση των χιλίων περιουσιακών στοιχείων, το πρότυπο αναφέρει ότι όλα τα εν λόγω περιουσιακά στοιχεία θα πρέπει να αξιολογηθούν για τις απαιτήσεις ασφάλειας των πληροφοριών τους, έναντι κάθε πιθανής απειλής. Ο μεγάλος αριθμός συνδυασμών περιουσιακών στοιχείων/απειλών παρέχουν μια μεγάλη πρόκληση για την πρώτη επανάληψη μέσω του κύκλου PDCA.

Μια δεύτερη αδυναμία που παρατηρεί είναι ότι οι σύγχρονοι οργανισμοί νιώθουν την ανάγκη να μοιράζονται πληροφορίες εκτός των φυσικών τους ορίων, με συνεργαζόμενους οργανισμούς. Ο προσδιορισμός του αντικειμένου και των ορίων του συστήματος ISMS γίνεται δύσκολος, δεδομένου ότι είναι δυνατό δύο ή περισσότεροι οργανισμοί να συμπεριλαμβάνονται σε αυτό. Η εξωτερική αξιολόγηση όλων των συνεργαζόμενων οργανισμών έναντι των απαιτήσεων του προτύπου ίσως μπορεί να μειώσει αυτό το πρόβλημα. Επίσης, μια μεταξύ τους συμφωνία, σε σχετικά μικρό βαθμό λεπτομέρειας, όπως τα επίπεδα ασφάλειας των πληροφοριών θα βοηθήσει περισσότερο προς αυτήν την κατεύθυνση.

2.3.5. Λάθη κατά την εφαρμογή του προτύπου ISO 27001

Οι Solms (2004) αναγνωρίζουν ότι υπάρχει ένας μεγάλος αριθμός κοινών επαναλαμβανόμενων λαθών που συναντώνται σε συστήματα διαχείρισης ασφάλειας πληροφοριών διάφορων οργανισμών. Αν έστω και ένα από αυτά αγνοηθεί ή δε ληφθεί σοβαρά υπόψη, τότε θα ανακύψουν στον οργανισμό σοβαρά προβλήματα στην υλοποίηση και διατήρηση ενός κατάλληλου συστήματος διαχείρισης ασφάλειας πληροφοριών. Στην συνέχεια θα αναλυθούν αυτά τα λάθη καθώς και οι λόγοι που η ύπαρξη τους προκαλεί προβλήματα ασφάλειας πληροφοριών.

Ένα συχνό λάθος είναι η πολύ μικρή ανταλλαγή απόψεων με άλλους ειδικούς στην ασφάλεια των πληροφοριών. Η βασική ιδέα της ανταλλαγής απόψεων σε θέματα ασφάλειας πληροφοριών είναι η έννοια του «να διδάσκεται ένας οργανισμός από τις επιτυχημένες εμπειρίες ασφάλειας πληροφοριών των άλλων». Και αυτό επειδή, σε ένα μεγάλο βαθμό οι απειλές ασφάλειας πληροφοριών, οι κίνδυνοι και τα επιλεγμένα μέτρα αντιμετώπισης είναι σχεδόν ίδια για όλους τους οργανισμούς. Το αποτέλεσμα της μικρής ανταλλαγής απόψεων είναι η σπατάλη χρόνου και χρήματος προκειμένου να βρει ο οργανισμός μια λύση, η οποία είναι ήδη καταγεγραμμένη και εφαρμοσμένη από έναν άλλο οργανισμό.

Ιδιαίτερα σημαντικό σφάλμα είναι και η μη συνειδητοποίηση ότι η «πολιτική ασφάλειας πληροφοριών» είναι απολύτως απαραίτητη. Η κατάλληλη πολιτική ασφάλειας πληροφοριών είναι η «καρδιά» και η βάση ενός επιτυχημένου συστήματος διαχείρισης ασφάλειας πληροφοριών- (ISMS). Πρέπει να είναι σαφής, συνοπτική (έως 3 σελίδες) και υπογεγραμμένη από τη Διοίκηση. Αυτός είναι ο πιο διαφανής τρόπος με το οποίο η Διοίκηση αποδεικνύει τη δέσμευση και το ενδιαφέρον της σε ζητήματα ασφάλειας πληροφοριών του οργανισμού. Συχνά όμως οι πολιτικές αυτές λείπουν, δεν είναι ενημερωμένες, είναι άγνωστες στο προσωπικό, δεν εφαρμόζονται ή δεν υπάρχουν τεκμηριωμένες αποδείξεις επανεξέτασής τους. Η συνέπεια όλων αυτών είναι όλες οι προσπάθειες του οργανισμού για ασφάλεια πληροφοριών θα είναι ατελέσφορες και δεν θα αποδεικνύουν ένα υψηλό επίπεδο δέσμευσης.

Επιπρόσθετο σφάλμα είναι η μη εξασφάλιση του κατάλληλου διαχωρισμού καθηκόντων. Με άλλα λόγια, η ύπαρξη μιας οργανωσιακής δομής διαχείρισης ασφάλειας πληροφοριών είναι απαραίτητη. Με την έννοια ότι έχουν καθοριστεί οι αρμοδιότητες, υπάρχει επικοινωνία μεταξύ των εμπλεκομένων και συμμετοχή της Διοίκησης στην ασφάλεια πληροφοριών. Οι περιγραφές θέσεων εργασίας όμως δεν είναι πάντα ενημερωμένες και όταν αυτές υπάρχουν σπάνια περιέχουν οποιαδήποτε απαίτηση ασφάλειας πληροφοριών για όλο το προσωπικό. Σε γενικές γραμμές, ελάχιστες οδηγίες υπάρχουν σχετικά με την αναφορά συμβάντων ασφαλείας.

Οτιδήποτε έχει σχέση με την ασφάλεια πληροφοριών αυτομάτως αναφέρεται μόνο στον «Υπεύθυνο Ασφάλειας Πληροφοριών», ο οποίος όμως στην πραγματικότητα δεν έχει την «κυριότητα» καμίας πληροφορίας απλά είναι ο επιβλέπων. Η ευθύνη για την ασφάλεια πληροφοριών πρέπει να είναι μοιρασμένη σε όλους τους εργαζομένους, και όχι μόνο στον «Υπεύθυνο Ασφάλειας Πληροφοριών». Όταν οι «ιδιοκτήτες» της πληροφορίας δεν είναι επακριβώς καθορισμένοι και δεν έχουν οριστεί υπεύθυνοι για την ασφάλεια της πληροφορίας που είναι υπό τον έλεγχό τους, τότε σοβαροί κίνδυνοι ανακύπτουν.

Οι Calder και Watkins (2006) παρατηρούν ότι τα περισσότερα συστήματα πληροφοριών δεν έχουν σχεδιαστεί από την αρχή για να είναι ασφαλή. Τα τεχνικά μέτρα ασφαλείας έχουν περιορισμένη ικανότητα να προστατεύσουν ένα σύστημα πληροφοριών. Τα συστήματα διαχείρισης πληροφοριών και οι διαδικαστικοί έλεγχοι είναι απαραίτητα στοιχεία κάθε πραγματικά ασφαλούς συστήματος πληροφοριών και για να είναι αποτελεσματικό, χρειάζεται προσεκτικό σχεδιασμό και προσοχή σε κάθε λεπτομέρεια.

Ο Dey (2007)αναφέρει στο άρθρο του ένα ακόμη σύνηθες σφάλμα, τη μη αλλαγή της οργανωσιακής κουλτούρας. Είναι σημαντικό να υπάρχει και μια αλλαγή στην κουλτούρα του οργανισμού όσον αφορά τη διαχείριση της πληροφορίας αλλά και την προστασία της γενικότερα. Οι εργαζόμενοι, από την Διοίκηση μέχρι τους τελικούς χρήστες, πρέπει να εμπλακούν ενεργά στο σχεδιασμό, στην υλοποίηση αλλά και στη διατήρηση του «Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών» μέσα στον οργανισμό. Ο Ashenden (2008) συμπληρώνει επί του θέματος ότι ενώ πολλοί πιστεύουν ότι η αλλαγή στην κουλτούρα μπορεί να επέλθει μέσω της τεχνολογίας και της διεργασίας, περιστατικά σε οργανισμούς υψηλού κύρους, όπως στην Εφορία Ην.Βασιλείου -HMRC (Her Majesty's Revenue & Customs), στον Οργανισμό Αδειοδότησης Οδηγών και Οχημάτων Ην.Βασιλείου – MoD (Ministry of Defence) και στο Υπουργείο Άμυνας Ην.Βασιλείου, αποδεικνύουν την αποτυχία της τεχνολογίας και της διεργασίας να προστατεύσουν την ασφάλεια των πληροφοριών. Σε κάθε μια από αυτές τις περιπτώσεις διαφαίνεται ότι ο χρήστης δεν κατείχε την κουλτούρα, τεχνικές βασισμένες στην εμπειρία, ώστε να διαχειριστεί την ασφάλεια της πληροφορίας προς τη σωστή κατεύθυνση.

Ο Humphreys (2008) εντοπίζει επιπλέον λάθη σε συστήματα διαχείρισης ασφάλειας πληροφοριών. Ένα από αυτά είναι ότι δεν ελέγχονται οι συστάσεις των συμβασιούχων ή των συμβούλων, δεν εξακριβώνεται η προηγούμενη απασχόληση του εργαζομένου, ούτε γίνεται έρευνα για το ποινικό του μητρώο. Αυτό μπορεί να επιτρέψει σε κάποιον εγκληματία να έχει πρόσβαση σε κρίσιμες πληροφορίες του οργανισμού.

Επίσης, οι «Συμφωνίες Εμπιστευτικότητας», ενώ απαιτούν από όλο το προσωπικό να υπογράψει μια δήλωση ότι έχει λάβει γνώση και έχει κατανοήσει πλήρως τις πολιτικές ασφάλειας πληροφοριών, σπανίως χρησιμοποιούνται από τον οργανισμό, δεν καταγράφονται σε κεντρικό επίπεδο αλλά ακόμα και όταν το προσωπικό τις υπογράφει δεν καταλαβαίνει τί πραγματικά υπογράφει.

Ακόμα, επισημαίνει ότι δεν υπάρχει επαρκής ευαισθητοποίηση και δεν πραγματοποιούνται αρκετά εκπαιδευτικά προγράμματα. Η ευαισθητοποίηση όμως των χρηστών είναι απαραίτητη για το καλό του οργανισμού. Όλοι οι χρήστες πρέπει να είναι ενήμεροι για τους κινδύνους που συνδέονται με το πληροφοριακό σύστημα του οργανισμού, εξοικειωμένοι με τις πολιτικές ασφάλειας και τις διαδικασίες και να αποτελούν αυτές μέρος της καθημερινής τους εργασιακής ημέρας. Ο οργανισμός πρέπει να διαθέτει μια κατανοητή κατάρτιση ευαισθητοποίησης σε θέματα ασφάλειας πληροφοριών μέσω τακτικών ενημερωτικών δελτίων και εγκυκλίων που θα ενημερώνουν το προσωπικό για τις τελευταίες εξελίξεις. Ενώ, θα πρέπει και να επανεξετάζει ή να αναπροσαρμόζει το πρόγραμμα ευαισθητοποίησης του όταν κρίνεται απαραίτητο. Παρότι τα παραπάνω είναι προφανή, σε πολλούς οργανισμούς δεν υπάρχουν τα κατάλληλα προγράμματα ευαισθητοποίησης και οι χρήστες δεν έχουν γνώση των κινδύνων ασφάλειας πληροφοριών καθώς και της ζημιάς που μπορούν να προκαλέσουν. Ακόμα χειρότερα συχνά δε γνωρίζουν την πολιτική ασφάλειας πληροφοριών και τις διαδικασίες του οργανισμού. Οι χρήστες όμως δε γίνεται να καθιστούν υπεύθυνοι για προβλήματα ασφάλειας εάν δεν έχουν ενημερωθεί προηγουμένως για το ποια είναι αυτά και πώς μπορούν να αποφευχθούν. Το φαινόμενο που παρατηρείται είναι το σύστημα διαχείρισης ασφάλειας του οργανισμού να γνωρίζει την αποτυχία όταν οι χρήστες δεν είναι εκπαιδευμένοι προς αυτήν την κατεύθυνση.

Συγχρόνως, ο συγγραφέας παρατηρεί ένα σφάλμα σχετικά με τη διαχείριση των «Εναπομεινάντων Κινδύνων» που αναφέρει το πρότυπο. Εδώ υπάρχουν δύο ακραίες περιπτώσεις, είτε σπάνια υπάρχει μία επίσημη αποδοχή του εναπομείναντα κινδύνου εκ μέρος του οργανισμού, είτε ξοδεύονται υπέρογκα ποσά στην προσπάθεια εξάλειψής του. Όσον αφορά την πρώτη περίπτωση, το πρότυπο με σαφήνεια αναφέρει ότι ο οργανισμός πρέπει να λάβει τη γραπτή έγκριση της διοίκησης όσον αφορά τους προτεινόμενους εναπομένοντες κινδύνους. Ενώ, σχετικά με τη δεύτερη, μια γενική αρχή είναι ο οργανισμός να δαπανήσει ακριβώς όσα απαιτούνται για την ασφάλεια των πληροφοριών του-δηλαδή ούτε πολύ λίγα αλλά ούτε και πάρα πολλά- διότι υπάρχει ένα όριο πέραν του οποίου όσο περισσότερα χρήματα ξοδεύει για την ασφάλεια των πληροφοριών τόσο θα είναι φθίνουσα η απόδοση των επενδύσεων του οργανισμού. Μια άλλη επιλογή είναι η ελαχιστοποίηση των κινδύνων και η μεγιστοποίηση των επενδύσεων του οργανισμού στον τομέα της ασφάλειας. Όποια και αν είναι η τελική επιλογή του οργανισμού για τη διαχείριση του κινδύνου θα υπάρχει πάντα ένας υπολειπόμενος κίνδυνος που ποτέ δεν μπορεί να μειωθεί στο

μηδέν. Όσο περισσότερα χρήματα ξοδεύονται στην προσπάθεια μείωσης αυτού του εναπομείναντα κινδύνου πέραν ενός ορισμένου σημείου, τόσο πιθανότερο είναι ο οργανισμός να έρθει αντιμέτωπος με ταχύτατα φθίνουσες αποδόσεις δίχως πραγματικό όφελος.

Ο Ashenden (2008) συμπληρώνει τρία ακόμα λάθη που πρέπει να αποφευχθούν. Ένα από αυτά είναι ο μη σωστός προσδιορισμός της ταυτότητας του «Υπεύθυνου Ασφάλειας Πληροφοριών». Μια από τις δυσκολίες που αντιμετωπίζει ένας «Υπεύθυνος Ασφάλειας Πληροφοριών» είναι ότι αμφιταλαντεύεται σχετικά με το ποια συμπεριφορά πρέπει να επιδεικνύει, σκληρή και αυστηρή ή φιλική και συναδελφική. Στη μια περίπτωση ο ρόλος τους είναι εκείνος του εξειδικευμένου τεχνικού που αποφασίζει λαμβάνοντας υπόψη μόνο την ασφάλεια πληροφοριών δίχως τη συμμετοχή των υπαλλήλων, δίνει εντολές και ελέγχει. Όμως, μια τέτοια συμπεριφορά έχει ως αποτέλεσμα οι εργαζόμενοι να θεωρούν εσφαλμένα ότι εφόσον ο «Υπεύθυνος Ασφάλειας Πληροφοριών» τους ελέγχει επειδή δεν μπορούν να ελέγξουν τον εαυτό τους, δεν χρειάζεται να ανησυχούν οι ίδιοι για απαιτήσεις ασφάλειας πληροφοριών, ο «Υπεύθυνος» θα ενδιαφερθεί για αυτές. Αλλά, από την πλευρά αν επιλέξει τη πιο συναδελφική στάση και ενθαρρύνει τους χρήστες να λαμβάνουν αποφάσεις σχετικά με την ασφάλεια πληροφοριών τότε είναι πιθανό να συμβούν περισσότερα περιστατικά και λάθη, τουλάχιστον βραχυπρόθεσμα. Δυστυχώς η έρευνα έχει δείξει ότι οι δύο αυτοί ρόλοι πολλές φορές συγχέονται και αυτό οδηγεί σε αντιφατικά μηνύματα προς τους χρήστες.

Ένα δεύτερο λάθος που ο συγγραφέας τονίζει είναι ότι παρατηρείται όλο και σε περισσότερους οργανισμούς τα τελευταία χρόνια η αντίληψη ότι η ασφάλεια πληροφοριών είναι ένα τεχνικό ζήτημα και για αυτό πρέπει να διαχειρίζεται από τεχνικό προσωπικό. Αυτή η αντίληψη το μόνο που πετυχαίνει είναι να αποσυνδέει την ασφάλεια πληροφοριών από τον επιχειρησιακό της χαρακτήρα. Δυστυχώς υπάρχει ένας σημαντικός αριθμός οργανισμών όπου η ασφάλεια πληροφοριών παραμένει ένα τεχνικό μόνο κομμάτι τους. Αλλά ακόμα και σε οργανισμούς με πιο ώριμη προσέγγιση υπάρχει χάσμα μεταξύ εκείνων που είναι υπεύθυνοι για την ασφάλεια πληροφοριών και της Διοίκησης. Η Διοίκηση καθιστά κάποιον ως «Υπεύθυνο Ασφάλειας Πληροφοριών» και περιμένει από αυτόν να κάνει τα πάντα μόνος του. Πολύ συχνά ο «Υπεύθυνος Ασφάλειας Πληροφοριών» είναι ένα πρόσωπο της τεχνολογίας πληροφοριών-IT (Information Technology) που αναφέρεται στο Τμήμα Πληροφορικής και δεν έχει τη δυνατότητα να απευθυνθεί κατευθείαν στη Διοίκηση. Στην πραγματικότητα, αυτό εξυπηρετεί τον «Υπεύθυνο Ασφάλειας Πληροφοριών», διότι με αυτόν τον τρόπο σοβαρά θέματα έχουν μικρή πιθανότητα να φτάσουν στη Διοίκηση, εκτός εάν κάποιο είναι τόσο καταστροφικό που δεν μπορεί να κρυφτεί λόγος που υπάρχει αυτό το χάσμα είναι η επικοινωνία. Έχει επισημανθεί ότι η γλώσσα της ασφάλειας πληροφοριών τείνει να είναι τεχνική και εξειδικευμένη και ως αποτέλεσμα τα μέλη της Διοίκησης δυσκολεύονται να την κατανοήσουν και να

δεσμευτούν. Η συνέπεια όμως αυτού του σφάλματος είναι ο «Υπεύθυνος Ασφάλειας Πληροφοριών» να συνειδητοποιήσει ότι δεν μπορεί να κάνει σωστά τη δουλειά του και είτε να συνεχίσει είτε να παραιτηθεί. Και στις δυο όμως περιπτώσεις ο οργανισμός θα έρθει αντιμέτωπος με σοβαρούς κινδύνους, αφού το σύστημα διαχείρισης ασφάλειας πληροφοριών δε θα έχει πλήρως υλοποιηθεί.

Τέλος, εντοπίζει ένα τρίτο σφάλμα το οποίο αφορά το μη σωστό προσδιορισμό των ικανοτήτων που πρέπει να διαθέτει ο «Υπεύθυνος Ασφάλειας Πληροφοριών». Ο ρόλος όμως ενός υπευθύνου για την ασφάλεια των πληροφοριών είναι πλέον πολυδιάστατος και πολύπλοκος. Ανάμεσα στις ικανότητες που πρέπει να διαθέτει είναι ένα υψηλό επίπεδο τεχνικών γνώσεων όπως λειτουργικά συστήματα (Linux, Unix), πυρότοιχους, πρωτόκολλα εκπομπής, κρυπτογράφηση, αλλά και γνώσεις σχετικά με το πρότυπο διαχείρισης ασφάλειας πληροφοριών ISO 27001 όπως διεργασίες, πολιτικές, αξιολόγηση κινδύνων, σχετική νομοθεσία και τέλος ικανότητα να αλλάξει την οργανωσιακή κουλτούρα και να εισάγει προγράμματα ευαισθητοποίησης. Στην πράξη όμως έχει συχνά παρατηρηθεί να μην είναι κανένας επιφορτισμένος με το έργο του τακτικού ελέγχου της ασφάλειας, αλλά να αποτελεί εργασία μερικής απασχόλησης για κάποιον από τον τομέα της πληροφορικής, ο οποίος όμως ανά πάσα στιγμή μπορεί να αποσπαστεί από το καθήκον προκειμένου να κάνει κάποια άλλη εργασία.

Ο Broderick (2006) συγκέντρωσε τα πιο δημοφιλή από τα προαναφερθείσα λάθη στον παρακάτω πίνακα διαχωρίζοντας το μύθο από την πραγματικότητα.

ΜΥΘΟΣ	ΠΡΑΓΜΑΤΙΚΟΤΗΤΑ
Ένα ISMS είναι ένα πρότυπο που καθορίζει τεχνικές απαιτήσεις ασφαλείας.	Ένα ISMS είναι ένα σύστημα διαχείρισης, όχι ένα τεχνικό πρότυπο ασφάλειας πληροφοριών.
Μόνο εταιρείες ασφαλείας ή εμπειρογνώμονες ασφαλείας εφαρμόζουν ένα ISMS μέσα στον οργανισμό τους.	Οι περισσότερες εταιρείες που έχουν ένα σύστημα διαχείρισης ποιότητας, εφαρμόζουν ένα ISMS. Το ISMS μπορεί να μη χρησιμοποιεί πάντα ένα επίσημο πλαίσιο, όπως αυτό συνιστάται από το ISO/IEC 27001:2005, αλλά παραμένει ένα σύνολο διεργασιών που ανταποκρίνεται στις ανάγκες της επιχείρησης.
Η υλοποίηση ενός ISMS καθοδηγείται από το Τμήμα Ασφάλειας του εκάστοτε οργανισμού.	Η αρχική ιδέα της χρήσης ενός ISMS ενδέχεται να προέρχεται από το Τμήμα Ασφάλειας ενός οργανισμού.

	Η ανάπτυξη όμως, η υλοποίησή του και η συμμόρφωση με ένα ISMS πρέπει να καθοδηγείται αποκλειστικά από τη Διοίκηση, ειδάλλως θα αποτύχει. Εάν η Διοίκηση δεν πιστεύει στο ISMS κανένας στον οργανισμό δεν θα πιστέψει.
Η συμμόρφωση με ένα ISMS είναι δύσκολη και ακριβή.	Αρχικά αυτό μπορεί να ισχύει, αλλά μόνο έως ότου ο οργανισμός υιοθετήσει μια κουλτούρα προστασίας της πληροφορίας. Όταν αυτή η κουλτούρα θα έχει γίνει βίωμα, η συμμόρφωση και η λειτουργία σύμφωνα με ένα ISMS θα είναι απλά άλλη μια διεργασία που οι χρήστες των πληροφοριών μέσα στον οργανισμό θα πρέπει να ακολουθούν. Η αποφυγή έστω και ενός σοβαρού κινδύνου το χρόνο σίγουρα καλύπτει το κόστος συμμόρφωσης με το ISO 27001.
Η πληροφορία μπορεί να είναι πλήρως προστατευμένη χρησιμοποιώντας μόνο την τεχνολογία.	Η προστασία των πληροφοριών συχνά απαιτεί την εφαρμογή τεχνολογίας, αλλά πάντα απαιτεί τη χρήση των ανθρώπων και των διεργασιών. Με άλλα λόγια, είναι ένα σύστημα που εκτελούν οι άνθρωποι βασισμένοι σε καθιερωμένες διεργασίες. Εάν η προστασία παρέχεται με τη χρήση παροδικών μηχανισμών κατά περίπτωση, τότε η αποτελεσματικότητα της προστασίας δεν θα μπορεί να ελεγχθεί. Η αποτελεσματικότητα όμως της προστασίας είναι ζωτικής σημασίας για να αποδειχθεί η συμμόρφωση με τους εθνικούς και τοπικούς κανονισμούς, ανεξαρτήτως των καλών επιχειρηματικών δραστηριοτήτων του οργανισμού.
Ένα ISMS και ένας εθνικός ή τοπικός κανονισμός, όπως για παράδειγμα ο “EU Data Protection Directive” για την	Παρά το γεγονός ότι ένα βασικό σύνολο ειδικών απαιτήσεων ασφαλείας συχνά συνιστάται από το ISMS, οι απαιτήσεις

προστασία προσωπικών δεδομένων, δεν μπορούν να συμβαδίσουν και συνεπώς πρέπει να αντιμετωπίζονται χωριστά.	αυτές δεν εμποδίζουν την προσθήκη τυχόν πρόσθετων ή πιο περιοριστικών απαιτήσεων ασφαλείας.

2.3.6. Εμπειρική ανασκόπηση

Πρόσφατα ο Boehmer (2008) παρατήρησε ότι το ISO27001: 2005, ως ένα πιστοποιημένο σύστημα διαχείρισης ασφάλειας πληροφοριών-ISMS, εδραιώνεται ολοένα και περισσότερο ως το πρότυπο ασφάλειας στους οργανισμούς. Ο Humphreys (2008)συμπληρώνει ότι στην πραγματικότητα το πρότυπο αυτό σχεδιάστηκε να είναι αρκετά ευέλικτο ώστε να χρησιμοποιείται από όλα τα είδη οργανισμών εμπορικούς, κυβερνητικούς, μικρούς, μεσαίους, μεγάλους και μέσα σε ένα ευρύ φάσμα επιχειρηματικών τομέων. Συγκεκριμένα, το πρότυπο ISO 27001 έχει καθιερωθεί ως η «κοινή γλώσσα» στη διαχείριση της ασφάλειας των πληροφοριών. Μόνο το 2008 καταγράφηκαν περισσότεροι από 4.600 πιστοποιημένοι οργανισμοί σε όλο τον κόσμο (www.iso27001cerificates.com).

Παρότι το ISO 27001 θεωρείται ένα από τα πιο σημαντικά πρότυπα, λόγω του ότι είναι σχετικά καινούριο, δεν υπάρχει στη βιβλιογραφία πληθώρα συγγραμμάτων σε επίπεδο εμπειρικής έρευνας. Ωστόσο, υπάρχουν ορισμένοι συγγραφείς που έχουν πραγματοποιήσει αξιόλογη έρευνα σε εφαρμοσμένα συστήματα διαχείρισης ασφάλειας πληροφοριών-ISMS που έχουν πιστοποιηθεί κατά ISO 27001 και έχουν καταγράψει τα συμπεράσματά τους.

Μια τέτοια μελέτη περίπτωσης κατέγραψε ο Kenning (2001). Ο συγγραφέας παρουσιάζει την περίπτωση πιστοποίησης ενός από τους πρώτους οργανισμούς που πιστοποιήθηκαν με το πρότυπο ISO 17799, το οποίο υπήρξε προπάτορας του προτύπου ISO 27001. Ο οργανισμός αυτός ήταν ο «SETT-Ομάδα Αξιολόγησης της Ασφάλειας & Δοκιμών (Security Evaluation &Test Team)», ο οποίος στην πραγματικότητα ήταν μια μονάδα ενός μεγαλύτερου οργανισμού και αποτελούνταν από πέντε άτομα.

Ο συγγραφέας αναφέρει ότι η μεγαλύτερη πρόκληση που αντιμετώπισε ο οργανισμός ήταν ότι ως μέρος ενός μεγαλύτερου οργανισμού είχε περιορισμένο έλεγχο σε μεγάλες περιοχές όπως η πολιτική και οι διεργασίες που συνδέονταν με την ασφάλεια και είχαν τεθεί σε επίπεδο εταιρείας. Για παράδειγμα, το πρότυπο ISO 17799 έχει προδιαγραφές σχετικά με την πρόσληψη του προσωπικού, αλλά τέτοια θέματα τα χειριζόταν το Τμήμα Ανθρώπινου Δυναμικού της εταιρείας.

Αυτό είναι ένα από τα λάθη που εντόπισε ο Humphreys (2008) σε εφαρμοσμένα συστήματα διαχείρισης ασφάλειας πληροφοριών και αναφέρθηκε παραπάνω. Συγκεκριμένα, επειδή την πρόσληψη προσωπικού τη χειρίζεται το Τμήμα

Ανθρώπινου Δυναμικού και όχι οι εμπλεκόμενες Διευθύνσεις στο «Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών», δεν πληρούνται οι απαιτήσεις του προτύπου σχετικά με την πρόσληψη. Για παράδειγμα, δε γίνεται έρευνα για το ποινικό του μητρώο. Αυτό μπορεί να επιτρέψει σε κάποιον εγκληματία να έχει πρόσβαση σε κρίσιμες πληροφορίες του οργανισμού.

Τελικά, αυτό που επέλεξε να κάνει ο οργανισμός ήταν να αναγνωρίσει όλες τις διασυνδέσεις μεταξύ εκείνου και του εξωτερικού περιβάλλοντος (συμπεριλαμβανομένης και της υπόλοιπης εταιρείας) και εφάρμοσε τους κατάλληλους ελέγχους.

Επίσης, ο οργανισμός, βασιζόμενος στην εμπειρία του, ανέφερε ότι η βασική διαφορά μεταξύ του προτύπου ISO 17799 και του ISO 9001 είναι ότι το ISO 17799 έχει απαιτήσεις ασφάλειας. Αυτό σημαίνει ότι υπάρχουν έλεγχοι οι οποίοι μπορούν είτε να υιοθετηθούν από τον οργανισμό είτε να δικαιολογηθεί ο αποκλεισμός τους. Το συμπέρασμα του συγγραφέα ήταν ότι το πρότυπο μπορεί να θεωρηθεί ως ένα πρότυπο διαχείρισης της ποιότητας με μια προσέγγιση ασφάλειας πληροφοριών.

Αλλά και η παρούσα διπλωματική εργασία θέλει να συνεισφέρει σε αυτό ακριβώς το επίπεδο εμπειρικής έρευνας. Συγκεκριμένα, στόχος είναι να παρουσιαστούν τα αποτελέσματα της έρευνας αναφορικά με το βαθμό κατά τον οποίο το σύστημα διαχείρισης ασφάλειας κρίσιμων αεροναυτικών πληροφοριών που εφαρμόζει η Υ.Π.Α (Υπηρεσία Πολιτικής Αεροπορίας) πληροί τις απαιτήσεις του προτύπου ISO/IEC 27001:2005 «Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών-Απαιτήσεις».

Η ποιότητα των αεροναυτικών δεδομένων που χρησιμοποιούνται στις βάσεις δεδομένων της Υ.Π.Α (Υπηρεσία Πολιτικής Αεροπορίας) είναι ζωτικής σημασίας για την ασφαλή πλοήγηση αεροσκαφών.

Ειδικότερα, οι απαιτήσεις για την ασφάλεια των αεροναυτικών πληροφοριών που εμπεριέχονται στο «Εγχειρίδιο AIP (Aeronautical Information Publication)», καθορίζονται στο Παράρτημα 15 της Διεθνούς Συμβάσεως του Διεθνούς Οργανισμού Πολιτικής Αεροπορίας-ICAO (International Civil Aviation Organization).

Μία έρευνα όμως που διεξήχθη το 2003 από τον Ευρωπαϊκό Οργανισμό για την Ασφάλεια της Αεροναυτιλίας-EUROCONTROL σε εθνικά «Εγχειρίδια AIP» αποκάλυψε ότι το επίπεδο ασφάλειας των αεροναυτικών πληροφοριών είναι χαμηλότερο από το απαιτούμενο σύμφωνα με τα πρότυπα του Διεθνούς Οργανισμού Πολιτικής Αεροπορίας-ICAO.

Η έρευνα πραγματοποιήθηκε σε 25.357 αρχεία, το καθένα με 49 στοιχεία δεδομένων από εθνικά Εγχειρίδια AIP. Τα αποτελέσματα της έρευνας έδειξαν ότι περίπου το 11,5% των αρχειοθετημένων «Εγχειρίδιων AIP» περιλάμβαναν τουλάχιστον μια αναγνωρισμένη ασυνέπεια.

Μερικές από αυτές τις ασυνέπειες αναφέρονται παρακάτω :

- Διαφορετική μορφοποίηση μεταξύ ενοτήτων του ίδιου εγγράφου
- Μη ορθές τιμές
- Ελλιπή δεδομένα για ορισμένους αεροδιαδρόμους
- Ασυνεπής, ελλιπής και αντιφατική χρήση ακρωνυμίων για τα ραδιοβοηθήματα (π.χ. VOR, TDVOR) καθώς και για τα Αεροδρόμια
- Ασυνεπής μορφή των θερμοκρασιών ή καθόλου αναφορά σε θερμοκρασίες ανά αεροδρόμιο
- Αντιφατική και ελλιπής δημοσίευση τεχνικών χαρακτηριστικών ραδιοβοηθημάτων (π.χ. ισχύς ακτινοβολίας, συχνότητα λειτουργίας, μαγνητικές διακυμάνσεις)
- Δεν χρησιμοποιούσαν όλες οι χώρες κοινό σύστημα μέτρησης για προσδιορισμό υψόμετρου και απόστασης (κυρίως, μέτρα, πόδια, χιλιόμετρα, ναυτικά μίλια).

Το πρόβλημα είναι ότι ο χειροκίνητος έλεγχος του εγχειριδίου από τον πιλότο είναι ανέφικτος. Η οθόνη των οργάνων πρέπει να συγκρίνεται κάθε φορά από τον πιλότο με τις πληροφορίες του Εγχειριδίου. Ο όγκος όμως των δεδομένων είναι μεγάλος και ο κύκλος ισχύος ορισμένων επιχειρησιακά σημαντικών πληροφοριών εξαιρετικά μικρός.

Με στόχο την ανακούφιση του χειριστή από αυτό το βάρος, η ποιότητα των δεδομένων πρέπει να διασφαλίζεται σε όλα τα στάδια της διεργασίας έκδοσης και ενημέρωσης του Εγχειριδίου Αεροναυτικών Πληροφοριών -AIP.

Προκειμένου να συνεισφέρει η παρούσα διπλωματική εργασία σε επίπεδο εμπειρικής έρευνας το «Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών-ISMS», της Υ.Π.Α εξετάστηκε σε επόμενο κεφάλαιο ως προς το σχεδιασμό, την υλοποίηση, τον έλεγχο και τη συνεχή βελτίωσή του, ώστε να προκύψει ο βαθμός κατά τον οποίο πληροί τις απαιτήσεις του προτύπου.

3. ΜΕΘΟΔΟΛΟΓΙΑ & ΕΡΕΥΝΑ

3.1. Εισαγωγή

Βασικός στόχος της παρούσας διπλωματικής εργασίας ήταν να συνεισφέρει σε επίπεδο εμπειρικής έρευνας αναφορικά με το πρότυπο ISO/IEC 27001:2005 «Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών-Απαιτήσεις».

Για το σκοπό αυτό επιλέχθηκε ένα υπαρκτό, εν λειτουργία σύστημα διαχείρισης ασφάλειας πληροφοριών, το «Σύστημα Διαχείρισης Ασφάλειας Αεροναυτικών Πληροφοριών» της Υ.Π.Α (Υπηρεσία Πολιτικής Αεροπορίας).

Συγκεκριμένα, μελετήθηκε ο βαθμός κατά τον οποίο το σύστημα διαχείρισης κρίσιμων αεροναυτικών πληροφοριών που εφαρμόζει η Υ.Π.Α πληροί τις απαιτήσεις του προτύπου ISO/IEC 27001:2005.

Στο κεφάλαιο αυτό θα παρουσιαστεί η έρευνα που διεξήχθη στον οργανισμό, ούτος ώστε να συγκεντρωθούν όλες εκείνες οι απαραίτητες πληροφορίες για τη μελέτη του συστήματος διαχείρισης ασφάλειας αεροναυτικών πληροφοριών που εφαρμόζει η Υ.Π.Α.

Παράλληλα, θα γίνει αναφορά και στη μεθοδολογία που ακολουθήθηκε προκειμένου να επιτευχθεί ο προαναφερόμενος βασικός στόχος.

3.2. Μεθοδολογία-Έρευνα

Στο σχήμα που ακολουθεί παρουσιάζεται συνοπτικά η διαδικασία που ακολουθήθηκε στην μεθοδολογία που πραγματοποιήθηκε.

Τα πρώτα βήματα εστιάζουν στην κατανόηση της έννοιας και της σημαντικότητας των αεροναυτικών πληροφοριών, που εμπεριέχονται σε ένα «Εγχειρίδιο AIP», καθώς και της βασικής διεργασίας έκδοσης και ενημέρωσης του συγκεκριμένου εγχειριδίου.

Τα επόμενα βήματα, αφορούν την κατανόηση του προτύπου και των απαιτήσεων του σε βάθος και ακολούθως τη σύγκριση της υφιστάμενης διεργασίας με αυτές τις απαιτήσεις με απώτερο σκοπό να εντοπιστούν πιθανές αποκλίσεις.

Διαδικασία Μεθοδολογίας-Έρευνας

ΠΕΡΙΓΡΑΦΗ ΕΓΧΕΙΡΙΔΙΟΥ ΑΙΡ → **ΑΠΟΤΥΠΩΣΗ ΒΑΣΙΚΗΣ ΔΙΕΡΓΑΣΙΑΣ ΕΚΔΟΣΗΣ ΑΙΡ** → **ΑΠΟΤΥΠΩΣΗ ΠΡΟΤΥΠΟΥ ISO/IEC 27001** → **ΣΥΓΚΡΙΣΗ ΑΠΑΙΤ.ΠΡΟΤΥΠΟΥ & ΒΑΣΙΚΗΣ ΔΙΕΡΓΑΣΙΑΣ ΕΚΔΟΣΗΣ ΕΓΧ.ΑΙΡ**

Ειδικότερα, έγινε αρχικά προσπάθεια να κατανοηθεί η έννοια της «Υπηρεσίας Παροχής Αεροναυτικών Πληροφοριών AIS (Aeronautical Information Service)», καθώς και ο λόγος που το «Εγχειρίδιο Αεροναυτικών Πληροφοριών-AIP», το οποίο εκδίδει και ενημερώνει η Υ.Π.Α, είναι ζωτικής σημασίας, ενώ εν συνεχεία μελετήθηκε η βασική διεργασία, «Έκδοση & Ενημέρωση του Εγχειριδίου Αεροναυτικών Πληροφοριών AIP (Aeronautical Information Publication)».

Πραγματοποιήθηκαν επιτόπιες έρευνες στην Υπηρεσία Πολιτικής Αεροπορίας, που περιλάμβαναν εύρεση του οργανογράμματος του οργανισμού, συνεντεύξεις με στελέχη των εμπλεκόμενων διευθύνσεων, μελέτη της Διεθνούς Συμβάσεως του Διεθνούς Οργανισμού Πολιτικής Αεροπορίας ICAO (International Civil Aviation Organization) και του Παραρτήματός της 15 (Annex 15).

Συγκεντρώνοντας τα παραπάνω στοιχεία αποτυπώθηκε διαγραμματικά η βασική διεργασία «Έκδοση & Ενημέρωση του Εγχειριδίου Αεροναυτικών Πληροφοριών AIP (Aeronautical Information Publication)» και αναλύθηκε ως προς τις παραμέτρους της, όπως ανθρώπινοι πόροι, υποδομές /εξοπλισμός και υποδιεργασίες.

Προκειμένου να αναλυθεί η βασική διεργασία στις τρείς υποδιεργασίες της, «Συλλογή και καταγραφή αεροναυτικών πληροφοριών», «Επεξεργασία αεροναυτικών πληροφοριών», «Έκδοση & διανομή Εγχειριδίου AIP» και να αποτυπωθούν αυτές αναζητήθηκε ένας όγκος πληροφοριών.

Οι πληροφορίες αυτές συλλέχθηκαν από εγχειρίδια, οδηγίες, έντυπα, εταιρικές παρουσιάσεις, αρχεία και την παρακολούθηση της ηλεκτρονικής εφαρμογής **eAIP.wiz@rd**.

Ειδικά, η επιτόπια παρουσίαση της προαναφερόμενης ηλεκτρονικής εφαρμογής συντέλεσε σημαντικά στην αποτύπωση της δεύτερης συγκεκριμένα υποδιεργασίας, αφού έδωσε τη δυνατότητα προσομοίωσης της υποδιεργασίας, αλλά ταυτόχρονα και την ευκαιρία να παρακολουθηθεί μια πραγματική επεξεργασία αεροναυτικών πληροφοριών στην πράξη.

Επίσης, αξιόλογα στοιχεία προέκυψαν και από τη μελέτη ενός πρόσφατου «Εγχειριδίου Αεροναυτικών Πληροφοριών AIP». Όπως, τί είδους αεροναυτικές πληροφορίες εμπεριέχει, από ποιές ενότητες αποτελείται, πώς ενημερώνεται.

Με την αξιοποίηση αυτών των δεδομένων η κάθε υποδιεργασία αποτυπώθηκε διαγραμματικά με μορφή διαγράμματος ροής και αναλύθηκε ως προς το σκοπό, το πεδίο εφαρμογής, τους εμπλεκόμενους, τη διαδικασία της, τα έντυπα και τις όποιες εξειδικευμένες οδηγίες της.

Δεύτερο βήμα ήταν η αναλυτική παρουσίαση των απαιτήσεων του προτύπου ISO/IEC 27001:2005 «Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών-Απαιτήσεις». Το πρότυπο αποτελείται από οκτώ ενότητες και δύο παραρτήματα. Στις τρείς πρώτες ενότητες γίνεται αναφορά στην ορολογία, ενώ από την τέταρτη ενότητα ξεκινούν οι απαιτήσεις του προτύπου.

Το πρότυπο αναζητήθηκε ολόκληρο στον Ελληνικό Οργανισμό Τυποποίησης (ΕΛΟΤ), στην εργασία όμως παρουσιάστηκε μόνο η τέταρτη ενότητα, δηλαδή μόνο οι απαιτήσεις.

Οι οποίες είναι οι ακόλουθες, «4.Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών ISMS-Γενικές Απαιτήσεις», «5.Ευθύνη Διοίκησης», «6.Εσωτερικές Επιθεωρήσεις ISMS», «7.Ανασκόπηση Διοίκησης ISMS», «8.Βελτίωση ISMS» καθώς και το πρώτο παράρτημα, «ΠΑΡΑΡΤΗΜΑ Α.Στόχοι ελέγχων & έλεγχοι».

Στη συνέχεια, έχοντας αποτυπώσει τη βασική διεργασία και έχοντας παρουσιάσει τις απαιτήσεις του προτύπου εμβαθύναμε περισσότερο πραγματοποιώντας μια σύγκριση ανάμεσα στην υφιστάμενη διεργασία έκδοσης και ενημέρωσης του Εγχειριδίου AIP, σε σχέση με αυτές τις απαιτήσεις.

Ειδικότερα, ελέγχθηκε, μέσω επιτόπιων ελέγχων εγγράφων, εντύπων, αρχείων, εγχειριδίων, συνεντεύξεων με στελέχη, κάθε μια απαίτηση ξεχωριστά αν υλοποιείται και σε ποιό βαθμό.

Παράλληλα, ο βαθμός ικανοποίησης της απαίτησης του προτύπου ακολουθείται από επεξηγηματική ανάλυση με τεκμηριωμένα στοιχεία, τα οποία προέκυψαν από την έρευνα που διεξήχθη στον οργανισμό.

Απώτερος σκοπός αυτής της σύγκρισης ήταν να προκύψει εάν το σύστημα διαχείρισης ασφάλειας κρίσιμων αεροναυτικών πληροφοριών που εφαρμόζει η Υ.Π.Α είναι πιστοποιήσιμο κατά το πρότυπο ISO/IEC 27001:2005.

Ενώ, όπου εντοπίστηκε απόκλιση μεταξύ της απαίτησης του προτύπου και της βασικής διεργασίας, όπως διεξάγεται από τον οργανισμό, προτάθηκαν τρόποι οι οποίοι θα μπορούσαν να συμβάλλουν στη σύγκλιση της διεργασίας στις απαιτήσεις του προτύπου.

Τέλος, δεν παραλήφθηκε να γίνει αναφορά και στο ΠΑΡΑΡΤΗΜΑ Α του προτύπου «Στόχοι ελέγχων & έλεγχοι». Συγχρόνως, αναζητήθηκε η «Δήλωση Εφαρμοσιμότητας» του οργανισμού, η οποία περιλαμβάνει τους στόχους ελέγχων, τους ελέγχους, και την αιτιολόγηση της επιλογής τους. Στη συνέχεια, ελέγχθηκε σε ποιό βαθμό οι έλεγχοι και οι στόχοι ελέγχων που ο οργανισμός έχει επιλέξει

συμπίπτουν με εκείνους που το πρότυπο απαιτεί στον Πίνακα Α του ΠΑΡΑΡΤΗΜΑΤΟΣ Α, πώς αποτυπώνονται σχηματικά στο διάγραμμα ροής της κάθε υποδιεργασίας και εάν είναι επαρκείς.

Και με το παράρτημα αυτό κλείνει η μελέτη του συστήματος διαχείρισης κρίσιμων αεροναυτικών πληροφοριών που εφαρμόζει η Υ.Π.Α μέσα από το πρίσμα των απαιτήσεων του προτύπου ISO/IEC 27001:2005.

4. ΒΑΣΙΚΗ ΔΙΕΡΓΑΣΙΑ ΕΚΔΟΣΗΣ & ΔΙΑΝΟΜΗΣ «ΕΓΧΕΙΡΙΔΙΟΥ ΑΕΡΟΝΑΥΤΙΚΩΝ ΠΛΗΡΟΦΟΡΙΩΝ-AIP» (Aeronautical Information Publication)

4.1. Εισαγωγή

Η παρούσα διπλωματική εργασία θέλοντας να μελετήσει την εφαρμογή του προτύπου ISO/IEC 27001:2005 σε εμπειρικό επίπεδο επέλεξε έναν οργανισμό που διαχειρίζεται κρίσιμες πληροφορίες, την Υ.Π.Α (Υπηρεσία Πολιτικής Αεροπορίας). Ο λόγος που επιλέχτηκε ο συγκεκριμένος οργανισμός είναι ότι η ποιότητα των αεροναυτικών πληροφοριών που εμπεριέχονται στο «Εγχειρίδιο Αεροναυτικών Πληροφοριών-AIP»,το οποίο εκδίδει και ενημερώνει, είναι ζωτικής σημασίας για την ασφαλή πλοήγηση αεροσκαφών.

Το «Εγχειρίδιο Αεροναυτικών Πληροφοριών-AIP» εκδίδεται και ενημερώνεται μέσω της υλοποίησης μιας προκαθορισμένης και τυποποιημένης αλληλουχίας ενεργειών, η οποία μετατρέπει την εισερχόμενη αεροναυτική πληροφορία, μόνιμης φύσης ή προσωρινής αλλαγής, σε εξερχόμενο Εγχειρίδιο. Αυτός είναι και ο λόγος που θα την ορίσουμε ως τη βασική διεργασία έκδοσης και ενημέρωσης του Εγχειριδίου.

Στο παρόν κεφάλαιο θα αναλυθεί ο όρος «Αεροναυτικές Πληροφορίες», θα αποτυπωθεί η εν λόγω βασική διεργασία, οι απαιτούμενοι πόροι για την υλοποίησή της καθώς και οι τρείς υποδιεργασίες στις οποίες αναλύεται, «Συλλογή & καταγραφή αεροναυτικών πληροφοριών», «Επεξεργασία αεροναυτικών πληροφοριών» και τέλος «Έκδοση & διανομή «Εγχειριδίου Αεροναυτικών Πληροφοριών-AIP».

4.2. Αεροναυτικές Πληροφορίες (Aeronautical Information)

Ο χειριστής οποιουδήποτε τύπου αεροσκάφους, είτε αυτό είναι ένα μικρό ιδιωτικό είτε ένα μεγάλο τζετ, πρέπει να έχει στη διάθεσή του ένα ευρύ φάσμα πληροφοριών σχετιζόμενο με τις λειτουργικές εγκαταστάσεις και τις υπηρεσίες αεροναυτιλίας τις οποίες ενδέχεται να χρησιμοποιήσει.

Για παράδειγμα, ο πιλότος πρέπει να γνωρίζει τους κανονισμούς που σχετίζονται με τα σημεία εισόδου και διέλευσης του εναέριου χώρου της κάθε χώρας στην οποία πρόκειται να ταξιδέψει. Επίσης πρέπει να γνωρίζει τα χαρακτηριστικά των αεροδρομίων, των αεροδιαδρόμων, των ραδιοβοηθημάτων, των συστημάτων επικοινωνίας, των συχνοτήτων επικοινωνίας, των μετεωρολογικών συνθηκών και επίσης να γνωρίζει ποιά αεροδρόμια αλλά και ποιά ραδιοβοηθήματα είναι διαθέσιμα καθώς και τις διαδικασίες και τους κανονισμούς που σχετίζονται με αυτά. Το σύνολο αυτών των πληροφοριών είναι γνωστό διεθνώς ως Αεροναυτικές Πληροφορίες (Aeronautical Information).

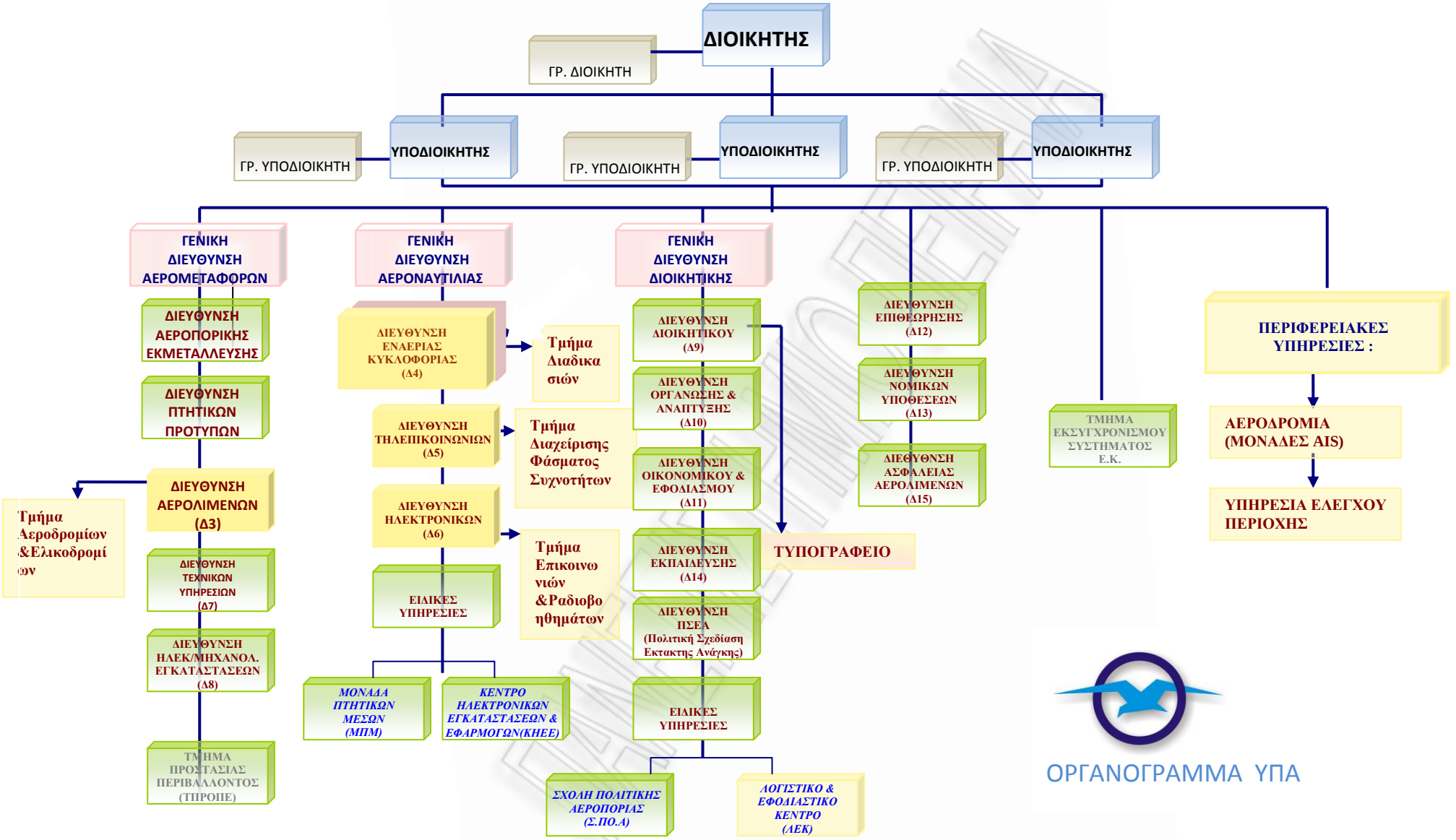
Κάθε αλλαγή στα συστήματα ή τις υπηρεσίες, που ενδέχεται να έχει αντίκτυπο στην απρόσκοπτη πτήση του αεροσκάφους πρέπει να φτάνει έγκαιρα σαν πληροφορία στον πιλότο. Κατά κανόνα οι πληροφορίες αυτές σχεδόν πάντα πρέπει να λαμβάνονται πριν την απογείωση και σε ορισμένες μόνο περιπτώσεις κατά τη διάρκεια της πτήσης.

4.3. Υπηρεσία Παροχής Αεροναυτικών Πληροφοριών AIS (Aeronautical Information Services)

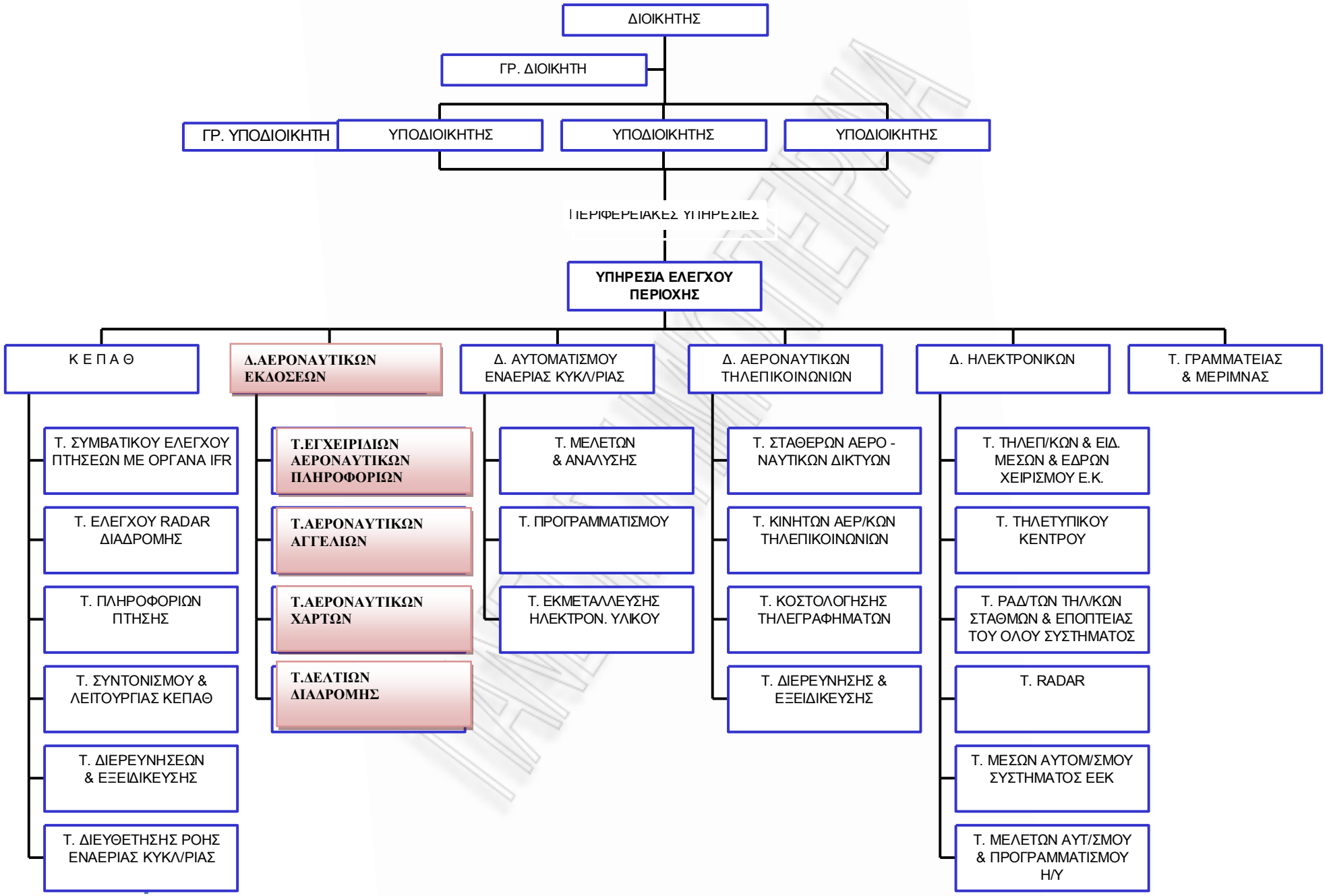
Κάθε κράτος είναι υπεύθυνο σύμφωνα με τη Διεθνή Σύμβαση του Διεθνούς Οργανισμού Πολιτικής Αεροπορίας ICAO (International Civil Aviation Organization) και το Παράρτημα 15 (Annex 15) να διασφαλίζει μέσω μιας Υπηρεσίας που διεθνώς είναι γνωστή ως *«Υπηρεσία Παροχής Αεροναυτικών Πληροφοριών-AIS (Aeronautical Information Services)»* τη συλλογή και τη διανομή των αεροναυτικών πληροφοριών που είναι απαραίτητες για την *ασφάλεια*, *κανονικότητα* και *αποτελεσματικότητα* της διεθνούς και εθνικής αεροναυτιλίας εντός του εναέριου χώρου της επικράτειας μιας χώρας καθώς και του εναέριου χώρου υπεράνω των Διεθνών Υδάτων για τα οποία την ευθύνη παροχής υπηρεσιών αεροναυτιλίας έχει το εν λόγω κράτος.

Στην Ελλάδα η Υπηρεσία AIS παρέχεται από την ΥΠΑ-Υπηρεσία Πολιτικής Αεροπορίας, η οποία υπάγεται στο Υπουργείο Μεταφορών και Επικοινωνιών και το οργανόγραμμα της οποίας παρουσιάζεται αναλυτικά παρακάτω.

Το δεύτερο οργανόγραμμα αποτελεί συνέχεια του πρώτου, εφόσον δείχνει αναλυτικά τις Διευθύνσεις που υπάγονται στην Υπηρεσία Ελέγχου Περιοχής. Από αυτές τις Διευθύνσεις στην παρούσα εργασία μας ενδιαφέρει η Διεύθυνση Αεροναυτικών Εκδόσεων και τα Τμήματα αυτής.



ΟΡΓΑΝΟΓΡΑΜΜΑ ΥΠΑ


ΔΙΟΙΚΗΤΗΣ
ΓΡ. ΔΙΟΙΚΗΤΗ
ΓΡ. ΥΠΟΔΙΟΙΚΗΤΗ
ΥΠΟΔΙΟΙΚΗΤΗΣ
ΥΠΟΔΙΟΙΚΗΤΗΣ
ΥΠΟΔΙΟΙΚΗΤΗΣ
ΠΕΡΙΦΕΡΕΙΑΚΕΣ ΥΠΗΡΕΣΙΕΣ
ΥΠΗΡΕΣΙΑ ΕΛΕΓΧΟΥ ΠΕΡΙΟΧΗΣ
Κ Ε Π Α Θ
Δ.ΑΕΡΟΝΑΥΤΙΚΩΝ ΕΚΔΟΣΕΩΝ
Δ. ΑΥΤΟΜΑΤΙΣΜΟΥ ΕΝΑΕΡΙΑΣ ΚΥΚΛ/ΡΙΑΣ
Δ. ΑΕΡΟΝΑΥΤΙΚΩΝ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ
Δ. ΗΛΕΚΤΡΟΝΙΚΩΝ
Τ. ΓΡΑΜΜΑΤΕΙΑΣ & ΜΕΡΙΜΝΑΣ
Τ. ΣΥΜΒΑΤΙΚΟΥ ΕΛΕΓΧΟΥ ΠΤΗΣΕΩΝ ΜΕ ΟΡΓΑΝΑ IFR
Τ. ΕΛΕΓΧΟΥ RADAR ΔΙΑΔΡΟΜΗΣ
Τ. ΠΛΗΡΟΦΟΡΙΩΝ ΠΤΗΣΗΣ
Τ. ΣΥΝΤΟΝΙΣΜΟΥ & ΛΕΙΤΟΥΡΓΙΑΣ ΚΕΠΑΘ
Τ. ΔΙΕΡΕΥΝΗΣΕΩΝ & ΕΞΕΙΔΙΚΕΥΣΗΣ
Τ. ΔΙΕΥΘΕΤΗΣΗΣ ΡΟΗΣ ΕΝΑΕΡΙΑΣ ΚΥΚΛ/ΡΙΑΣ
Τ.ΕΓΧΕΙΡΙΔΙΩΝ ΑΕΡΟΝΑΥΤΙΚΩΝ ΠΛΗΡΟΦΟΡΙΩΝ
Τ.ΑΕΡΟΝΑΥΤΙΚΩΝ ΑΓΓΕΛΙΩΝ
Τ.ΑΕΡΟΝΑΥΤΙΚΩΝ ΧΑΡΤΩΝ
Τ.ΔΕΛΤΙΩΝ ΔΙΑΔΡΟΜΗΣ
Τ. ΜΕΛΕΤΩΝ & ΑΝΑΛΥΣΗΣ
Τ. ΠΡΟΓΡΑΜΜΑΤΙΣΜΟΥ
Τ. ΕΚΜΕΤΑΛΛΕΥΣΗΣ ΗΛΕΚΤΡΟΝ. ΥΛΙΚΟΥ
Τ. ΣΤΑΘΕΡΩΝ ΑΕΡΟ - ΝΑΥΤΙΚΩΝ ΔΙΚΤΥΩΝ
Τ. ΚΙΝΗΤΩΝ ΑΕΡ/ΚΩΝ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ
Τ. ΚΟΣΤΟΛΟΓΗΣΗΣ ΤΗΛΕΓΡΑΦΗΜΑΤΩΝ
Τ. ΔΙΕΡΕΥΝΗΣΗΣ & ΕΞΕΙΔΙΚΕΥΣΗΣ
Τ. ΤΗΛΕΠ/ΚΩΝ & ΕΙΔ. ΜΕΣΩΝ & ΕΔΡΩΝ ΧΕΙΡΙΣΜΟΥ Ε.Κ.
Τ. ΤΗΛΕΤΥΠΙΚΟΥ ΚΕΝΤΡΟΥ
Τ. ΡΑΔ/ΤΩΝ ΤΗΛ/ΚΩΝ ΣΤΑΘΜΩΝ & ΕΠΟΠΤΕΙΑΣ ΤΟΥ ΟΛΟΥ ΣΥΣΤΗΜΑΤΟΣ
Τ. RADAR
Τ. ΜΕΣΩΝ ΑΥΤΟΜ/ΣΜΟΥ ΣΥΣΤΗΜΑΤΟΣ ΕΕΚ
Τ. ΜΕΛΕΤΩΝ ΑΥΤ/ΣΜΟΥ & ΠΡΟΓΡΑΜΜΑΤΙΣΜΟΥ Η/Υ

Στο οργανόγραμμα εμφανίζονται με έντονο κίτρινο χρώμα οι Διευθύνσεις αλλά και τα Τμήματα της ΥΠΑ που είναι υπεύθυνα για την παροχή της εν λόγω Υπηρεσίας Παροχής Αεροναυτικών Πληροφοριών-AIS. Πιο συγκεκριμένα υπεύθυνες ορίζονται οι παρακάτω Διευθύνσεις :

1. Διευθύνσεις της Κεντρικής Διοίκησης υπεύθυνες μεταξύ άλλων και για τη συλλογή Αεροναυτικών Πληροφοριών AIS καθώς και τα αντίστοιχα αρμόδια Τμήματά τους :

ΔΙΕΥΘΥΝΣΗ	ΑΡΜΟΔΙΟ ΤΜΗΜΑ
Δ/νση Αερολιμένων (Δ3)	Τμήμα Αεροδρομίων & Ελικοδρομίων
Δ/νση Εναέριας Κυκλοφορίας (Δ4)	Τμήμα Διαδικασιών
Δ/νση Τηλεπικοινωνιών (Δ5)	Τμήμα Διαχείρισης Φάσματος Συχνοτήτων
Δ/νση Ηλ.Συστημάτων Αεροναυτιλίας (Δ6)	Τμήμα Επικοινωνιών & Ραδιοβοηθημάτων

Η Διεύθυνση Αερολιμένων (Δ3) χρησιμοποιεί ειδικές πληροφορίες τις οποίες λαμβάνει από :

- Διεύθυνση Τεχνικών Υπηρεσιών (Δ7)
- Διεύθυνση Η/Μ Εγκαταστάσεων (Δ8)
- ΕΜΥ (Εθνική Μετεωρολογική Υπηρεσία)

2. Διεύθυνση Αεροναυτικών Εκδόσεων (Ε1) που υπάγεται στην Υπηρεσία Ελέγχου Περιοχής (ΥΕΠ), η οποία με τη σειρά της ανήκει στις Περιφερειακές Υπηρεσίες της Κεντρικής Διοίκησης. Η Διεύθυνση Αεροναυτικών Εκδόσεων AIP περιλαμβάνει τα εξής Τμήματα:

   - Τμήμα Εγχειριδίων Αεροναυτικών Πληροφοριών-AIP (Ε1/Α)
   - Τμήμα Αεροναυτικών Αγγελιών-NOTAM (Ε1/Β)
   - Τμήμα Αεροναυτικών Χαρτών-CHARTS (Ε1/Γ)
   - Τμήμα Δελτίων Διαδρομής προ-πτήσεως-PIB (Ε1/Δ)

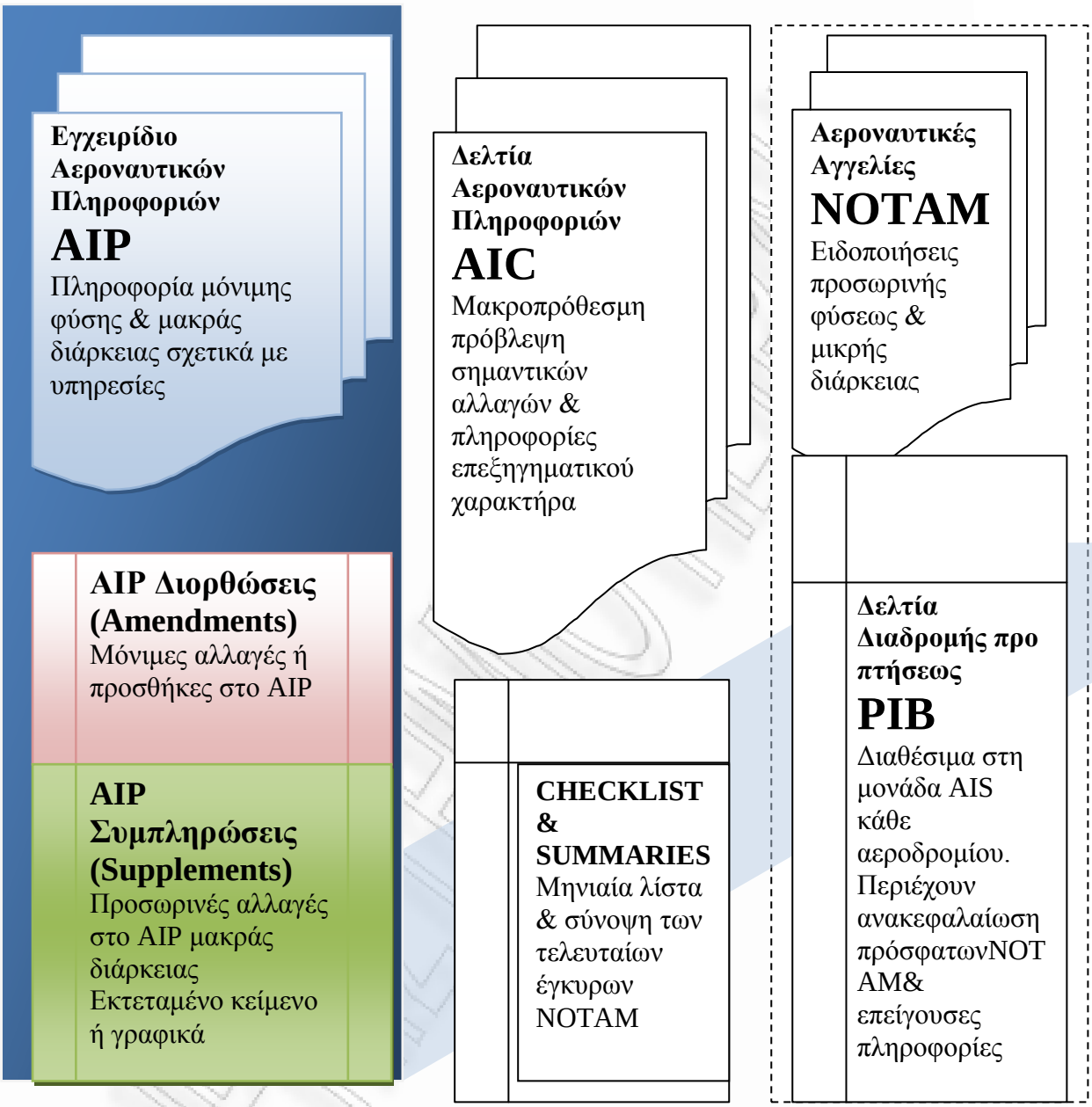
3. Μονάδες AIS εγκατεστημένες σε κάθε αεροδρόμιο

4. Το Τυπογραφείο, το οποίο υπάγεται στη Διεύθυνση Διοικητικού (Δ9)

5. Το Λογιστικό & Εφοδιαστικό Κέντρο (ΛΕΚ) που ανήκει στις Διοικητικές Υπηρεσίες

4.4. Ολοκληρωμένο Πακέτο Αεροναυτικών Πληροφοριών - IAIP (Integrated Aeronautical Information Package)

Η Διεύθυνση Αεροναυτικών Εκδόσεων με βάση την παραπάνω οργανωτική δομή παρέχει το σύνολο αυτών των πληροφοριών με τη μορφή ενός ολοκληρωμένου πακέτου αεροναυτικών πληροφοριών-IAIP (Integrated Aeronautical Information Package) το οποίο εκδίδεται σε έντυπη και ηλεκτρονική μορφή και ανταλλάσσεται μεταξύ των κρατών. Το *Πακέτο* αυτό περιλαμβάνει τα εξής :



Σχήμα 4.3 | **Πηγή** : Διεθνής Σύμβαση Διεθνούς Οργανισμού Πολιτικής Αεροπορίας ICAO (International Civil Aviation Organization), Παράρτημα 15 (Annex 15)

Στην παρούσα εργασία θα μελετηθεί το κατά πόσο η διαδικασία έκδοσης του AIP και η ενημέρωση αυτού με Διορθώσεις (Amendments) και Συμπληρώσεις (Supplements) πληροί τις απαιτήσεις του προτύπου ασφάλειας πληροφοριών ISO/IEC 27001.

4.5. Εγχειρίδιο Αεροναυτικών Πληροφοριών - AIP (Aeronautical Information Publication)

Το Εγχειρίδιο Αεροναυτικών Πληροφοριών AIP είναι το βασικό έγγραφο αεροναυτιλίας, ο προορισμός του οποίου είναι κυρίως να ικανοποιήσει τις διεθνείς προδιαγραφές για την ανταλλαγή μόνιμων αεροναυτικών πληροφοριών και μακράς διάρκειας προσωρινών αλλαγών που είναι σημαντικές για την αεροναυτιλία.

Το ελληνικό AIP δημοσιεύεται σε δύο ξεχωριστούς τόμους σε μια χαλαρή μορφή βιβλιοδεσίας (ντοσιέ) ώστε να ενημερώνεται εύκολα, με κείμενο στην αγγλική γλώσσα.

Α) ΤΟΜΟΣ Ι

- GEN (General)- Γενικά
- AGA (Aerodromes and obstruction charts)-Αεροδρόμια & χάρτες εμποδίων
- COM (Communication)-Επικοινωνία
- MET (Meteorology)-Μετεωρολογία
- RAC (Air Traffic Rules & Services)-Κανόνες Εναέριας Κυκλοφορίας & Υπηρεσίες
- FAL (Facilitation)-Εγκαταστάσεις
- SAR (Search & Rescue)-Έρευνα & Διάσωση

Β) ΤΟΜΟΣ ΙΙ-ΧΑΡΤΕΣ

- Γενικές Πληροφορίες σχετικά με Χάρτες & Διαγράμματα
- Χάρτες με Πρότυπες Διαδικασίες Αναχωρήσεις με όργανα (Standard Departure Chart-Instrument -SID)
- Χάρτες με Πρότυπες Διαδικασίες Άφιξης με όργανα (Standard Arrival Chart-Instrument (STAR)
- Χάρτες προσέγγισης με όργανα (Instrument Approach Chart-ICAO)
- Χάρτες τερματικής περιοχής με εξ όψεως διαδρόμους (Terminal Area Charts with VFR Routes)

Όλες οι εκδόσεις του AIP μπορούν να αποκτηθούν από τους συνδρομητές από τη Διεύθυνση Αεροναυτικών Εκδόσεων (Ε1). Οι συνδρομητές είναι ιδιώτες πιλότοι, αεροπορικές εταιρείες, πολεμική αεροπορία, Υπηρεσία έρευνας και διάσωσης και οι πάροχοι αεροναυτιλίας των κρατών (ANSPs-Air Navigation Services Providers).

4.6. Βασική Διεργασία (Process)

4.6.1. Γενικά

Ως Διεργασία ορίζεται το σύνολο αλληλένδετων δραστηριοτήτων, με αλληλεπιδράσεις που μετασχηματίζουν εισερχόμενα σε αποτελέσματα(Λαγοδήμος,2007).

4.6.2. Βασική Διεργασία Έκδοσης & Ενημέρωσης Εγχειριδίου Αεροναυτικών Πληροφοριών–AIP

Το «Εγχειρίδιο Αεροναυτικών Πληροφοριών-AIP» εκδίδεται και ενημερώνεται μέσω της υλοποίησης μιας προκαθορισμένης και τυποποιημένης αλληλουχίας ενεργειών, η οποία μετατρέπει την εισερχόμενη αεροναυτική πληροφορία, μόνιμης φύσης ή προσωρινής αλλαγής, σε εξερχόμενο Εγχειρίδιο. Αυτός είναι και ο λόγος που θα την ορίσουμε ως τη βασική διεργασία έκδοσης και ενημέρωσης του Εγχειριδίου.

Η εν λόγω βασική διεργασία αποτελείται από τις εξής τρείς αλληλένδετες δραστηριότητες :

- τη συλλογή
- την επεξεργασία και
- την έκδοση/διανομή

Οι ενέργειες που απαιτούνται για την υλοποίηση αυτών των δραστηριοτήτων τυποποιούνται στις εξής τρείς αντίστοιχες διαδικασίες (θα αναλυθούν στη συνέχεια) :

- Διαδικασία 1-Συλλογή & καταγραφή αεροναυτικών πληροφοριών
- Διαδικασία 2-Επεξεργασία αεροναυτικών πληροφοριών
- Διαδικασία 3-Έκδοση & διανομή «Εγχειριδίου Αεροναυτικών Πληροφοριών-AIP»

Το εξερχόμενο κάθε μιας δραστηριότητας αποτελεί το εισερχόμενο της αμέσως επόμενης με τελικό αποτέλεσμα της διεργασίας το «Εγχειρίδιο».

Η διεργασία παρουσιάζεται στο παρακάτω σχήμα.

ΒΑΣΙΚΗ ΔΙΕΡΓΑΣΙΑ ΕΚΔΟΣΗΣ & ΕΝΗΜΕΡΩΣΗΣ
Εγχειριδίου Αεροναυτικών Πληροφοριών-AIP

Αεροναυτικές Πληροφορίες

Τυποποιημένα Ενδιάμεσα Έγγραφα

Τυποποιημένα Τελικά Έγγραφα (σε μορφή pdf αρχείου)

Εγχειρίδιο AIP

ΣΥΛΛΟΓΗ & ΚΑΤΑΓΡΑΦΗ → **ΕΠΕΞΕΡΓΑΣΙΑ** → **ΕΚΔΟΣΗ & ΔΙΑΝΟΜΗ**

Εμπλεκόμενοι:
-Δ/νση Αερολιμένων (Δ3)
-Τμήμα Αεροδρομίων & Ελικοδρομίων
-Δ/νση Εναέριας Κυκλοφορίας (Δ4)
-Τμήμα Διαδικασιών Εναέριας Κυκλοφορίας
-Δ/νση Τηλεπικοινωνιών (Δ5)
-Τμήμα Διαχείρισης Φάσματος Συχνοτήτων
-Δ/νση Ηλ.Συστημάτων Αεροναυτιλίας (Δ6)
-Τμήμα Επικοινωνιών & Ραδιοβοηθημάτων
-Γενικός Διευθυντής Αεροναυτιλίας
-Κεντρική Γραμματεία

Εμπλεκόμενοι:
-Δ/νση Αεροναυτικών Εκδόσεων (Ε1)
-Τμήμα Εγχειριδίων Αεροναυτικών Πληροφοριών AIP (Ε1/Α)
-Τμήμα Αεροναυτικών Αγγελιών NOTAM (Ε1/Β)

Εμπλεκόμενοι:
-Τμήμα Εγχειριδίων Αεροναυτικών Πληροφοριών (AIP)
-Λογιστικό & Εφοδιαστικό Κέντρο (ΛΕΚ)
-Τυπογραφείο ΥΠΑ
-Συνδρομητές

ΟΡΟΛΟΓΙΑ ΣΧΗΜΑΤΩΝ :

Εισροή/Εκροή | **Διαδικασία** | **Εμπλεκόμενοι Διαδικασίας** | **Πολλαπλά Έγγραφα**

4.6.3. Ανάλυση Βασικής Διεργασίας

Οι Διευθύνσεις της Κεντρικής Διοίκησης σε συνεργασία με τα αντίστοιχα αρμόδια Τμήματά τους όπως αναφέρονται παρακάτω :

ΔΙΕΥΘΥΝΣΗ	ΑΡΜΟΔΙΟ ΤΜΗΜΑ
Δ/νση Αερολιμένων (Δ3)	Τμήμα Αεροδρομίων & Ελικοδρομίων
Δ/νση Εναέριας Κυκλοφορίας (Δ4)	Τμήμα Διαδικασιών
Δ/νση Τηλεπικοινωνιών (Δ5)	Τμήμα Διαχείρισης Φάσματος Συχνοτήτων
Δ/νση Ηλ.Συστημάτων Αεροναυτιλίας (Δ6)	Τμήμα Επικοινωνιών & Ραδιοβοηθημάτων

συλλέγουν τις αεροναυτικές πληροφορίες, χρησιμοποιώντας και επιπρόσθετες πληροφορίες τις οποίες λαμβάνουν από δυο άλλες Διευθύνσεις :

- Δ/νση Τεχνικών Υπηρεσιών (Δ7)
- Δ/νση Η/Μ Εγκαταστάσεων (Δ8)

οι οποίες επίσης υπάγονται στην Κεντρική Διοίκηση καθώς επίσης και από την Εθνική Μετεωρολογική Υπηρεσία (ΕΜΥ).

Οι Διευθύνσεις (Δ3,Δ4,Δ5,Δ6) εφόσον συλλέξουν τις πληροφορίες και τις καταγράψουν με μια τυποποιημένη δομή, τις διαβιβάζουν με τη μορφή «Ενδιάμεσων Εγγράφων Αεροναυτικών Πληροφοριών» στη Διεύθυνση Αεροναυτικών Εκδόσεων (Ε1), όπου το αρμόδιο τμήμα της Τμήμα Εγχειριδίων Αεροναυτικών Πληροφοριών AIP (Ε1/Α) αναλαμβάνει την επεξεργασία τους ώστε να εγκριθούν ως «Τελικά Έγγραφα Αεροναυτικών Πληροφοριών» και να δοθεί εντολή για την επίσημη έκδοση και διανομή τους ως «Εγχειρίδιο Αεροναυτικών Πληροφοριών AIP» στους τελικούς χρήστες.

Οι τελικοί χρήστες του Εγχειριδίου Αεροναυτικών Πληροφοριών AIP είναι αρχικά τα Αεροδρόμια τα οποία έχουν την ευθύνη και την υποχρέωση να διατηρούν στις Μονάδες AIS τους ενημερωμένα Εγχειρίδια Αεροναυτικών Πληροφοριών.

Άλλοι χρήστες είναι οι διάφοροι συνδρομητές που προμηθεύονται το Εγχειρίδιο, οι οποίοι είναι ιδιώτες πιλότοι, αεροπορικές εταιρείες, η Πολεμική αεροπορία, η Υπηρεσία έρευνας και διάσωσης και οι πάροχοι αεροναυτιλίας των Κρατών (Υπηρεσία Πολιτικής Αεροπορίας-ΥΠΑ του κάθε Κράτους).

4.6.4. Στοιχεία της Διεργασίας

Στη διεργασία έκδοσης και διανομής του «Εγχειριδίου Αεροναυτικών Πληροφοριών– AIP» είναι απαραίτητο να υπάρχουν τυποποιημένες διαδικασίες και επαρκείς πόροι.

Όσον αφορά τους επαρκείς πόρους, το υψηλά εξειδικευμένο και ικανό προσωπικό, οι κατάλληλες υποδομές, ο απαραίτητος εξοπλισμός αποτελούν τις προϋποθέσεις για την ταχεία παροχή ακριβή αεροναυτικών πληροφοριών.

Οπότε διακρίνουμε τρείς άξονες της βασικής διεργασίας :

1. Ανθρώπινοι Πόροι
2. Υποδομές/ Εξοπλισμός
3. Διαδικασίες

1) Ανθρώπινοι Πόροι

Α) Προσωπικό

Ένας γενικός οδηγός όσον αφορά τις ελάχιστες απαιτήσεις για προσωπικό δίνεται στον ακόλουθο πίνακα :

ΜΟΝΑΔΑ	ΑΡΙΘΜΟΣ ΥΠΑΛΛΗΛΩΝ
Διευθύνσεις (Δ3,Δ4,Δ5,Δ6)	
Μεγάλες	5-10
Μικρές	3-6
Διεύθυνση Εκδόσεων (Ε1)	
Μεγάλη	3-6
Μικρή	1-2
Τμήμα AIP (Ε1/Α)(24 ώρες)	
Μεγάλα	3
Μικρά	1
Τυπογραφείο	
Μεγάλο	3
Μικρό	1
Λογιστικό & Εφοδιαστικό Κέντρο (ΛΕΚ)	
Μεγάλο	3
Μικρό	1
Μονάδες AIS	
Μεγάλο Αεροδρόμιο	5-6
Μικρό Αεροδρόμιο	2+

Β) Εκπαίδευση

Έχει τεθεί μία κοινή βάση για το βάθος και το εύρος των γνώσεων, των δεξιοτήτων και τη συμπεριφορά που πρέπει να τηρείται από όλους τους υπαλλήλους που εμπλέκονται στη διεργασία έκδοσης και ενημέρωσης του Εγχειριδίου.

Το Έγγραφο 7192, Μέρος 3 «Εγχειρίδιο Κατάρτισης», περιλαμβάνει αναλυτικό πρόγραμμα κατάρτισης και παρέχει οδηγίες στα Κράτη για την προετοιμασία των αντίστοιχων προγραμμάτων σπουδών που θα χρησιμοποιηθούν σε μαθήματα για την κατάρτιση των υπαλλήλων.

2) Υποδομές/Εξοπλισμός

Α) Υποδομές

Ένας γενικός οδηγός όσον αφορά τις ελάχιστες απαιτήσεις για εγκαταστάσεις δίνεται στον ακόλουθο πίνακα :

ΜΟΝΑΔΑ	ΥΠΟΔΟΜΕΣ σε τ.μ
Διευθύνσεις (Δ3,Δ4,Δ5,Δ6)	
Μεγάλες	28-93+
Μικρές	14
Διεύθυνση Εκδόσεων (Ε1)	
Μεγάλη	28-93+
Μικρή	14
Τμήμα AIP (Ε1/Α)(24 ώρες)	
Μεγάλα	28-37
Μικρά	14
Τυπογραφείο	
Μεγάλο	25
Μικρό	14
Λογιστικό & Εφοδιαστικό Κέντρο	

(ΛΕΚ)	
Μεγάλο	28-37
Μικρό	14
Μονάδες AIS	
Μεγάλο Αεροδρόμιο	28+
Μικρό Αεροδρόμιο	14

Β) Εξοπλισμός

Εκτός από το βασικό εξοπλισμό γραφείου και τις γραφικές πρώτες ύλες, πρέπει να παρέχεται στους εμπλεκομένους της βασικής διεργασίας ο ακόλουθος εξοπλισμός :

- Προσωπικοί ηλεκτρονικοί υπολογιστές σε κάθε θέση (τερματικό πελάτης-Client)
- Εκτυπωτές
- Σύνδεση στο διαδίκτυο
- Τηλέφωνα
- Φωτοτυπικό μηχάνημα ειδικό και για έγγραφα Εγχειριδίου Αεροναυτικών Πληροφοριών-AIP
- Ηλεκτρονικός σαρωτής (scanner)
- Τηλεαντιγραφικό μηχάνημα (telefax)
- Αξιόπιστο Ρολόι που να δείχνει την τοπική ώρα
- Ρολόι « time-stamp», σε ώρα Γκρίνουιτς και σε τοπική ώρα

Γ) Χρήση Αυτοματοποίησης

Η χρήση της αυτοματοποίησης στη διεργασία AIP έχει εισαχθεί με την πρόθεση να παρέχεται μια πιο αποτελεσματική και ποιοτική υπηρεσία στους συνδρομητές του Εγχειριδίου.

Σήμερα, χρησιμοποιείται μία ηλεκτρονική εφαρμογή, το **eAIP.wiz@rd**, στην οποία θα αναφερθούμε αναλυτικά στη συνέχεια της εργασίας.

Το **eAIP.wiz@rd**κατασκευάστηκε προκειμένου :

- να βοηθήσει στην αυτοματοποίηση των απαιτήσεων της Διεθνούς Συμβάσεως του Διεθνούς Οργανισμού Πολιτικής Αεροπορίας ICAO (International Civil Aviation

Organization) όπως αυτές περιγράφονται στο Παράρτημα 15 (Annex 15) του ICAO

- να υποστηρίξει τον χρήστη καθ'όλη τη ροή της διεργασίας συλλογής, επεξεργασίας και έκδοσης των αεροναυτικών πληροφοριών ως «Εγχειρίδιο Αεροναυτικών Πληροφοριών-AIP»
- να συνεισφέρει στη δημιουργία βάσεων δεδομένων για τη διαχείριση αυτών των πληροφοριών
- να αποφευχθεί η διπλή καταχώρηση της ίδιας πληροφορίας
- να δημιουργήσει τις προϋποθέσεις προκειμένου να διευκολύνει τη χρήση του Εγχειριδίου κατά τη διάρκεια της πτήσης

Η εφαρμογή **eAIP.wiz@rd** για να λειτουργήσει χρειάζεται τα ακόλουθα :

ΜΗΧΑΝΗΜΑ	**Ελάχιστες απαιτήσεις για τεχνικά χαρακτηριστικά του μηχανήματος (hardware)**	**Ελάχιστες απαιτήσεις για λογισμικό (software)**
Διακομιστή Βάσεων Δεδομένων (Data base Server)	Σχεσιακή Βάση Δεδομένων SQL με δυνατότητες πολλών χρηστών (multiuser) και διαδικτυακές δυνατότητες (networking)	Πρόγραμμα Βάσης Δεδομένων: Oracle 9.0.1 ή Oracle 8.1.7
Διακομιστή Εφαρμογής (ApplicationServer)	▪ Multitasking (πολλών εργασιών) ▪ Multiuser (πολλών χρηστών) ▪ Multithreads (πολυνημματικό)	Λειτουργικά συστήματα : ▪ HP-UX11.x. ή ▪ Sun Solaris 8 ή ▪ Windows NT
Τερματικό πελάτης (Client)	▪ Κεντρική μονάδα επεξεργασίας (CPU) PentiumIII ▪ Χωρητικότητα μνήμης RAM 128 MB ▪ Διαθέσιμος χώρος στο σκληρό δίσκο 400 MB	Λειτουργικά συστήματα : ▪ Windows NT ή Windows 2000 ▪ Adobe Frame Maker 7.0 ▪ Adobe Acrobat 5.0 + ▪ Adobe Distiller 5.0 +

4.7. Βασικές Διαδικασίες Λειτουργίας (Procedures)

4.7.1. Γενικά

Οι Διαδικασίες γενικότερα τυποποιούν τις ενέργειες που απαιτούνται για την υλοποίηση των δραστηριοτήτων ενός οργανισμού ή μιας επιχείρησης.

Το σύνολο των διαδικασιών λειτουργίας πρέπει να απεικονίζει την υλοποίηση της σχετικής διεργασίας. Συγκεκριμένα οι διαδικασίες καθορίζουν τον τρόπο με τον οποίο υλοποιούνται οι διεργασίες, με βάση τις δεδομένες οργανωτικές δομές.

Οι Διαδικασίες εμπεριέχουν τεχνογνωσία του οργανισμού ή της επιχείρησης, στην προκειμένη περίπτωση της Υπηρεσίας Πολιτικής Αεροπορίας, γεγονός που τις καθιστά έγγραφα περιορισμένης κυκλοφορίας και κατά συνέπεια έχουν αυστηρά καθορισμένους παραλήπτες.

Η μορφή των Διαδικασιών είναι τυποποιημένη και εμπεριέχει τα ακόλουθα στοιχεία :

- Σκοπός: Σύντομη περιγραφή του αντικειμένου που καλύπτει η Διαδικασία.
- Πεδίο Εφαρμογής: Δ/σεις, Τμήματα & θέσεις εργασίας που αφορά η Διαδικασία.
- Εμπλεκόμενοι: Οι διοικητικές θέσεις που εμπλέκονται άμεσα στην υλοποίηση της Διαδικασίας.
- Περιγραφή Διαδικασίας: Περιγραφή όλων των ενεργειών που σχετίζονται με την υλοποίηση της Διαδικασίας, με τη σειρά που εκτελούνται.
- Έντυπα: Κατάλογος με όλα τα σχετικά έντυπα που χρησιμοποιούνται.
- Εξειδικευμένες Οδηγίες: Παρέχουν όλες τις λεπτομέρειες εκτέλεσης επιμέρους ενεργειών μιας διαδικασίας.

Πλην των ανωτέρω, συνηθίζεται να επισυνάπτεται και ένα διάγραμμα ροής (flow-chart) ή μια συνοπτική περιγραφή της ροής ενεργειών (βήματα) της διαδικασίας. Κάθε Διαδικασία είναι αριθμημένη με αύξοντα αριθμό αρίθμησης (Λαγοδήμος, 2007).

4.7.2. Υποδιεργασίες της βασικής διεργασίας «Έκδοσης & Ενημέρωσης Εγχειριδίου AIP»

ΥΠΟΔΙΕΡΓΑΣΙΑ 1

ΣΥΛΛΟΓΗ & ΚΑΤΑΓΡΑΦΗ ΤΩΝ ΑΕΡΟΝΑΥΤΙΚΩΝ ΠΛΗΡΟΦΟΡΙΩΝ

Σκοπός :

Να γίνει η συλλογή και η καταγραφή των αεροναυτικών πληροφοριών, είτε αυτές είναι πρωταρχικές πληροφορίες είτε πληροφορίες αλλαγής, που αφορούν:

- Αεροδρόμια και Ελικοδρόμια.
- Γενικούς Κανονισμούς & Διαδικασίες, Αεροδιαδρόμους, Ραδιοβοηθήματα, Προειδοποιήσεις.
- Εθνικούς Κανονισμούς & Απαιτήσεις, Πίνακες & κωδικούς, Υπηρεσίες, Χρεώσεις για Αεροδρόμια/Ελικοδρόμια & για παροχή αεροναυτικών πληροφοριών.

Με τελικό σκοπό τη δημιουργία των αντίστοιχων σε κάθε κατηγορία ενδιάμεσων εγγράφων προκειμένου να προωθηθούν προς περαιτέρω ειδική επεξεργασία.

Πεδίο Εφαρμογής :

Η υποδιεργασία συλλογής και καταγραφής των αεροναυτικών πληροφοριών αφορά :

Α) Τη Γενική Δ/ση Αερομεταφορών και ειδικότερα τις παρακάτω διευθύνσεις της :
-Διεύθυνση Αερολιμένων(Δ3)
-Διεύθυνση Τεχνικών Υπηρεσιών (Δ7)
-Διεύθυνση Η/Μ Εγκαταστάσεων (Δ8)

Β) Τη Γενική Δ/ση Αεροναυτιλίας και ειδικότερα τις εξής διευθύνσεις της :
-Διεύθυνση Εναέριας Κυκλοφορίας (Δ4)
-Διεύθυνση Τηλεπικοινωνιών (Δ5)
-Διεύθυνση Ηλ.Συστημάτων Αεροναυτιλίας (Δ6)

Γ) Τις Περιφερειακές Υπηρεσίες της ΥΠΑ και συγκεκριμένα :
-τα Αεροδρόμια (τα οποία διαθέτουν Μονάδες AIS)
-την Υπηρεσία Ελέγχου Περιοχής (ΥΕΠ) , στην οποία εντάσσεται και η Δ/νση Αεροναυτικών Εκδόσεων (Ε1)

Εμπλεκόμενοι :

-Διεύθυνση Αερολιμένων (Δ3)/ Τμήμα Αεροδρομίων & Ελικοδρομίων

-Διεύθυνση Εναέριας Κυκλοφορίας (Δ4)/ Τμήμα Διαδικασιών Εναέριας Κυκλοφορίας
-Διεύθυνση Τηλεπικοινωνιών (Δ5)/ Τμήμα Διαχείρισης Φάσματος Συχνοτήτων
-Διεύθυνση Ηλ.Συστημάτων Αεροναυτιλίας (Δ6)/ Τμήμα Επικοινωνιών και Ραδιοβοηθημάτων
-Γενικός Διευθυντής Αεροναυτιλίας
-Κεντρική Γραμματεία

Περιγραφή Διαδικασίας :

Προκειμένου να συγκεντρωθούν οι πρωταρχικές αεροναυτικές πληροφορίες ή πληροφορίες αλλαγών στις υπάρχουσες αεροναυτικές πληροφορίες που αφορούν τις εξής τρείς κατηγορίες:

- Αεροδρόμια και Ελικοδρόμια.
- Γενικούς Κανονισμούς & Διαδικασίες, Αεροδιαδρόμους, Δρομολόγια, Ραδιοβοηθήματα, Προειδοποιήσεις.
- Εθνικούς Κανονισμούς & Απαιτήσεις, Πίνακες & κωδικούς, Υπηρεσίες, Χρεώσεις για Αεροδρόμια/Ελικοδρόμια & για παροχή αεροναυτικών πληροφοριών.

ενεργοποιούνται οι κύριες αρμόδιες για τη κάθε μια κατηγορία αντίστοιχα διευθύνσεις, οι οποίες είναι οι ακόλουθες:

- Διεύθυνση Αερολιμένων (Δ3)
- Διεύθυνση Εναέριας Κυκλοφορίας (Δ4)
- Διεύθυνση Τηλεπικοινωνιών (Δ5) & Διεύθυνση Ηλ.Συστημάτων Αεροναυτιλίας (Δ6)

Τότε ο διευθυντής της κάθε μιας από τις παραπάνω διευθύνσεις μέσω ενός Υπηρεσιακού Σημειώματος «Ανάθεσης συγκέντρωσης ή αλλαγής πληροφοριών», ανάλογα την περίπτωση, καθιστά το αρμόδιο τμήμα της διεύθυνσης του υπεύθυνο για την πρωταρχική συλλογή των εξειδικευμένων αυτών πληροφοριών ή για την αλλαγή κάποιων ήδη υφιστάμενων πληροφοριών. Τα αρμόδια τμήματα που αντιστοιχούν στις εν λόγω διευθύνσεις είναι τα παρακάτω:

- Τμήμα Αεροδρομίων & Ελικοδρομίων
- Τμήμα Διαδικασιών Εναέριας Κυκλοφορίας
- Τμήμα Διαχείρισης Φάσματος Συχνοτήτων & Τμήμα Επικοινωνιών και Ραδιοβοηθημάτων

Οι πρωταρχικές πληροφορίες συλλέγονται και καταγράφονται σε μια τυποποιημένη φόρμα πολλών σελίδων, με δεδομένη μορφή, η οποία περιγράφεται αναλυτικά στην Εξειδικευμένη Οδηγία Ι και λέγεται «Υποδειγματικό Μοντέλο Παρουσίασης Αεροναυτικών Πληροφοριών-AICM (Aeronautical Information Conceptual Model)».Το μοντέλο αυτό περιέχει πληροφορίες που χωρίζονται σε τρείς ενότητες με τις εξής διεθνώς καθιερωμένες ονομασίες:

- «AD_HP» (πληροφορίες για αεροδρόμια & ελικοδρόμια)
- «ENR» (πληροφορίες για γενικούς κανονισμούς & διαδικασίες)

- «GEN» (πληροφορίες για εθνικούς κανονισμούς & απαιτήσεις)

Οι αλλαγές διαχωρίζονται σε κατηγορίες με βάση μια συγκεκριμένη διαδικασία που αναλύεται στην Εξειδικευμένη Οδηγία ΙΙ και ανάλογα με τον τύπο τους καταγράφονται στα αντίστοιχα ενδιάμεσα έντυπα αλλαγών με τις εξής διεθνώς καθιερωμένες ονομασίες :

- Ενδιάμεσο Έντυπο «Διόρθωση AIP»
- Ενδιάμεσο Έντυπο «Διόρθωση AIRACAIP»
- Ενδιάμεσο Έντυπο «Συμπλήρωση AIP»
- Ενδιάμεσο Έντυπο «Συμπλήρωση AIRACAIP»
- Ενδιάμεσο Έντυπο «Αεροναυτικής Αγγελίας NOTAM»

Τα νέα αυτά έγγραφα (η εννοιολογική σημασία των οποίων αναφέρεται στο ΠΑΡΑΡΤΗΜΑ Ι) εγκρίνονται αρχικά από τον προϊστάμενο του αρμόδιου τμήματος και έπειτα από τον διευθυντή της αντίστοιχης διεύθυνσης με μια απλή υπογραφή τους πάνω στο έγγραφο.

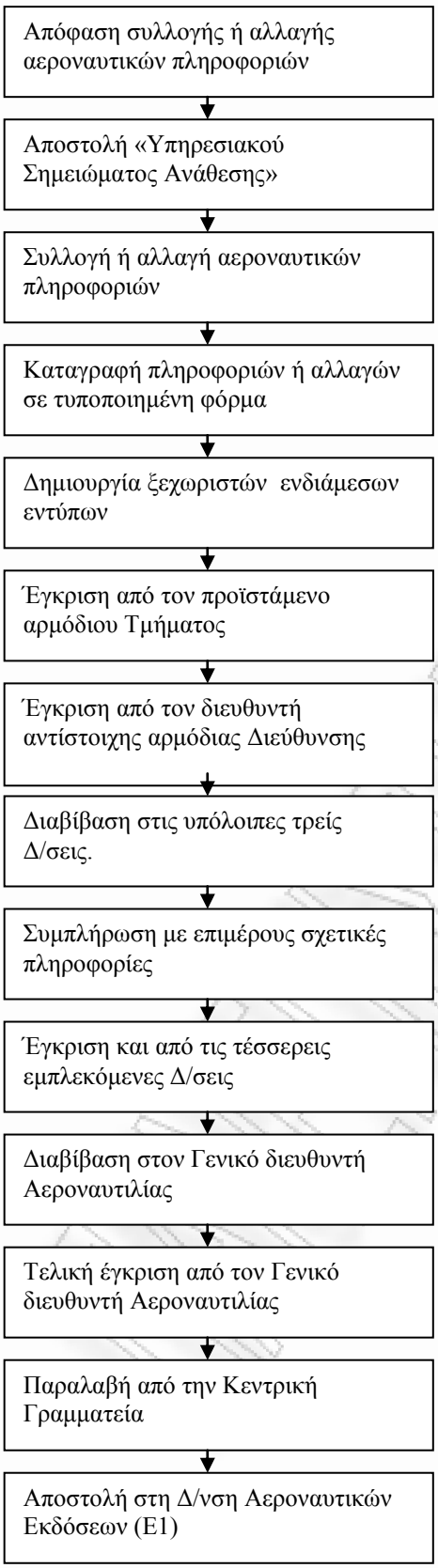
Εν συνεχεία, το καθένα από αυτά διαβιβάζεται από την κύρια αρμόδια διεύθυνση, η οποία αρχικά το εξέδωσε, διαδοχικά στις υπόλοιπες τρείς συναρμόδιες διευθύνσεις προκειμένου να συμπληρωθούν επιμέρους πληροφορίες και να τύχουν της έγκρισής τους, έτσι ώστε στο τέλος οι διευθυντές και των τεσσάρων διευθύνσεων να έχουν προσυπογράψει τα έγγραφα.

Τέλος, τα εν λόγω έγγραφα διαβιβάζονται στον Γενικό Διευθυντή Αεροναυτιλίας προς έγκριση. Ο Γενικός δίνει την τελική έγκριση με μια υπογραφή του σε καθένα από τα έγγραφα. Τα ενδιάμεσα αυτά έγγραφα τα παραλαμβάνει η Κεντρική Γραμματεία η οποία αναλαμβάνει την αποστολή τους στη Διεύθυνση Αεροναυτικών Εκδόσεων (Ε1) μέσω υπηρεσιακής αλληλογραφίας προκειμένου να υποβληθούν σε ειδική επεξεργασία.

Έντυπα : (ΠΑΡΑΡΤΗΜΑ ΙV)

-Υπηρεσιακό Σημείωμα «Ανάθεσης συγκέντρωσης ή αλλαγής πληροφοριών» (Δ.1.1)
-Ενδιάμεσο Έντυπο «Διόρθωση AIP» (Δ.1.2)
-Ενδιάμεσο Έντυπο «Διόρθωση AIRAC AIP» (Δ.1.3)
-Ενδιάμεσο Έντυπο «Συμπλήρωση AIP» (Δ.1.4)
-Ενδιάμεσο Έντυπο «Συμπλήρωση AIRAC AIP» (Δ.1.5)
-Ενδιάμεσο Έντυπο «Αεροναυτικής Αγγελίας NOTAM» (Δ.1.6)

ΔΙΑΓΡΑΜΜΑ ΡΟΗΣ ΥΠΟΔΙΕΡΓΑΣΙΑΣ 1:



ΥΠΟΔΙΕΡΓΑΣΙΑ 2
ΕΠΕΞΕΡΓΑΣΙΑ ΤΩΝ ΑΕΡΟΝΑΥΤΙΚΩΝ ΠΛΗΡΟΦΟΡΙΩΝ

Σκοπός :

Να γίνει η ειδική επεξεργασία των αεροναυτικών πληροφοριών που έχουν συλλεχθεί και καταγραφεί σε ενδιάμεσα έγγραφα. Αυτό αναλύεται στον έλεγχο της εγκυρότητας των πληροφοριών αυτών, είτε πρόκειται για πρωτογενείς πληροφορίες είτε για πληροφορίες αλλαγών που ενδεχομένως να προέκυψαν.

Με τελικό σκοπό τη δημιουργία των αντίστοιχων σε κάθε κατηγορία τελικών εγγράφων που θα αποτελούν το Εγχειρίδιο Αεροναυτικών Πληροφοριών AIP και την προώθησή τους για έκδοση και διανομή.

Πεδίο Εφαρμογής :

Η διαδικασία επεξεργασίας των αεροναυτικών πληροφοριών αφορά :

Α) Τη Γενική Δ/ση Αερομεταφορών και ειδικότερα τις παρακάτω διευθύνσεις της :
-Διεύθυνση Αερολιμένων(Δ3)
-Διεύθυνση Τεχνικών Υπηρεσιών (Δ7)
-Διεύθυνση Η/Μ Εγκαταστάσεων (Δ8)

Β) Τη Γενική Δ/ση Αεροναυτιλίας και ειδικότερα τις εξής διευθύνσεις της :
-Διεύθυνση Εναέριας Κυκλοφορίας (Δ4)
-Διεύθυνση Τηλεπικοινωνιών (Δ5)
-Διεύθυνση Ηλ.Συστημάτων Αεροναυτιλίας (Δ6)

Γ) Τις Περιφερειακές Υπηρεσίες της ΥΠΑ και συγκεκριμένα :
-τα Αεροδρόμια (τα οποία διαθέτουν Μονάδες AIS)
-την Υπηρεσία Ελέγχου Περιοχής (ΥΕΠ), στην οποία εντάσσεται και η Δ/ση Αεροναυτικών Εκδόσεων (Ε1) μαζί με τα Τμήματά της, Τμήμα Αεροναυτικών Πληροφοριών AIP (Ε1/Α), Τμήμα Αεροναυτικών Αγγελιών NOTAM (Ε1/Β)

Εμπλεκόμενοι :

-Δ/νση Αεροναυτικών Εκδόσεων (Ε1)
-Τμήμα Εγχειριδίων Αεροναυτικών Πληροφοριών AIP (Ε1/Α)
-Τμήμα Αεροναυτικών Αγγελιών NOTAM (Ε1/Β)

Περιγραφή Διαδικασίας :

Προκειμένου να επεξεργαστούν οι αρχικές αεροναυτικές πληροφορίες που έχουν συλλεχθεί ή να επεξεργαστούν οι πληροφορίες που αφορούν αλλαγές που ενδέχεται να προέκυψαν σε κάποιο ή και σε όλα τα παραπάνω έγγραφα, και οι οποίες αναγράφονται στα εξής ενδιάμεσα έγγραφα :

- «Διόρθωση AIP»
- «Διόρθωση AIRAC AIP»
- «Συμπλήρωση AIP»
- «Συμπλήρωση AIRAC AIP»
- «Αεροναυτικής Αγγελίας NOTAM»

ενεργοποιείται η κύρια αρμόδια για την επεξεργασία των αεροναυτικών πληροφοριών Διεύθυνση, η οποία είναι η ακόλουθη:

- Διεύθυνση Αεροναυτικών Εκδόσεων (Ε1)

Αρχικά, η Διεύθυνση Αεροναυτικών Εκδόσεων (Ε1) παραλαμβάνει τα ενδιάμεσα έγγραφα και έπειτα, είτε πρόκειται για πρωτογενή πληροφορία είτε για πληροφορία αλλαγής, ο διευθυντής της παραπάνω διεύθυνσης καθιστά το αρμόδιο Τμήμα Εγχειριδίων Αεροναυτικών Πληροφοριών AIP (Ε1/Α) της διεύθυνσης του, υπεύθυνο για τον έλεγχο της εγκυρότητας και ορθότητας των εξειδικευμένων αυτών πληροφοριών, μέσω συγκρίσεως τους με στοιχεία που έχει στη διάθεσή του σε ηλεκτρονικές βάσεις δεδομένων μέσω της ηλεκτρονικής εφαρμογής **eAIP.wiz@rd**. Η διαδικασία περιγράφεται αναλυτικά στην Εξειδικευμένη Οδηγία ΙΙΙ.

Στην περίπτωση που κάποια πληροφορία δεν είναι ορθή το αντίστοιχο έντυπο στο οποίο η λανθασμένη πληροφορία αναγράφεται αποστέλλεται πίσω στην αρμόδια διεύθυνση προς διόρθωση συνοδευόμενο με Υπηρεσιακό Σημείωμα «Λανθασμένης καταχώρησης πληροφορίας». Το διορθωμένο πια έντυπο εφόσον επιστρέψει στη Διεύθυνση (Ε1) επανελέγχεται από το Τμήμα Εγχειριδίων Αεροναυτικών Πληροφοριών AIP (Ε1/Α).

Εφόσον όλες οι πληροφορίες ελεγχθούν και είναι σωστές, τα προαναφερθέντα ενδιάμεσα έγγραφα εγκρίνονται ως τα τελικά έγγραφα, αρχικά από τον προϊστάμενο του Τμήματος Εγχειριδίων Αεροναυτικών Πληροφοριών AIP (Ε1/Α) και έπειτα από τον διευθυντή της Διεύθυνσης Αεροναυτικών Εκδόσεων (Ε1) με μια απλή υπογραφή τους πάνω στο κάθε έγγραφο.

Στο τέλος, ο διευθυντής της Διεύθυνσης (Ε1) διαχωρίζει τα τελικά αυτά έγγραφα πληροφοριών ανά κατηγορία. Τα έγγραφα που κατατάσσονται ως «Αεροναυτική Πληροφορία AIP» αποτελούν μέρος του Εγχειριδίου Αεροναυτικών Πληροφοριών AIP

και για αυτό η Διεύθυνση (Ε1) αναθέτει την επίσημη έκδοσή τους στο Τμήμα Εγχειριδίων Αεροναυτικών Πληροφοριών AIP (Ε1/Α).

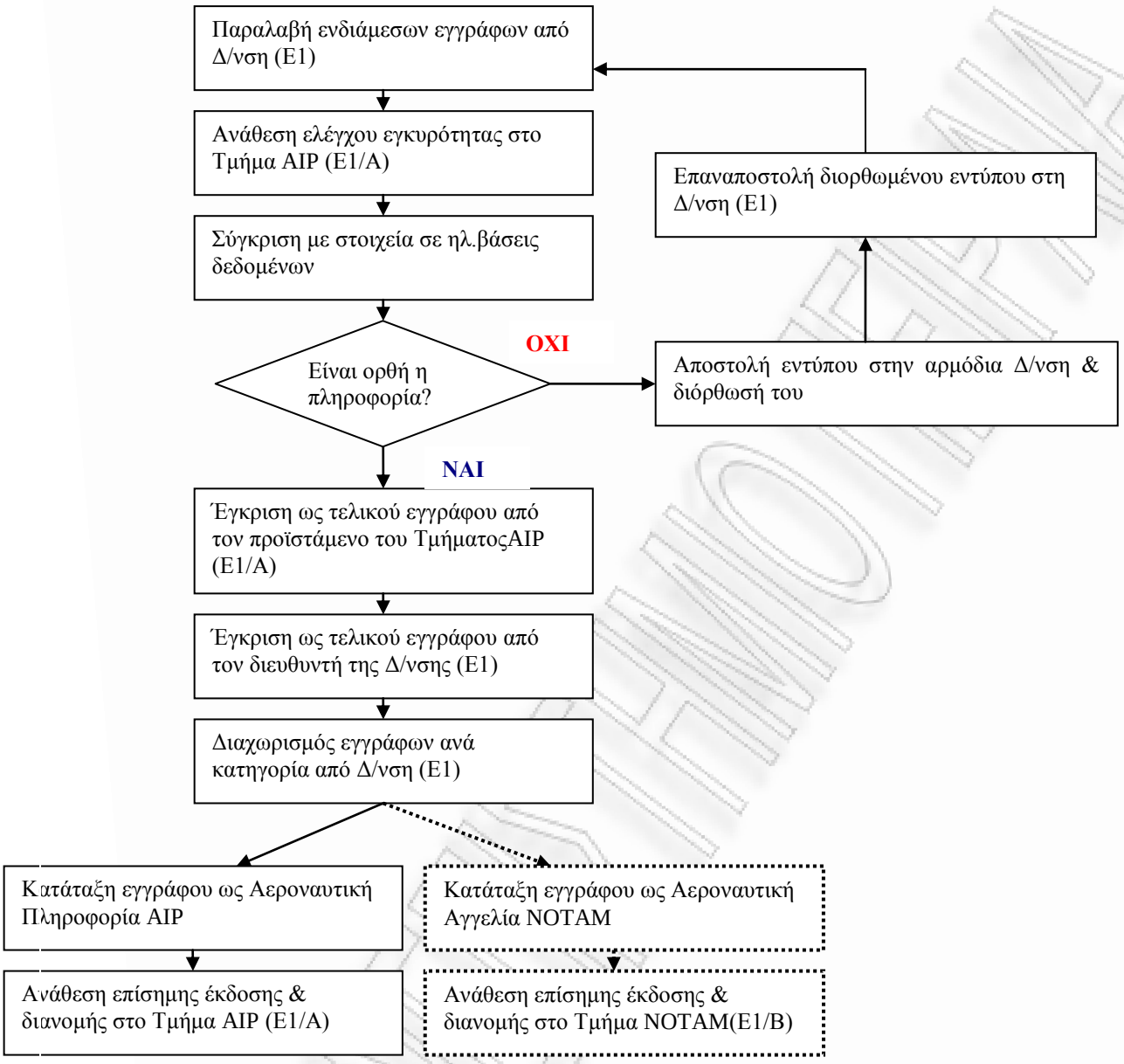
Τα έγγραφα που κατατάσσονται ως «Αεροναυτική Αγγελία NOTAM» δεν αποτελούν μέρος του Εγχειριδίου Αεροναυτικών Πληροφοριών AIP και η Διεύθυνση (Ε1) αναθέτει την επίσημη έκδοσή τους στο Τμήμα Αεροναυτικών Αγγελιών NOTAM (Ε1/Β).

Η εννοιολογική σημασία μιας «Αεροναυτικής Αγγελίας NOTAM» αναφέρεται αναλυτικά στο Παράρτημα. Επειδή όμως, όπως προαναφέρθηκε, οι «Αεροναυτικές Αγγελίες NOTAM» δεν αποτελούν μέρος του Εγχειριδίου Αεροναυτικών Πληροφοριών AIP δεν θα αναλυθούν περαιτέρω.

Έντυπα : (ΠΑΡΑΡΤΗΜΑ IV)

-Υπηρεσιακό Σημείωμα «Λανθασμένης καταχώρησης πληροφοριών» (Δ.2.1)
-Τελικό Έντυπο «Διόρθωση AIP» (Δ.2.2)
-Τελικό Έντυπο «Διόρθωση AIRAC AIP» (Δ.2.3)
-Τελικό Έντυπο «Συμπλήρωση AIP» (Δ.2.4)
-Τελικό Έντυπο «Συμπλήρωση AIRAC AIP» (Δ.2.5)
-Τελικό Έντυπο «Αεροναυτικής Αγγελίας NOTAM (Δ.2.6)

ΔΙΑΓΡΑΜΜΑ ΡΟΗΣ ΥΠΟΔΙΕΡΓΑΣΙΑ 2 :



ΥΠΟΔΙΕΡΓΑΣΙΑ 3
ΕΚΔΟΣΗ & ΔΙΑΝΟΜΗ ΕΓΧΕΙΡΙΔΙΟΥ ΑΕΡΟΝΑΥΤΙΚΩΝ ΠΛΗΡΟΦΟΡΙΩΝ AIP

Σκοπός :

Να γίνει η έκδοση του Εγχειριδίου Αεροναυτικών Πληροφοριών AIP και η διανομή του στα αεροδρόμια και στους συνδρομητές του.

Πεδίο Εφαρμογής :

Η διαδικασία έκδοσης και διανομής του Εγχειριδίου Αεροναυτικών Πληροφοριών αφορά :

Α) Τη Γενική Δ/ση Αερομεταφορών και ειδικότερα τις παρακάτω διευθύνσεις της :
-Διεύθυνση Αερολιμένων(Δ3)
-Διεύθυνση Τεχνικών Υπηρεσιών (Δ7)
-Διεύθυνση Η/Μ Εγκαταστάσεων (Δ8)

Β) Τη Γενική Δ/ση Αεροναυτιλίας και ειδικότερα τις εξής διευθύνσεις της :
-Διεύθυνση Εναέριας Κυκλοφορίας (Δ4)
-Διεύθυνση Τηλεπικοινωνιών (Δ5)
-Διεύθυνση Ηλ.Συστημάτων Αεροναυτιλίας (Δ6)

Γ) Τις Περιφερειακές Υπηρεσίες της ΥΠΑ και συγκεκριμένα :
-τα Αεροδρόμια (τα οποία διαθέτουν Μονάδες AIS)
-την Υπηρεσία Ελέγχου Περιοχής (ΥΕΠ), στην οποία εντάσσεται και η Δ/ση Αεροναυτικών Εκδόσεων (Ε1) & το Τμήμα Εγχειριδίων Αεροναυτικών Πληροφοριών AIP (Ε1/Α)

Εμπλεκόμενοι :

-Διεύθυνση Αεροναυτικών Εκδόσεων (Ε1)
-Τμήμα Εγχειριδίων Αεροναυτικών Πληροφοριών AIP (Ε1/Α)
-Τυπογραφείο Υπηρεσίας Πολιτικής Αεροπορίας (ΥΠΑ)
-Λογιστικό & Εφοδιαστικό Κέντρο (ΛΕΚ)
-Συνδρομητές

Περιγραφή Διαδικασίας :

Προκειμένου να τυπωθούν τα εγκεκριμένα τελικά έγγραφα που έχουν χαρακτηριστεί ως «Αεροναυτική πληροφορία AIP» και αποτελούν το «Εγχειρίδιο Αεροναυτικών Πληροφοριών AIP» και τα οποία είναι τα εξής:

- «Διόρθωση AIP»
- «Διόρθωση AIRAC AIP»
- «Συμπλήρωση AIP»
- «Συμπλήρωση AIRAC AIP»

ενεργοποιείται το κύριο αρμόδιο Τμήμα για την έκδοση του «Εγχειριδίου Αεροναυτικών Πληροφοριών AIP», που είναι το ακόλουθο :

- Τμήμα Εγχειριδίων Αεροναυτικών Πληροφοριών AIP (Ε1/Α)

Αρχικά, το Τμήμα Εγχειριδίων (Ε1/Α) παραλαμβάνει τα έγγραφα από τη Διεύθυνση Αεροναυτικών Εκδόσεων (Ε1) έπειτα, ο προϊστάμενος του εν λόγω Τμήματος τα αποστέλλει σε μορφή pdf αρχείου συνοδευόμενα από ένα Υπηρεσιακό Σημείωμα «Ανάθεσης έκδοσης εγγράφων» στο Τυπογραφείο της Υ.Π.Α.

Το Τυπογραφείο καθίσταται πλέον υπεύθυνο για την άριστη εκτύπωση των αποστελλομένων σελίδων AIP (ΠΑΡΑΡΤΗΜΑ ΙΙ-Εξειδικευμένη Οδηγία IV). Στην περίπτωση που πρόκειται για την πρώτη έκδοση του Εγχειριδίου, τα έγγραφα συμπληρώνονται σε δύο ντοσιέ με πλαστικό κάλυμμα και φέρουν τους εξής τίτλους :

1. AIP Ελλάδος Τόμος Ι
2. AIP Ελλάδος Τόμος ΙΙ

Εφόσον εκδοθούν επιστρέφουν στο Τμήμα (Ε1/Α) το οποίο είναι πλέον υπεύθυνο για την έγκαιρη και ανελλιπή διανομή του αιτούμενου και ενημερωμένου «Εγχειριδίου Αεροναυτικών Πληροφοριών AIP» στους συνδρομητές του σε άριστη κατάσταση.

Αρχικά, κάθε υποψήφιος συνδρομητής, εσωτερικού ή εξωτερικού, Εγχειριδίου Αεροναυτικών Πληροφοριών AIP υποβάλλει σχετική αίτηση, «Αίτηση χορήγησης Αεροναυτικών Εκδόσεων» στο Τμήμα (Ε1/Α) ακόμα και μέσω ηλεκτρονικού ταχυδρομείου. Για τους υποψήφιους συνδρομητές του εξωτερικού υπάρχει η αντίστοιχη αίτηση σε ξενόγλωσσο κείμενο.

Έπειτα, το Τμήμα (Ε1/Α) καλείται να ελέγξει εάν ο εκάστοτε συνδρομητής πληροί τις προϋποθέσεις για δωρεάν χορήγηση του Εγχειριδίου ή εμπίπτει στην κατηγορία των συνδρομητών που λαμβάνουν το Εγχειρίδιο επί πληρωμή :

1. *Δωρεάν* σε :

- Διεθνείς Οργανισμούς, Υπηρεσίες των Υπουργείων Εξωτερικών και Εθνικής Άμυνας.
- Κράτη-μέλη του Διεθνούς Οργανισμού Πολιτικής Αεροπορίας ICAO (International Civil Aviation Organization) επί αμοιβαιότητα. Η Υ.Π.Α υποχρεούται βάσει του Διεθνούς Οργανισμού Πολιτικής Αεροπορίας να διαθέτει δωρεάν μία σειρά Αεροναυτικών Ε σε κάθε κράτος μέλος του ICAO που το ζητά.
- Οργανικές Μονάδες Υ.Π.Α (για υπηρεσιακή χρήση). Οι Οργανικές Μονάδες της Υ.Π.Α δύναται να προμηθεύονται πλήρη σειρά των Αεροναυτικών Εκδόσεων από το αρμόδιο Τμήμα (Ε1/Α) διατυπώνοντας σε αυτήν γραπτώς το σχετικό αίτημα.

Το Τμήμα (Ε1/Α) εκδίδει τότε «Εγκριτική Απόφαση *δωρεάν* χορήγησης Αεροναυτικών Εκδόσεων» και την κοινοποιεί στο Λογιστικό & Εφοδιαστικό Κέντρο (ΛΕΚ).

Στη συνέχεια το Τμήμα (Ε1/Α) παραδίδει ή αποστέλλει ταχυδρομικά στον συνδρομητή, εγκαίρως τις αιτούμενες ενημερωμένες εκδόσεις. Ο συνδρομητής παραλαμβάνοντας το αιτούμενο Εγχειρίδιο ή μηνιαίες διορθώσεις αυτού υπογράφει «Αποδεικτικό παραλαβής» αυτού. Σε περίπτωση αποστολής του Εγχειριδίου με το ταχυδρομείο, η απόδειξη του ταχυδρομείου υποκαθιστά την απόδειξη παραλαβής από τον συνδρομητή, ενώ μέσω ηλεκτρονικού ταχυδρομείου απαραίτητη είναι η επιβεβαίωση της παραλαβής ως απόδειξη παραλαβής από τον συνδρομητή.

Παράλληλα, καταχωρεί στους σχετικούς πίνακες συνδρομητών τα πλήρη στοιχεία του συνδρομητή :

- Πλήρη στοιχεία αποστολής Εγχειριδίου (Πλήρη στοιχεία : δ/νση αποδέκτη, τηλέφωνο κλπ).
- Διεύθυνση συνδρομητή (Πλήρη στοιχεία : δ/νση υπόχρεου πληρωμής, τηλέφωνο ή φαξ κλπ).
- Παρεχόμενες Αεροναυτικές Εκδόσεις.
- Πληροφορίες ανανέωσης και πληρωμής ετήσιας συνδρομής.

και αρχειοθετεί τα σχετικά δικαιολογητικά :

- Αίτηση χορήγησης
- Αποδεικτικό παραλαβής

Και συγχρόνως αποστέλλει αντίγραφα τους μαζί με το σχετικό «Έντυπο Διάθεσης Αεροναυτικών Εκδόσεων» στο Λογιστικό & Εφοδιαστικό Κέντρο (ΛΕΚ).

2. *Επί πληρωμή* σε :

- Κράτη-μέλη του Διεθνούς Οργανισμού Πολιτικής Αεροπορίας ICAO για κάθε επιπλέον σειρά που παρέχεται
- Ιδιωτικοί Οργανισμοί και Ιδρύματα
- Φυσικά ή νομικά πρόσωπα
- Αερολέσχες

Το Τμήμα (Ε1/Α) εκδίδει τότε «Εγκριτική Απόφαση *επί πληρωμής* χορήγησης Αεροναυτικών Εκδόσεων» και διαβιβάζει μέσω αυτής την αίτηση στο Λογιστικό & Εφοδιαστικό Κέντρο (ΛΕΚ).

Το Λογιστικό & Εφοδιαστικό Κέντρο (ΛΕΚ) εκδίδει μηχανογραφικά Χρηματική Εντολή (για συνδρομητές εσωτερικού) ή Τιμολόγιο (για συνδρομητές εξωτερικού) & τους τα αποστέλλει με συστημένο ταχυδρομείο (ΠΑΡΑΡΤΗΜΑ ΙΙ-Εξειδικευμένη Οδηγία V).

Το Τμήμα (Ε1/Α) μόλις λάβει από το συνδρομητή αντίγραφο του αποδεικτικού κατάθεσης του αναλογούντος ποσού στον Ειδικό Λογαριασμό της Υ.Π.Α, που τηρείται στην Τράπεζα της Ελλάδος,(ΠΑΡΑΡΤΗΜΑ ΙΙ-Εξειδικευμένη Οδηγία VI), αναλαμβάνει την έγκαιρη αποστολή του αιτούμενου και ενημερωμένου «Εγχειριδίου Αεροναυτικών Πληροφοριών AIP» σε άριστη κατάσταση.

Ο συνδρομητής παραλαμβάνοντας το αιτούμενο Εγχειρίδιο ή μηνιαίες διορθώσεις αυτού υπογράφει «Αποδεικτικό παραλαβής» αυτού. Σε περίπτωση αποστολής του Εγχειριδίου με το ταχυδρομείο, η απόδειξη του ταχυδρομείου υποκαθιστά την απόδειξη παραλαβής από τον συνδρομητή, ενώ μέσω ηλεκτρονικού ταχυδρομείου απαραίτητη είναι η επιβεβαίωση της παραλαβής ως απόδειξη παραλαβής από τον συνδρομητή.

Στη συνέχεια, το Τμήμα (Ε1/Α) καταχωρεί τον συνδρομητή στους σχετικούς πίνακες συνδρομητών, εσωτερικού και εξωτερικού, αρχειοθετώντας τα σχετικά δικαιολογητικά :

- Αίτηση χορήγησης
- Απόδειξη κατάθεσης
- Αποδεικτικό παραλαβής

Και συγχρόνως αποστέλλει αντίγραφα τους μαζί με το σχετικό «Έντυπο Διάθεσης Αεροναυτικών Εκδόσεων» στο Λογιστικό & Εφοδιαστικό Κέντρο (ΛΕΚ).

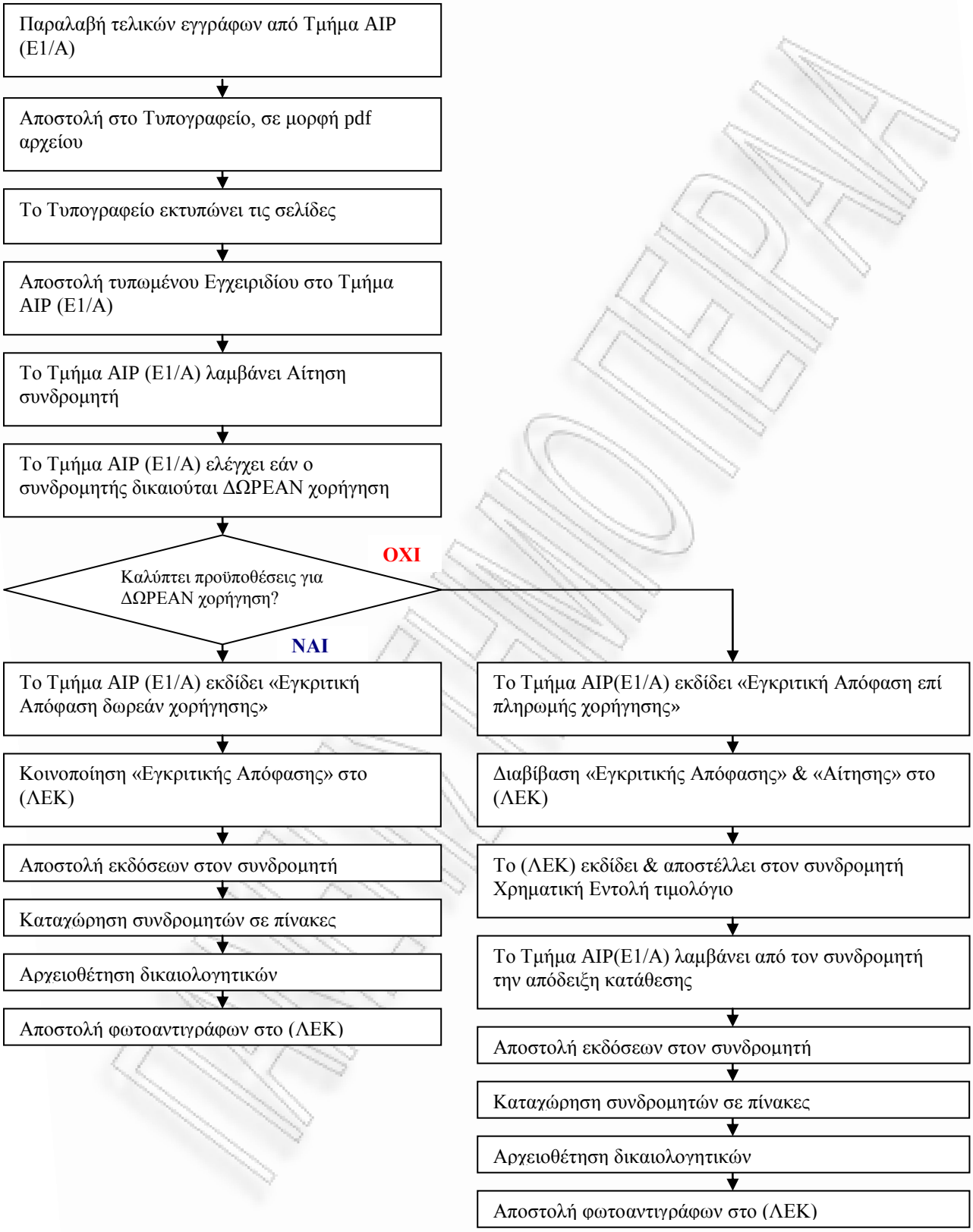
Το Τμήμα (Ε1/Α) τηρεί επίσης αρχείο :

- σελίδων Εκδόσεων Αεροναυτικών Πληροφοριών. Τηρεί σε ειδικά ενθέμια τις σελίδες που ισχύουν για υπηρεσιακή χρήση και για τον σκοπό συμπλήρωσης των εκδόσεων για αποστολή σε νέους συνδρομητές.
- κενών πλαστικών καλυμμάτων. Έχει τη φροντίδα παρακολούθησης αποθεμάτων των καλυμμάτων AIS καθώς και τη μέριμνα προμήθειας των αναγκαίων ποσοτήτων

Έντυπα : (ΠΑΡΑΡΤΗΜΑ IV)

-Υπηρεσιακό Σημείωμα «Ανάθεσης έκδοσης εγγράφων» (Δ.3.1)
-Αίτηση «Χορήγησης Αεροναυτικών Εκδόσεων» (Δ.3.2)
-Αίτηση «Χορήγησης Αεροναυτικών Εκδόσεων» σε ξενόγλωσσο κείμενο (Δ.3.3)
-Εγκριτική «Απόφαση Διάθεσης Αεροναυτικών Εκδόσεων» (Δ.3.4)
-Αποδεικτικό «Παραλαβής Αεροναυτικών Εκδόσεων» (Δ.3.5)
-Έντυπο «Διάθεσης Αεροναυτικών Εκδόσεων» (Δ.3.6)

ΔΙΑΓΡΑΜΜΑ ΡΟΗΣ ΥΠΟΔΙΕΡΓΑΣΙΑΣ 3 :



5. ΣΥΣΤΗΜΑ ΔΙΑΧΕΙΡΙΣΗΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ ISO/IEC 27001:2005

5.1. Εισαγωγή

Το πρότυπο ISO/IEC 27001:2005 αποτελείται από οκτώ ενότητες και δύο παραρτήματα. Στις τρείς πρώτες ενότητες γίνεται αναφορά στην ορολογία, ενώ από την τέταρτη ενότητα ξεκινούν οι απαιτήσεις του προτύπου. Στο παρόν κεφάλαιο θα αποτυπωθούν αυτές οι απαιτήσεις. Συγκεκριμένα, οι«4.Σύστημα Διαχείρισης Ασφάλειας ΠληροφοριώνISMS-Γενικές Απαιτήσεις»,«5.Ευθύνη Διοίκησης»,«6.Εσωτερικές Επιθεωρήσεις ISMS»,«7.Ανασκόπηση Διοίκησης ISMS», «8.Βελτίωση ISMS» καθώς και το «ΠΑΡΑΡΤΗΜΑ Α.Στόχοι ελέγχων & έλεγχοι».

Παράλληλα, θα πραγματοποιείται μια σύγκριση της βασικής διεργασίας έκδοσης και ενημέρωσης του Εγχειριδίου AIP, όπως αποτυπώθηκε στο προηγούμενο κεφάλαιο, σε σχέση με τις απαιτήσεις του προτύπου, ώστε να προκύψει ο βαθμός κατά τον οποίο το σύστημα διαχείρισης ασφάλειας κρίσιμων αεροναυτικών πληροφοριών που εφαρμόζει η Υ.Π.Α πληροί τις απαιτήσεις του προτύπου ISO/IEC 27001:2005 «Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών-Απαιτήσεις».

Τέλος, όπου προκύπτει απόκλιση μεταξύ της απαίτησης του προτύπου και της υπάρχουσας προσέγγισης του οργανισμού, θα παρουσιάζονται προτάσεις και τρόποι οι οποίοι θα συμβάλλουν στη σύγκλιση της διεργασίας στις απαιτήσεις του προτύπου.

5.2. Γενικές Απαιτήσεις

Απαίτηση 4

ΣΥΣΤΗΜΑ ΔΙΑΧΕΙΡΙΣΗΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ

4.1 Γενικές απαιτήσεις

Ο οργανισμός πρέπει να δημιουργήσει, εφαρμόσει, λειτουργήσει, παρακολουθήσει, ελέγξει, διατηρήσει και βελτιώσει ένα τεκμηριωμένο Σύστημα ISMS στο πλαίσιο της συνολικής οργάνωσης των επιχειρηματικών δραστηριοτήτων και των κινδύνων που αντιμετωπίζει. Για τους σκοπούς του διεθνούς προτύπου οι διαδικασίες που χρησιμοποιούνται βασίζονται στο μοντέλο PDCA.

4.2 Καθιέρωση/δημιουργία και διαχείριση του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών – ISMS (Information Security Management System)

4.2.1 Καθιέρωση του ISMS

Ο οργανισμός πρέπει να πράξει τα εξής :

α) Να καθορίσει το αντικείμενο και τα όρια του συστήματος ISMS από την άποψη των χαρακτηριστικών της δουλειάς, του οργανισμού, της θέσης του, των στοιχείων ενεργητικού και της τεχνολογίας του, καθώς και να συμπεριλάβει λεπτομέρειες τυχόν εξαιρέσεων από το αντικείμενο καθώς και την αιτιολόγηση τους (βλ. 1.2).

Ναι, ο οργανισμός έχει διατυπώσει ως αντικείμενο του συστήματος ISMS την καθιέρωση μιας επίσημης και σαφής προσέγγισης της συστηματικής διαχείρισης της ασφάλειας πληροφοριών για την εκπλήρωση των υποχρεώσεων ασφάλειας πληροφοριών που θέτουν η Ελληνική Νομοθεσία, οι Ευρωπαϊκές Οδηγίες και η Διεθνής Σύμβαση του Διεθνούς Οργανισμού Πολιτικής Αεροπορίας ICAO (International Civil Aviation Organization) με το Παράρτημα 15 (Annex 15). Με τον όρο «συστηματική διαχείριση ασφάλειας πληροφοριών» νοείται η εναρμόνιση των διαδικασιών κατά την παροχή αεροναυτικών πληροφοριών μέσω της ύπαρξης ικανού προσωπικού, κοινών διαδικασιών και κοινής ερμηνείας των κανονισμών.

Η πολιτική ασφάλειας πληροφοριών καθορίζει ως όρια του συστήματος όλες τις μονάδες του οργανισμού που επηρεάζουν και επηρεάζονται από το σύστημα, δηλώνοντας ότι στο σύστημα ISMS συμμετέχουν οι μονάδες εκείνες του οργανισμού που παρέχουν υπηρεσίες αεροναυτικών πληροφοριών. Ειδικότερα, η Διεύθυνση Αερολιμένων (Δ3) , η Διεύθυνση Εναέριας Κυκλοφορίας (Δ4), η Διεύθυνση Τηλεπικοινωνιών (Δ5), η Διεύθυνση Ηλ.Συστημάτων Αεροναυτιλίας (Δ6), η Διεύθυνση Αεροναυτικών Εκδόσεων (Ε1) μαζί με το τμήμα της Τμήμα Εγχειριδίων Αεροναυτικών Πληροφοριών-AIP (Ε1/Α).

β) Να καθορίσει μια πολιτική ISMS βασισμένη στα χαρακτηριστικά της δουλειάς, στον οργανισμό, στη θέση του, στα στοιχεία ενεργητικού και στην τεχνολογία του, η οποία :

1. θα περιλαμβάνει ένα πλαίσιο για τον καθορισμό των στόχων και θα καθιερώνει μια γενική κατεύθυνση και τις αρχές για την ανάληψη δράσης λαμβάνοντας υπόψη την ασφάλεια των πληροφοριών

Ναι, ο οργανισμός έχει επίσημα διατυπώσει ότι στόχος είναι η εναρμόνιση συστημάτων και διαδικασιών κατά την παροχή υπηρεσιών Αεροναυτικών πληροφοριών (AIS-Aeronautical Information Services). Επίσης, έχει εντοπίσει ότι μέσον για την επίτευξη του στόχου είναι η ύπαρξη ικανού προσωπικού, κοινών διαδικασιών και κοινή ερμηνεία των κανονισμών.

2. θα λαμβάνει υπόψη τη δουλειά και τις νομικές ή κανονιστικές απαιτήσεις, και τις συμβατικές υποχρεώσεις ασφαλείας

Ναι, ο οργανισμός διαθέτει πολιτική ασφαλείας πληροφοριών η οποία έχει καθοριστεί από την Ελληνική Νομοθεσία (Αεροπορικό Κώδικα, Νόμους, Π.Δ, Υπουργικές Αποφάσεις κα), από τις Ευρωπαϊκές Οδηγίες που έχουν ενσωματωθεί στην Ελληνική Νομοθεσία καθώς και από τις απαιτήσεις που περιγράφονται στη Διεθνή Σύμβαση του Διεθνούς Οργανισμού Πολιτικής Αεροπορίας ICAO (International Civil Aviation Organization) και το Παράρτημα 15 (Annex 15).

3. θα ευθυγραμμίζεται με τη στρατηγική διαχείρισης κινδύνων του οργανισμού, μέσα στο πλαίσιο της οποίας η εγκατάσταση και συντήρηση του ISMS θα λάβει χώρα

Ναι, η πολιτική ασφάλειας πληροφοριών αναφέρει ότι υπάρχουν διαδικασίες εντοπισμού των κινδύνων, αξιολόγησης και μείωσης της επικινδυνότητας, οι οποίες αποτελούν και τη βάση του συστήματος.

4. θα καθορίζει τα κριτήρια βάσει των οποίων θα αξιολογηθεί ο κίνδυνος

Ναι, οι ενδεχόμενοι κίνδυνοι αξιολογούνται ανάλογα με τη σοβαρότητα των συνεπειών τους στην ασφάλεια πληροφοριών και ανάλογα με την πιθανότητα εμφάνισής τους.

5. θα έχει εγκριθεί από τη διοίκηση

Ναι, η πολιτική ασφάλειας πληροφοριών έχει εγκριθεί και υπογραφεί από τον Διοικητή της Υπηρεσίας Πολιτικής Αεροπορίας.

γ) Να καθορίσει την «προσέγγιση εκτίμησης κινδύνου» του οργανισμού

1. να προσδιορίσει μια μεθοδολογία αξιολόγησης κινδύνων που είναι κατάλληλη για το ISMS, για την ασφάλεια των πληροφοριών της δουλειάς, και για τις νομικές και κανονιστικές απαιτήσεις

2. να αναπτύξει κριτήρια για την αποδοχή των κινδύνων και να προσδιορίσει τα αποδεκτά επίπεδα κινδύνου

Η μεθοδολογία αξιολόγησης κινδύνων που τελικά θα επιλεγεί πρέπει να διασφαλίζει ότι οι αξιολογήσεις των κινδύνων παράγουν συγκρίσιμα και αναπαράξιμα αποτελέσματα.

Ναι, ο οργανισμός έχει εκπονήσει διαδικασίες εντοπισμού του κινδύνου, αξιολόγησης και μείωσης της επικινδυνότητας. Οι διαδικασίες αυτές είναι τεκμηριωμένες και θα αναλυθούν παρακάτω. Τα αποτελέσματα παρουσιάζονται σε συγκριτικούς πίνακες.

(Risk Identification)

δ) Να εντοπίσει τους κινδύνους

1. να εντοπίσει τα περιουσιακά στοιχεία που εμπίπτουν στο αντικείμενο εφαρμογής του ISMS και τους ιδιοκτήτες αυτών των περιουσιακών στοιχείων

Ναι, ο οργανισμός έχει εντοπίσει τους κινδύνους :
-στον εξοπλισμό
-στον ανθρώπινο παράγοντα (χρήστες & διαχειριστές του συστήματος)
-στις διαδικασίες

Σημείωση :

(ο όρος "ιδιοκτήτης" προσδιορίζει ένα άτομο που έχει την εγκεκριμένη ευθύνη διαχείρισης για τον έλεγχο της παραγωγής, την ανάπτυξη, τη συντήρηση, τη χρήση και την ασφάλεια των στοιχείων του ενεργητικού. Με τον όρο "ιδιοκτήτης" δεν σημαίνει ότι το άτομο έχει πραγματικά δικαιώματα ιδιοκτησίας στο περιουσιακό στοιχείο)

2. να προσδιορίσει τις απειλές για τα περιουσιακά αυτά στοιχεία

Ναι, ο οργανισμός έχει εντοπίσει τις απειλές :

- στον εξοπλισμό : φυσική καταστροφή (σεισμός, τσουνάμι), ξαφνικές καταστροφές (μπλάκ-ουτ), ατύχημα (πυρκαγιά), κλοπή, τρομοκρατικές ενέργειες (9/11), ιούς, διάρκεια ζωής

- στον ανθρώπινο παράγοντα (χρήστες & διαχειριστές του συστήματος) : λανθασμένη καταχώρηση, παράλειψη καταχώρησης, απώλεια εντύπου, παράνομη πρόσβαση

- στις διαδικασίες :αλλαγή διαδικασίας δίχως έγκαιρη ενημέρωση και εκπαίδευση προσωπικού

3. να προσδιορίσει τα τρωτά σημεία που θα μπορούσαν να προκύψουν αναλύοντας τις απειλές

Ναι, ο οργανισμός αναλύοντας τις παραπάνω απειλές προσδιόρισε τα τρωτά σημεία :

- Έλλειψη back-up,ασφάλειας χώρου, χρήση λογισμικού anti-virus, έλλειψη ανιχνευτών καπνού, έλλειψη γεννήτριας, ελλιπή συντήρηση
- Ελλιπής εκπαίδευση προσωπικού, όχι χρήση προσωπικών κωδικών
- Ανύπαρκτη εκπαίδευση προσωπικού όσον αφορά τις αλλαγές

4. να προσδιορίσει τις επιπτώσεις που ενδέχεται να έχει η απώλεια της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας στα περιουσιακά στοιχεία

Ναι, ο οργανισμός προσδιόρισε τις επιπτώσεις :

- Κακή λειτουργία
- Απώλεια φήμης
- Νομικές κυρώσεις

(Risk Assessment)

ε) Να αναλύσει και αξιολογήσει τους κινδύνους

1. να αξιολογήσει τις επιχειρηματικές επιπτώσεις στον οργανισμό που

μπορεί να προκύψουν από αποτυχίες στη διαχείριση της ασφάλειας, λαμβάνοντας υπόψη τις συνέπειες της απώλειας της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των στοιχείων του ενεργητικού

Ναι, ο οργανισμός στο στάδιο αυτό αξιολογεί και κατηγοριοποιεί τους ενδεχόμενους κινδύνους που έχει εντοπίσει ανάλογα με τα αποτελέσματα και τη σοβαρότητα των συνεπειών τους στην ασφάλεια πληροφοριών.

Ένας ενδεχόμενος κίνδυνος διαβαθμίζεται όσον αφορά τη σοβαρότητά του σύμφωνα με τον ακόλουθο Πίνακα 1.

Βαθμός Σοβαρότητας	**Επιπτώσεις**
3 Μέγιστος βαθμός	Μείζων Συμβάν
2	Σημαντικό Συμβάν
1 Ελάχιστος βαθμός	Ρουτίνας Συμβάν (καμία άμεση επίπτωση)

Για παράδειγμα,

Λάθος «συντεταγμένες αεροδρομίων»	Βαθμός Σοβαρότητας : 3
Λάθος «συντεταγμένες ραδιοβοηθημάτων»	Βαθμός Σοβαρότητας : 2
Λάθος «υπόλοιπα δεδομένα»	Βαθμός Σοβαρότητας : 1

2. να αξιολογήσει τη ρεαλιστική πιθανότητα να συμβούν αποτυχίες στη διαχείριση της ασφάλειας δεδομένου των απειλών που επικρατούν και των τρωτών σημείων, και να αξιολογήσει και τις επιπτώσεις που συνδέονται με αυτά τα περιουσιακά στοιχεία, καθώς και τους ελέγχους που εφαρμόζονται σήμερα

Ναι, ο οργανισμός έχει εκτιμήσει τη ρεαλιστική πιθανότητα εμφάνισης του κινδύνου χρησιμοποιώντας ποιοτική διαβάθμιση, όπως παρουσιάζεται στον παρακάτω Πίνακα 2.

Πιθανότητα Εμφάνισης Κινδύνου			
Ποιοτική Διαβάθμιση	**1 Απίθανο**	**2 Πιθανό**	**3 Συχνό**
	Απίθανο να συμβεί στη διάρκεια ζωής του συστήματος	Πιθανό να συμβεί μια φορά στη διάρκεια ζωής του συστήματος	Πιθανό να συμβεί μια ή περισσότερες φορές στη ζωή του συστήματος

3. να εκτιμήσει τα επίπεδα των κινδύνων

Ναι, ο οργανισμός έχει υιοθετήσει την ευρέως γνωστή μέθοδο του πολλαπλασιασμού των δυο βαθμολογιών ώστε να προκύψουν τα τελικά επίπεδα κινδύνου, την οποία αναφέρει και ο Humphreys (2008) :

Επίπεδο κινδύνου = (Βαθμός σοβαρότητας κινδύνου) * (Βαθμός πιθανότητας εμφάνισης κινδύνου)

Ο οργανισμός εκτιμά τα επίπεδα του κινδύνου και τα αναλύει στον Πίνακα 3.

Πιθανότητα Εμφάνισης Ενδεχόμενου Κινδύνου

Επίπεδο Κινδύνου	**1 Απίθανο**	**2 Πιθανό**	**3 Συχνό**
3 Μείζων Συμβάν	3	6	9
2 Σοβαρό Συμβάν	2	4	6
1 Συμβάν Ρουτίνας	1	2	3

4. να αποφασίσει εάν οι κίνδυνοι είναι αποδεκτοί ή αν απαιτούν θεραπεία με βάση τα κριτήρια για την αποδοχή κινδύνων που συστάθηκαν πριν (βλ. 4.2.1.γ.2)

Ναι, ο οργανισμός διαθέτει μια τεκμηριωμένη διαδικασία αποδοχής των κινδύνων. Συγκεκριμένα, ο οργανισμός χαρακτηρίζει ένα πιθανό κίνδυνο «αποδεκτό» για επίπεδα 1 & 2 ή «μη αποδεκτό» για επίπεδα 6 & 9. Για τις ενδιάμεσες καταστάσεις, επίπεδα 3 & 4, ο κίνδυνος χαρακτηρίζεται επανεξεταστέος και είναι απαραίτητη η λήψη μέτρων

ελαχιστοποίησης ή μείωσής του ώστε να γίνει τουλάχιστον «ανεκτός». Ο οργανισμός αποφασίζει σύμφωνα με τον παρακάτω Πίνακα 4.

Πιθανότητα Εμφάνισης Ενδεχόμενου Κινδύνου

Σοβαρότητα Κινδύνου	**1 Απίθανο**	**2 Πιθανό**	**3 Συχνό**
3	*Επανεξεταστέος*	*Μη-αποδεκτός*	*Μη-αποδεκτός*
2	*Επανεξεταστέος*	*Επανεξεταστέος*	*Μη-αποδεκτός*
1	*Αποδεκτός*	*Αποδεκτός*	*Επανεξεταστέος*

(Potential risk treatment)

στ) Να προσδιορίσει και να αξιολογήσει τις εναλλακτικές επιλογές για την αντιμετώπιση των κινδύνων. Πιθανές ενέργειες περιλαμβάνουν:

1. εφαρμογή κατάλληλων ελέγχων ***(Μείωση κινδύνου)***

Ναι, ο οργανισμός όταν διαπιστώσει ότι ένας κίνδυνος είναι μεγαλύτερος από τα προκαθορισμένα επίπεδα ασφαλείας, δηλαδή «Μη-αποδεκτός» ή «επανεξεταστέος», εφαρμόζει κατάλληλους ελέγχους που μειώνουν την επικινδυνότητα ή την πιθανότητα εμφάνισης του κινδύνου ή και των δύο μαζί.

2. εν γνώσει του ο οργανισμός και αντικειμενικά να αποδεχτεί τους κινδύνους, με την προϋπόθεση ότι ο οργανισμός πληροί σαφώς τις πολιτικές και τα κριτήρια για την ανάληψη κινδύνων (βλ. 4.2.1.γ.2.) ***(Αποδοχή)***

Ναι, ο οργανισμός εν γνώσει του και αντικειμενικά, εφόσον πληρούνται τα κριτήρια που αναφέρθηκαν στο 4.2.1.ε.4. και Πίνακα 4, αποδέχεται κινδύνους. Αποδέχεται δηλαδή την απώλεια όταν συμβαίνει. Η αποδοχή κινδύνου είναι μια βιώσιμη στρατηγική του οργανισμού για τους μικρούς κινδύνους και για τους πολύ μεγάλους κινδύνους που έχουν όμως πολύ μικρή πιθανότητα να συμβούν.

3. αποφυγή των κινδύνων ***(Αποφυγή)***

Ναι, ο οργανισμός έχει υιοθετήσει τη μέθοδο της αποφυγής για ορισμένους κινδύνους. Ειδικότερα :

- έχει εγκαταστήσει ειδικά προγράμματα (anti-virus software), προκειμένου να αποφύγει τον κίνδυνο εμφάνισης ιών.
- χρησιμοποιεί «τροφοδοτικά αδιάλειπτης λειτουργίας (UPS-Un interruptible power supply)», ώστε να αποφύγει τον κίνδυνο διακοπής των δραστηριοτήτων του οργανισμού ή της απώλειας κρίσιμων αεροναυτικών πληροφοριών εξαιτίας μιας πτώσης τάσης ρεύματος.

4. μεταφορά των κινδύνων που συνδέονται με την επιχείρηση σε άλλα μέρη (π.χ. ασφαλιστές, προμηθευτές) ***(Μεταβίβαση)***

Ναι, ο οργανισμός έχει μεταφέρει ορισμένους κινδύνους. Συγκεκριμένα :

- έχει ασφαλίσει τον εξοπλισμό του και τις εγκαταστάσεις του σε περίπτωση πυρκαγιάς, σεισμού, πλημμύρας.
- έχει φροντίσει στις συμβάσεις με τους προμηθευτές του εξοπλισμού ή του λογισμικού του να υπάρχουν ρήτρες για αποζημίωση σε περίπτωση βλάβης ή κακής λειτουργίας όταν αυτή οφείλεται αποκλειστικά στον προμηθευτή.

(Create risk management plan)

ζ) Να επιλέξει στόχους ελέγχων και τους ελέγχους για την αντιμετώπιση των κινδύνων

Οι στόχοι των ελέγχων και οι έλεγχοι πρέπει να επιλέγονται και να εφαρμόζονται με τέτοιο τρόπο ώστε να καλύπτουν τις ανάγκες που προσδιορίστηκαν από την αξιολόγηση των κινδύνων και τη διεργασία θεράπευσης των κινδύνων.
Η επιλογή αυτή πρέπει να λαμβάνει υπόψη τα κριτήρια για την αποδοχή των κινδύνων (βλ. 4.2.1.γ.2), καθώς και τις νομοθετικές, κανονιστικές και συμβατικές απαιτήσεις.

Οι στόχοι των ελέγχων και οι έλεγχοι από το Παράρτημα Α, πρέπει να επιλέγονται ως μέρος αυτής της διαδικασίας ως κατάλληλοι για να καλύψουν τις απαιτήσεις που προσδιορίστηκαν.

Η λίστα με τους στόχους των ελέγχων και τους έλεγχοι που παρατίθενται στο Παράρτημα Α δεν είναι εξαντλητική και επιπλέον στόχοι ελέγχου και έλεγχοι μπορούν επίσης να επιλέγονται

Ναι, ο οργανισμός έχοντας συνυπολογίσει τους παράγοντες αυτούς έχει επιλέξει από τον Πίνακα Α.1 του προτύπου συγκεκριμένους στόχους ελέγχων και ελέγχους για τον κάθε κίνδυνο ξεχωριστά.

Ορισμένοι από αυτούς τους ελέγχους είναι «καλές γενικές πρακτικές» και έχουν εφαρμοστεί σε όλο το σύστημα διαχείρισης ασφάλειας πληροφοριών του οργανισμού ούτος ώστε να εξασφαλιστεί η εύρυθμη λειτουργία του, ενώ κάποιοι άλλοι είναι «έλεγχοι σε επίπεδο διεργασίας» και εφαρμόζονται σε συγκεκριμένα σημεία πάνω στη βασική διεργασία έκδοσης και ενημέρωσης του «Εγχειριδίου Αεροναυτικών Πληροφοριών (AIP)».

Οι δύο αυτές κατηγορίες περιγράφονται αναλυτικά στο Κεφάλαιο 5, Ενότητα 5.7.

η) Να λάβει την έγκριση της διοίκησης όσον αφορά τους προτεινόμενους εναπομένοντες κινδύνους

«Εναπομείναντας κίνδυνος» είναι ο κίνδυνος που δε γίνεται μηδέν, που δηλαδή απομένει ακόμα και μετά τη λήψη των σχετικών μέτρων αντιμετώπισης.

Ναι, υπάρχει μία επίσημη αποδοχή του εναπομείναντα κινδύνου εκ μέρος του οργανισμού.

θ) Να λάβει την άδεια της διοίκησης για την υλοποίηση και τη λειτουργία του ISMS

Ναι, ο οργανισμός έχει λάβει γραπτή και υπογεγραμμένη άδεια από τη Διοίκηση για τη λειτουργία ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ISMS).

ι) Να συντάξει μια Δήλωση Εφαρμοσιμότητας

Μια Δήλωση Εφαρμοσιμότητας πρέπει να ετοιμαστεί η οποία περιλαμβάνει τα ακόλουθα:

1. τους στόχους των ελέγχων και τους ελέγχους που επιλέχτηκαν στο (4.2.1.ζ) και την αιτιολόγηση της επιλογής τους
2. τους στόχους των ελέγχων και τους ελέγχους που εφαρμόστηκαν πρόσφατα και
3. ο αποκλεισμός κάθε στόχου ελέγχων και ελέγχου του παραρτήματος Α και την αιτιολόγηση του αποκλεισμού τους

Η Δήλωση Εφαρμοσιμότητας παρέχει μια περίληψη των αποφάσεων που αφορούν τη θεραπεία των κινδύνων. Δικαιολογεί εξαιρέσεις, παρέχει τη διασταύρωση ότι κανένας

έλεγχος δεν έχει παραληφθεί από απροσεξία.

Ναι, ο οργανισμός έχει συντάξει μια «Δήλωση Εφαρμοσιμότητας» η οποία περιλαμβάνει τους 13 στόχους ελέγχων και τους ελέγχους που επιλέχθηκαν από το Παράρτημα Α του προτύπου και τους οποίους τώρα εφαρμόζει καθώς και την αιτιολόγηση της επιλογής τους. (Κεφάλαιο 5,Ενότητα 5.7).

4.2.2 Εφαρμογή και λειτουργία του ISMS

Ο οργανισμός πρέπει να κάνει τα ακόλουθα :

α) Να διατυπώσει ένα σχέδιο μείωσης κινδύνου που θα προσδιορίζει την κατάλληλη διαχείριση, τους πόρους, τις ευθύνες και τις προτεραιότητες για τη διαχείριση των κινδύνων για την ασφάλεια των πληροφοριών (βλ. *Απαίτηση 5*)

Ναι, ο οργανισμός προκειμένου να λειτουργήσουν οι έλεγχοι έχει διατυπώσει ένα «Σχέδιο Μείωσης Κινδύνου (Risk Treatment Plan) » το οποίο προσδιορίζει γραπτώς τη διαδικασία, τις ευθύνες και τις προτεραιότητες για την αντιμετώπιση των μη συμμορφώσεων και των συμβάντων που ενδέχεται να προκύψουν εξαιτίας των τελευταίων και παρουσιάζεται αναλυτικά στο ΠΑΡΑΡΤΗΜΑ ΙΙΙ.

β) Να εφαρμόσει το σχέδιο μείωσης κινδύνου προκειμένου να επιτευχθούν οι προκαθορισμένοι στόχοι ελέγχων, το οποίο περιλαμβάνει την εξέταση της χρηματοδότησης και την κατανομή των ρόλων και των αρμοδιοτήτων

Ναι, ο οργανισμός εφαρμόζει το Σχέδιο Μείωσης Κινδύνου (Risk Treatment Plan) που έχει διατυπώσει όταν προκύψει κάποια μη συμμόρφωση.

Συγκεκριμένα, μόλις εντοπιστεί μη συμμόρφωση με τις απαιτήσεις του προτύπου, με ευθύνη των Διευθυντών των μονάδων λαμβάνονται τα άμεσα διορθωτικά μέτρα και εκδίδεται μια «Αναφορά ασφάλειας» προς τη Διοίκηση. Στο συντομότερο δυνατό χρόνο με ευθύνη πάλι των Διευθυντών των εμπλεκόμενων μονάδων συγκεντρώνονται τα απαραίτητα στοιχεία. Υποβάλλονται προτάσεις, λαμβάνονται τα απαραίτητα διορθωτικά μέτρα, επαληθεύονται και αποστέλλεται ένα ενημερωτικό σημείωμα στη Διοίκηση.

γ) Να εφαρμόσει τους ελέγχους που επιλέγηκαν στο (4.2.1.ζ) ώστε να ικανοποιηθούν οι στόχοι των ελέγχων

Ναι, ο οργανισμός εφαρμόζει τους ελέγχους που επιλέχθηκαν στο (4.2.1.ζ).

δ) Να καθορίσει πώς θα μετρηθεί η αποτελεσματικότητα των ελέγχων ή των ομάδων ελέγχων που επιλέγηκαν και να προσδιορίσει πώς αυτές οι μετρήσεις πρέπει να χρησιμοποιούνται για την αξιολόγηση της αποτελεσματικότητας του ελέγχου στην παραγωγή συγκρίσιμων και επαναλαμβανόμενων αποτελεσμάτων (βλ. 4.2.3.γ)

Σημείωση :
η μέτρηση της αποτελεσματικότητας των ελέγχων επιτρέπει στους managers και στο προσωπικό να αποφασίσουν πόσο καλά οι έλεγχοι επιτυγχάνουν τους προκαθορισμένους στόχους ελέγχων που έχουν τεθεί.

Όχι, ο οργανισμός δεν έχει καθορίσει μέθοδο μέτρησης της αποτελεσματικότητας των ελέγχων.

ε) Να εφαρμόσει προγράμματα κατάρτισης και ευαισθητοποίησης (βλ. 5.2.2)

Ναι, ο οργανισμός πραγματοποιεί προγράμματα κατάρτισης και ευαισθητοποίησης.

Οι αρμόδιοι υπάλληλοι για την εισαγωγή και επεξεργασία αεροναυτικών πληροφοριών συμμετέχουν σε εξάμηνα εκπαιδευτικά σεμινάρια σε αντίστοιχα Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών τα οποία πραγματοποιούνται τόσο στην Ελλάδα όσο και στο εξωτερικό.

Στόχος αυτών των σεμιναρίων είναι η εκπαίδευση του εμπλεκόμενου προσωπικού σε νέες τεχνικές, συστήματα ή διαδικασίες που χρησιμοποιούν άλλα ευρωπαϊκά κράτη.

στ) Να διαχειρίζεται τη λειτουργία του ISMS

Ναι, ο οργανισμός διαχειρίζεται ο ίδιος τη λειτουργία του συστήματος.

ζ) Να διαχειρίζεται τους πόρους για το ISMS (βλέπε 5.2)

Ναι, διαχειρίζεται τους πόρους για το σύστημα.

η) Να εφαρμόσει διαδικασίες και άλλους ελέγχους ικανούς να επιτρέψουν την ταχεία ανίχνευση συμβάντων ασφαλείας και την αντιμετώπιση των συμβάντων ασφαλείας (βλ.4.2.3.α)

Όχι, ο οργανισμός δεν εφαρμόζει επιπλέον ελέγχους πέραν εκείνων που έχει επιλέξει από το Παράρτημα Α του προτύπου και τους έχει συμπεριλάβει στη «Δήλωση Εφαρμοσιμότητάς» του (Κεφάλαιο 5, Ενότητα 5.7).

4.2.3 Παρακολούθηση και επανεξέταση του ISMS

Ο οργανισμός πρέπει να κάνει τα ακόλουθα :

α) Να εκτελεί την παρακολούθηση και την επανεξέταση των διαδικασιών και άλλων ελέγχων για να :

Ναι, ο οργανισμός παρακολουθεί την αποτελεσματικότητα του συστήματος σε «επίπεδο διεργασίας» μέσω ελέγχων που έχει επιλέξει από το Παράρτημα Α του προτύπου και τους οποίους εφαρμόζει σε συγκεκριμένα κρίσιμα σημεία σε κάθε υποδιεργασία. (Κεφάλαιο 5- Ενότητα 5.7)

1. εντοπίζει έγκαιρα σφάλματα κατά την επεξεργασία των αποτελεσμάτων

Ναι, αφού με τη χρήση αυτών των ελέγχων (αναφέρονται στο Παράρτημα) σε κομβικά σημεία της διεργασίας κατορθώνει να εντοπίζει έγκαιρα τυχόν σφάλματα.

2. αναγνωρίζει έγκαιρα επιτυχημένες ή μη απόπειρες παραβίασης της ασφάλειας και περιστατικά ασφαλείας

Ναι, οι έλεγχοι αυτοί επιτρέπουν και τον έγκαιρο εντοπισμό κάποιας απόπειρας παραβίασης.

3. επιτρέπει στη διοίκηση να αποφασίζει εάν οι δραστηριότητες ασφαλείας θα ανατίθενται σε ανθρώπους ή θα εφαρμόζονται από την εκτέλεση της τεχνολογίας της πληροφορίας, όπως είναι αναμενόμενο

Ναι, διότι μέσα από τους ελέγχους αυτούς διαφαίνεται αν κάποιο σημείο της διεργασίας θα ήταν προτιμότερο και ασφαλέστερο να αυτοματοποιηθεί πλήρως.

4. βοηθά στον εντοπισμό γεγονότων ασφάλειας και έτσι να αποτρέψει να συμβούν επεισόδια ασφάλειας ,με τη χρήση των δεικτών

Όχι, δεν χρησιμοποιεί δείκτες ούτε γίνεται ανάλυση τάσεων.

5. αποφασίζει το αν οι ενέργειες που λαμβάνονται για την επίλυση μιας παραβίασης της ασφάλειας ήταν αποτελεσματικές

Ναι, οι Διευθυντές έχουν αναλάβει την εποπτεία για την αποτελεσματικότητα των διορθωτικών ενεργειών.

Συνεπώς, η απαίτηση ικανοποιείται μερικώς.

β) Να προβαίνει τακτικά σε εξέταση της αποτελεσματικότητας του ISMS

(συμπεριλαμβανομένων να ικανοποιείται η ISMS πολιτική και οι στόχοι, και την επανεξέταση των ελέγχων της ασφάλειας) λαμβάνοντας υπόψη τα αποτελέσματα των επιθεωρήσεων ασφάλειας, των συμβάντων, των αποτελεσμάτων από τις μετρήσεις αποτελεσματικότητας, τις προτάσεις και τις πληροφορίες (feedback) από όλα τα ενδιαφερόμενα μέρη

Όχι, ο οργανισμός δεν προβαίνει τακτικά σε εξέταση της αποτελεσματικότητας του συστήματος. Μπορεί να εξετάζει την αποτελεσματικότητα του ISMS μέσω ελέγχων σε επίπεδο διεργασίας, σε επίπεδο «Εσωτερικών Επιθεωρήσεων» και σε επίπεδο «Ανασκοπήσεων» όμως οι έλεγχοι αυτοί δε γίνονται τακτικά και προγραμματισμένα, βάσει μιας καταγεγραμμένης διαδικασίας και δεν καταγράφονται τα ευρήματά τους.
Εφόσον δεν καταγράφονται τα ευρήματα δεν μπορούν να ληφθούν υπόψη.

Συγκεκριμένα, ο οργανισμός,
- δεν λαμβάνει υπόψη σε μια εξέταση του ISMS προηγούμενα ευρήματα.
- δεν λαμβάνει υπόψη τα αποτελέσματα μετρήσεων αποτελεσματικότητας διότι δεν διενεργεί τέτοιες.
- δεν λαμβάνει υπόψη τις «Αναφορές Ασφάλειας».
- λαμβάνει υπόψη μόνο την ανατροφοδότηση (feedback) από τα ενδιαφερόμενα μέρη.

Άρα, η απαίτηση ικανοποιείται μερικώς.

γ) Να μετράει την αποτελεσματικότητα των ελέγχων προκειμένου να επαληθεύσει ότι οι απαιτήσεις ασφάλειας ικανοποιούνται (βλ. 4.2.2.δ)

Όχι, ο οργανισμός δεν μετράει την αποτελεσματικότητα των ελέγχων, αφού όπως προαναφέρθηκε και στο (4.2.2.δ), δεν έχει καθορίσει μια τέτοια μέθοδο μέτρησης.

δ) Να επανεξετάζει τις αξιολογήσεις των κινδύνων σε προγραμματισμένα διαστήματα και να αναθεωρεί τους εναπομείναντες κινδύνους και τα καθορισμένα αποδεκτά επίπεδα κινδύνων, λαμβάνοντας υπόψη τις αλλαγές στα εξής:

1. τον οργανισμό
2. την τεχνολογία
3. τους επιχειρηματικούς στόχους και τις διαδικασίες

4. τις προσδιορισμένες απειλές
5. την αποτελεσματικότητα των ελέγχων που εφαρμόζονται
6. τα εξωτερικά γεγονότα, όπως οι αλλαγές στο νομικό και κανονιστικό περιβάλλον, αλλαγμένες συμβατικές υποχρεώσεις, καθώς και αλλαγές στο κοινωνικό κλίμα

Ναι, οι Διευθυντές σε ετήσια βάση πραγματοποιούν συσκέψεις όπου επανεξετάζουν σε συνεργασία με τη Διοίκηση την αξιολόγηση των κινδύνων λαμβάνοντας υπόψη καινούριες τεχνολογίες και αλλαγές σε νομοθετικές και κανονιστικές απαιτήσεις. Πολλές φορές παρουσιάζονται σε τέτοιες συσκέψεις και αποτελεσματικές βελτιώσεις που έχουν εισάγει αεροδρόμια άλλων κρατών.

ε) Να διενεργεί εσωτερικούς ελέγχους στο ISMS σε προγραμματισμένα διαστήματα (βλ. *Απαίτηση 6*)

Όχι, η απαίτηση αυτή δεν ικανοποιείται. Ο οργανισμός διενεργεί εσωτερικούς ελέγχους στο ISMS, όμως οι έλεγχοι αυτοί δε γίνονται τακτικά και προγραμματισμένα, βάσει μιας καταγεγραμμένης διαδικασίας και δεν καταγράφονται τα ευρήματά τους.

στ) Να προβαίνει σε ανασκόπηση του ISMS σε τακτική βάση για να εξασφαλίσει ότι το αντικείμενο παραμένει επαρκές και ότι οι βελτιώσεις στη διεργασία του ISMS είναι αναγνωρίσιμες (βλ. 7.1)

Όχι, η απαίτηση αυτή δεν ικανοποιείται. Ο οργανισμός διενεργεί ανασκοπήσεις στο ISMS αλλά όχι προγραμματισμένα, βάσει μιας καταγεγραμμένης διαδικασίας και όταν γίνονται τα αποτελέσματα δεν τεκμηριώνονται και δε διατηρούνται σε αρχεία.

ζ) Να ενημερώνει (update) τα σχέδια ασφαλείας για να ληφθεί υπόψη τα ευρήματα των δραστηριοτήτων παρακολούθησης και επανεξέτασης

Ναι, σε περίπτωση όποιων αλλαγών τα σχέδια ασφαλείας ενημερώνονται.

η) Να καταγράφει τις δράσεις και τα γεγονότα που θα μπορούσαν να έχουν αντίκτυπο στην αποτελεσματικότητα ή την εκτέλεση του ISMS (βλ. 4.3.3)

Ναι, τα αποτελέσματα και τα συμπεράσματα από τη διαδικασία εντοπισμού, αξιολόγησης και μείωσης των κινδύνων σε συστήματα και διαδικασίες τεκμηριώνονται.

4.2.4 Συντήρηση και βελτίωση του ISMS

Ο οργανισμός πρέπει τακτικά να κάνει τα εξής :

α) Να εφαρμόζει τις προσδιορισμένες βελτιώσεις στο ISMS

Ναι, όλες οι προτάσεις του προσωπικού καταγράφονται, αξιολογούνται από και όσες από αυτές θεωρούνται ουσιαστικές για τη βελτίωση του ISMS υλοποιούνται. Επίσης, εγκρίνεται η χρήση εξοπλισμού που έχει μελετηθεί ότι θα συντελέσει στη βελτίωση των επιπέδων ασφάλειας πληροφοριών.

β) Να λαμβάνει κατάλληλα διορθωτικά και προληπτικά μέτρα σύμφωνα με το 8.2 και 8.3. Να εφαρμόζει τα διδάγματα που αντλήθηκαν από την εμπειρία στην ασφάλεια των άλλων οργανισμών και από την εμπειρία του ίδιου του οργανισμού

Ναι, ο οργανισμός αναφέρει εγγράφως ότι όλα τα μαθήματα που πηγάζουν από διερευνήσεις συμβάντων και άλλων σχετικών με την ασφάλεια πληροφοριών ζητημάτων εφαρμόζονται. Μερικά τέτοια διδάγματα είναι, για παράδειγμα, η μη αποκάλυψη προσωπικού κωδικού σε συνάδελφο, η επαλήθευση της τελικής πληροφορίας, η διατήρηση αντιγράφων ασφαλείας και άλλα. Τη σύνταξη και αποστολή ενημερωτικού σημειώματος για το συμβάν προς το προσωπικό. Τα ενημερωτικά σημειώματα έχουν ως στόχο τη διασπορά της πληροφορίας για τους παράγοντες που οδήγησαν στο συμβάν ώστε να διδαχτούν από αυτό και να μην επαναληφτεί.

γ) Να κοινοποιεί τις δράσεις και τις βελτιώσεις σε όλα τα ενδιαφερόμενα μέρη με ένα επίπεδο λεπτομέρειας ανάλογο με τις περιστάσεις και, κατά περίπτωση, να συμφωνούν για το πώς θα προχωρήσουν

Ναι, ο οργανισμός αναφέρει εγγράφως ότι οι δράσεις και οι βελτιώσεις διαδίδονται ευρέως στον οργανισμό μέσω της «Αυτοματοποιημένης διασποράς των πληροφοριών για συμβάντα», όπου ενδιαφέρον έχουν οι πληροφορίες για το συμβάν και όχι για τους συμμετέχοντες. Η διασπορά των πληροφοριών γίνεται με :

- προγραμματισμένες συγκεντρώσεις ομάδων εργασίας σε χώρους που έχουν ανακύψει ζητήματα ασφάλειας πληροφοριών

- με την έκδοση ενημερωτικών σημειωμάτων ασφάλειας πληροφοριών σε περιπτώσεις συμβάντων, για την ενημέρωση του προσωπικού για το είδος του συμβάντος, τα αίτια που το προκάλεσαν και τα διορθωτικά μέτρα που έχουν ληφθεί για τη μη επανάληψή του.

δ) Να διασφαλίζει ότι οι βελτιώσεις επιτυγχάνουν τους στόχους που ήθελαν

Ναι, γίνεται επαλήθευση των ενεργειών που ανελήφθησαν από τον ίδιο τον Διευθυντή που τις πραγματοποίησε. Δεν καταγράφεται όμως η επαλήθευση αυτή σε κάποιο έντυπο ούτως ώστε και να αποδεικνύεται. Συνεπώς, η απαίτηση ικανοποιείται μερικώς.

4.3 Απαιτήσεις τεκμηρίωσης

4.3.1 Γενικά

Η τεκμηρίωση πρέπει να περιλαμβάνει πρακτικά των αποφάσεων της Διοίκησης, να εξασφαλίζει ότι οι δράσεις είναι σύμφωνες με τις αποφάσεις και τις πολιτικές της διοίκησης, και να διασφαλίσει ότι τα καταγεγραμμένα αποτελέσματα είναι αναπαράξιμα.

Είναι σημαντικό να είναι σε θέση να αποδείξει τη σχέση μεταξύ των επιλεγμένων ελέγχων και των αποτελεσμάτων της αξιολόγησης του κινδύνου και της διαδικασίας θεράπευσης του κινδύνου, και στη συνέχεια, με την πολιτική και τους στόχους του ISMS.

Η τεκμηρίωση του ISMS πρέπει να περιλαμβάνει:

α) τεκμηριωμένες δηλώσεις της πολιτικής (βλ. 4.2.1β) και των στόχων του ISMS
β) το πεδίο εφαρμογής του ISMS (βλ. 4.2.1α)
γ) τις διαδικασίες και τους ελέγχους για την υποστήριξη του ISMS
δ) περιγραφή της μεθοδολογίας αξιολόγησης κινδύνου (βλ. 4.2.1ζ)
ε) την έκθεση αξιολόγησης των κινδύνων (βλ. 4.2.1γεως 4.2.1ζ)
στ) το σχέδιο θεράπευσης κινδύνου (βλ. 4.2.2β)
ζ) τις τεκμηριωμένες διαδικασίες που απαιτούνται από τον οργανισμό προκειμένου να διασφαλίζει τον αποτελεσματικό σχεδιασμό, λειτουργία και έλεγχο των διαδικασιών του για την ασφάλεια των πληροφοριών και να περιγράψει τον τρόπο μέτρησης της αποτελεσματικότητας των ελέγχων (βλ. 4.2.3γ)
η) τα αρχεία που απαιτούνται από το προκείμενο Διεθνές Πρότυπο (βλ. 4.3.3) και
i) τη Δήλωση Εφαρμοσιμότητας

Ναι, ο οργανισμός διαθέτει ένα «Εγχειρίδιο Διαχείρισης της Ασφάλειας Αεροναυτικών Πληροφοριών», το οποίο τεκμηριώνει το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών, περιγράφοντας όλα τα παραπάνω και είναι υπογεγραμμένο από τη Διοίκηση. Το Εγχειρίδιο ανασκοπείται μία φορά κάθε χρόνο με ευθύνη της Διοίκησης.

4.3.2 Έλεγχος Εγγράφων

Έγγραφα που απαιτούνται από το ISMS πρέπει να προστατεύονται και να ελέγχονται. Μια τεκμηριωμένη διαδικασία πρέπει να καθιερωθεί προκειμένου να καθορίσει τις

ενέργειες της Διοίκησης που απαιτούνται για να:

α) εγκρίνει τα έγγραφα ως προς την επάρκειά τους πριν από την έκδοση
β) διασφαλίζει την επανεξέταση και ενημέρωση των εγγράφων όπου κρίνεται αναγκαία και την επανέγκριση των εγγράφων
γ) διασφαλίσει ότι οι αλλαγές και η τρέχουσα έκδοση των εγγράφων έχουν προσδιοριστεί
δ) εξασφαλίζει ότι οι σχετικές εκδόσεις των εγγράφων που χρησιμοποιούνται είναι διαθέσιμα σε σημεία χρήσης
ε) εξασφαλίζει ότι τα έγγραφα παραμένουν ευανάγνωστα και ευκόλως εντοπίσιμα
στ) εξασφαλίζει ότι τα έγγραφα είναι διαθέσιμα σε εκείνους που τα χρειάζονται, και να μεταφέρονται, να αποθηκεύονται και εν τέλει να διατίθενται σύμφωνα με τις διαδικασίες που εφαρμόζονται για την ταξινόμησή τους
ζ) εξασφαλίζει ότι τα έγγραφα εξωτερικής προέλευσης είναι εντοπίσιμα
η) εξασφαλίζει ότι η διανομή των εγγράφων ελέγχεται
θ) να αποτρέπει την ακούσια χρήση απαρχαιωμένων εγγράφων και
ι) να εφαρμόζει τον κατάλληλο προσδιορισμό σε αυτά, εφόσον διατηρούνται για οιονδήποτε σκοπό

Ναι, ο οργανισμός διαθέτει μια τεκμηριωμένη διαδικασία για τα παραπάνω.

4.3.3 Έλεγχος Αρχείων

Τα αρχεία πρέπει να τηρούνται και να διατηρούνται προκειμένου να παρέχουν αποδεικτικά στοιχεία για τη συμμόρφωση προς τις απαιτήσεις και την αποτελεσματική λειτουργία του ISMS. Τα αρχεία πρέπει να προστατεύονται και να ελέγχονται. Το ISMS πρέπει να λαμβάνει υπόψη τυχόν σχετικές νομικές και κανονιστικές απαιτήσεις και τις συμβατικές υποχρεώσεις. Τα αρχεία πρέπει να παραμένουν ευανάγνωστα, ευκόλως αναγνωρίσιμα και ανακτήσιμα.

Πολιτική του οργανισμού είναι να τηρούνται αρχεία με τη μορφή Φακέλων, που διατηρούνται, κατατάσσονται, προστατεύονται και είναι προσπελάσιμα στο αρμόδιο εξουσιοδοτημένο προσωπικό.

Στις Διευθύνσεις που είναι αρμόδιες για την παροχή αεροναυτικών πληροφοριών τα Έγγραφα που έχουν χρησιμοποιηθεί τοποθετούνται σε Φακέλους και κατόπιν οι Φάκελοι σε Αρχειοθήκες.

Οι Διευθυντές των εμπλεκόμενων Διευθύνσεων είναι υπεύθυνοι και για τη τήρηση των παρακάτω Αρχείων Ασφαλείας με τη μορφή Φακέλων :

- Φάκελοι διαδικασιών εντοπισμού, αξιολόγησης και μείωσης Κινδύνων
- Φάκελοι αναφορών ασφαλείας
- Φάκελοι ανάλυσης ενδεχόμενων κινδύνων
- Φάκελοι εκπαιδεύσεων

Οι έλεγχοι που απαιτούνται για την αναγνώριση, την αποθήκευση, προστασία, ανάκτηση, τον χρόνο διατήρησης και τη διάθεση των αρχείων πρέπει να είναι τεκμηριωμένοι και να εφαρμόζονται.

Όχι, δεν γίνεται επιβεβαίωση της τεκμηρίωσης.

Αρχεία πρέπει να φυλάσσονται σχετικά με την απόδοση της διαδικασίας όπως περιγράφεται στο (4.2) καθώς και για όλα τα σημαντικά γεγονότα της ασφάλειας που σχετίζονται με το ISMS.

Πράγματι, τα αποτελέσματα και τα συμπεράσματα από τη διαδικασία εντοπισμού, αξιολόγησης και μείωσης των κινδύνων σε συστήματα και διαδικασίες τεκμηριώνονται και διατηρούνται για όλη τη διάρκεια ζωής του συστήματος με σκοπό να παρέχουν επιχειρήματα και αποδείξεις ότι το σύστημα πληροί τις απαιτούμενες προδιαγραφές ασφαλείας.
Η τεκμηρίωση αποτελεί απόδειξη ότι οι κίνδυνοι έχουν αναγνωριστεί, αξιολογηθεί και αντιμετωπιστεί και ότι έχουν επιτευχθεί τα επιθυμητά επίπεδα ασφάλειας πληροφοριών.

Δεν υφίσταται όμως τεκμηρίωση των διορθωτικών και προληπτικών ενεργειών που λαμβάνονται. Δεν υπάρχει σχετικό έντυπο, άρα δεν τηρείται και αντίστοιχο αρχείο.

Συνεπώς, η απαίτηση ικανοποιείται μερικώς.

5.2.1. Προτάσεις

Ο οργανισμός προκειμένου να ικανοποιεί τις απαιτήσεις του προτύπου πρέπει να καθιερώσει μια μέθοδο μέτρησης της αποτελεσματικότητας των ελέγχων που εφαρμόζει. Η εν λόγω μέτρηση θα επιτρέπει στη Διοίκηση και στο προσωπικό να αποφασίζει πόσο καλά οι έλεγχοι επιτυγχάνουν τους προκαθορισμένους στόχους ελέγχων που έχουν τεθεί.

Μια τέτοια μέθοδος μέτρησης θα μπορούσε να είναι η χρήση δεικτών. Για παράδειγμα :

Επίπεδο Αποτελεσματικότητας	% εντοπισμένων μη-συμμορφώσεων
(Υψηλή) 5	90-100 % των μη-συμμορφώσεων
4	70-90 % των μη-συμμορφώσεων
3	50-70 %των μη-συμμορφώσεων
2	30-50 % των μη-συμμορφώσεων
(Χαμηλή) 1	0-30 % των μη-συμμορφώσεων

Επίσης, ο οργανισμός πρέπει σύμφωνα με το πρότυπο μετά την υλοποίηση του σχεδιασμού του συστήματος να καθιερώσει μια τεκμηριωμένη διαδικασία αξιολόγησης της ασφάλειάς του. Συγκεκριμένα, οφείλει να παρακολουθεί τις διαδικασίες και τους ελέγχους που εφαρμόζει προκειμένου να επιβεβαιώσει ότι το σύστημα λειτουργεί, ικανοποιώντας την πολιτική ασφάλειας πληροφοριών, τους προδιαγεγραμμένους στόχους και απαιτήσεις.

Η αξιολόγηση αυτή πρέπει να είναι μια συνεχής διαδικασία η οποία θα εκτελείται κατά τη διάρκεια της υλοποίησης του συστήματος και θα συνεχίζεται να εκτελείται ανά τακτά χρονικά διαστήματα σε όλη τη διάρκεια ζωής του και θα σταματά μόνο μετά την απόσυρση ή την αντικατάστασή του.

Εναλλακτικά, θα μπορούσε να συσταθεί μια «Διεύθυνση Ασφάλειας Πληροφοριών» και την ευθύνη για τη συνεχή εποπτεία της ασφάλειας σε όλο το φάσμα των δραστηριοτήτων του παρόχου αεροναυτικών πληροφοριών να έχει ο «Υπεύθυνος Ασφάλειας Πληροφοριών», ο οποίος θα πρέπει μεταξύ άλλων :

- να μπορεί να ανιχνεύει αλλαγές, σε διαδικασίες ή συστήματα, τέτοιας μορφής που θα μπορούσαν να απειλήσουν τα επιθυμητά επίπεδα ασφαλείας.

- να αναλύει τις ενδεχόμενες τάσεις για συμβάντα και να προτείνει διορθωτικά μέτρα στους Διευθυντές των μονάδων και στη Διοίκηση.

Μία μέθοδος για την αποτελεσματική λειτουργία της εποπτείας ασφαλείας θα μπορούσε να είναι η εκπόνηση τυχαίων ελέγχων από τον «Υπεύθυνο Ασφάλειας Πληροφοριών» σε

κανονικές συνθήκες εργασίας στις εμπλεκόμενες Διευθύνσεις και στα αντίστοιχα Τμήματά τους.

Οι πληροφορίες που θα συλλέγονται δεν θα έχουν στόχο την αποκάλυψη συμβάντων που δεν έχουν αναφερθεί ή αξιολόγηση της επάρκειας του προσωπικού, αλλά τον εντοπισμό και στη συνέχεια την αποτελεσματική διαχείριση των απειλών και των λαθών που πιθανόν να οδηγούσαν σε συμβάν. Ο «Υπεύθυνος Ασφάλειας Πληροφοριών» θα μπορεί έπειτα να αξιοποιεί τα στοιχεία που θα έχουν συγκεντρωθεί για στατιστικές αναλύσεις.

Εφόσον ο οργανισμός καθιερώσει μέθοδο μέτρησης της αποτελεσματικότητας των ελέγχων και διαδικασία αξιολόγησης του συστήματος, τότε η Διοίκηση θα πρέπει κατά το πρότυπο να επανεξετάζει την αποτελεσματικότητα του συστήματος λαμβάνοντας υπόψη τα αποτελέσματα των παραπάνω μετρήσεων καθώς και των εσωτερικών επιθεωρήσεων ως εισερχόμενα στην ανασκόπησή της..

Όσον αφορά τη συντήρηση και βελτίωση του συστήματος, ο οργανισμός οφείλει να διασφαλίζει ότι οι βελτιώσεις επιτυγχάνουν τους στόχους που είχαν τεθεί. Ένας τρόπος θα ήταν να καθορίζει ο οργανισμός σε ετήσια βάση στόχους για τη βελτίωση των επιπέδων ασφάλειας πληροφοριών σε συνδυασμό με ένα σύστημα υποχρεωτικών αναφορών περιστατικών, που θα αφορούν τη διαχείριση αεροναυτικών πληροφοριών, με σκοπό την καταγραφή μεγάλου όγκου συμβάντων έχοντας σαν δείκτες απόδοσης τον αριθμό των αναφερόμενων περιστατικών.

Τέλος, ο οργανισμός οφείλει να ικανοποιεί την απαίτηση του προτύπου για ύπαρξη τεκμηρίωσης και επιβεβαίωσης αυτής. Την ευθύνη επιβεβαίωσης της τεκμηρίωσης για τα Αρχεία που τηρούν οι Διευθύνσεις καλύτερο θα ήταν να έχει ο «Υπεύθυνος Ασφάλειας Πληροφοριών», ενώ για τα Αρχεία Ασφαλείας που θα τηρεί ο ίδιος ευθύνη επιβεβαίωσης να έχει η Διοίκηση.

Συγκεκριμένα, ο Υπεύθυνος Ασφάλειας Πληροφοριών να είναι υπεύθυνος για τη τήρηση των παρακάτω Αρχείων Ασφαλείας με τη μορφή Φακέλων :

- Φάκελοι συμβάντων
- Φάκελοι διαδικασιών εντοπισμού, αξιολόγησης και μείωσης Κινδύνων
- Φάκελοι αναφορών ασφαλείας
- Φάκελοι ανάλυσης ενδεχόμενων κινδύνων
- Φάκελοι εκπαιδεύσεων
- Φάκελοι Επιθεωρήσεων (να προστεθούν) &Φάκελοι Ανασκοπήσεων(να προστεθούν)

5.3. Ευθύνη της Διοίκησης

5.3.1. Εφαρμογή Απαιτήσεων

Απαίτηση 5

ΕΥΘΥΝΗ ΤΗΣ ΔΙΟΙΚΗΣΗΣ

5.1 Δέσμευση Διοίκησης

Η διοίκηση οφείλει να αποδείξει τη δέσμευσή της για το σχεδιασμό, την υλοποίηση, τον έλεγχο, τη συντήρηση και βελτίωση του ISMS με τον εξής τρόπο :

α) θεσπίζοντας μιας πολιτική ISMS

Ναι, η Διοίκηση αποδεικνύει τη δέσμευσή της για το σχεδιασμό του συστήματος, έχοντας θεσπίσει και υπογράψει μια πολιτική ISMS η οποία εξασφαλίζει μια επίσημη και σαφή προσέγγιση του οργανισμού στον συγκεκριμένο τομέα της διαχείρισης της ασφάλειας πληροφοριών με βάση τις εγχώριες και διεθνείς απαιτήσεις ασφαλείας.

β) εξασφαλίζοντας ότι οι στόχοι και τα σχέδια του ISMS έχουν καθιερωθεί

Ναι, η Διοίκηση του οργανισμού δείχνει τη δέσμευσή της για το σχεδιασμό του συστήματος έχοντας εξασφαλίσει ότι οι στόχοι του ISMS έχουν καθιερωθεί και τεκμηριωθεί στη «Δήλωση Εφαρμοσιμότητας» του οργανισμού.

γ) θεσπίζοντας ρόλους και αρμοδιότητες για την ασφάλεια των πληροφοριών

Η Διοίκηση αναφέρει γραπτώς ότι όλοι όσοι ασχολούνται με θέματα ασφάλειας πληροφοριών στην παροχή αεροναυτικών πληροφοριών έχουν ατομική ευθύνη για τις πράξεις τους, ότι οι διευθυντές έχουν ευθύνη για τις επιδόσεις ασφαλείας των τμημάτων τους και ότι η ανώτατη διοίκηση φέρει συλλογική ευθύνη για την ασφάλεια πληροφοριών.

Δεν έχει όμως θεσπίσει συγκεκριμένους ρόλους για να εξασφαλίσει τη συστηματική διαχείριση της ασφάλειας πληροφοριών, όπως έναν «Υπεύθυνο Ασφάλειας Πληροφοριών».

Συγκεκριμένα, την ευθύνη διαχείρισης ζητημάτων που αφορούν την ασφάλεια των πληροφοριών έχουν αναλάβει οι Διευθυντές των Διευθύνσεων που εμπλέκονται στη διεργασία έκδοσης και ενημέρωσης του Εγχειριδίου AIP.

Οι Διευθυντές έχουν αναλάβει τα ακόλουθα :

- Εκπόνηση διαδικασίας εντοπισμού, αξιολόγησης και μείωσης κινδύνων
- Η εποπτεία για την αποτελεσματικότητα των ληφθέντων διορθωτικών μέτρων
- Έκδοση αναφορών ασφαλείας όταν διαταράσσονται τα επιθυμητά επίπεδα ασφάλειας
- Καθορισμός ελέγχων και στόχων ελέγχων
- Υποβολή προτάσεων στη διοίκηση για εκπαίδευση προσωπικού σε θέματα διαχείρισης της ασφάλειας πληροφοριών ή για προμήθεια νέων συστημάτων εξοπλισμού σε σχέση με την ασφάλεια
- Ενθάρρυνση προσωπικού για την υποβολή προτάσεων που θα συμβάλλουν στη βελτίωση των επιπέδων ασφαλείας και αξιολόγηση αυτών των προτάσεων

Συνεπώς, η Διοίκηση αποδεικνύει μερικώς τη δέσμευσή της όσον αφορά την υλοποίηση του συστήματος.

δ) επικοινωνώντας στον οργανισμό τη σημασία της επίτευξης των στόχων της ασφάλειας των πληροφοριών και της συμμόρφωσης με την πολιτική ασφάλειας των πληροφοριών, τις αρμοδιότητές της σύμφωνα με τη νομοθεσία και την ανάγκη για συνεχή βελτίωση

Ναι, η Διοίκηση έχει εδραιώσει μια «Νοοτροπία Ασφάλειας Πληροφοριών». Η οποία είναι κάτι περισσότερο από την μηχανικά πιστή εφαρμογή κανονισμών και διαδικασιών. Είναι το σύνολο εκείνο των αρχών και των νοοτροπιών του προσωπικού που αποδεικνύει ότι η ασφάλεια των πληροφοριών είναι η πρώτη προτεραιότητα σε όλο το φάσμα δραστηριοτήτων του οργανισμού.

Το σύνολο του προσωπικού ενθαρρύνεται στην :

- Υποβολή εθελουσίων αναφορών σε περιπτώσεις συμβάντων
- Επώνυμη υποβολή προτάσεων για τη διατήρηση ή βελτίωση των αποδεκτών επιπέδων ασφαλείας.

ε) παρέχοντας επαρκής πόρους για τη δημιουργία, υλοποίηση, λειτουργία,

παρακολούθηση, έλεγχο, διατήρηση και βελτίωση του ISMS (βλ. 5.2.1)

Ναι, η Διοίκηση εγκρίνει τις μελέτες για παροχή εξοπλισμού αλλά και για την εκπαίδευση του προσωπικού.

στ) αποφασίζοντας τα κριτήρια για την αποδοχή των κινδύνων και των αποδεκτών επιπέδων κινδύνου

Ναι, η Διοίκηση αναφέρει ρητά ότι τα κριτήρια για την αποδοχή των κινδύνων είναι η σοβαρότητα και η πιθανότητα εμφάνισης τους.

Επίσης, τα αποδεκτά επίπεδα κινδύνου είναι μικροί κίνδυνοι και πολύ μεγάλοι κίνδυνοι, που έχουν όμως πολύ μικρή πιθανότητα να συμβούν.

ζ) διασφαλίζοντας ότι οι εσωτερικοί έλεγχοι του ISMS διεξάγονται (βλ. *Απαίτηση 6*) και

Όχι, η Διοίκηση δεν αποδεικνύει τη δέσμευσή της για τον έλεγχο του ISMS. Ειδικότερα, δεν έχει καθιερώσει ένα «Πρόγραμμα Εσωτερικών Επιθεωρήσεων», ούτε έχει εξασφαλίσει την ύπαρξη μιας τεκμηριωμένης διαδικασίας διεξαγωγής αυτών των επιθεωρήσεων.

η) διεξάγοντας η διοίκηση ανασκοπήσεις του ISMS (βλ.*Απαίτηση 7*)

Όχι. η Διοίκηση δεν αποδεικνύει τη δέσμευσή της για τον έλεγχο του ISMS μέσω των ανασκοπήσεων. Η Διοίκηση δεν έχει καθιερώσει μια τεκμηριωμένη διαδικασία διεξαγωγής τακτικών και προγραμματισμένων ανασκοπήσεων.

5.2 Διαχείριση των πόρων

5.2.1 Παροχή των πόρων

Ο οργανισμός πρέπει να προσδιορίζει και να παρέχει τους πόρους που απαιτούνται για:

α) να καθιερώσει, εφαρμόσει, λειτουργήσει, παρακολουθήσει, ελέγξει, διατηρήσει και βελτιώσει ένα ISMS

β) να διασφαλίσει ότι οι διαδικασίες ασφάλειας των πληροφοριών υποστηρίζουν τις επιχειρηματικές απαιτήσεις

γ) να εντοπίζει και να αντιμετωπίζει τις νομικές και κανονιστικές απαιτήσεις ασφάλειας και τις συμβατικών υποχρεώσεις

δ) να διατηρεί την απαιτούμενη ασφάλεια με την ορθή εφαρμογή όλων των εγκατεστημένων ελέγχων

ε) να προβαίνει σε ανασκοπήσεις όταν κρίνεται αναγκαίο, και να αντιδρά αναλόγως με τα αποτελέσματα αυτών, και

στ) όπου απαιτείται, να βελτιώνει την αποτελεσματικότητα του ISMS

Ναι, ο οργανισμός έχει προσδιορίσει τους πόρους που απαιτούνται στη διεργασία έκδοσης και διανομής του «Εγχειριδίου Αεροναυτικών Πληροφοριών– AIP», ούτως ώστε να πληρούνται οι παραπάνω απαιτήσεις του προτύπου.

Συγκεκριμένα, για την ταχεία παροχή ακριβή αεροναυτικών πληροφοριών ο οργανισμός παρέχει τους εξής πόρους :

1.υψηλά εξειδικευμένο και ικανό προσωπικό

Έχει προσδιορίσει σε έναν πίνακα τον ελάχιστο αριθμό εξειδικευμένων υπαλλήλων που χρειάζεται κάθε εμπλεκόμενη στη διεργασία έκδοσης και διανομής του «Εγχειριδίου Αεροναυτικών Πληροφοριών– AIP» Διεύθυνση και φροντίζει για τη συνεχή πληρότητα σε ανθρώπινο δυναμικό.

2. κατάλληλες υποδομές

Έχει προσδιορίσει σε έναν πίνακα τις ελάχιστες απαιτήσεις για εγκαταστάσεις κάθε εμπλεκόμενης στη διεργασία έκδοσης και διανομής του «Εγχειριδίου Αεροναυτικών Πληροφοριών– AIP» Διεύθυνσης και φροντίζει για την ύπαρξη και συντήρηση αυτών των εγκαταστάσεων.

3. απαραίτητος εξοπλισμός

Εκτός από το βασικό εξοπλισμό γραφείου και τις γραφικές πρώτες ύλες, η Διοίκηση παρέχει στους εμπλεκομένους της βασικής διεργασίας τον ακόλουθο εξοπλισμό :

- Προσωπικοί ηλεκτρονικοί υπολογιστές σε κάθε θέση (τερματικό πελάτης-Client)
- Εκτυπωτές
- Σύνδεση στο διαδίκτυο
- Τηλέφωνα
- Φωτοτυπικό μηχάνημα ειδικό και για έγγραφα Εγχειριδίου Αεροναυτικών Πληροφοριών-AIP
- Ηλεκτρονικός σαρωτής (scanner)
- Τηλεαντιγραφικό μηχάνημα (telefax)

- Αξιόπιστο Ρολόι που να δείχνει την τοπική ώρα
- Ρολόι « time-stamp», σε ώρα Γκρίνουιτς και σε τοπική ώρα

4. χρήση αυτοματοποίησης (ηλεκτρονική εφαρμογή eAIP.wiz@rd)

Η Διοίκηση παρέχει στη Διεύθυνση Αεροναυτικών Εκδόσεων (Ε1) και συγκεκριμένα στο Τμήμα Εγχειριδίων Αεροναυτικών Πληροφοριών AIP (Ε1/Α) την ηλεκτρονική εφαρμογή, eAIP.wiz@rd. Με την πρόθεση να αυτοματοποιηθούν οι απαιτήσεις της Διεθνούς Συμβάσεως του Διεθνούς Οργανισμού Πολιτικής Αεροπορίας ICAO, να υπάρχει μεγαλύτερος έλεγχος και κατά συνέπεια να παρέχεται μια πιο αποτελεσματική και ποιοτική υπηρεσία στους συνδρομητές του Εγχειριδίου.

5.2.2 Εκπαίδευση, ευαισθητοποίηση και ικανότητα

Ο οργανισμός να εξασφαλίζει ότι το σύνολο του προσωπικού, στο οποίο έχουν ανατεθεί αρμοδιότητες που ορίζονται στο ISMS, είναι ικανό για την εκτέλεση των απαιτούμενων καθηκόντων με το να :

α) προσδιορίζει την απαραίτητη ικανότητα που πρέπει να διαθέτει το προσωπικό που εκτελεί εργασίες που επηρεάζουν το ISMS

Ναι, ο οργανισμός προσδιορίζει εγγράφως τα απαραίτητα προσόντα που πρέπει να διαθέτει το προσωπικό προκειμένου να καταφέρουν να υλοποιήσουν και να διατηρήσουν ένα Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ISMS). Συγκεκριμένα :

- *Κουλτούρα Ασφάλειας*, για να μπορέσουν να τη μεταφέρουν σε όλο το φάσμα του οργανισμού
- *Προνοητικότητα*, ώστε να προβλέπουν τι θα μπορούσε να συμβεί και να ενεργούν με τέτοιο τρόπο ώστε να αποφεύγεται ή να μειώνεται η πιθανότητα. Πρέπει να έχουν πίστη ότι τα συμβάντα μπορούν να αποφευχθούν
- *Δημιουργικότητα*, ώστε να αναγνωρίζουν απειλές και κινδύνους καθώς επίσης να βρίσκουν τρόπους για την αντιμετώπισή τους
- *Υπευθυνότητα*, σε θέματα ασφάλειας πληροφοριών
- *Εμπειρία*, στη διαχείριση αεροναυτικών πληροφοριών

β) παρέχει κατάρτιση ή να λαμβάνει άλλες ενέργειες (π.χ. πρόσληψη ικανού προσωπικού) για την ικανοποίηση αυτών των αναγκών

Ναι, δίνεται ιδιαίτερη έμφαση στην εκπαίδευση για καθήκοντα που αφορούν την ασφάλεια πληροφοριών. Έχει τεθεί μία κοινή βάση για το βάθος και το εύρος των γνώσεων, των δεξιοτήτων και τη συμπεριφορά που πρέπει να τηρείται από όλους τους υπαλλήλους που εμπλέκονται στη διεργασία έκδοσης και ενημέρωσης του Εγχειριδίου.

Το Έγγραφο 7192, Μέρος 3 «Εγχειρίδιο Κατάρτισης», περιλαμβάνει αναλυτικό πρόγραμμα κατάρτισης και παρέχει οδηγίες στα Κράτη για την προετοιμασία των αντίστοιχων προγραμμάτων σπουδών που θα χρησιμοποιηθούν σε μαθήματα για την κατάρτιση των υπαλλήλων.

Επίσης, πραγματοποιούνται εκπαιδευτικά σεμινάρια τόσο στην Ελλάδα όσο και στο εξωτερικό σε αντίστοιχα Συστήματα Διαχείρισης Ασφάλειας Αεροναυτικών Πληροφοριών. Την ευθύνη για την εκπαίδευση έχει η Διεύθυνση Εκπαίδευσης.

Όσον αφορά την πρόληψη ικανού προσωπικού την ευθύνη έχει ο ίδιος ο οργανισμός με τις διαδικασίες που ορίζουν οι νόμοι για προσλήψεις υπαλλήλων του Δημοσίου.

γ) να αξιολογεί την αποτελεσματικότητα των ενεργειών που έγιναν (κατάρτιση) και

Ναι, η Διεύθυνση Εκπαίδευσης (Δ14) του οργανισμού αξιολογεί την αποτελεσματικότητα της κατάρτισης μέσω διαφόρων μεθόδων πχ ερωτηματολογίων.

δ) να τηρεί αρχεία της εκπαίδευσης, της κατάρτισης, των δεξιοτήτων, της εμπειρίας και των προσόντων (βλ. 4.3.3)

Ναι, ο οργανισμός τεκμηριώνει ότι το σύνολο του προσωπικού διαθέτει την κατάλληλη εμπειρία και τα απαραίτητα προσόντα σχετικά με τα συγκεκριμένα καθήκοντα που αναλαμβάνει. Τηρούνται φάκελοι εκπαιδεύσεων καθώς και αρχεία με τα βιογραφικά του προσωπικού.

Ο οργανισμός πρέπει επίσης να διασφαλίσει ότι όλο το εμπλεκόμενο προσωπικό γνωρίζει τη σημασία των δραστηριοτήτων ασφάλειας των πληροφοριών και τον τρόπο με τον οποίο οι δραστηριότητες αυτές συμβάλλουν στην επίτευξη των στόχων του ISMS.

Ναι, η απαίτηση αυτή του προτύπου ικανοποιείται. Την ευθύνη επιβεβαίωσης ότι το σύνολο του εμπλεκόμενου προσωπικού έχει επίγνωση για όλες τις σχετικά με την ασφάλεια πληροφοριών αρμοδιότητές του σε σχέση με τη γενικότερη πολιτική για την ασφάλεια πληροφοριών έχουν οι Διευθυντές των εμπλεκομένων Διευθύνσεων στη διεργασία έκδοσης και ενημέρωσης του AIP.

5.3.2. Προτάσεις

Η Διοίκηση του οργανισμού σύμφωνα με το πρότυπο πρέπει να αποδεικνύει τη δέσμευσή της εξασφαλίζοντας ότι οι στόχοι του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ISMS) έχουν καθιερωθεί. Αυτό θα μπορούσε να το πετύχει καθορίζοντας σε ετήσια βάση στόχους για τη βελτίωση των επιπέδων ασφάλειας πληροφοριών (Safety Targets).

Επίσης, πρέπει να αποδεικνύει τη δέσμευσή της θεσπίζοντας ρόλους και αρμοδιότητες για την ασφάλεια των πληροφοριών. Προκειμένου, λοιπόν, η Διοίκηση να ικανοποιεί την απαίτηση αυτή του προτύπου θα μπορούσε να προβεί στη σύσταση μιας Διεύθυνσης Ασφάλειας Πληροφοριών η οποία θα είναι αρμόδια για τη συστηματική διαχείριση της ασφάλειας πληροφοριών.

Η Διοίκηση πρέπει να θεσπίσει συγκεκριμένους ρόλους. Την ευθύνη διαχείρισης ζητημάτων που αφορούν την ασφάλεια των πληροφοριών να έχει ο Υπεύθυνος Ασφάλειας Πληροφοριών (Information Safety Manager).

Επίσης, να αναθέσει σε αυτόν συγκεκριμένες αρμοδιότητες :

- Την προώθηση της πολιτικής της ασφάλειας πληροφοριών
- Εκπόνηση διαδικασίας εντοπισμού, αξιολόγησης και μείωσης κινδύνων
- Συνεργασία με όλους τους εμπλεκομένους για ζητήματα που ανακύπτουν στις περιοχές ευθύνης τους και για λήψη διορθωτικών μέτρων ή διενέργεια αλλαγών σε υφιστάμενες διαδικασίες
- Η εποπτεία για την αποτελεσματικότητα των ληφθέντων διορθωτικών μέτρων
- Έκδοση αναφορών ασφαλείας όταν διαταράσσονται τα επιθυμητά επίπεδα ασφάλειας
- Καθορισμός ελέγχων και στόχων ελέγχων
- Σύνταξη «Προγραμμάτων Εσωτερικών Επιθεωρήσεων» και διενέργεια Εσωτερικών Επιθεωρήσεων
- Ανασκόπηση στοιχείων που προκύπτουν από συμβάντα και επιθεωρήσεις, ώστε να διαπιστωθεί η αποτελεσματικότητα των ελέγχων στη βελτίωση των επιπέδων ασφάλειας
- Λειτουργία ως ανεξάρτητου συμβούλου στους Διευθυντές των μονάδων
- Υποβολή προτάσεων στη διοίκηση για εκπαίδευση προσωπικού σε θέματα διαχείρισης της ασφάλειας πληροφοριών ή για προμήθεια νέων συστημάτων εξοπλισμού σε σχέση με την ασφάλεια
- Ενθάρρυνση προσωπικού για την υποβολή προτάσεων που θα συμβάλλουν στη βελτίωση των επιπέδων ασφαλείας και αξιολόγηση αυτών των προτάσεων

Τέλος, σύμφωνα με τις απαιτήσεις του προτύπου, η Διοίκηση πρέπει να δείχνει τη δέσμευσή της διασφαλίζοντας ότι οι εσωτερικοί έλεγχοι αλλά και οι ανασκοπήσεις του

συστήματος διεξάγονται. Αυτή η απαίτηση μπορεί να ικανοποιηθεί με το να εγκρίνει το «Πρόγραμμα Εσωτερικών Επιθεωρήσεων» που θα έχει προηγουμένως συντάξει ο Υπεύθυνος Ασφάλειας Πληροφοριών και πραγματοποιώντας ανασκόπηση των στοιχείων που θα προκύπτουν από συμβάντα και επιθεωρήσεις ασφαλείας

ΣΧΕΔΙΟ ΘΕΡΑΠΕΥΣΗΣ ΚΙΝΔΥΝΟΥ

Στο «Σχέδιο Θεράπευσης Κινδύνου» αναφέρεται ότι όταν προκύψει κάποια μη συμμόρφωση με τις απαιτήσεις του προτύπου, η οποία ενδέχεται να καταλήξει σε συμβάν ασφάλειας πληροφοριών, λαμβάνονται άμεσα μέτρα, συμπληρώνεται μια «Αναφορά Ασφαλείας» και ξεκινά η ανάλυση από τους Διευθυντές των μονάδων που έλαβε χώρα.

Μια πρόταση είναι εφόσον θα έχει συσταθεί «Διεύθυνση Ασφάλειας Πληροφοριών» η ανάλυση να γίνεται συγκεντρωτικά από τον «Υπεύθυνο Ασφάλειας Πληροφοριών» και όχι μεμονωμένα από την κάθε Διεύθυνση ξεχωριστά. Ο οργανισμός με αυτόν τον τρόπο θα αντιμετωπίζεται ως σύνολο και όχι ως ξεχωριστές μονάδες.

Τέλος, οι Διορθωτικές και Προληπτικές ενέργειες δεν πρέπει μόνο να λαμβάνονται αλλά και να παρακολουθούνται ως προς την αποτελεσματικότητά τους.

5.4. Εσωτερικές Επιθεωρήσεις του ISMS

5.4.1. *Εφαρμογή Απαιτήσεων*

Απαίτηση 6

ΕΣΩΤΕΡΙΚΕΣ ΕΠΙΘΕΩΡΗΣΕΙΣ ΤΟΥ ISMS

Ο οργανισμός πρέπει να διενεργεί εσωτερικούς ελέγχους στο ISMS σε προγραμματισμένα διαστήματα για να αποφασίζει εάν οι στόχοι των ελέγχων, οι έλεγχοι, οι διεργασίες και οι διαδικασίες του ISMS:

i. συμμορφώνονται με τις απαιτήσεις του παρόντος διεθνούς προτύπου και τη σχετική νομοθεσία ή κανονισμούς
ii. συμμορφώνονται με τις προσδιορισμένες απαιτήσεις ασφάλειας των πληροφοριών
iii. εφαρμόζονται αποτελεσματικά και να διατηρούνται και
iv. εκτελούνται όπως αναμένεται

Όχι, η απαίτηση δεν ικανοποιείται, διότι ο οργανισμός δε διενεργεί εσωτερικούς ελέγχους στο ISMS σε προγραμματισμένα χρονικά διαστήματα.

Την ευθύνη για την επιβεβαίωση συμμόρφωσης των διαδικασιών με κανονισμούς, προδιαγραφές και πρακτικές που έχουν σχέση με την Ασφάλεια έχουν οι Διευθυντές των μονάδων στα πλαίσια της πολιτικής για την ασφάλεια των αεροναυτικών πληροφοριών που εφαρμόζει η Υ.Π.Α.

Οι Διευθυντές των εμπλεκόμενων μονάδων ελέγχουν, όποτε εκείνοι κρίνουν απαραίτητο, τις Διευθύνσεις τους εάν οι διαδικασίες συμμορφώνονται με τη σχετική νομοθεσία, τους κανονισμούς και τις απαιτήσεις για την ασφάλεια των πληροφοριών.

Ένα παράδειγμα βασισμένο στη Διαδικασία 2 «Επεξεργασία Αεροναυτικών Πληροφοριών», οι Διευθυντές ελέγχουν :

- εάν κατά τη διάρκεια εισαγωγής των δεδομένων στην ηλεκτρονική εφαρμογή eaip@Wizard έχει υπογράψει ο αρμόδιος υπάλληλος με τα αρχικά του στο κάτω τμήμα της εν λόγω σελίδας

- εάν ο αρμόδιος υπάλληλος που ήταν υπεύθυνος για τον έλεγχο της ορθότητας των δεδομένων έχει σημειώσει με πράσινο χρώμα τα σωστά εισαχθέντα δεδομένα και με πορτοκαλί τα δεδομένα που εισήχθηκαν λανθασμένα
- εάν έχει κάνει τις προβλεπόμενες διορθώσεις και αν έχει σημειώσει εκ νέου με πράσινο χρώμα τα διορθωμένα δεδομένα και έχει υπογράψει στο κάτω τμήμα της σελίδας
- εάν τα πρωτότυπα υπογεγραμμένα έγγραφα έχουν αρχειοθετηθεί

Οι έλεγχοι όμως αυτοί δεν γίνονται τακτικά και προγραμματισμένα, ούτε καταγράφονται τα ευρήματά τους. Συνεπώς, ο οργανισμός δεν προβαίνει σε Εσωτερικές Επιθεωρήσεις όπως τις ορίζει το παρόν πρότυπο.

Ένα πρόγραμμα ελέγχου πρέπει να σχεδιάζεται, λαμβάνοντας υπόψη τη σημασία των διαδικασιών και των περιοχών που πρόκειται να ελεγχθούν, καθώς και τα αποτελέσματα προηγούμενων ελέγχων. Επίσης, πρέπει να καθορίζει τα κριτήρια ελέγχου, το πεδίο εφαρμογής, τη συχνότητα και τις μεθόδους.

Όχι, δεν συντάσσεται από τους Διευθυντές ένα «Πρόγραμμα Εσωτερικών Επιθεωρήσεων» το οποίο θα εγκρίνεται από την Διοίκηση και θα ορίζει τη συχνότητα των Εσωτερικών Επιθεωρήσεων, τις περιοχές που πρόκειται να ελεγχθούν, τις μεθόδους και τα κριτήρια.

Η επιλογή των ελεγκτών και η διεξαγωγή των ελέγχων πρέπει να εξασφαλίζουν την αντικειμενικότητα και την αμεροληψία της διαδικασίας ελέγχου. Οι ελεγκτές δεν πρέπει να ελέγχουν δικό τους έργο.

Όχι, δεν διασφαλίζεται αντικειμενικότητα και αμεροληψία ακόμα και σε αυτούς τους υποτυπώδεις ελέγχους που διεξάγονται από τους Διευθυντές των μονάδων. Ο λόγος είναι ότι οι Διευθυντές επιθεωρούν μεν τους υφισταμένους τους όμως ενδέχεται να αποκρύψουν μια μη συμμόρφωση ή μια δυσλειτουργία προκειμένου να μην εκτεθούν στους άλλους Διευθυντές ή στη Διοίκηση και επηρεάσει αυτό αρνητικά την αξιολόγησή τους.

Οι ευθύνες και οι απαιτήσεις για τον σχεδιασμό και τη διεξαγωγή ελέγχων, καθώς και για την αναφορά των αποτελεσμάτων και τη διατήρηση αρχείων (βλ. 4.3.3) πρέπει να ορίζεται σε μια τεκμηριωμένη διαδικασία.

Όχι, δεν υπάρχει τεκμηριωμένη διαδικασία. Ο κάθε Διευθυντής ελέγχει υποτυπωδώς και όποτε εκείνος κρίνει απαραίτητο την ομαλή λειτουργία της διαδικασίας στην οποία η Διεύθυνσή του εμπλέκεται. Ενδεχόμενοι κίνδυνοι αν διαπιστωθούν καταγράφονται και τηρούνται σε φακέλους, «Φάκελοι ανάλυσης κινδύνων», προκειμένου να συζητηθούν σε κάποια σύσκεψη και να αντιμετωπιστούν.

Τα στελέχη που είναι υπεύθυνα για την περιοχή την οποία ελέγχουν, πρέπει να εξασφαλίζει ότι λαμβάνονται χωρίς αδικαιολόγητη καθυστέρηση δράσεις για την εξάλειψη των μη συμμορφώσεων που διαπιστώθηκαν και για τον εντοπισμό των αιτιών τους. Δραστηριότητες επαλήθευσης (follow-up) περιλαμβάνουν την επαλήθευση των δράσεων που αναλήφθηκαν και την αναφορά των αποτελεσμάτων επαληθεύσεως (βλ.*Απαίτηση 8*)

Ναι, τα στελέχη που είναι υπεύθυνα για τον εσωτερικό έλεγχο, στη συγκεκριμένη περίπτωση οι Διευθυντές των μονάδων, πραγματοποιούν τεκμηριωμένη επαλήθευση.

Οι Διευθυντές όταν εντοπιστεί μια μη συμμόρφωση την καταγράφουν στο ημερήσιο ημερολόγιο της Διεύθυνσής τους, λαμβάνουν από κοινού διορθωτικά μέτρα, επιβεβαιώνουν την εξάλειψή της και συντάσσουν μια αναφορά, το έντυπο «ΑΝΑΦΟΡΑ ΑΣΦΑΛΕΙΑΣ» (ΠΑΡΑΡΤΗΜΑ IV-Έντυπο 8.1), προς τη Διοίκηση. Η «ΑΝΑΦΟΡΑ ΑΣΦΑΛΕΙΑΣ» περιλαμβάνει τη μη συμμόρφωση, τη δράση και τα αποτελέσματα της επαληθεύσεως.

Η επιβεβαίωση εξάλειψης τη μη συμμόρφωσης από την πλευρά των Διευθυντών σημαίνει να έχουν διασφαλίσει ότι ο κίνδυνος έχει μειωθεί στο χαμηλότερο επίπεδο, στο οποίο μπορεί να διαχειριστεί.

5.4.2. Προτάσεις

Ο οργανισμός οφείλει σύμφωνα με το πρότυπο να διενεργεί Εσωτερικές Επιθεωρήσεις σε προγραμματισμένα διαστήματα προκειμένου να διασφαλίσει στους Διευθυντές των μονάδων ότι όλες οι αεροναυτικές πληροφορίες που εντάσσονται στα πλαίσια των καθηκόντων τους παρέχονται με ασφάλεια, για να εισάγει βελτιώσεις όπου απαιτούνται, και για να επιβεβαιώνει συμμόρφωση των λειτουργικών διαδικασιών με τις απαιτήσεις του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών.

Αρχικά, πρέπει να καθιερωθεί μια τεκμηριωμένη διαδικασία Εσωτερικών Επιθεωρήσεων του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών, η οποία θα περιγράφει τον τρόπο με τον οποίο θα διενεργούνται οι Εσωτερικές Επιθεωρήσεις στο Σύστημα.

Ο οργανισμός πρέπει να ορίσει έναν «Υπεύθυνο Ασφάλειας Πληροφοριών» ο οποίος θα είναι πιστοποιημένος από αρμόδιο φορέα και θα τεθεί υπεύθυνος για την ετήσια σύνταξη «Προγράμματος Εσωτερικών Επιθεωρήσεων» και τέλος θα είναι ειδικά εκπαιδευμένος ως «Εσωτερικός Επιθεωρητής» για την ορθή διεξαγωγή αυτών.

Με αυτόν τον τρόπο δε θα διαταράσσεται η αρχή ανεξαρτησίας επιθεωρητή–επιθεωρούμενου και θα διασφαλίζεται αντικειμενικότητα και αμεροληψία, εφόσον όλες

οι Διευθύνσεις και τα Τμήματα αυτών θα επιθεωρούνται από τον «Υπεύθυνο Ασφάλειας Πληροφοριών» και όχι από τους Διευθυντές των μονάδων, οι οποίοι δεν θα έχουν πια την αρμοδιότητα να επιθεωρούν δικό τους έργο.

Οι εσωτερικές επιθεωρήσεις όλων των εμπλεκομένων στη διεργασία Διευθύνσεων θα πραγματοποιούνται συστηματικά μια φορά το χρόνο, ή έκτακτα εφόσον κριθεί απαραίτητο.

Το πρόγραμμα των Εσωτερικών Επιθεωρήσεων θα συντάσσεται σε ετήσια βάση από τον Υπεύθυνο Ασφάλειας Πληροφοριών, θα εγκρίνεται από τη Διοίκηση και θα αναγράφεται στο έντυπο «ΕΤΗΣΙΟ ΠΡΟΓΡΑΜΜΑ ΕΠΙΘΕΩΡΗΣΕΩΝ» (ΠΑΡΑΡΤΗΜΑ IV-Έντυπο 6.1).

Το εύρος, η μέθοδος και τα κριτήρια των Εσωτερικών Επιθεωρήσεων θα καθορίζονται από τον «Υπεύθυνο Ασφάλειας Πληροφοριών». Επίσης, τα αποτελέσματα προηγουμένων Εσωτερικών Επιθεωρήσεων θα λαμβάνονται υπόψη στην προετοιμασία της επιθεώρησης.

Το προσωπικό που εμπλέκεται στις υπό επιθεώρηση διαδικασίες θα ενημερώνεται, γραπτώς, τουλάχιστον ένα μήνα πριν την επιθεώρηση.

Με αυτόν τον τρόπο θα επιθεωρείται η συμμόρφωση της διεργασίας έκδοσης και ενημέρωσης του Εγχειριδίου AIP ως προς τις απαιτήσεις του προτύπου στην ολότητά της και όχι κάθε Διεύθυνση ξεχωριστά.

Στόχος θα είναι ο «Υπεύθυνος Ασφάλειας Πληροφοριών» να εντοπίσει τυχόν δυσλειτουργίες στις Διευθύνσεις οι οποίες εμπλέκονται στη διεργασία έκδοσης και ενημέρωσης του Εγχειριδίου AIP.

Αμέσως μετά το τέλος της επιθεώρησης, ο Υπεύθυνος Ασφάλειας Πληροφοριών θα συζητά τα αποτελέσματα με τον Διευθυντή της επιθεωρούμενης μονάδας και το εμπλεκόμενο προσωπικό.

Αναφορά της επιθεώρησης θα συντάσσεται από τον Υπεύθυνο Ασφάλειας Πληροφοριών και θα κοινοποιείται στους Διευθυντές των εμπλεκομένων μονάδων, μέσω του εντύπου «ΑΝΑΦΟΡΑ ΕΠΙΘΕΩΡΗΣΗΣ» (ΠΑΡΑΡΤΗΜΑ IV-Έντυπο 6.2). Στο έντυπο αυτό θα καταγράφονται μη συμμορφώσεις και παρατηρήσεις. Η αναφορά θα κοινοποιείται στη Διοίκηση.

Για κάθε μη συμμόρφωση ή παρατήρηση θα εκδίδεται έντυπο «ΔΙΟΡΘΩΤΙΚΕΣ ΚΑΙ ΠΡΟΛΗΠΤΙΚΕΣ ΕΝΕΡΓΕΙΕΣ» από τον Υπεύθυνο Ασφάλειας Πληροφοριών.

Κοινοποίηση της αναφοράς επιθεώρησης στους επιθεωρούμενους θα γίνεται από τον Υπεύθυνο Ασφάλειας Πληροφοριών, για ενδεχόμενη λήψη μέτρων. Η «ΑΝΑΦΟΡΑ ΕΠΙΘΕΩΡΗΣΗΣ» θα υπογράφεται από τον Διευθυντή της μονάδας που επιθεωρήθηκε, με ευθύνη του οποίου θα ενημερώνεται και όλο το υπόλοιπο προσωπικό της μονάδας.

Υπεύθυνος για την παρακολούθηση εκτέλεσης των διορθωτικών ενεργειών θα είναι αυτός που θα ορίζεται στο εκάστοτε έντυπο «ΔΙΟΡΘΩΤΙΚΕΣ ΚΑΙ ΠΡΟΛΗΠΤΙΚΕΣ ΕΝΕΡΓΕΙΕΣ», ενώ υπεύθυνος για την τελική επαλήθευσή τους θα είναι ο Υπεύθυνος Ασφάλειας Πληροφοριών.

Επίσης, ο τελευταίος θα είναι αρμόδιος και για την τήρηση Φακέλων Επιθεωρήσεων, οι οποίοι θα περιλαμβάνουν τα συμπληρωμένα έντυπα «ΕΤΗΣΙΟ ΠΡΟΓΡΑΜΜΑ ΕΠΙΘΕΩΡΗΣΕΩΝ» και «ΑΝΑΦΟΡΑ ΕΠΙΘΕΩΡΗΣΗΣ». Ενώ, αντίγραφα του εντύπου «ΑΝΑΦΟΡΑ ΕΠΙΘΕΩΡΗΣΗΣ» θα δίνονται και στις επιθεωρούμενες Διευθύνσεις (η κάθε Διεύθυνση θα τηρεί αυτά που την αφορούν).

Η «ΑΝΑΦΟΡΑ ΕΠΙΘΕΩΡΗΣΗΣ» με τα αποτελέσματα των επιθεωρήσεων θα κοινοποιείται και στη Διοίκηση, ώστε να αποτελεί εισερχόμενο για όταν αυτή προβεί σε ανασκόπηση του συστήματος.

5.5. Ανασκόπηση του ISMS από τη Διοίκηση

5.5.1. Εφαρμογή Απαιτήσεων

Απαίτηση 7

ΑΝΑΣΚΟΠΗΣΗ ΤΟΥ ISMS ΑΠΟ ΤΗ ΔΙΟΙΚΗΣΗ

7.1 Γενικά

(4.2.3.στ)

Η διοίκηση πρέπει να ανασκοπεί το σύστημα ISMS του οργανισμού σε προγραμματισμένα διαστήματα (τουλάχιστον μία φορά το χρόνο) για να εξασφαλίζει τη συνεχιζόμενη καταλληλότητα, επάρκεια και αποτελεσματικότητα του. Η ανασκόπηση αυτή πρέπει να περιλαμβάνει την αξιολόγηση ευκαιριών βελτίωσης και την ανάγκη για αλλαγές στο ISMS, συμπεριλαμβανομένης της πολιτικής ασφάλειας των πληροφοριών και των στόχων ασφάλειας πληροφοριών. Τα αποτελέσματα των ανασκοπήσεων πρέπει να τεκμηριώνονται με σαφήνεια και πρέπει να διατηρούνται σε αρχεία (βλ. 4.3.3)

Η Διοίκηση ενίοτε ανασκοπεί το σύστημα ως προς την καταλληλότητα, την επάρκεια και την αποτελεσματικότητά του.

Η ανασκόπηση όμως αυτή δεν γίνεται προγραμματισμένα και όταν γίνεται τα αποτελέσματα δεν τεκμηριώνονται και δεν διατηρούνται σε αρχεία.

Συνεπώς, η απαίτηση ικανοποιείται μερικώς.

7.2 Εισερχόμενα ανασκοπήσεων

Τα εισερχόμενα σε μια ανασκόπηση της Διοίκησης πρέπει να περιλαμβάνουν πληροφορίες σχετικές με :

α) αποτελέσματα των επιθεωρήσεων και των ανασκοπήσεων του ISMS

Όχι, δεν υπάρχουν τέτοιου είδους εισερχόμενα. Τα ευρήματα των όποιων υποτυπωδών ελέγχων και ανασκοπήσεων γίνονται δεν καταγράφονται.

β) ανατροφοδότηση από τα ενδιαφερόμενα μέρη

Ναι, η ανατροφοδότηση από τα ενδιαφερόμενα μέρη αποτελεί εισερχόμενο. Η Διοίκηση λαμβάνει υπόψη καταγεγραμμένες αναφορές του προσωπικού αλλά και τεκμηριωμένες αναφορές των τελικών χρηστών, όπως αεροδρόμια, αεροπορικές εταιρείες, ιδιώτες πιλότοι.

Λαμβάνει μάλιστα σοβαρά υπόψη τις παρατηρήσεις μιας κατηγορίας τελικών χρηστών, των «Παρόχων Δεδομένων» (Data Service Providers), οι οποίοι είναι ιδιωτικές εταιρείες που αντικείμενο εργασιών τους είναι η συγκέντρωση Εγχειριδίων AIP από όλο τον κόσμο, η ορθή και έγκαιρη ενημέρωσή τους και η παροχή τους προς τρίτους. Οι πιο γνωστές μεταξύ άλλων είναι οι Jeppesen, LIDO, EAG. Αλλά και οι εταιρείες που κατασκευάζουν το λογισμικό του συστήματος διαχείρισης πληροφοριών όπως οι Thales, Abitech.

Επειδή οι απαιτήσεις αυτών των εταιρειών ως προς την εγκυρότητα και πληρότητα των αεροναυτικών πληροφοριών είναι ιδιαίτερα υψηλές λειτουργούν και ως ελεγκτικοί μηχανισμοί. Με αποτέλεσμα η ανατροφοδότηση από αυτές να είναι πολύ σημαντική.

γ) τεχνικές ή διαδικασίες, οι οποίες θα μπορούσαν να χρησιμοποιηθούν στον οργανισμό για να βελτιώσουν τις επιδόσεις και την αποτελεσματικότητα του ISMS

Ναι, η Διοίκηση αξιοποιεί ως εισερχόμενα νέες τεχνικές, συστήματα ή διαδικασίες που χρησιμοποιούν άλλα ευρωπαϊκά κράτη. Για τις εξελίξεις αυτές ενημερώνεται μέσω εισηγήσεων που συντάσσει το αρμόδιο για την εισαγωγή και επεξεργασία αεροναυτικών πληροφοριών προσωπικό.

Πιο συγκεκριμένα, προγραμματισμένες αλλά και έκτακτες συναντήσεις πραγματοποιούνται σε διάφορες ευρωπαϊκές χώρες από τον «Ευρωπαϊκό Οργανισμό για την Ασφάλεια της Πολιτικής Αεροπορίας» (EUROCONTROL).

Οι αρμόδιοι υπάλληλοι για την εισαγωγή και επεξεργασία αεροναυτικών πληροφοριών όλων των ευρωπαϊκών χωρών συμμετέχουν σε προγραμματισμένες και τακτικές «Ομάδες Εργασίας» (Working Groups), οι οποίες πραγματοποιούνται σε διάφορες ευρωπαϊκές χώρες.

Παράλληλα, οι Διευθυντές των Διευθύνσεων Αεροναυτικών Εκδόσεων (Ε1), στο οποίο υπάγεται και το Τμήμα Εγχειριδίων Αεροναυτικών Πληροφοριών AIP (Ε1/Α),όλων των ευρωπαϊκών χωρών, συμμετέχουν σε προγραμματισμένες αλλά και έκτακτες συναντήσεις που πραγματοποιούνται 4-5 φορές το χρόνο σε διάφορες ευρωπαϊκές χώρες.

Οι τελικές εισηγήσεις και των δυο αποτελούν εισερχόμενο της Διοίκησης της Υπηρεσίας Πολιτικής Αεροπορίας.

δ) την κατάσταση των προληπτικών και διορθωτικών ενεργειών

Όχι, η Διοίκηση δεν ανασκοπεί τις προληπτικές και διορθωτικές ενέργειες.

Οι Διευθυντές όταν εντοπιστεί μια απειλή ή μη-συμμόρφωση λαμβάνουν προληπτικά ή αντίστοιχα διορθωτικά μέτρα, επιβεβαιώνουν την εξάλειψή της και συντάσσουν μια Αναφορά Ασφάλειας προς τη Διοίκηση η οποία περιλαμβάνει την απειλή ή τη μη-συμμόρφωση, τη δράση και τα αποτελέσματα της επαληθεύσεως. Η Διοίκηση όμως δεν προβαίνει σε τακτική ανασκόπηση των αναφορών αυτών, ούτως ώστε να διασφαλίσει ότι δεν θα συμβεί ή επαναληφθεί κάποιο συμβάν.

Επίσης, δεν υπάρχει κάποιο έντυπο όπως για παράδειγμα, «ΔΙΟΡΘΩΤΙΚΕΣ & ΠΡΟΛΗΠΤΙΚΕΣ ΕΝΕΡΓΕΙΕΣ», το οποίο να συμπληρώνεται. Συνεπώς, η Διοίκηση δεν μπορεί να ανατρέξει σε τέτοιου είδους αρχείο, ούτως ώστε να ανασκοπήσει την κατάσταση των διορθωτικών και προληπτικών ενεργειών.

ε) τα τρωτά σημεία και τις απειλές που δεν προσδιορίζονται επαρκώς στην προηγούμενη αξιολόγηση κινδύνου

Ναι, η Διοίκηση εξετάζει νέα τρωτά σημεία ή απειλές που ενδέχεται να προέκυψαν πρόσφατα και ως εκ τούτου να μην είχαν ενταχθεί και αξιολογηθεί στην προηγούμενη «Αξιολόγηση Κινδύνων».

Για παράδειγμα, εάν διαπιστώθηκε πρόσφατα ότι ένας χρήστης δεν φυλάσσει τον απόρρητο κωδικό πρόσβασής του στην ηλεκτρονική εφαρμογή «Eaip@Wizard», αλλά αντιθέτως τον έχει κοινοποιήσει σε συναδέλφους του προκειμένου να καταχωρούν δεδομένα δικής του αρμοδιότητας.

Το συγκεκριμένο εισερχόμενο της Διοίκησης προκύπτει από τις «Αναφορές Ενδεχόμενων Κινδύνων», την ευθύνη για την σύνταξη των οποίων φέρουν οι Διευθυντές των εμπλεκομένων στη διεργασία μονάδων.

στ) τα αποτελέσματα από τις μετρήσεις αποτελεσματικότητας

Όχι, η Διοίκηση δεν μπορεί να λάβει υπόψη τα αποτελέσματα από τις μετρήσεις αποτελεσματικότητας, διότι ο οργανισμός δεν πραγματοποιεί τέτοιου είδους μετρήσεις (4.2.2.δ, 4.2.3.γ).

ζ) δράσεις επαλήθευσης (follow-up actions) από τις προηγούμενες ανασκοπήσεις της Διοίκησης

Όχι, δεν υπάρχουν δράσεις επαλήθευσης, διότι τα αποτελέσματα των προηγούμενων ανασκοπήσεων δεν έχουν τεκμηριωθεί και δεν έχουν διατηρηθεί σε αρχεία. Οπότε, καθίσταται αδύνατη η σύγκριση και η επαλήθευση.

η) τυχόν αλλαγές που θα μπορούσαν να επηρεάσουν το ISMS και

Ναι, η Διοίκηση λαμβάνει υπόψη αλλαγές που ενδέχεται να επηρεάσουν την ορθή λειτουργία του συστήματος, όπως οι αλλαγές στο νομικό και κανονιστικό περιβάλλον ή αλλαγμένες συμβατικές υποχρεώσεις.

θ) συστάσεις για βελτίωση

Ναι, η Διοίκηση λαμβάνει υπόψη της τις συστάσεις για βελτίωση από Διεθνείς Οργανισμούς, όπως από το Διεθνή Οργανισμό Πολιτικής Αεροπορίας ICAO (International Civil Aviation Organization). Τέτοιες συστάσεις μπορεί να είναι η βελτίωση των επιθυμητών επιπέδων ασφάλειας πληροφοριών, η ποιοτική αναβάθμιση της Υπηρεσίας Πολιτικής Αεροπορίας και άλλες.

7.3 Εξερχόμενα ανασκοπήσεων

Τα εξερχόμενα από την ανασκόπηση της Διοίκησης πρέπει να περιλαμβάνουν όλες τις αποφάσεις και τις ενέργειες που σχετίζονται με τα ακόλουθα :

α) τη βελτίωση της αποτελεσματικότητας του ISMS

Ναι, η Διοίκηση διαθέτει τεκμηριωμένες αποφάσεις όσον αφορά βελτιώσεις και εποικοδομητικές αλλαγές στο ISMS, οι οποίες λαμβάνονται κατόπιν συζητήσεως μεταξύ των Διοικητών των Υπηρεσιών Πολιτικής Αεροπορίας όλων των Ευρωπαϊκών χωρών σε «Συμβούλια Διοικητών» (Provision Councils), τα οποία λαμβάνουν χώρα δύο φορές ετησίως με έδρα τις Βρυξέλλες.

β) ανανέωση του σχεδίου εκτίμησης των κινδύνων και του σχεδίου θεράπευσης κινδύνων

Όχι, η Διοίκηση δεν προβαίνει στις απαραίτητες ενέργειες για ανανέωση του σχεδίου εκτίμησης κινδύνων και του σχεδίου θεράπευσης κινδύνων. Τα σχέδια αυτά καταγράφηκαν την πρώτη φορά και δεν ανασκοπούνται προγραμματισμένα και τακτικά από τη Διοίκηση και συνεπώς δεν ανανεώνονται.

γ) την τροποποίηση των διαδικασιών και των ελέγχων που επηρεάζουν την ασφάλεια των πληροφοριών, όπως απαιτείται, ώστε να ανταποκριθούν στα εσωτερικά ή εξωτερικά συμβάντα που ενδέχεται να επηρεάσουν το ISMS, συμπεριλαμβανομένων των αλλαγών σε:

1) επιχειρηματικές απαιτήσεις
2) απαιτήσεις ασφαλείας
3) επιχειρηματικές διαδικασίες που επηρεάζουν τις υφιστάμενες επιχειρηματικές απαιτήσεις
4) κανονιστικές ή νομικές απαιτήσεις
5) συμβατικές υποχρεώσεις και
6) τα επίπεδα του κινδύνου ή / και κριτήρια για την αποδοχή κινδύνων

Ναι, η Διοίκηση προβαίνει στην τροποποίηση των διαδικασιών και των ελέγχων που εφαρμόζει μόλις διαπιστωθεί τεκμηριωμένα η αναποτελεσματικότητά τους ή μόλις αλλάξουν οι απαιτήσεις ασφάλειας ή κάποιο από τα παραπάνω στοιχεία.

Συγκεκριμένα, η Διοίκηση σε περίπτωση που κρίνει απαραίτητη την τροποποίηση κάποιας διαδικασίας, αναθέτει στο εμπλεκόμενο τμήμα την προσαρμογή της διαδικασίας στα νέα δεδομένα. Εφόσον η νέα διαδικασία εγκριθεί από τη Διοίκηση τίθεται σε ισχύ και η παλαιότερη επίσημα καταργείται.

δ) τις ανάγκες σε πόρους

Ναι, η Διοίκηση έχει στη διάθεσή της επίσημα έγγραφα που αποδεικνύουν αποφάσεις της για εξασφάλιση των αναγκαίων πόρων. Ενδεικτικά, μερικές τέτοιες ενέργειες είναι, προκηρύξεις πρόσληψης κατάλληλου προσωπικού, διενέργεια διαγωνισμών ανάθεσης έργου για αγορά εξοπλισμού (ηλεκτρονικοί υπολογιστές, διακομιστές, εφαρμογές).

ε) βελτίωση στο πώς η αποτελεσματικότητα των ελέγχων υπολογίζεται

Όχι, η Διοίκηση δεν έχει προβεί σε κάποια ενέργεια μέχρι στιγμής, ούτος ώστε να βελτιωθεί η μέτρηση της αποτελεσματικότητας των ελέγχων, η οποία μέχρι στιγμής δεν παρακολουθείται ούτε μετράται.

Μια τέτοια ενέργεια εκ μέρους της Διοίκησης θα ήταν η καθιέρωση μιας επίσημης μεθόδου μέτρησης της αποτελεσματικότητας των ελέγχων.

5.5.2. Προτάσεις

Ο οργανισμός δεν διαθέτει καταγεγραμμένη διαδικασία ανασκόπησης. Η Διοίκηση ενίοτε ανασκοπεί το σύστημα ως προς την καταλληλότητα, την επάρκεια και την αποτελεσματικότητά του.

Η ανασκόπηση όμως αυτή δεν γίνεται προγραμματισμένα και όταν γίνεται τα αποτελέσματα δεν τεκμηριώνονται και δεν διατηρούνται σε αρχεία.

Η Διοίκηση οφείλει να καθιερώσει μια τεκμηριωμένη διαδικασία ανασκόπησης, η οποία να στοχεύει στο διαρκή έλεγχο και την αξιολόγηση των αποτελεσμάτων του Συστήματος με απώτερο σκοπό τη συνεχή βελτίωση.

Η ανασκόπηση του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών από τη Διοίκηση, θα πρέπει να εκτελείται μια φορά ετησίως, αλλά και κάθε φορά που θα κρίνεται απαραίτητο από αυτήν.

Ανασκόπηση του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών θα γίνεται από τη Γενική Διεύθυνση του οργανισμού με εισήγηση του Υπεύθυνου Ασφάλειας Πληροφοριών ή με απόφαση της Διοίκησης.

Την επιτροπή ανασκόπησης θα συνιστούν ο Διοικητής Πολιτικής Αεροπορίας, ο Υποδιοικητής, ο Γενικός Διευθυντής Αεροναυτιλίας, οι Διευθυντές των εμπλεκομένων μονάδων και ο Υπεύθυνος Ασφάλειας Πληροφοριών.

Υπεύθυνος για τον καθορισμό του χρόνου σύγκλησης της επιτροπής θα είναι ο Υπεύθυνος Ασφάλειας Πληροφοριών. Πρόεδρος των συσκέψεων θα είναι ο Διοικητής Πολιτικής Αεροπορίας.

Η ατζέντα των συσκέψεων της επιτροπής θα προετοιμάζεται γραπτώς με ευθύνη του Υπεύθυνου Ασφάλειας Πληροφοριών, μετά από συνεννόηση με τα υπόλοιπα μέλη της και αντίγραφό της θα μοιράζεται σε όλους όσους πρόκειται να συμμετάσχουν στην επιτροπή τουλάχιστον μία μέρα πριν από τη σύγκλισή της.

Η Διοίκηση οφείλει να συμπεριλάβει ως εισερχόμενα στην ανασκόπησή της όσα διαπιστώθηκε παραπάνω ότι δε λαμβάνει υπόψη της. Ενδεικτικά, αναφέρονται τα ακόλουθα :

- Αποτελέσματα Εσωτερικών Επιθεωρήσεων και πρακτικά προηγούμενων Ανασκοπήσεων του ISMS.
- Την κατάσταση των προληπτικών και διορθωτικών ενεργειών.

Η ανασκόπηση να περιλαμβάνει τα έντυπα «Αναφορά Ασφαλείας» καθώς και τα έντυπα που θα εισαχθούν στο Σύστημα «ΔΙΟΡΘΩΤΙΚΕΣ & ΠΡΟΛΗΠΤΙΚΕΣ ΕΝΕΡΓΕΙΕΣ», (όπως θα αναφέρουμε στις απαιτήσεις 8., 8.3 του προτύπου, ενότητα 5.6 Βελτίωση ISMS), τα οποία θα επισυνάπτονται μαζί με τις αντίστοιχες «Αναφορές Ασφάλειας». Να διερευνώνται τυχόν προβλήματα στην εφαρμογή του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών, διορθωτικές και προληπτικές ενέργειες που προτάθηκαν και η πρόοδος υλοποίησης τους.

- Τα αποτελέσματα από τις μετρήσεις αποτελεσματικότητας.
  Αποτελέσματα, δηλαδή, ανάλυσης δεικτών και άλλων στοιχείων που περιγράφουν την επίδοση του οργανισμού όσον αφορά την ασφάλεια των αεροναυτικών πληροφοριών.
  (Όπως αναφέραμε και στις απαιτήσεις 4.2.2.δ & 4.2.3.γ, ενότητα 5.2 Γενικές Απαιτήσεις), ο οργανισμός πρέπει να καθιερώσει έναν τρόπο μέτρησης της αποτελεσματικότητας των ελέγχων. Η ανασκόπηση των αποτελεσμάτων αυτών των μετρήσεων θα επαληθεύει ότι οι απαιτήσεις ασφάλειας πληροφοριών ικανοποιούνται.

- Τις δράσεις επαλήθευσης (follow-up actions) από τις προηγούμενες ανασκοπήσεις της Διοίκησης.
  Τεκμηριωμένη, δηλαδή, εισήγηση του Υπεύθυνου Ασφάλειας Πληροφοριών, για το βαθμό επίτευξης των σκοπών και των στόχων που θα έχουν τεθεί στην προηγούμενη ανασκόπηση.

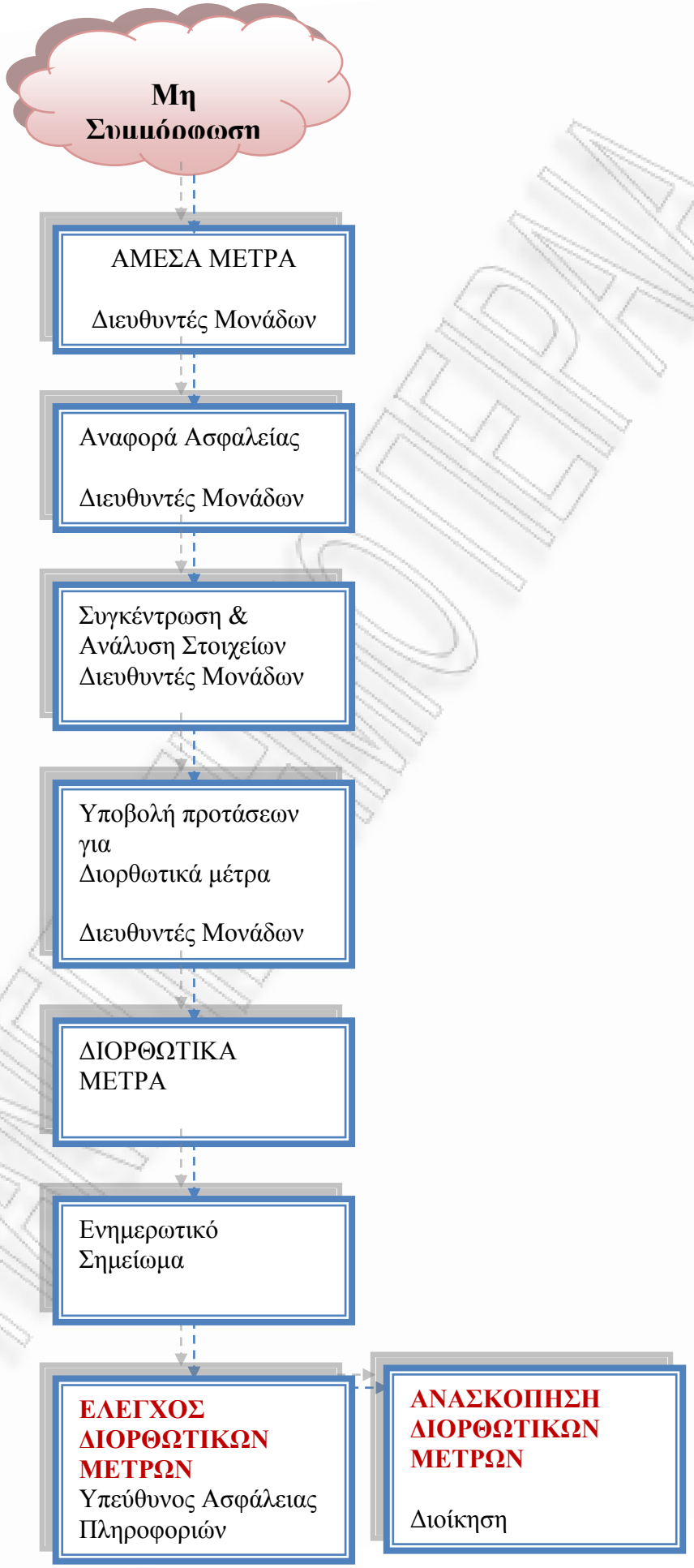
Έπειτα από ανάλυση των ανωτέρω θα καταγράφονται στο έντυπο «ΠΡΑΚΤΙΚΑ ΑΝΑΣΚΟΠΗΣΗΣ» (ΠΑΡΑΡΤΗΜΑ IV-Έντυπο 7) οι στόχοι που θέτει ο οργανισμός, συμπεριλαμβανομένων ενδεχόμενων αποφάσεων για αλλαγές όσον αφορά το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών. Σε κάθε συνάντηση ανασκόπησης θα γίνεται σύγκριση των αποτελεσμάτων σε σχέση με τους προηγούμενους στόχους. Με αυτό τον τρόπο θα μετρούνται και θα αξιολογούνται:

- Η βελτίωση της αποτελεσματικότητας του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών ISMS.
- Η βελτίωση της παροχής υπηρεσίας.
- Η βελτίωση του σχεδίου εκτίμησης και του σχεδίου θεράπευσης κινδύνου.
- Η βελτίωση της μέτρησης της αποτελεσματικότητας των ελέγχων.
- Οι ανάγκες σε πόρους (ανθρώπινο δυναμικό, εξειδικευμένες δεξιότητες, τεχνολογία, οικονομικοί πόροι) για την επίτευξη των σκοπών.

Τα πρακτικά της κάθε σύσκεψης θα καταγράφονται στο έντυπο «ΠΡΑΚΤΙΚΑ ΑΝΑΣΚΟΠΗΣΗΣ», το οποίο συμπληρωμένο θα τηρείται από τον Υπεύθυνο Ασφάλειας

Πληροφοριών και θα αρχειοθετείται μαζί με την ατζέντα των συσκέψεων της επιτροπής στον «Φάκελο Ανασκοπήσεων» που θα δημιουργηθεί.

Τέλος, πρέπει να διορθωθεί και η «Διαδικασία Διαχείρισης Μη Συμμόρφωσης», και να προστεθεί και το βήμα της Ανασκόπησης, όπως φαίνεται στο ακόλουθο διάγραμμα :


Μη Συμμόρφωση
ΑΜΕΣΑ ΜΕΤΡΑ
Διευθυντές Μονάδων
Αναφορά Ασφαλείας
Διευθυντές Μονάδων
Συγκέντρωση & Ανάλυση Στοιχείων
Διευθυντές Μονάδων
Υποβολή προτάσεων για Διορθωτικά μέτρα
Διευθυντές Μονάδων
ΔΙΟΡΘΩΤΙΚΑ ΜΕΤΡΑ
Ενημερωτικό Σημείωμα
ΕΛΕΓΧΟΣ ΔΙΟΡΘΩΤΙΚΩΝ ΜΕΤΡΩΝ
Υπεύθυνος Ασφάλειας Πληροφοριών
ΑΝΑΣΚΟΠΗΣΗ ΔΙΟΡΘΩΤΙΚΩΝ ΜΕΤΡΩΝ
Διοίκηση

5.6. Βελτίωση του ISMS

5.6.1. *Εφαρμογή Απαιτήσεων*

Απαίτηση 8

ΒΕΛΤΙΩΣΗ ΤΟΥ ISMS

8.1 Συνεχής Βελτίωση

Ο οργανισμός πρέπει συνεχώς να βελτιώνει την αποτελεσματικότητα του ISMS μέσω της χρήσης της πολιτικής ασφάλειας πληροφοριών, των αντικειμενικών σκοπών για την ασφάλεια των πληροφοριών, των αποτελεσμάτων της επιθεώρησης, της ανάλυσης καταγεγραμμένων γεγονότων, των διορθωτικών και των προληπτικών ενεργειών και της ανασκόπησης από τη Διοίκηση (βλ. *Απαίτηση 7*).

8.2 Διορθωτικές Ενέργειες

Ο οργανισμός πρέπει να αναλαμβάνει ενέργειες για την εξάλειψη της αιτίας των μη συμμορφώσεων με τις απαιτήσεις του ISMS, έτσι ώστε να αποτραπεί η επανεμφάνισή τους.

Πρέπει να καθιερωθεί μια τεκμηριωμένη διαδικασία για διορθωτικές ενέργειες , ώστε να καθορίζονται απαιτήσεις για:

α) αναγνώριση μη συμμορφώσεων

Ναι, ο οργανισμός διαθέτει μια τεκμηριωμένη διαδικασία αναγνώρισης μη συμμορφώσεων (ΠΑΡΑΡΤΗΜΑ ΙΙΙ -σελ.150- «Διαδικασία Διαχείρισης μη συμμορφώσεων». Οποιοδήποτε μέλος του προσωπικού ανακαλύπτει μη συμμόρφωση ή δυσλειτουργία του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών, ενημερώνει το ημερήσιο ημερολόγιο της Διεύθυνσής του και επικοινωνεί με τον Διευθυντή της αντίστοιχης μονάδας.

β) προσδιορισμό των αιτιών των μη συμμορφώσεων

Ναι, ο οργανισμός διαθέτει μια τεκμηριωμένη διαδικασία προσδιορισμού των αιτιών των μη συμμορφώσεων. Ο Διευθυντής στη συνέχεια αναζητά τα αίτια της μη συμμόρφωσης μέσω συγκέντρωσης και ανάλυσης στοιχείων, για παράδειγμα από ηλεκτρονικά αρχεία καταγραφής του συστήματος, συμπληρωμένα έντυπα, αναφορές των εμπλεκομένων και άλλα, με τελικό σκοπό να αναγνωρίσει τους παράγοντες που την προκάλεσαν.

γ) αξιολόγηση της ανάγκης για ενέργειες, ώστε να εξασφαλιστεί ότι οι μη συμμορφώσεις δεν θα επαναληφθούν

Ναι, ο οργανισμός πραγματοποιεί αξιολόγηση της ανάγκης για ενέργειες, ώστε να διασφαλιστεί ότι οι μη συμμορφώσεις δεν θα επαναληφθούν. Συγκεκριμένα, ο Διευθυντής αξιολογεί τη σημαντικότητα και αναζητά μεθόδους επίλυσης του προβλήματος. (ΠΑΡΑΡΤΗΜΑ ΙΙΙ -σελ.149- «Προτεραιότητες για την αντιμετώπιση μη συμμορφώσεων».

δ) καθορισμό και υλοποίηση διορθωτικών ενεργειών που απαιτούνται

Ναι, σε περίπτωση που απαιτείται χειρισμός μη συμμόρφωσης, για οτιδήποτε αφορά το σύστημα, τότε την ευθύνη για την αποκατάσταση της μη συμμόρφωσης έχει ο Διευθυντής της μονάδας στην οποία εντοπίστηκε.

Αν η μη συμμόρφωση κλείνει άμεσα με μια απλή ενέργεια (τοπική αποκατάσταση), τότε αυτή η ενέργεια υλοποιείται από τον αρμόδιο Διευθυντή μονάδας και εκδίδεται μια αναφορά Ασφαλείας «Έντυπο Αναφοράς Βλαβών, Συμβάντων & Ατυχημάτων» (ΠΑΡΑΡΤΗΜΑ IV- Έντυπο 8.1) προς τη Διοίκηση, διαφορετικά ο αρμόδιος προβαίνει σε διορθωτική ενέργεια για τη μη συμμόρφωση.

ε) αρχειοθέτηση των αποτελεσμάτων των ενεργειών που ανελήφθησαν (βλ. 4.3.3) και

Όχι, η διαδικασία για διορθωτικές ενέργειες δεν είναι τεκμηριωμένη. Δεν συμπληρώνεται κάποιο έντυπο, συνεπώς δεν τηρούνται και σχετικά αρχεία. Απλά όταν κρίνεται απαραίτητο αποστέλλεται στη Διοίκηση κάποιο ενημερωτικό σημείωμα.

στ) ανασκόπηση των διορθωτικών ενεργειών που αναλαμβάνονται

Ναι, γίνεται επαλήθευση των ενεργειών που ανελήφθησαν από τον ίδιο τον Διευθυντή που τις πραγματοποίησε. Δεν καταγράφεται όμως η επαλήθευση αυτή σε κάποιο έντυπο ούτως ώστε και να αποδεικνύεται.

8.3 Προληπτικές Ενέργειες

Ο οργανισμός πρέπει να προσδιορίσει ενέργειες για την εξάλειψη των αιτιών των πιθανών μη συμμορφώσεων με τις απαιτήσεις του ISMS, έτσι ώστε να προλαμβάνεται η εμφάνισή τους. Οι προληπτικές ενέργειες που λαμβάνονται πρέπει να είναι ανάλογες με τις επιπτώσεις των πιθανών προβλημάτων.

Πρέπει να καθιερωθεί μια τεκμηριωμένη διαδικασία για προληπτικές ενέργειες , ώστε να καθορίζονται απαιτήσεις για:

α) αναγνώριση πιθανών μη συμμορφώσεων και των αιτιών τους

Ναι, γίνεται αναγνώριση πιθανών μη συμμορφώσεων και των αιτιών τους. Οποιοδήποτε μέλος του προσωπικού εκτιμά ότι κάποιο λειτουργικό κομμάτι του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών, μπορεί να οδηγήσει σε μη συμμόρφωση ή δυσλειτουργία, ενημερώνει το ημερήσιο ημερολόγιο της Διεύθυνσής του και επικοινωνεί με τον Διευθυντή της αντίστοιχης μονάδας.

β) αξιολόγηση της ανάγκης για λήψη ενεργειών έτσι ώστε να προληφθεί η εμφάνιση μη συμμορφώσεων

Ναι, ο Διευθυντής αξιολογεί τη σημαντικότητα και αναθέτει ή όχι σε κάποιο υπάλληλο της μονάδας του τη διερεύνηση και ανεύρεση μεθόδων επίλυσης του προβλήματος.

δ) προσδιορισμό και υλοποίηση προληπτικών ενεργειών που απαιτούνται

Ναι, μετά τη διερεύνηση υλοποιούνται οι απαιτούμενες προληπτικές ενέργειες με ευθύνη του ίδιου υπαλλήλου στον οποίο είχε ανατεθεί και η διερεύνηση και η ανεύρεση μεθόδων επίλυσης.

ε) αρχειοθέτηση των αποτελεσμάτων των ενεργειών που ανελήφθησαν (βλ. 4.3.3) και

Όχι, η διαδικασία για προληπτικές ενέργειες δεν είναι τεκμηριωμένη. Δεν συμπληρώνεται κάποιο έντυπο, συνεπώς δεν τηρούνται και σχετικά αρχεία.

στ) ανασκόπηση των προληπτικών ενεργειών που αναλαμβάνονται

Ναι, γίνεται επαλήθευση των ενεργειών που ανελήφθησαν από τον ίδιο υπάλληλο που τις πραγματοποίησε. Δεν καταγράφεται όμως η επαλήθευση αυτή σε κάποιο έντυπο ούτως ώστε και να αποδεικνύεται.

5.6.2. *Προτάσεις*

Ο οργανισμός πράγματι λαμβάνει ενέργειες για την εξάλειψη των αιτιών των «μη συμμορφώσεων» αλλά και των «πιθανών μη συμμορφώσεων», έτσι ώστε να εξασφαλίζεται η μη επανάληψη των πρώτων και να προλαμβάνεται η εμφάνισή των τελευταίων.

Δεν έχει όμως καθιερώσει μια τεκμηριωμένη διαδικασία για τη λήψη διορθωτικών και προληπτικών ενεργειών. Δεν συμπληρώνεται κάποιο έντυπο και δε γίνεται σωστή ανασκόπηση των ενεργειών που πραγματοποιήθηκαν.

Αρχικά, ο οργανισμός οφείλει σύμφωνα με το πρότυπο να προσδιορίσει μια τεκμηριωμένη διαδικασία στην οποία να περιγράφεται ο τρόπος διαπίστωσης ανάγκης, αναφοράς και παρακολούθησης των διορθωτικών και προληπτικών ενεργειών με απώτερο σκοπό τη διαρκή βελτίωση του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών και γενικότερα της λειτουργίας του. Η διαδικασία αυτή θα ενεργοποιείται όταν προκύψει ανάγκη καταγραφής και παρακολούθησης διορθωτικής ή προληπτικής ενέργειας. Μία τέτοια τεκμηριωμένη διαδικασία που θα μπορούσε να εφαρμόσει ο οργανισμός είναι η ακόλουθη :

Οποιοδήποτε μέλος του προσωπικού θα εκτιμά ότι κάποιο λειτουργικό κομμάτι του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών, μπορεί να οδηγήσει σε μη συμμόρφωση ή δυσλειτουργία, ή θα ανακαλύπτει μια «μη συμμόρφωση» του Συστήματος, θα συνεχίσει να ενημερώνει το ημερήσιο ημερολόγιο της Διεύθυνσής του και να συμπληρώνει μια Αναφορά Ασφαλείας το έντυπο «Αναφορά Βλαβών, Συμβάντων & Ατυχημάτων» (ΠΑΡΑΡΤΗΜΑ IV-Έντυπο 8.1) αλλά θα πρέπει να επικοινωνεί και με τον «Υπεύθυνο Ασφάλειας Πληροφοριών» και όχι μόνο με τον αντίστοιχο Διευθυντή.

Στη συνέχεια, ο «Υπεύθυνος Ασφάλειας Πληροφοριών» θα συμπληρώνει το έντυπο «ΔΙΟΡΘΩΤΙΚΕΣ & ΠΡΟΛΗΠΤΙΚΕΣ ΕΝΕΡΓΕΙΕΣ» (ΠΑΡΑΡΤΗΜΑ IV-Έντυπο 8.2) σε συνεργασία με τον Διευθυντή της μονάδας που αφορά η παρατήρηση.

Ο «Υπεύθυνος Ασφάλειας Πληροφοριών», και όχι ο Διευθυντής της μονάδας, θα αξιολογεί τη σημαντικότητα και θα αναθέτει ή όχι στον αντίστοιχο Διευθυντή μονάδας τη διερεύνηση και ανέρευση μεθόδων επίλυσης του προβλήματος.

Μετά τη διερεύνηση, το έντυπο «ΔΙΟΡΘΩΤΙΚΕΣ & ΠΡΟΛΗΠΤΙΚΕΣ ΕΝΕΡΓΕΙΕΣ» θα συμπληρώνεται με τις απαιτούμενες διορθωτικές ή προληπτικές ενέργειες και θα κοινοποιείται στον Γενικό Διευθυντή, ούτως ώστε να αποτελέσει εισερχόμενο σε μελλοντική Ανασκόπηση της Διοίκησης.

Η εφαρμογή της πρότασης για την επίλυση του προβλήματος θα γίνεται με ευθύνη του Διευθυντή της αντίστοιχης μονάδας και όχι μόνο με ευθύνη του υπαλλήλου που εκτέλεσε την διορθωτική ή προληπτική ενέργεια.

Σε περίπτωση που απαιτείται χειρισμός «μη συμμόρφωσης», για οτιδήποτε αφορά το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών, τότε την ευθύνη για την αποκατάσταση της «μη συμμόρφωσης» θα έχει ο «Υπεύθυνος Ασφάλειας Πληροφοριών», σε συνεργασία με τον Διευθυντή της μονάδας που παρατηρήθηκε.

Επίσης, ο εκτελών της διορθωτικής ή προληπτικής ενέργειας δε θα μπορεί να είναι ο ίδιος που θα κάνει και την επαλήθευση υλοποίησης αυτής στο έντυπο « ΔΙΟΡΘΩΤΙΚΕΣ & ΠΡΟΛΗΠΤΙΚΕΣ ΕΝΕΡΓΕΙΕΣ».

Τέλος, υπεύθυνος για την τήρηση αρχείων των συμπληρωμένων εντύπων Διορθωτικών και Προληπτικών Ενεργειών θα είναι ο «Υπεύθυνος Ασφάλειας Πληροφοριών», ενώ αντίγραφα τους θα δίνονται και στις Διευθύνσεις και θα τηρούνται σε αρχείο από τον Προϊστάμενο της εκάστοτε Διεύθυνσης (η κάθε Διεύθυνση θα τηρεί αυτά που την αφορούν).

5.7. Παράρτημα προτύπου:ΠΑΡΑΡΤΗΜΑ Α «Στόχοι ελέγχων & Έλεγχοι»

ΠΑΡΑΡΤΗΜΑ Α ΠΡΟΤΥΠΟΥ

«Στόχοι Ελέγχων & Έλεγχοι»

Οι στόχοι ελέγχων και οι έλεγχοι που αναγράφονται στον Πίνακα Α.1 του Παραρτήματος Α του προτύπου ISO/IEC 27001:2005 προέρχονται από εκείνους που αναφέρονται στο πρότυπο ISO/IEC 17799:2005 στις παραγράφους 5 έως 15.

Η λίστα αυτή δεν είναι εξαντλητική ούτε όμως και υποχρεωτική. Μπορούν κάθε φορά να επιλέγονται επιπλέον ή λιγότεροι έλεγχοι, ανάλογα με τις ανάγκες του κάθε οργανισμού.

Στο στάδιο σχεδιασμού ενός «Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ISMS-Information Security Management System)» μια βασική απαίτηση του προτύπου ISO/IEC 27001:2005 είναι να συντάξει ο οργανισμός μια «Δήλωση Εφαρμοσιμότητας» (απαίτηση 4.2.1.ι).

Η «Δήλωση Εφαρμοσιμότητας» πρέπει να περιλαμβάνει τους στόχους ελέγχων και τους ελέγχους που επιλέχθηκαν από το Παράρτημα Α του προτύπου καθώς και την αιτιολόγηση της επιλογής τους.

Ειδικότερα, η επιλογή των στόχων ελέγχων και των ελέγχων πρέπει να γίνεται σύμφωνα με τα κριτήρια της απαίτησης 4.2.1.ζ. Λαμβάνοντας, δηλαδή, υπόψη τις απαιτήσεις ασφαλείας που προκύπτουν από τη διαδικασία αξιολόγησης κινδύνων, τη διαδικασία αντιμετώπισής τους και τις διάφορες νομικές ή κανονιστικές απαιτήσεις.

Πράγματι, ο οργανισμός έχοντας συνυπολογίσει τους παράγοντες αυτούς έχει εντοπίσει και καταγράψει τους κινδύνους που απειλούν την ασφάλεια των κρίσιμων αεροναυτικών πληροφοριών του, οι οποίοι παρουσιάζονται παρακάτω :

1. Εξάντληση χρόνου ζωής εξοπλισμού
2. Φυσικές & εξωτερικές απειλές (σεισμός, πλημμύρα, πυρκαγιά, τρομοκρατική ενέργεια)
3. Πτώση τάσης ρεύματος
4. Ιοί

5. Όχι συγχρονισμός ρολογιών συστήματος
6. Λανθασμένη καταχώρηση, παράλειψη καταχώρησης
7. Απώλεια εντύπου
8. Μη ιχνηλασιμότητα συμβάντος ασφάλειας πληροφοριών
9. Παράνομη πρόσβαση
10. Όχι επαλήθευση (cross-check) δεδομένων
11. Όχι επαλήθευση τελικής πληροφορίας

Επίσης, έχει επιλέξει από τον Πίνακα Α.1 συγκεκριμένους στόχους ελέγχων και ελέγχους για τον κάθε κίνδυνο ξεχωριστά. Ορισμένοι από αυτούς τους ελέγχους είναι «καλές γενικές πρακτικές» ενώ κάποιοι άλλοι είναι «έλεγχοι σε επίπεδο διεργασίας» και οι δύο αυτές κατηγορίες περιγράφονται αναλυτικά παρακάτω.

«Έλεγχοι ως "καλές γενικές πρακτικές"»

Υπάρχουν πέντε έλεγχοι οι οποίοι έχουν επιλεγεί από το Παράρτημα Α του προτύπου και έχουν εφαρμοστεί σε όλο το σύστημα διαχείρισης ασφάλειας πληροφοριών του οργανισμού ως «καλές γενικές πρακτικές» ούτος ώστε να εξασφαλιστεί η εύρυθμη λειτουργία του και οι οποίοι είναι οι εξής :

1. **Κίνδυνος :**

   Εξάντληση χρόνου ζωής εξοπλισμού

   Στόχος ελέγχου :

   Να αποτρέψει τη διακοπή των δραστηριοτήτων του οργανισμού εξαιτίας φθοράς του εξοπλισμού λόγω χρόνου

   Έλεγχος :

   (**Έλεγχος Α.9.2.4**)

   -Έλεγχος εφαρμογής προληπτικής συντήρησης βάσει του «Προγράμματος ελέγχου & προληπτικής συντήρησης»

   -Έλεγχος ύπαρξης ρήτρας στη σύμβαση για αποζημίωση σε περίπτωση βλάβης με υπαιτιότητα του κατασκευαστή

   Αιτιολόγηση :

   Ο έλεγχος αυτός επιλέχθηκε διότι ο εξοπλισμός πρέπει να συντηρείται σωστά ώστε να εξασφαλιστεί η συνέχιση της διαθεσιμότητας και της ακεραιότητας του

2. **Κίνδυνος :**

   Φυσικές & εξωτερικές απειλές (σεισμός, πλημμύρα, πυρκαγιά, τρομοκρατική ενέργεια)

Στόχος ελέγχου :

Να αποτρέψει μη εξουσιοδοτημένη πρόσβαση ή ανεπανόρθωτη ζημιά στις κρίσιμες αεροναυτικές πληροφορίες του οργανισμού

Έλεγχος :

(**Έλεγχος Α.9.1.4**)

-Έλεγχος ύπαρξης πυροσβεστήρων & ανιχνευτών καπνού

-Έλεγχος ύπαρξης μιας παρόμοιας εγκατάστασης (server) σε άλλη περιοχή (ο οργανισμός διαθέτει τέτοια στη Θεσσαλονίκη), η οποία να επικοινωνεί με την κεντρική εγκατάσταση (server) και να διαθέτει κατοπτρικά αρχεία

-Έλεγχος ύπαρξης ασφάλισης σε περίπτωση πυρκαγιάς, πλημμύρας

Αιτιολόγηση :

Ο έλεγχος αυτός επιλέχθηκε διότι οι κρίσιμες αεροναυτικές πληροφορίες πρέπει να προστατεύονται από καταστροφές λόγω πυρκαγιάς, πλημμύρας, σεισμού, έκρηξης, τρομοκρατικής ενέργειας και άλλων μορφών φυσικών ή προκαλούμενων από τον άνθρωπο καταστροφών

3. **Κίνδυνος :**

Πτώση τάσης ρεύματος

Στόχος ελέγχου :

Να αποτρέψει τη διακοπή των δραστηριοτήτων του οργανισμού ή την απώλεια κρίσιμων αεροναυτικών πληροφοριών εξαιτίας μιας πτώσης τάσης ρεύματος

Έλεγχος :

(**Έλεγχος Α9.2.2**)

-Έλεγχος ύπαρξης «τροφοδοτικών αδιάλειπτης λειτουργίας (UPS-Uninterruptible power supply)» καθώς και ορθή λειτουργία αυτών (π.χ. περιοδικά κλείνουν το ρεύμα και ελέγχουν εάν λειτουργούν τα τροφοδοτικά)

Αιτιολόγηση :

Ο έλεγχος αυτός επιλέχθηκε διότι ο εξοπλισμός πρέπει να προστατεύεται από πτώσεις τάσης ρεύματος αλλά και από άλλες επιπλοκές στα τροφοδοτικά αδιάλειπτης λειτουργίας

4. **Κίνδυνος :**

Ιοί

Στόχος ελέγχου :

Να διαφυλάξει την ακεραιότητα του λογισμικού και των κρίσιμων αεροναυτικών πληροφοριών

Έλεγχος :

(**Έλεγχος Α10.4.1**)

-Έλεγχος ύπαρξης ειδικών προγραμμάτων τα οποία καταγράφουν σε ξεχωριστά αρχεία τις επιθέσεις από ιούς (anti-virus software) καθώς και εάν είναι εγκατεστημένη η πιο ανανεωμένη έκδοση αυτών των προγραμμάτων

-Περιοδικός έλεγχος όλων αυτών των αρχείων για το εάν είναι «χτυπημένα» από ιό

Αιτιολόγηση :

Ο έλεγχος αυτός επιλέχθηκε διότι είναι απαραίτητο να είναι εγκατεστημένος κάποιος έλεγχος που θα διασφαλίζει τον εντοπισμό, την πρόληψη και την ανάκτηση, ώστε να προστατεύονται οι κρίσιμες αεροναυτικές πληροφορίες έναντι ιών που τις απειλούν

5. **Κίνδυνος :**

Όχι συγχρονισμός ρολογιών συστήματος

Στόχος ελέγχου :

Να διασφαλιστεί η αξιοπιστία των κρίσιμων αεροναυτικών πληροφοριών

Έλεγχος :

(**Ελεγχος Α10.10.6**)

-Έλεγχος ότι όλοι οι διαφορετικοί Η/Υ των εμπλεκόμενων μονάδων έχουν τον ίδιο χρόνο

Αιτιολόγηση :

Ο έλεγχος αυτός επιλέχθηκε διότι τα ρολόγια όλων των εμπλεκόμενων μονάδων του οργανισμού στο «Σύστημα διαχείρισης ασφάλειας πληροφοριών» πρέπει να είναι συγχρονισμένα βάσει ενός συμφωνημένου ακριβή χρόνου

«Έλεγχοι σε επίπεδο διεργασίας»

Υπάρχουν έξι έλεγχοι οι οποίοι έχουν επίσης επιλεγεί από το Παράρτημα Α του προτύπου και εφαρμόζονται σε συγκεκριμένα σημεία πάνω στη βασική διεργασία έκδοσης και ενημέρωσης του «Εγχειριδίου Αεροναυτικών Πληροφοριών (AIP)» και αναλύονται παρακάτω.

Ειδικότερα, στην Υποδιεργασία 1 «Συλλογή & Καταγραφή Αεροναυτικών Πληροφοριών» κάθε μία από τις τρείς αρμόδιες Διευθύνσεις (Δ3,Δ4,Δ5&6) αναλαμβάνει τη συλλογή των αντίστοιχων πρωταρχικών αεροναυτικών πληροφοριών ή την αλλαγή των υφιστάμενων αεροναυτικών πληροφοριών.

Τελικός σκοπός είναι η δημιουργία τριών ξεχωριστών ενδιάμεσων εντύπων (AD_HP, ENR, GEN), εάν πρόκειται για καινούρια πληροφορία, ή τη δημιουργία τριών αντίστοιχων ενδιάμεσων εντύπων (Διόρθωση AIP, Διόρθωση AIRACAIP, Συμπλήρωση AIP, Συμπλήρωση AIRACAIP), εάν πρόκειται για αλλαγή υφιστάμενης πληροφορίας, και τη διαβίβασή τους μεταξύ των τριών Διευθύνσεων προς περαιτέρω συμπλήρωση και τελική έγκριση. Κάθε αεροναυτική πληροφορία που καταχωρήθηκε φέρει τα στοιχεία του υπαλλήλου που τη χειρίστηκε.

Σε αυτά τα βασικά σημεία της Υποδιεργασίας 1 εντοπίστηκαν τρείς κίνδυνοι. Ο πρώτος είναι εκείνος της λανθασμένης καταχώρησης ή της παράλειψης καταχώρησης. Ο δεύτερος είναι η απώλεια κάποιου εντύπου κατά τη διάρκεια της διαβίβασής του. Ο τρίτος τέλος είναι η μη αναφορά των στοιχείων του υπαλλήλου που καταχώρησε ή τροποποίησε την αεροναυτική πληροφορία.

Για την εξάλειψη των παραπάνω κινδύνων ο οργανισμός επέλεξε από το Παράρτημα Α και εφαρμόζει επί της Υποδιεργασίας 1 τρείς συγκεκριμένους ελέγχους, οι οποίοι είναι οι εξής :

6. **Κίνδυνος :**

   Λανθασμένη καταχώρηση, παράλειψη καταχώρησης

   Στόχος ελέγχου :

   Η αποφυγή λαθών, παραλείψεων και τροποποιήσεων άνευ αδείας

   Έλεγχος :

   (**Ελεγχος Α12.2.1**)

   -Έλεγχος ορθής λειτουργίας μηχανισμών επαλήθευσης (π.χ. εσκεμμένη εισαγωγή λάθος πληροφορίας και εξακρίβωση εάν εντοπίστηκε εγκαίρως)

   Αιτιολόγηση :

   Ο έλεγχος αυτός επιλέχθηκε διότι η εισαγωγή δεδομένων πρέπει να επικυρώνεται ώστε να εξασφαλίζεται ότι τα δεδομένα αυτά είναι ορθά και κατάλληλα

7. **Κίνδυνος :**

   Απώλεια εντύπου

   Στόχος ελέγχου :

   Να διατηρήσει την ακεραιότητα και τη διαθεσιμότητα των αεροναυτικών πληροφοριών

   Έλεγχος :

   (**Ελεγχος Α10.5.1**)

   -Έλεγχος ύπαρξης αντιγράφων ασφαλείας σε αρχεία (back-up αρχεία) προηγούμενων μηνών, ετών

Αιτιολόγηση :

Ο έλεγχος αυτός επιλέχθηκε διότι πρέπει οι κρίσιμες αεροναυτικές πληροφορίες να είναι διαθέσιμες σε όσους έχουν εξουσιοδοτημένη πρόσβαση σε αυτές

8. **Κίνδυνος :**

Μη ιχνηλασιμότητα συμβάντος ασφάλειας πληροφοριών

Στόχος ελέγχου :

Να επιτευχτεί και να διατηρηθεί η κατάλληλη προστασία των κρίσιμων αεροναυτικών πληροφοριών του οργανισμού

Έλεγχος :

(**Έλεγχος A7.1.2**)

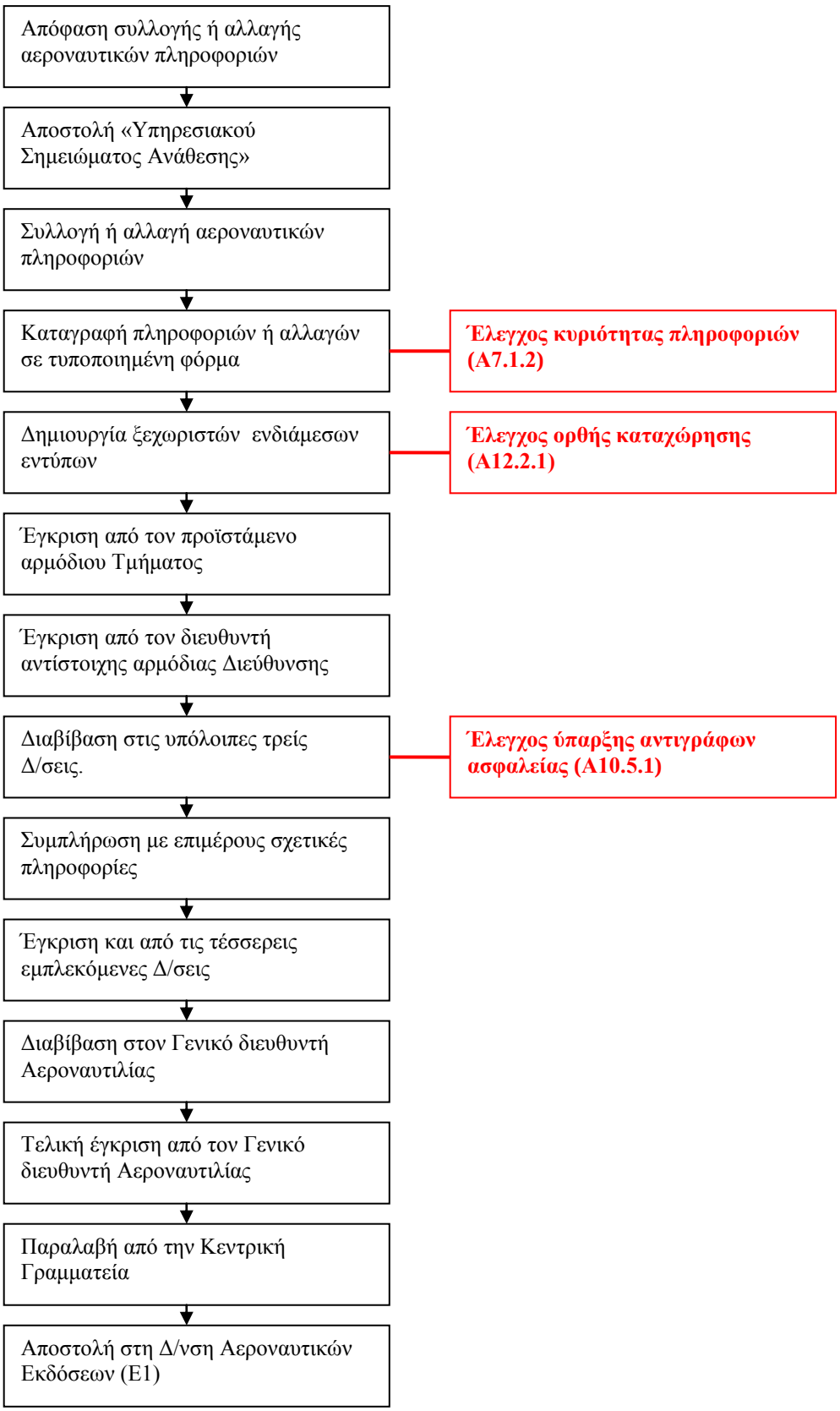
- Έλεγχος κυριότητας των αεροναυτικών πληροφοριών. (π.χ. για κάθε κρίσιμη αεροναυτική πληροφορία ποιος έχει οριστεί υπεύθυνος και πού φαίνεται αυτό στο σύστημα)

Αιτιολόγηση :

Ο έλεγχος αυτός επιλέχθηκε διότι όλες οι κρίσιμες αεροναυτικές πληροφορίες πρέπει να «ανήκουν» σε ένα προκαθορισμένο τμήμα του οργανισμού

Και οι οποίοι αποτυπώνονται και στη ροή ενεργειών της Υποδιεργασίας 1 παρακάτω:

ΔΙΑΔΙΚΑΣΙΑ
ΥΠΟΔΙΕΡΓΑΣΙΑΣ 1:



Στην Υποδιεργασία 2 «Επεξεργασία Αεροναυτικών Πληροφοριών» το Τμήμα Εγχειριδίων Αεροναυτικών Πληροφοριών-AIP (E1/A) αναλαμβάνει τον έλεγχο της εγκυρότητας των πληροφοριών που είναι καταγεγραμμένες σε κάποιο ή και στα τρία ενδιάμεσα έντυπα που προαναφέρθηκαν, μέσω συγκρίσεως τους με τα στοιχεία που διαθέτει σε ηλεκτρονικές βάσεις δεδομένων, χρησιμοποιώντας την ηλεκτρονική εφαρμογή eAIP@wizard. Κάθε αεροναυτική πληροφορία που επεξεργάζεται φέρει τα στοιχεία του υπαλλήλου που τη χειρίστηκε.

Μόλις τα έντυπα επαληθευτούν και εγκριθούν διαχωρίζονται στις εξής κατηγορίες :

-Αεροναυτική πληροφορία AIP

-Αεροναυτική αγγελία NOTAM

Και αναθέτεται η επίσημη έκδοση των «Αεροναυτικών Πληροφοριών AIP» στο τυπογραφείο της Υ.Π.Α.

Στο στάδιο αυτό της Υποδιεργασίας 2 εντοπίστηκαν τέσσερις κίνδυνοι. Συγκεκριμένα, ο πρώτος κίνδυνος είναι εκείνος της παράνομης πρόσβασης μη εξουσιοδοτημένων χρηστών στην ηλεκτρονική εφαρμογή eAIP@wizard. Ο δεύτερος είναι να μην πραγματοποιηθεί ορθά η επαλήθευση των αεροναυτικών πληροφοριών. Ο τρίτος είναι να μην αναφέρονται τα στοιχεία του υπαλλήλου που τις επεξεργάστηκε και τέλος ο τέταρτος είναι να μην ελεγχθούν οι πληροφορίες πριν αποσταλούν στο τυπογραφείο για τυχόν λάθος διαχωρισμό τους.

Για την εξάλειψη των παραπάνω κινδύνων ο οργανισμός επέλεξε από το Παράρτημα Α και εφαρμόζει επί της Υποδιεργασίας 2 τέσσερις συγκεκριμένους ελέγχους, ο τελευταίος από τους οποίους εφαρμόζεται όπως προαναφέρθηκε και στην Υποδιεργασία 1. Οι έλεγχοι αυτοί είναι οι εξής :

9. **Κίνδυνος :**

   Παράνομη πρόσβαση

   Στόχος ελέγχου :

   Να αποτραπεί η μη εξουσιοδοτημένη πρόσβαση σε κρίσιμες αεροναυτικές πληροφορίες

   Έλεγχος :

   (**Έλεγχος A11.5.2**)

   - Έλεγχος ύπαρξης ονόματος χρήστη (ID-user identification) και κωδικού πρόσβασης (password) καθώς και ορθής χρήσης αυτών

   Αιτιολόγηση :

   Ο έλεγχος αυτός επιλέχθηκε διότι κάθε χρήστης πρέπει να έχει ένα μοναδικό όνομα (ID) και κωδικό (password) για δική του χρήση μόνο.

10. Κίνδυνος :

Όχι επαλήθευση (cross-check) δεδομένων

Στόχος ελέγχου :

Η αποφυγή λαθών, παραλείψεων και τροποποιήσεων άνευ αδείας

Έλεγχος :

(**Έλεγχος A12.2.2**)

-Έλεγχος ύπαρξης μηχανισμών επαλήθευσης στην εφαρμογή eAip@wizard (π.χ. εσκεμμένη εισαγωγή λάθος πληροφορίας και εξακρίβωση εάν η εφαρμογή εμφάνισε κόκκινη προειδοποίηση "alert")

Αιτιολόγηση :

Ο έλεγχος αυτός επιλέχθηκε διότι είναι αναγκαίο να ενσωματωθούν έλεγχοι επαλήθευσης στην εφαρμογή eAip@wizard για την ανίχνευση πιθανών λαθών στις κρίσιμες αεροναυτικές πληροφορίες μέσω της επεξεργασίας ή εξαιτίας εσκεμμένων πράξεων

11. Κίνδυνος :

Όχι επαλήθευση τελικής πληροφορίας

Στόχος ελέγχου :

Η αποφυγή λαθών, παραλείψεων και τροποποιήσεων άνευ αδείας

Έλεγχος :

(**Έλεγχος A12.2.4**)

- Έλεγχος ορθής λειτουργίας μηχανισμών επαλήθευσης (π.χ. εσκεμμένη εισαγωγή λάθος πληροφορίας και εξακρίβωση εάν εντοπίστηκε)

Αιτιολόγηση :

Ο έλεγχος αυτός επιλέχθηκε διότι τα τελικά δεδομένα πρέπει να επικυρώνονται ώστε να εξασφαλίζεται ότι είναι ορθά αλλά και ότι η όλη διαδικασία επεξεργασίας είναι η κατάλληλη

12. Κίνδυνος :

Μη ιχνηλασιμότητα συμβάντος ασφάλειας πληροφοριών

Στόχος ελέγχου :

Να επιτευχτεί και να διατηρηθεί η κατάλληλη προστασία των κρίσιμων αεροναυτικών πληροφοριών του οργανισμού

Έλεγχος :

(**Έλεγχος A7.1.2**)

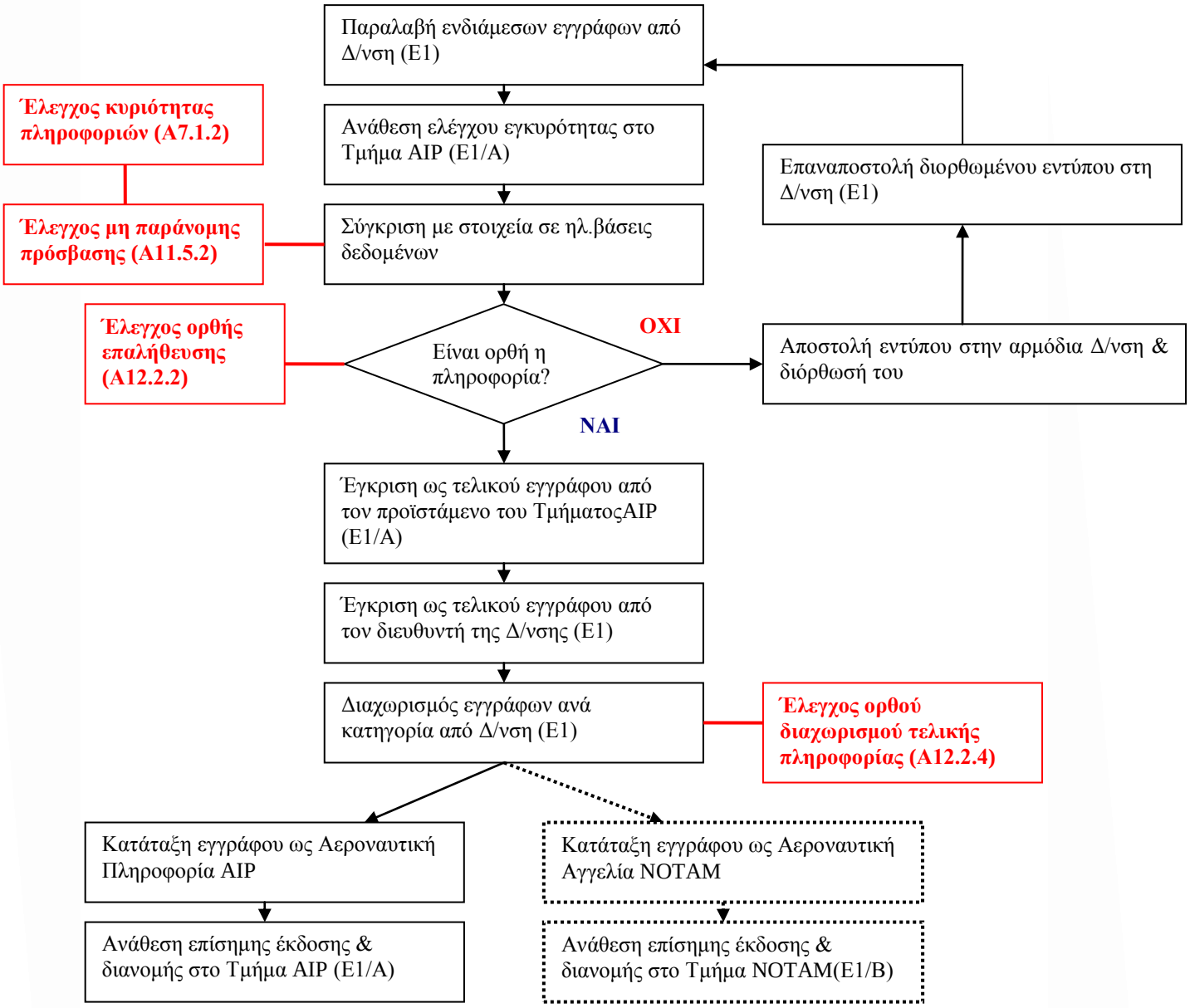
- Έλεγχος κυριότητας των αεροναυτικών πληροφοριών. (π.χ. για κάθε κρίσιμη αεροναυτική πληροφορία ποιος έχει οριστεί υπεύθυνος και πού φαίνεται αυτό στο σύστημα)

Αιτιολόγηση :

Ο έλεγχος αυτός επιλέχθηκε διότι όλες οι κρίσιμες αεροναυτικές πληροφορίες πρέπει να «ανήκουν» σε ένα προκαθορισμένο τμήμα του οργανισμού

Και οι οποίοι αποτυπώνονται και στη ροή ενεργειών της Υποδιεργασίας 2 παρακάτω:

ΔΙΑΔΙΚΑΣΙΑ
ΥΠΟΔΙΕΡΓΑΣΙΑΣ 2:



Στην Υποδιεργασία 3 «Έκδοση & Διανομή Εγχειριδίου Αεροναυτικών Πληροφοριών (AIP)» το τυπογραφείο της Υ.Π.Α παραλαμβάνει τις αεροναυτικές πληροφορίες σε μορφή pdf αρχείου και αναλαμβάνει την εκτύπωσή τους και την αποστολή του τυπωμένου πια εγχειριδίου πίσω στο Τμήμα Εγχειριδίων Αεροναυτικών Πληροφοριών-AIP (E1/A).

Στο σημείο αυτό εντοπίστηκε ο κίνδυνος να μην ελεγχθεί η ορθότητα της εκτυπωμένης έκδοσης προτού αποσταλεί στο Τμήμα Εγχειριδίων (E1/A).

Για την εξάλειψη του άνω κινδύνου ο οργανισμός επέλεξε από το Παράρτημα Α και εφαρμόζει επί της Υποδιεργασίας 3 τον ίδιο έλεγχο που προαναφέρθηκε στην Υποδιεργασία 2, οι οποίος είναι ο εξής :

13. Κίνδυνος :

Όχι επαλήθευση τελικής πληροφορίας

Στόχος ελέγχου :

Η αποφυγή λαθών, παραλείψεων και τροποποιήσεων άνευ αδείας

Έλεγχος :

(Ελεγχος A12.2.4)

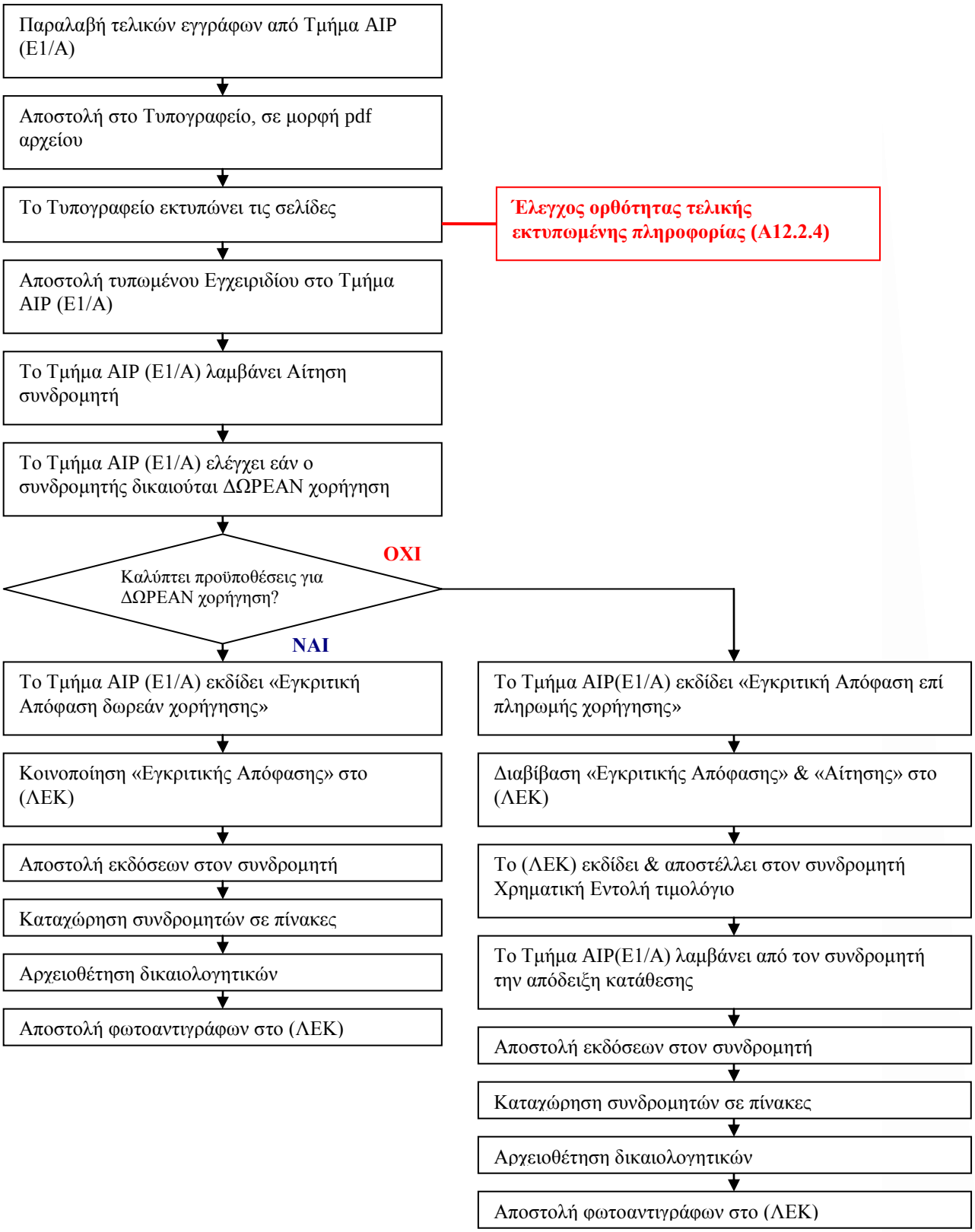
- Έλεγχος ορθής λειτουργίας μηχανισμών επαλήθευσης (π.χ. εσκεμμένη εισαγωγή λάθος πληροφορίας και εξακρίβωση εάν εντοπίστηκε)

Αιτιολόγηση :

Ο έλεγχος αυτός επιλέχθηκε διότι τα τελικά δεδομένα πρέπει να επικυρώνονται ώστε να εξασφαλίζεται ότι είναι ορθά αλλά και ότι η όλη διαδικασία επεξεργασίας είναι η κατάλληλη

Και ο οποίος αποτυπώνεται και στη ροή ενεργειών της Υποδιεργασίας 3 παρακάτω:

ΔΙΑΔΙΚΑΣΙΑ
ΥΠΟΔΙΕΡΓΑΣΙΑΣ 3:



ΒΑΘΜΟΣ ΙΚΑΝΟΠΟΙΗΣΗΣ ΑΠΑΙΤΗΣΕΩΝ ISO 27001

ΑΠΑΙΤΗΣΕΙΣ ISO 27001	**ΒΑΘΜΟΣ ΙΚΑΝΟΠΟΙΗΣΗΣ**
Απαίτηση 4 : *Καθιέρωση/δημιουργία και διαχείριση του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών – ISMS (Information Security Management System)*	○
Απαίτηση 5 : *Ευθύνη της Διοίκησης*	○
Απαίτηση 6 : *Εσωτερικές επιθεωρήσεις ISMS*	○
Απαίτηση 7 : *Ανασκόπηση ISMS από τη Διοίκηση*	○
Απαίτηση 8 : *Βελτίωση του ISMS*	○
ΑΠΑΙΤΗΣΗ ISO 27001 4 : Καθιέρωση/δημιουργία και διαχείριση του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών – ISMS (Information Security Management System)	**ΒΑΘΜΟΣ ΙΚΑΝΟΠΟΙΗΣΗΣ**
4.2.1 : Δημιουργία ISMS	●
4.2.2 : Εφαρμογή & λειτουργία ISMS	○
4.2.3 : Παρακολούθηση & επανεξέταση ISMS	○
4.2.4 : Συντήρηση & βελτίωση ISMS	○
4.3 : Απαιτήσεις τεκμηρίωσης	○
ΑΠΑΙΤΗΣΗ ISO 27001 5 : Ευθύνη της Διοίκησης	**ΒΑΘΜΟΣ ΙΚΑΝΟΠΟΙΗΣΗΣ**
5.1 : Δέσμευση Διοίκησης	○
5.2.1 : Διαχείριση των πόρων	●
5.2.2 : Εκπαίδευση, ευαισθητοποίηση & ικανότητα	●
ΑΠΑΙΤΗΣΗ ISO 27001 6 : Εσωτερικές Επιθεωρήσεις ISMS	**ΒΑΘΜΟΣ ΙΚΑΝΟΠΟΙΗΣΗΣ**
Διενέργεια προγραμματισμένων εσωτερικών ελέγχων	○
Πρόγραμμα Εσωτερικών Επιθεωρήσεων	~
Αντικειμενική & αμερόληπτη επιλογή Ελεγκτών	~
Ύπαρξη τεκμηριωμένης διαδικασίας	~
Επαλήθευση (follow-up) δράσεων που αναλήφθηκαν	●
ΑΠΑΙΤΗΣΗ ISO 27001 7 : Ανασκόπηση ISMS από τη Διοίκηση	**ΒΑΘΜΟΣ ΙΚΑΝΟΠΟΙΗΣΗΣ**
7.1 : Προγραμματισμένη & Τεκμηριωμένη ανασκόπηση	○
7.2 : Εισερχόμενα ανασκοπήσεων	○
7.3 : Εξερχόμενα ανασκοπήσεων	○
ΑΠΑΙΤΗΣΗ ISO 27001 8 : Βελτίωση του ISMS	**ΒΑΘΜΟΣ ΙΚΑΝΟΠΟΙΗΣΗΣ**
8.1 : Συνεχής Βελτίωση	○
8.2 : Διορθωτικές Ενέργειες	○
8.3 : Προληπτικές Ενέργειες	○

●: Πλήρης υιοθέτηση ○: Μερική υιοθέτηση ~: Μηδενική υιοθέτηση

6. ΣΥΜΠΕΡΑΣΜΑΤΑ-ΠΡΟΤΑΣΕΙΣ

6.1. Συμπεράσματα

Κάθε κράτος είναι υπεύθυνο σύμφωνα με τη Διεθνή Σύμβαση του Διεθνούς Οργανισμού Πολιτικής Αεροπορίας (ICAO-International Civil Aviation Organization) και το Παράρτημα 15 (Annex 15) να διασφαλίζει τη διαχείριση των κρίσιμων αεροναυτικών πληροφοριών του. Ειδικότερα, έχει οριστεί μία συγκεκριμένη Υπηρεσία ως υπεύθυνη για τη συλλογή και διανομή των αεροναυτικών πληροφοριών που είναι απαραίτητες για την ασφάλεια, κανονικότητα και αποτελεσματικότητα της διεθνούς και εθνικής αεροναυτιλίας εντός του εναέριου χώρου της επικράτειας μιας χώρας καθώς και του εναέριου χώρου υπεράνω των Διεθνών Υδάτων για τα οποία την ευθύνη παροχής υπηρεσιών αεροναυτιλίας έχει το εν λόγω κράτος (*Υπηρεσία Παροχής Αεροναυτικών Πληροφοριών-AIS Aeronautical Information Services)*. Στην Ελλάδα η Υπηρεσία AIS παρέχεται από την Υπηρεσία Πολιτικής Αεροπορίας (Υ.Π.Α), η οποία υπάγεται στο Υπουργείο Μεταφορών και Επικοινωνιών (και στο εξής θα αναφέρεται ως «Οργανισμός»).

Το βασικό έγγραφο αεροναυτιλίας είναι το «Εγχειρίδιο Αεροναυτικών Πληροφοριών-AIP (Aeronautical Information Publication)», προορισμός του οποίου είναι να ικανοποιήσει τις διεθνείς προδιαγραφές για την ανταλλαγή των μόνιμων αεροναυτικών πληροφοριών καθώς και των μόνιμων ή των προσωρινών, μακράς όμως διάρκειας, αλλαγών τους. Το ελληνικό Εγχειρίδιο AIP δημοσιεύεται με κείμενο στην αγγλική γλώσσα, σε δύο ξεχωριστούς τόμους και με χαλαρή μορφή βιβλιοδεσίας (ντοσιέ) ώστε να ενημερώνεται εύκολα.

Στην παρούσα εργασία μελετήθηκε ο βαθμός κατά τον οποίο το σύστημα διαχείρισης ασφάλειας κρίσιμων αεροναυτικών πληροφοριών που εφαρμόζει η Υ.Π.Α πληροί τις απαιτήσεις του προτύπου ISO/IEC 27001:2005 «Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών-Απαιτήσεις».

Το πρότυπο ISO/IEC 9001:2000 «Συστήματα Διαχείρισης Ποιότητας-Απαιτήσεις» εισήγαγε τον «Κύκλο του Deming-PDCA (Plan-Do-Check-Act)» για την διαχείριση της ποιότητας σε συστήματα διοίκησης. Αντίστοιχα, τα σημαντικότερα πρότυπα συστήματα διαχείρισης που ακολούθησαν (π.χ. ISO 14001: 2004) υιοθέτησαν το ίδιο μοντέλο. Το ISO/IEC 27001:2005 ακολουθώντας αυτή την τάση, βασίζεται επίσης στο μοντέλο PDCA.

Ειδικότερα, το ISO/IEC 27001:2005 χρησιμοποιεί τον «Κύκλο του Deming-PDCA», με στόχο την αποτελεσματική εφαρμογή ενός «Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ISMS-Information Security Management System)». Το υπάρχον σύστημα

διαχείρισης ασφάλειας πληροφοριών της Υ.Π.Α εξετάστηκε ως προς το σχεδιασμό, την υλοποίηση, τον έλεγχο και τη συνεχή βελτίωσή του ώστε να προκύψει ο βαθμός κατά τον οποίο πληροί τις απαιτήσεις του προτύπου. Ακολούθως τα τέσσερα αυτά στάδια αναλύονται.

Όσον αφορά το ***σχεδιασμό***, ο βασικός του ρόλος είναι να καθορίσει ο οργανισμός όλες τις προδιαγραφές του συστήματος. Στο πρότυπο ISO/IEC 27001:2005 ο σχεδιασμός ενός συστήματος διαχείρισης ασφάλειας πληροφοριών αναφέρεται στον προσδιορισμό του αντικειμένου και των ορίων του συστήματος, στη διατύπωση μιας πολιτικής ασφάλειας πληροφοριών («πολιτική ISMS»), στον εντοπισμό των κινδύνων, στην αξιολόγησή τους, στην αντιμετώπισή τους και τέλος στην επιλογή των κατάλληλων ελέγχων.

Ο οργανισμός έχει τεκμηριωμένα ορίσει ως αντικείμενο του συστήματος την εξασφάλιση μιας επίσημης και σαφούς προσέγγισης της συστηματικής διαχείρισης της ασφάλειας πληροφοριών για την εκπλήρωση των υποχρεώσεων ασφαλείας. Συγκεκριμένα, στόχος του συστήματος είναι η εναρμόνιση διαδικασιών κατά την παροχή αεροναυτικών πληροφοριών μέσω της ύπαρξης ικανού προσωπικού, κοινών διαδικασιών και κοινής ερμηνείας των κανονισμών. Ενώ ως όρια του συστήματος έχουν οριστεί όλες οι μονάδες του οργανισμού που επηρεάζουν και επηρεάζονται από το σύστημα.

Ο οργανισμός διαθέτει πολιτική ασφάλειας πληροφοριών η οποία έχει καθοριστεί από την ελληνική νομοθεσία (Αεροπορικό Κώδικα, Νόμους, Π.Δ, Υπ. Αποφάσεις κ.τ.λ.) από τις Ευρωπαϊκές Οδηγίες που έχουν ενσωματωθεί στην ελληνική νομοθεσία καθώς και από απαιτήσεις που περιγράφονται στη Διεθνή Σύμβαση του Διεθνούς Οργανισμού Πολιτικής Αεροπορίας (ICAO) και το Παράρτημα 15. Η πολιτική ασφάλειας πληροφοριών της ΥΠΑ, η οποία έχει εγκριθεί και υπογραφεί από τον Διοικητή της Υπηρεσίας, αναφέρει ότι υπάρχουν τεκμηριωμένες διαδικασίες εντοπισμού των κινδύνων, αξιολόγησης και μείωσης της επικινδυνότητάς τους, οι οποίες αποτελούν και τη βάση του συστήματος.

Πράγματι, αναφορικά με τον εντοπισμό των κινδύνων διαπιστώθηκε από τα έγγραφα ότι ο οργανισμός έχει αναγνωρίσει τους ακόλουθους :

- *στον εξοπλισμό*: φυσική καταστροφή (σεισμός, τσουνάμι), ξαφνικές καταστροφές (μπλάκ-ουτ), ατύχημα (πυρκαγιά), τρομοκρατικές ενέργειες (9/11), ιούς, εξάντληση διάρκεια ζωής
- *στον ανθρώπινο παράγοντα* (χρήστες & διαχειριστές του συστήματος): λανθασμένη καταχώρηση, παράλειψη καταχώρησης, απώλεια εντύπου, παράνομη πρόσβαση
- *στις διαδικασίες*: αλλαγή διαδικασίας δίχως έγκαιρη ενημέρωση και εκπαίδευση προσωπικού

Επίσης, ο οργανισμός έχει προβεί στην αξιολόγηση των παραπάνω κινδύνων. Συγκεκριμένα, αξιολογώντας και αναλύοντας την πιθανότητα εμφάνισής τους σε συνδυασμό με τη σοβαρότητα των συνεπειών τους, ο οργανισμός έχει εκτιμήσει τα «αποδεκτά επίπεδα κινδύνου» (Επίπεδα 1 & 2), τα «μη αποδεκτά» (Επίπεδα 6 & 9) καθώς και τις ενδιάμεσες καταστάσεις (Επίπεδα 3 & 4) όπου ο κίνδυνος χαρακτηρίζεται επανεξεταστέος και είναι απαραίτητη η λήψη μέτρων ελαχιστοποίησης ή μείωσής του, ώστε να γίνει τουλάχιστον «ανεκτός».

Σχετικά με την αντιμετώπιση των κινδύνων ο οργανισμός έχει προσδιορίσει εναλλακτικές επιλογές μείωσης της επικινδυνότητάς τους. Τέλος, όσον αφορά το σχεδιασμό του συστήματος, ο οργανισμός έχει καθιερώσει συγκεκριμένους ελέγχους για την αντιμετώπιση των κινδύνων οι οποίοι αναφέρονται στη «Δήλωση Εφαρμοσιμότητάς» του.

Ο οργανισμός λοιπόν κατά το στάδιο του σχεδιασμού καθορίζει σε μεγάλο βαθμό τις προδιαγραφές του συστήματος. Συγκεκριμένα, προσδιορίζονται αντικείμενο και όρια του συστήματος, διατυπώνεται η πολιτική ασφάλειας πληροφοριών, λαμβάνονται υπόψη νομικές και κανονιστικές απαιτήσεις, τίθενται τα κριτήρια εντοπισμού και αξιολόγησης των κινδύνων, καθορίζονται οι εναλλακτικές επιλογές μείωσης της επικινδυνότητας τους και τέλος επιλέγονται οι κατάλληλοι έλεγχοι.

Σχετικά με την ***υλοποίηση***, ο βασικός της ρόλος είναι να εφαρμόσει ο οργανισμός τις προδιαγραφές που όρισε κατά το σχεδιασμό. Σύμφωνα με το πρότυπο η υλοποίηση ενός συστήματος διαχείρισης ασφάλειας πληροφοριών περιλαμβάνει τη διατύπωση ενός «Σχεδίου Μείωσης Κινδύνου», την εφαρμογή του, την εφαρμογή των προεπιλεγμένων ελέγχων και την καθιέρωση μιας μεθόδου μέτρησης της αποτελεσματικότητάς τους.

Ο οργανισμός προκειμένου να λειτουργήσουν οι έλεγχοι έχει διατυπώσει ένα «Σχέδιο Μείωσης Κινδύνου (Risk Treatment Plan) » το οποίο προσδιορίζει γραπτώς τη διαδικασία, τις ευθύνες και τις προτεραιότητες για την αντιμετώπιση συμβάντων.

Επίσης, για την εύρυθμη εφαρμογή του «Σχεδίου Μείωσης Κινδύνου» ο οργανισμός έχει εξασφαλίσει τους απαιτούμενους πόρους :

-υψηλά εξειδικευμένο και ικανό προσωπικό
-εκπαιδευτικά σεμινάρια στην Ελλάδα και στο εξωτερικό
-κατάλληλες υποδομές
-απαραίτητο εξοπλισμό
-χρήση αυτοματοποίησης (ηλεκτρονική εφαρμογή **eAIP.wiz@rd**)

Όμως, η Διοίκηση δεν έχει θεσπίσει συγκεκριμένους ρόλους για να εξασφαλίσει τόσο την άρτια εφαρμογή του «Σχεδίου Μείωσης Κινδύνου» όσο και τη συστηματική διαχείριση

της ασφάλειας πληροφοριών. Την ευθύνη διαχείρισης τέτοιων ζητημάτων έχουν αναλάβει οι Διευθυντές των μονάδων που εμπλέκονται στη διεργασία έκδοσης και ενημέρωσης του Εγχειριδίου AIP.

Εναλλακτικά θα μπορούσε να συσταθεί «Διεύθυνση Ασφάλειας Πληροφοριών» και να ανατεθούν στον «Υπεύθυνο Ασφάλειας Πληροφοριών» συγκεκριμένες αρμοδιότητες. Μεταξύ άλλων, η ανάλυση ενός συμβάντος να γίνεται συγκεντρωτικά από αυτόν, και όχι από κάθε Διεύθυνση ξεχωριστά, να διενεργεί Εσωτερικές Επιθεωρήσεις και να επαληθεύει την αποτελεσματικότητα των διορθωτικών και προληπτικών μέτρων. Ο οργανισμός με αυτόν τον τρόπο θα αντιμετωπίζεται ως σύνολο και όχι ως ξεχωριστές μονάδες, παράλληλα η διεργασία έκδοσης και ενημέρωσης του Εγχειριδίου AIP θα επιθεωρείται στην ολότητά της και όχι από κάθε Διεύθυνση ξεχωριστά και τέλος θα διασφαλίζεται αντικειμενικότητα και αμεροληψία.

Αναφορικά με την εφαρμογή ελέγχων στο στάδιο της υλοποίησης, ο οργανισμός πράγματι εφαρμόζει τους ελέγχους εκείνους που είχε προεπιλέξει στο στάδιο του σχεδιασμού και είχε συμπεριλάβει στη «Δήλωση Εφαρμοσιμότητας» του. Δεν έχει όμως καθιερώσει μια μέθοδο μέτρησης της αποτελεσματικότητάς τους.

Ο οργανισμός θα μπορούσε να ορίσει μια τέτοια μέθοδο, όπως μια τεκμηριωμένη διαδικασία συνεχούς εποπτείας της αποτελεσματικής λειτουργίας των ελέγχων, μέσω της εκπόνησης εκτάκτων τυχαίων ελέγχων από τον «Υπεύθυνο Ασφάλειας Πληροφοριών» σε κανονικές συνθήκες εργασίας στις εμπλεκόμενες Διευθύνσεις και στα αντίστοιχα Τμήματά τους.

Τέλος, ο οργανισμός οφείλει κατά την υλοποίηση του συστήματος να ικανοποιεί την απαίτηση του προτύπου για ύπαρξη τεκμηρίωσης και επιβεβαίωσης αυτής. Όσον αφορά τα αρχεία που τηρούν οι Διευθύνσεις την ευθύνη επιβεβαίωσης τεκμηρίωσης θα έπρεπε να έχει ο «Υπεύθυνος Ασφάλειας Πληροφοριών», αντίθετα όσον αφορά τα αρχεία που τηρεί ο ίδιος ο Υπεύθυνος την ευθύνη θα έπρεπε να έχει η Διοίκηση.

Συμπερασματικά, όσον αφορά την υλοποίηση ο οργανισμός έχει καταγράψει «Σχέδιο Μείωσης Κινδύνου», το οποίο και εφαρμόζει όποτε προκύψει κάποιο συμβάν. Παρότι όμως έχει προνοήσει για την εξασφάλιση των απαιτούμενων πόρων, δεν έχει θεσπίσει συγκεκριμένους ρόλους, όπως έναν «Υπεύθυνο Ασφάλειας Πληροφοριών». Επίσης, ενώ εφαρμόζει όλους εκείνους τους ελέγχους που είχε επιλέξει κατά το στάδιο του σχεδιασμού, δεν μετράει την αποτελεσματικότητά τους. Συνεπώς, στο στάδιο της υλοποίησης ο οργανισμός ικανοποιεί σε κάποιο βαθμό τις απαιτήσεις του προτύπου, ωστόσο όχι πλήρως.

Ο ***έλεγχος*** με τη σειρά του διενεργείται τόσο στο στάδιο της υλοποίησης όσο και στο στάδιο του σχεδιασμού, έχοντας ως ρόλο να εξασφαλίσει στον οργανισμό την

αποτελεσματικότητα και την καταλληλότητα του συστήματος. Το πρότυπο ISO/IEC 27001:2005 αναφέρει ότι ο έλεγχος ενός συστήματος διαχείρισης ασφάλειας πληροφοριών πρέπει να έχει ως στόχο την αξιολόγηση της απόδοσής του. Στο τρέχον σύστημα διαχείρισης ασφάλειας πληροφοριών της Υ.Π.Α εξετάσαμε τρία επίπεδα ελέγχου. Συγκεκριμένα, μελετήθηκε ο έλεγχος σε επίπεδο διεργασίας, σε επίπεδο «Εσωτερικών Επιθεωρήσεων» και τέλος σε επίπεδο «Ανασκοπήσεων».

Σε επίπεδο διεργασίας, ο οργανισμός ελέγχει την αποτελεσματικότητα του συστήματος μέσω ελέγχων που έχει επιλέξει από το Παράρτημα Α του προτύπου και τους οποίους εφαρμόζει σε συγκεκριμένα κρίσιμα σημεία σε κάθε υποδιεργασία.

Συγκεκριμένα, στην Υποδιεργασία 1 «Συλλογή & καταγραφή αεροναυτικών πληροφοριών » εφαρμόζει δύο ελέγχους. Ο πρώτος έλεγχος (A.12.2.1) αφορά την επαλήθευση της αεροναυτικής πληροφορίας κατά τη διάρκεια καταγραφής της σε κάποιο από τα ενδιάμεσα έντυπα (AD_HP,ENR,GEN, Διόρθωση AIP, Συμπλήρωση AIP, Διόρθωση AIRAC AIP, Συμπλήρωση AIRAC AIP). Η επαλήθευση αυτή γίνεται προκειμένου να αποφευχθεί λανθασμένη καταχώρηση, όπως ανακριβείς συντεταγμένες, λάθος χαρακτηριστικά ραδιοβοηθημάτων κ.τ.λ. Ο δεύτερος έλεγχος (A10.5.1) αφορά την ύπαρξη αντιγράφων ασφαλείας, ούτως ώστε να εξαλειφθεί ο κίνδυνος που συνεπάγεται η απώλεια ενός εντύπου κατά τη διάρκεια διαβίβασης του στη Διεύθυνση Αεροναυτικών Εκδόσεων (Ε1).

Στην Υποδιεργασία 2 «Επεξεργασία αεροναυτικών πληροφοριών» ο οργανισμός έχει εισάγει πέντε ελέγχους. Οι τρεις από αυτούς (A11.3.1, A11.5.2, A8.3.3) αναφέρονται στην ορθή χρήση ονόματος χρήστη και κωδικού πρόσβασης. Αυτός ο έλεγχος είναι ιδιαίτερα σημαντικός σε αυτό το στάδιο όπου η επεξεργασία των κρίσιμων αεροναυτικών πληροφοριών γίνεται μέσω της αυτοματοποιημένης εφαρμογής eAip_wizard και η παράνομη πρόσβαση αποτελεί έναν κίνδυνο. Ο τέταρτος έλεγχος (A12.2.2) αφορά την επαλήθευση της εγκυρότητας των πληροφοριών που αναγράφονται στα ενδιάμεσα έντυπα με τα στοιχεία στις ηλεκτρονικές βάσεις δεδομένων. Ο τελευταίος έλεγχος (A12.2.4) σχετίζεται με την επαλήθευση της αξιοπιστίας και της ορθής κατάταξης της τελικής πληροφορίας από το Τμήμα Εγχειριδίων αεροναυτικών πληροφοριών-AIP (Ε1/Α) πριν αποσταλεί στο τυπογραφείο της Υ.Π.Α.

Στην Υποδιεργασία 3 «Έκδοση & διανομή Εγχειριδίου αεροναυτικών πληροφοριών - AIP» ο οργανισμός έχει εισάγει τον έλεγχο (A12.2.4) προκειμένου να γίνεται επαλήθευση της εγκυρότητας του τυπωμένου Εγχειριδίου ή των μεμονωμένων τυπωμένων σελίδων του από το Τμήμα Εγχειριδίων αεροναυτικών πληροφοριών-AIP (Ε1/Α). Ο έλεγχος αυτός έχει ως στόχο την τεκμηρίωση ορθής τύπωσης της κρίσιμης αεροναυτικής πληροφορίας όπως καταχωρήθηκε, προτού διανεμηθεί στους συνδρομητές.

Υπάρχει ένας τελευταίος έλεγχος (A7.1.2) ο οποίος είναι μείζονος σημασίας και εφαρμόζεται στις Υποδιεργασίες 1 και 2. Ο έλεγχος αυτός αφορά την κυριότητα των αεροναυτικών πληροφοριών. Αυτό σημαίνει ότι για κάθε κρίσιμη αεροναυτική πληροφορία πρέπει να αποδεικνύεται μέσα από το σύστημα ότι έχει οριστεί κάποιος υπεύθυνος για την ασφάλεια αυτής.

Αναφορικά με τον έλεγχο σε επίπεδο «Εσωτερικών Επιθεωρήσεων», την ευθύνη για την επιβεβαίωση συμμόρφωσης των διαδικασιών με κανονισμούς, προδιαγραφές και πρακτικές που έχουν σχέση με την Ασφάλεια έχουν οι Διευθυντές των εμπλεκόμενων μονάδων. Ο κάθε Διευθυντής ελέγχει υποτυπωδώς και όποτε εκείνος κρίνει απαραίτητο την ομαλή λειτουργία της διαδικασίας στην οποία η Διεύθυνσή του εμπλέκεται. Ενδεχόμενοι κίνδυνοι αν διαπιστωθούν καταγράφονται και τηρούνται σε «Φακέλους ανάλυσης κινδύνων», ενώ όταν εντοπιστεί μια μη συμμόρφωση την καταγράφουν στο ημερήσιο ημερολόγιο της Διεύθυνσής τους, λαμβάνουν διορθωτικά μέτρα, επιβεβαιώνουν την εξάλειψή της και συντάσσουν μια Αναφορά Ασφαλείας , συγκεκριμένα το έντυπο «ΑΝΑΦΟΡΑ ΒΛΑΒΩΝ,ΣΥΜΒΑΝΤΩΝ & ΑΤΥΧΗΜΑΤΩΝ», προς τη Διοίκηση, η οποία περιλαμβάνει τη μη συμμόρφωση, τη δράση και τα αποτελέσματα της επαληθεύσεως.

Οι έλεγχοι όμως αυτοί δε γίνονται τακτικά και προγραμματισμένα, βάσει μιας καταγεγραμμένης διαδικασίας, δεν καταγράφονται τα ευρήματά τους, ούτε διασφαλίζεται αντικειμενικότητα και αμεροληψία, αφού οι Διευθυντές ελέγχουν δικό τους έργο. Ο οργανισμός θα μπορούσε να καθιερώσει μια τεκμηριωμένη διαδικασία Εσωτερικών Επιθεωρήσεων, η οποία θα περιέγραφε τον τρόπο με τον οποίο θα διενεργούνται οι Εσωτερικές Επιθεωρήσεις στο σύστημα και με οδηγό αυτή να διενεργούσε Εσωτερικές Επιθεωρήσεις σε προγραμματισμένα χρονικά διαστήματα.

Όσον αφορά τον έλεγχο σε επίπεδο «Ανασκοπήσεων», η Διοίκηση ενίοτε ανασκοπεί το σύστημα ως προς την καταλληλότητα, την επάρκεια και την αποτελεσματικότητά του. Συγκεκριμένα, λαμβάνει υπόψη νέες τεχνικές, συστήματα ή διαδικασίες που χρησιμοποιούν άλλα ευρωπαϊκά κράτη καθώς και αλλαγές στο νομικό περιβάλλον, αλλαγμένες συμβατικές υποχρεώσεις ή συστάσεις για βελτίωση από το Διεθνή Οργανισμό Πολιτικής Αεροπορίας (ICAO-International Civil Aviation Organization). Για τις εξελίξεις αυτές ενημερώνεται σε προγραμματισμένες αλλά και έκτακτες συναντήσεις που πραγματοποιούνται σε διάφορες ευρωπαϊκές χώρες από τον «Ευρωπαϊκό Οργανισμό για την Ασφάλεια της Πολιτικής Αεροπορίας» (EUROCONTROL).

Επίσης, αναλύει την ανατροφοδότηση που λαμβάνει, με τη μορφή καταγεγραμμένων αναφορών, από τα ενδιαφερόμενα μέρη, προσωπικό και τελικοί χρήστες, όπως αεροδρόμια, αεροπορικές εταιρείες, ιδιώτες πιλότοι, εταιρίες «Πάροχοι Αεροναυτικών Δεδομένων» (Data Service Providers) και εξετάζει νέα τρωτά σημεία ή απειλές που ενδέχεται να προέκυψαν πρόσφατα από τις «Αναφορές Ενδεχόμενων Κινδύνων».

Μόλις διαπιστωθεί τεκμηριωμένα η αναποτελεσματικότητά των διαδικασιών και των ελέγχων που εφαρμόζονται ή μόλις αλλάξουν οι απαιτήσεις ασφάλειας ή κάποιο από τα παραπάνω στοιχεία, η Διοίκηση προβαίνει στην άμεση τροποποίησή τους προκειμένου να εισάγει βελτιώσεις και εποικοδομητικές αλλαγές στο σύστημα ISMS.

Η ανασκόπηση όμως αυτή δε γίνεται προγραμματισμένα, βάσει μιας καταγεγραμμένης διαδικασίας και όταν γίνεται τα αποτελέσματα δεν τεκμηριώνονται και δε διατηρούνται σε αρχεία. Επιπρόσθετα, από τον έλεγχο των εγγράφων δεν αποδεικνύεται η τακτική ανασκόπηση από τη Διοίκηση των προληπτικών και διορθωτικών ενεργειών, των «Αναφορών Ασφαλείας», των αποτελεσμάτων των Εσωτερικών Επιθεωρήσεων, των προηγούμενων Ανασκοπήσεων και του «Σχεδίου θεράπευσης κινδύνου», ούτως ώστε να διασφαλιστεί ότι δε θα συμβεί ή επαναληφθεί κάποια μη συμμόρφωση με τις απαιτήσεις του προτύπου.

Η Διοίκηση θα έπρεπε κατά το πρότυπο να επανεξετάζει την αποτελεσματικότητα του συστήματος λαμβάνοντας υπόψη τα αποτελέσματα των παραπάνω ως εισερχόμενα στην Ανασκόπησή της. Ένας τρόπος να το επιτύχει είναι να καθιερώσει μια τεκμηριωμένη διαδικασία Ανασκόπησης, η οποία θα γίνεται από τη Γενική Διεύθυνση του οργανισμού (Διοικητής Πολιτικής Αεροπορίας, Υποδιοικητής, Γενικός Διευθυντής Αεροναυτιλίας, Διευθυντές των εμπλεκομένων μονάδων, Υπεύθυνος Ασφάλειας Πληροφοριών) και θα στοχεύει στο διαρκή έλεγχο και την αξιολόγηση των αποτελεσμάτων του συστήματος με απώτερο σκοπό τη συνεχή βελτίωση.

Σχετικά λοιπόν με τον έλεγχο, από τα παραπάνω προκύπτει ότι ο οργανισμός σε επίπεδο διεργασίας ικανοποιεί πλήρως τις απαιτήσεις του προτύπου έχοντας επιλέξει και εφαρμόσει τους κατάλληλους ελέγχους σε συγκεκριμένα κρίσιμα σημεία σε κάθε διαδικασία. Σε επίπεδο όμως Εσωτερικών Επιθεωρήσεων και Ανασκοπήσεων, ενώ ελέγχει το σύστημα ως προς την καταλληλότητα, την επάρκεια και την αποτελεσματικότητά του, δεν το κάνει προγραμματισμένα, βάσει μιας καταγεγραμμένης διαδικασίας και τηρώντας αρχεία. Συνεπώς, αξιολογώντας συνολικά το στάδιο του ελέγχου, ο οργανισμός ικανοποιεί σε κάποιο βαθμό τις απαιτήσεις του προτύπου.

Η ***συνεχής βελτίωση,*** ως τελευταίο βήμα του «Κύκλου PDCA», έχει ως στόχο την αέναη βελτίωση της αποτελεσματικότητας του συστήματος που ο οργανισμός ήδη εφαρμόζει. Η συνεχής βελτίωση ενός συστήματος διαχείρισης ασφάλειας πληροφοριών περιλαμβάνει κατά το πρότυπο ISO/IEC 27001:2005 όλες εκείνες τις απαραίτητες ενέργειες που γίνονται εκ μέρους του οργανισμού προκειμένου να βελτιωθεί το επίπεδο ασφάλειας των πληροφοριών του. Το υπάρχον σύστημα διαχείρισης ασφάλειας πληροφοριών της Υ.Π.Α εξετάστηκε ως προς τη συνεχή βελτίωσή του σε επίπεδο τόσο διορθωτικών όσο και προληπτικών ενεργειών.

Η Υ.Π.Α θέλοντας να βελτιώσει την αποτελεσματικότητα του συστήματός της λαμβάνει ενέργειες για την εξάλειψη των αιτιών των «μη συμμορφώσεων» αλλά και των «πιθανών μη συμμορφώσεων», έτσι ώστε να εξασφαλίζεται η μη επανάληψη των πρώτων και να προλαμβάνεται η εμφάνισή των τελευταίων. Δεν έχει όμως καθιερώσει μια τεκμηριωμένη διαδικασία για τη λήψη διορθωτικών και προληπτικών ενεργειών, ούτε γίνεται ορθή επαλήθευση και ανασκόπηση αυτών.

Ο οργανισμός σύμφωνα με το πρότυπο πρέπει να προσδιορίσει μια τεκμηριωμένη διαδικασία στην οποία να περιγράφεται ο τρόπος διαπίστωσης ανάγκης, αναφοράς και παρακολούθησης των διορθωτικών και προληπτικών ενεργειών με απώτερο σκοπό τη διαρκή βελτίωση του Συστήματος. Μία ιδέα είναι να εισαχθεί στο σύστημα έντυπο «ΔΙΟΡΘΩΤΙΚΕΣ & ΠΡΟΛΗΠΤΙΚΕΣ ΕΝΕΡΓΕΙΕΣ» στο οποίο ο εκτελών την ενέργεια να είναι διαφορετικός από εκείνον που την επαληθεύει.

Η Διοίκηση έχει επίσης εδραιώσει μια «Νοοτροπία Ασφάλειας Πληροφοριών». Η οποία είναι κάτι περισσότερο από τη μηχανικά πιστή εφαρμογή κανονισμών και διαδικασιών. Το σύνολο του προσωπικού ενθαρρύνεται στην υποβολή εθελουσίων αναφορών συμβάντων και επώνυμων προτάσεων βελτίωσης. Όλες οι προτάσεις του προσωπικού καταγράφονται, αξιολογούνται και όσες από αυτές θεωρούνται ουσιαστικές για τη βελτίωση του συστήματος ISMS υλοποιούνται.

Ο οργανισμός αναφέρει μάλιστα εγγράφως ότι οι δράσεις και οι βελτιώσεις διαδίδονται ευρέως εσωτερικά μέσω της «Αυτοματοποιημένης διασποράς των πληροφοριών για συμβάντα», με ομάδες εργασίας σε χώρους που έχουν ανακύψει ζητήματα ασφάλειας πληροφοριών και με την έκδοση ενημερωτικών σημειωμάτων ασφάλειας πληροφοριών σε περιπτώσεις συμβάντων, για την ενημέρωση του προσωπικού.

Γενικότερα όμως, ο οργανισμός οφείλει κατά το πρότυπο να διασφαλίζει ότι οι βελτιώσεις επιτυγχάνουν τους στόχους που είχαν τεθεί. Ένας τρόπος θα ήταν να καθορίζει η Διοίκηση σε ετήσια βάση στόχους για τη βελτίωση των επιπέδων ασφάλειας πληροφοριών. Επιπρόσθετα, θα μπορούσε να διαθέτει ένα σύστημα υποχρεωτικών αναφορών περιστατικών, με σκοπό την καταγραφή μεγάλου όγκου συμβάντων και την αξιοποίηση του αριθμού των αναφερόμενων περιστατικών σαν δείκτη απόδοσης.

Συνεπώς, αναφορικά με τη συνεχή βελτίωση, ο οργανισμός πληροί μερικώς την απαίτηση του προτύπου για ύπαρξη διορθωτικών και προληπτικών ενεργειών. Ο λόγος είναι ότι λαμβάνει μεν διορθωτικές και προληπτικές ενέργειες όταν αυτό απαιτείται, αλλά δε διαθέτει μια καταγεγραμμένη διαδικασία, ούτε γίνεται τεκμηρίωση, επαλήθευση και ανασκόπηση αυτών.

Λαμβάνοντας υπόψη όλα τα παραπάνω, συμπεραίνεται ότι ενώ οι απαιτήσεις του προτύπου ISO/IEC 27001:2005 στο μεγαλύτερο μέρος τους ικανοποιούνται από το

υφιστάμενο σύστημα διαχείρισης ασφάλειας πληροφοριών της Υ.Π.Α, υπάρχουν και ορισμένες που δεν πληρούνται. Η παρούσα διπλωματική εργασία εντόπισε αυτά τα σημεία και πραγματοποίησε προτάσεις προς αυτήν την κατεύθυνση. Οι προτάσεις αυτές αν εφαρμοστούν θα συνεισφέρουν στην ανάπτυξη, υλοποίηση και διατήρηση ενός συστήματος πιστοποιήσιμου κατά ISO/IEC 27001:2005 και θα εξασφαλίσουν στον οργανισμό την αποτελεσματική αλληλεπίδραση χρηστών, τεχνολογίας και διαδικασιών. Κατά συνέπεια, η Υ.Π.Α θα κατορθώσει να διαφυλάξει την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των αεροναυτικών πληροφοριών της και να ελαχιστοποιήσει τους κινδύνους που απειλούν την ασφάλειά τους.

6.2. Προτάσεις για περαιτέρω έρευνα

Η διπλωματική όμως αυτή έχει και επιπρόσθετους απώτερους σκοπούς. Ένας εκ των οποίων είναι να αποτελέσει εφαλτήριο για περαιτέρω έρευνα στο πεδίο της ασφάλειας των αεροναυτικών πληροφοριών. Ειδικότερα, θα μπορούσε να μελετηθεί η πιθανότητα ανάπτυξης πιστοποιήσιμων κατά ISO 27001 συστημάτων διαχείρισης ασφάλειας πληροφοριών και σε άλλες διεργασίες του συγκεκριμένου οργανισμού.

Η συγκεκριμένη εργασία, λόγω του τεράστιου όγκου των αεροναυτικών πληροφοριών που διαχειρίζεται η Διεύθυνση Αεροναυτικών Εκδόσεων της Υ.Π.Α, εστίασε σε ένα μόνο μέρος του ολοκληρωμένου πακέτου αεροναυτικών πληροφοριών-IAIP (Integrated Aeronautical Information Package). Υπάρχουν όμως και άλλες διεργασίες που ενώ αναφέρθηκαν εν συντομία δεν μελετήθηκαν και στις οποίες θα μπορούσε να ερευνηθεί η δυνατότητα υλοποίησης ενός παρόμοιου συστήματος.

Αναφορικά, μια από αυτές είναι η διεργασία έκδοσης αεροναυτικών αγγελιών NOTAM, οι οποίες είναι ειδοποιήσεις προσωρινής φύσεως, μικρής διάρκειας & άμεσης εφαρμογής. Μια άλλη είναι η διεργασία έκδοσης δελτίων αεροναυτικών πληροφοριών AIC (Aeronautical Information Circulars), τα οποία είναι διοικητικής φύσεως και αφορούν προβλέψεις σημαντικών αλλαγών και πληροφορίες επεξηγηματικού και συμβουλευτικού χαρακτήρα οι οποίες δεν πληρούν τις προϋποθέσεις για τη δημοσίευσή τους στο εγχειρίδιο AIP. Ιδιαίτερα σημαντικές είναι και άλλες δύο διεργασίες, η πρώτη είναι εκείνη της έκδοσης δελτίων διαδρομής προ πτήσεως PIB (Pre-flight Information Bulleting) και η δεύτερη της συλλογής και επεξεργασίας των μετά πτήσεως πληροφοριών (Post-flight Information). Τα πρώτα περιλαμβάνουν ανακεφαλαίωση των πιο προσφάτων αεροναυτικών αγγελιών NOTAM και επείγουσες πληροφορίες, ενώ τα δεύτερα αναφέρουν κάθε ανεπάρκεια ουσιαστικής για την ασφάλεια σημασίας που παρατηρήθηκε κατά τη διάρκεια της πτήσης. Τέλος, δεν θα μπορούσε να μην αναφερθεί η διεργασία έκδοσης και ενημέρωσης των αεροναυτικών χαρτών (Aeronautical Charts).

Στις προαναφερθείσες διεργασίες θα μπορούσε να διερευνηθεί η δυνατότητα ανάπτυξης ενός πιστοποιήσιμου κατά ISO 27001 συστήματος διαχείρισης ασφάλειας πληροφοριών, διότι οι αεροναυτικές πληροφορίες που επεξεργάζονται είναι κρίσιμες, πρέπει να παρέχονται σε μια δεδομένη μορφή και σειρά ,να είναι έγκυρες και αξιόπιστες.

Επιπρόσθετα, ένας δεύτερος στόχος της εργασίας ήταν να δώσει κίνητρα για την πραγματοποίηση εμπειρικών ερευνών στο πεδίο της εφαρμογής του προτύπου ISO/IEC 27001:2005 «Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών-Απαιτήσεις». Όπως προαναφέρθηκε επειδή το πρότυπο είναι σχετικά καινούριο, δεν υπάρχει στη βιβλιογραφία πληθώρα εμπειρικών ερευνών. Στην παρούσα διπλωματική δεν έγινε μελέτη σε αυτό το επίπεδο, αλλά θα είχε ενδιαφέρον να πραγματοποιηθούν εμπειρικές έρευνες σε οργανισμούς που έχουν ήδη εφαρμόσει το συγκεκριμένο πρότυπο, προκειμένου να εξεταστούν διάφορα θέματα, τα οποία αναπτύχθηκαν στη βιβλιογραφική ανασκόπηση μόνο θεωρητικά.

Αναφορικά, θα μπορούσε να επιλεγεί ένα δείγμα επιχειρήσεων που εφαρμόζουν το πρότυπο και να ερωτηθούν οι εμπλεκόμενοι μέσα από δομημένες συνεντεύξεις σχετικά με ποικίλα θέματα. Ορισμένα από αυτά είναι, τί προβλήματα αντιμετώπισαν, σε ποιό βαθμό ήταν σοβαρά, ποιά οφέλη προέκυψαν, σε ποιό βαθμό είναι ικανοποιημένοι, ποιά σφάλματα έγιναν, σε ποιό βαθμό ήταν κοινά, πόσο χρήσιμο θεωρούν το πρότυπο, σε ποιό βαθμό πιστεύουν ότι η εφαρμογή του είναι ακριβή και διάφορα άλλα. Στη συνέχεια να γίνει έρευνα πεδίου και ποσοτική έρευνα. Τέτοιου είδους έρευνες θα συντελούσαν στην μελέτη του προτύπου σε πραγματικές συνθήκες και συγχρόνως στη βαθύτερη κατανόησή του.

Τελευταίος στόχος, αλλά ιδιαίτερα σημαντικός, είναι να αποτελέσει η εργασία αφορμή για περαιτέρω έρευνα σχετικά με δύο θέματα τα οποία προέκυψαν από τη μελέτη του συστήματος διαχείρισης ασφάλειας πληροφοριών της Υ.Π.Α και τα οποία θεωρούνται ιδιαίτερα κρίσιμα για την επιτυχία της εφαρμογής του προτύπου ISO 27001:2005.

Το πρώτο, είναι το πρόβλημα της αδυναμίας κατανόησης και εφαρμογής του προτύπου από τους εργαζομένους. Συνθέτοντας όλα όσα αναφέρθηκαν, διαπιστώθηκε ότι στο συγκεκριμένο οργανισμό που μελετήθηκε, την Υ.Π.Α, οι εργαζόμενοι δεν κατανοούν ακριβώς την ανάγκη να εφαρμόσουν τις διαδικασίες και συνδυαστικά με το γεγονός ότι δεν πιέζονται από εσωτερικές επιθεωρήσεις και ανασκοπήσεις της διοίκησης, το αποτέλεσμα είναι να μην εφαρμόζεται το πρότυπο.

Το δεύτερο θέμα που διαπιστώθηκε είναι η αδυναμία της διοίκησης να δείξει την δέσμευσή της. Από όσα παρουσιάστηκαν προέκυψε ότι η διοίκηση παρότι υπογράφει την πολιτική ασφάλειας ISMS, δεν αποδεικνύει με επιπρόσθετους τρόπους την έμπρακτη δέσμευσή της, όπως με τη διενέργεια τακτικών ανασκοπήσεων.

Ευχής έργον θα ήταν η εργασία αυτή να δώσει κίνητρο να διερευνηθούν τα προαναφερθείσα θέματα σε βάθος, λόγω της σημαντικότητας και της χρησιμότητας τους στην υλοποίηση ενός επιτυχημένου συστήματος διαχείρισης ασφάλειας πληροφοριών κατά το πρότυπο ISO 27001:2005.

7. ΠΑΡΑΡΤΗΜΑΤΑ

7.1.1. ΠΑΡΑΡΤΗΜΑ Ι - ΟΡΟΛΟΓΙΑ

Δελτία Αεροναυτικών Πληροφοριών –AIC
(Aeronautical Information Circulars)

Τα Δελτία Αεροναυτικών Πληροφοριών AIC περιλαμβάνουν πληροφορίες οι οποίες :

- δεν πληρούν τις προϋποθέσεις για την έκδοση Αγγελίας ή τη δημοσίευσή τους στο Εγχειρίδιο Αεροναυτικών Πληροφοριών-AIP
- έχουν σχέση με τη μακροπρόθεσμη πρόβλεψη οποιασδήποτε σημαντικής αλλαγής στη νομοθεσία, στους κανόνες, στις διαδικασίες ή στις εγκαταστάσεις, που δύναται να επηρεάσει την ασφάλεια των πτήσεων καθώς και πληροφορίες ή κοινοποιήσεις επεξηγηματικού ή συμβουλευτικού χαρακτήρα σχετικά με τεχνικά, νομικά ή αμιγώς διοικητικά θέματα.

Τα Δελτία Αεροναυτικών Πληροφοριών AIC χωρίζονται ανά θέμα και εκδίδονται σε δύο τόμους (Α και Β). Ο τόμος Α περιέχει πληροφορίες που επηρεάζουν τη διεθνή πολιτική αεροπορία και διανέμεται διεθνώς, ενώ ο τόμος Β περιέχει πληροφορίες που αφορούν μόνο την εθνική υπηρεσία πολιτικής αεροπορίας διανέμεται εθνικά.

Διορθώσεις AIP (AIP Amendments -AIP AMDT)

Το Εγχειρίδιο Αεροναυτικών Πληροφοριών AIP, διορθώνεται ή επανεκδίδεται σε τέτοια τακτά χρονικά διαστήματα, ώστε να διατηρείται πάντα ενημερωμένο. Οι διορθώσεις εκδίδονται με τη μορφή νέων σελίδων που αντικαθιστούν παλαιότερες σελίδες.

Διορθώσεις (Amendments) στο AIP γίνονται μέσω της αντικατάστασης των σχετικών φύλλων που έχουν προκύψει ***μόνιμες αλλαγές***.
Υπάρχουν δύο είδη διορθώσεων του AIP :

- Τακτική Διόρθωση AIP (AIP AMDT), εκδίδεται όπως και όταν απαιτείται και ενσωματώνει ***μόνιμες αλλαγές*** στο AIP, οι οποίες τίθενται σε ισχύ από την αναγραφόμενη ημερομηνία δημοσίευσής τους.

- AIRAC AIP Διόρθωση (AIRAC AIP AMDT), εκδίδεται σύμφωνα με το σύστημα AIRAC, ενσωματώνει ***επιχειρησιακά σημαντικές μόνιμες αλλαγές*** στο AIP, οι οποίες τίθενται σε ισχύ από την αναγραφόμενη AIRAC ημερομηνία έναρξης ισχύος και όχι από την αναγραφόμενη ημερομηνία δημοσίευσής τους.

Σύντομη περιγραφή των θεμάτων που θίγονται από την τροποποίηση, δίνονται στο εξώφυλλο του AIP Amendments. Νέα πληροφορία που έχει εισαχθεί στις σελίδες του AIP αναγνωρίζεται από μια κάθετη γραμμή ή ένα βέλος στο αριστερό ή δεξί περιθώριο της αλλαγής/συμπλήρωσης.

Κάθε σελίδα του AIP και κάθε αντικαθιστάμενη σελίδα του AIP που εισάγεται με ένα Amendment, συμπεριλαμβανομένου και του εξωφύλλου του AIP Amendments, έχει ημερομηνία. Η ημερομηνία αυτή αποτελείται από την ημέρα, το μήνα (ονομαστικά) και έτος της ημερομηνίας δημοσίευσης (τακτική AIP AMDT) ή την AIRAC ημερομηνία έναρξης ισχύος (AIRAC AIP AMDT). Κάθε εξώφυλλο AIP Amendments περιλαμβάνει αναφορές στον αύξων αριθμό των στοιχείων αυτών, αν υπάρχει, του AIP Package που έχουν ενσωματωθεί στο AIP με την τροποποίηση και συνεπώς ακυρώθηκαν.

Κάθε τροποποίηση του AIP που αφορά τον τόμο I αλλά και κάθε τροποποίηση του AIP που αφορά τον τόμο II καθώς και τα AIRAC AIP AMDT, κατανέμεται αντίστοιχα με ξεχωριστό αύξοντα αριθμό. Οι αριθμοί αυτοί είναι συνεχόμενοι και με βάση το ημερολογιακό έτος. Το έτος, το οποίο αναγράφεται με δύο ψηφία, είναι ένα μέρος του αύξοντα αριθμού της τροποποίησης, πχ, AIP AMDT 1/03, AIRAC AIP AMDT 1/03.

Μια λίστα των σελίδων του AIP που περιέχει αριθμό σελίδας /τίτλο διαγράμματος και πραγματική ημερομηνία δημοσίευσης ημέρα, το μήνα (ονομαστικά) και το έτος των πληροφοριών εκδίδονται εκ νέου με κάθε τροποποίηση και είναι αναπόσπαστο μέρος του AIP.

Συμπληρώσεις AIP (AIP Supplements -AIP SUP)

Οι Συμπληρώσεις (Supplements) στο AIP αφορούν ***προσωρινές αλλαγές*** του AIP.
Υπάρχουν δύο είδη συμπληρώσεων :

- Συμπλήρωση AIP (AIP SUP),
  1. Προσωρινές αλλαγές ***μακράς διάρκειας*** (τριών μηνών και πλέον).
  2. Πληροφορίες ***μικρής διάρκειας*** οι οποίες αποτελούνται από εκτεταμένο ***κείμενο ή/και γραφικά***, οι οποίες συμπληρώνουν τη μόνιμη πληροφορία που εμπεριέχεται στο AIP.

- Συμπλήρωση AIRAC AIP (AIRAC AIP SUP), είναι ***επιχειρησιακά σημαντικές προσωρινές αλλαγές*** στο AIP, εκδίδονται σύμφωνα με το σύστημα AIRAC, το οποίο παρουσιάζεται παρακάτω, και τις καθιερωμένες ημερομηνίες του. Οι οποίες τίθενται σε ισχύ από την αναγραφόμενη AIRAC ημερομηνία έναρξης ισχύος και όχι από την αναγραφόμενη ημερομηνία δημοσίευσής τους.

Συμπληρώματα του AIP δημοσιεύονται σε κίτρινο χαρτί προκειμένου να ξεχωρίζουν από το υπόλοιπο AIP. Κάθε συμπλήρωμα του AIP (κανονικό ή AIRAC) διατίθεται με ένα

αύξοντα αριθμό που είναι συνεχόμενος και βασισμένος στο ημερολογιακό έτος, πχ,AIP SUP 1/03, AIRAC AIP SUP 1/03.

Ένα συμπλήρωμα AIP διατηρείται στο AIP, εφόσον το σύνολο ή μέρος του περιεχομένου του εξακολουθεί να ισχύει. Η διάρκεια ισχύος των πληροφοριών που περιέχονται στο Συμπλήρωμα AIP θα αναφέρεται κανονικά στο ίδιο συμπλήρωμα. Εναλλακτικά, ένα NOTAM μπορεί να χρησιμοποιηθεί για να αναφέρει τις αλλαγές στην περίοδο ισχύος ή την ακύρωση του συμπληρώματος.

Ο κατάλογος σημείων ελέγχου των συμπληρωμάτων που ισχύει σήμερα εκδίδεται στην μηνιαία έντυπη σε απλή γλώσσα περίληψη των NOTAM.

Σύστημα AIRAC

Για τον έλεγχο και τη ρύθμιση των ***επιχειρησιακά σημαντικών αλλαγών*** που απαιτούν τροποποιήσεις σε διαγράμματα, εγχειρίδια κλπ οι αλλαγές αυτές, όποτε αυτό είναι δυνατό, εκδίδονται σε προκαθορισμένες ημερομηνίες, σύμφωνα με το σύστημα AIRAC. Ο παρακάτω πίνακας δείχνει τις ενδεικτικές AIRAC ημερομηνίες για τα προσεχή έτη.

2009	2010	2011	2012
15 Ιανουαρίου			
12 Φεβρουαρίου			
12 Μαρτίου			
9 Απριλίου			
7 Μαΐου			
4 Ιουνίου			
2 Ιουλίου			
30 Ιουλίου			
27 Αυγούστου			
24 Σεπτεμβρίου			
22 Οκτωβρίου			
19 Νοεμβρίου			
17 Δεκεμβρίου			

Αυτό το είδος των πληροφοριών θα δημοσιεύεται ως AIRAC AIP AMDT ή AIRAC AIP SUP.

Η AIRAC πληροφορία εκδίδεται έτσι ώστε ο χρήστης να τη λαμβάνει όχι αργότερα από 28 ημέρες και για μεγάλες αλλαγές όχι αργότερα από 56 ημέρες, πριν την ημερομηνία έναρξης ισχύος.

Αν ένα AIRAC AIP AMDT ή SUP δεν μπορεί να παραχθεί λόγω έλλειψης χρόνου, τότε ένα NOTAM με σαφή σήμανση AIRAC, εκδίδεται. Ένα τέτοιο NOTAM αμέσως ακολουθείται από ένα AMDT ή SUP.

Αεροναυτικές Αγγελίες NOTAM

Περιλαμβάνουν πληροφορίες προσωρινής φύσης και μικρής διάρκειας, σχετικά με την εγκατάσταση, την παρούσα κατάσταση ή την αλλαγή οποιασδήποτε αεροναυτικής λειτουργίας, υπηρεσίας, διαδικασίας ή επικινδυνότητας, η έγκαιρη γνώση των οποίων είναι απαραίτητη στο προσωπικό των πτήσεων.

NOTAM «Ενεργοποίησης» (“trigger”NOTAM)

Στην περίπτωση που εκδίδεται μία Διόρθωση AIP (AIP AMDT) ή μία Συμπλήρωση AIP (AIP SUP) μέσω διαδικασιών AIRAC, πρέπει δημοσιεύεται και ένα NOTAM «Ενεργοποίησης» (“trigger” NOTAM). Ο σκοπός ενός τέτοιου NOTAM είναι να χρησιμεύει ως υπενθύμιση στα Δελτία Διαδρομής προ πτήσεως-(PIB-preflight information bulletin) της έναρξης ισχύος των λειτουργικά σημαντικών μόνιμων ή προσωρινών αλλαγών του AIP, έτσι ώστε οι χρήστες να γνωρίζουν τις αλλαγές που ενδέχεται να επηρεάσουν τις πτήσεις τους.

Επίσης εξυπηρετεί εκείνους τους που είναι υπεύθυνοι για την ενημέρωση των AIPs, παρακινώντας τους να εισάγουν μία νέα Διόρθωση AIP ή μία νέα Συμπλήρωση AIP στην ημερομηνία έναρξης ισχύος.

Ένα NOTAM «Ενεργοποίησης» πρέπει να περιλαμβάνει μία σύντομη περιγραφή του περιεχομένου των Διορθώσεων ή των Συμπληρώσεων, την ημερομηνία έναρξης ισχύος και τον αριθμό αναφοράς. Τέλος, πρέπει να τεθεί σε ισχύ την ίδια ημερομηνία με την Διόρθωση ή τη Συμπλήρωση και να παραμείνει σε ισχύ, ως υπενθύμιση στο Δελτίο Διαδρομής προ πτήσεως-PIB, μέχρι να εκδοθεί ο επόμενος Κατάλογος των Έγκυρων Αεροναυτικών Αγγελιών (Checklist/Summary of NOTAM).

7.1.2. ΠΑΡΑΡΤΗΜΑ ΙΙ - ΕΞΕΙΔΙΚΕΥΜΕΝΕΣ ΟΔΗΓΙΕΣ

Εξειδικευμένη Οδηγία Ι

Υποδειγματικό Μοντέλο Παρουσίασης Αεροναυτικών Πληροφοριών-AICM (Aeronautical Information Conceptual Model)

Οι αεροναυτικές πληροφορίες μέχρι πρότινος παρουσιάζονταν σε ελεύθερο κείμενο. Επειδή όμως κρίθηκε επιτακτική η ανάγκη να παρουσιάζονται οι εν λόγω πληροφορίες με συγκεκριμένο τρόπο και μορφή το 2003 αναπτύχθηκε από το "Euro control" ένα Υποδειγματικό Μοντέλο Παρουσίασης Αεροναυτικών Πληροφοριών-AICM (Aeronautical Information Conceptual Model).

Το Μοντέλο αυτό περιέχει τον τύπο των δεδομένων που απαιτούνται, τις σχέσεις που υπάρχουν μεταξύ τους και τέλος τη δομή με την οποία πρέπει να αναπαρίστανται τα αεροναυτικά δεδομένα (αεροδρόμια, ραδιοβοηθήματα, εμπόδια κλπ).

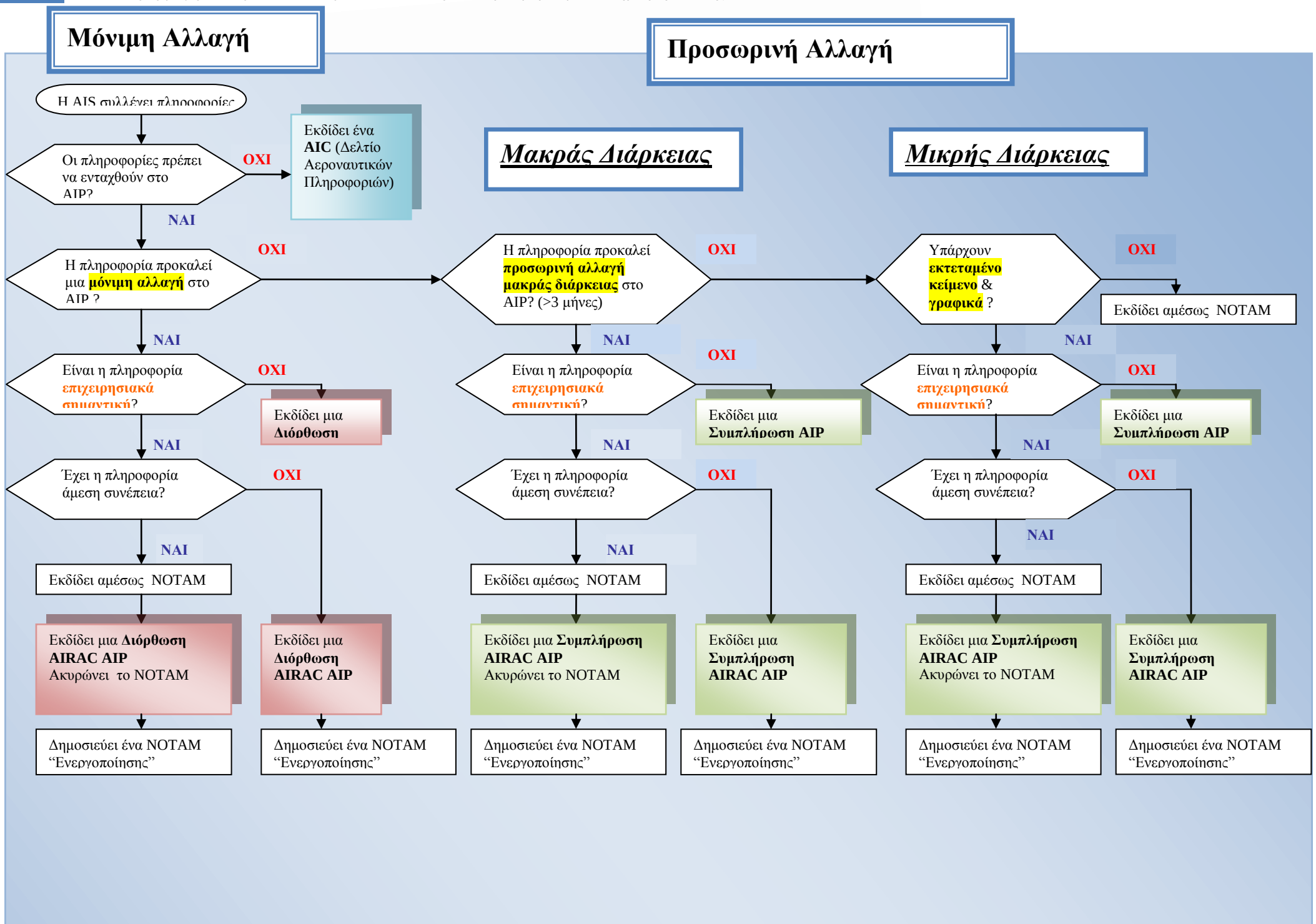
Το Μοντέλο αυτό αρχικά βασίστηκε πάνω στις απαιτήσεις του Διεθνούς Οργανισμού Πολιτικής Αεροπορίας-ICAO (International Civil Aviation Organization) και το Παράρτημα 15 (Annex 15) που καθορίζουν τη Διεθνή ανταλλαγή αεροναυτικών πληροφοριών καθώς και πάνω σε βιομηχανικά πρότυπα όπως το ARINC 424.

Εξειδικευμένη Οδηγία ΙΙ

Διαδικασία κατάταξης αλλαγών ανάλογα με τον τύπο τους

Όταν προκύπτει μια αλλαγή στις αεροναυτικές πληροφορίες ακολουθείται από την αντίστοιχη Διεύθυνση και το αντίστοιχο Τμήμα της η ακόλουθη διαδικασία (Σχήμα).

Τύπος Αλλαγών	Προσωρινές Αλλαγές μικρής διάρκειας	Προσωρινές Αλλαγές μεγάλης διάρκειας
Φυσικά χαρακτηριστικά αεροδρομίου	Εργασίες κοντά στο διάδρομο ενός αεροδρομίου : Περίοδος διακοπής λειτουργίας < 3 μήνες.	Εργασίες κοντά στο διάδρομο ενός αεροδρομίου : Περίοδος διακοπής λειτουργίας > 3 μήνες.
Διευκολύνσεις που παρέχει το αεροδρόμιο	Εργασίες συντήρησης σε ένα ραδιοβοήθημα.	Αλλαγές με σημαντικό επιχειρησιακό αντίκτυπο: εγκατάσταση ραδιοβοηθήματος, μηχανήματος μετεωρολογικών προβλέψεων, ενισχύσεις ραδιοπλοήγησης.
Τύπος & θέση ραδιοβοηθημάτων (VOR,DME)	Προσωρινές αλλαγές σε θέση ραδιοβοηθημάτων, συχνότητες, σήματα κλήσης, θέση, ύψος & φωτισμό εμποδίων πλοήγησης.	Μόνιμες αλλαγές σε θέση ραδιοβοηθημάτων, συχνότητες, σήματα κλήσης, θέση, ύψος & φωτισμό εμποδίων πλοήγησης περιόδους συντήρησης.
Διαδικασίες εναέριας κυκλοφορίας	Προσωρινές αλλαγές σε διαδικασίες αναμονής & προσέγγισης, διαδικασίες προσγείωσης & απογείωσης.	Μόνιμες αλλαγές σε διαδικασίες αναμονής & προσέγγισης, διαδικασίες προσγείωσης & απογείωσης, διαδικασίες ελάττωσης του θορύβου.
Υπηρεσίες	Ώρες λειτουργίας αεροδρομίου, λοιπών εγκαταστάσεων & υπηρεσιών.	Τελωνείο, Κέντρο Υγείας. Αλλαγή στους τροχοδρόμους , θέσεις για ΤΑΧΙ, παρκινγκ (parking)


Μόνιμη Αλλαγή
Προσωρινή Αλλαγή
Η AIS συλλέγει πληροφορίες
Οι πληροφορίες πρέπει να ενταχθούν στο AIP?
ΟΧΙ
Εκδίδει ένα AIC (Δελτίο Αεροναυτικών Πληροφοριών)
ΝΑΙ
Μακράς Διάρκειας
Μικρής Διάρκειας
Η πληροφορία προκαλεί μια μόνιμη αλλαγή στο AIP ?
ΟΧΙ
Η πληροφορία προκαλεί προσωρινή αλλαγή μακράς διάρκειας στο AIP? (>3 μήνες)
ΟΧΙ
Υπάρχουν εκτεταμένο κείμενο & γραφικά ?
ΟΧΙ
Εκδίδει αμέσως NOTAM
ΝΑΙ
Είναι η πληροφορία επιχειρησιακά σημαντική?
ΟΧΙ
Εκδίδει μια Διόρθωση
ΝΑΙ
Είναι η πληροφορία επιχειρησιακά σημαντική?
ΟΧΙ
Εκδίδει μια Συμπλήρωση AIP
ΝΑΙ
Είναι η πληροφορία επιχειρησιακά σημαντική?
ΟΧΙ
Εκδίδει μια Συμπλήρωση AIP
ΝΑΙ
Έχει η πληροφορία άμεση συνέπεια?
ΟΧΙ
ΝΑΙ
Έχει η πληροφορία άμεση συνέπεια?
ΟΧΙ
ΝΑΙ
Έχει η πληροφορία άμεση συνέπεια?
ΟΧΙ
ΝΑΙ
Εκδίδει αμέσως NOTAM
Εκδίδει αμέσως NOTAM
Εκδίδει αμέσως NOTAM
Εκδίδει μια Διόρθωση AIRAC AIP Ακυρώνει το NOTAM
Εκδίδει μια Διόρθωση AIRAC AIP
Εκδίδει μια Συμπλήρωση AIRAC AIP Ακυρώνει το NOTAM
Εκδίδει μια Συμπλήρωση AIRAC AIP
Εκδίδει μια Συμπλήρωση AIRAC AIP Ακυρώνει το NOTAM
Εκδίδει μια Συμπλήρωση AIRAC AIP
Δημοσιεύει ένα NOTAM "Ενεργοποίησης"
Δημοσιεύει ένα NOTAM "Ενεργοποίησης"
Δημοσιεύει ένα NOTAM "Ενεργοποίησης"
Δημοσιεύει ένα NOTAM "Ενεργοποίησης"
Δημοσιεύει ένα NOTAM "Ενεργοποίησης"
Δημοσιεύει ένα NOTAM "Ενεργοποίησης"

Περιγραφή Διαδικασίας ενεργοποίησης εγγράφων

Αρχικά κρίνεται εάν η αλλαγή αυτή πρέπει να ενταχθεί στο Εγχειρίδιο Αεροναυτικών Πληροφοριών AIP.

Εάν η πληροφορία αναφέρεται σε μακροπρόθεσμη πρόβλεψη οποιασδήποτε σημαντικής αλλαγής στη νομοθεσία, στους κανόνες, στις διαδικασίες ή στις εγκαταστάσεις, που δύναται να επηρεάσει την ασφάλεια των πτήσεων καθώς και σε κοινοποιήσεις επεξηγηματικού ή συμβουλευτικού χαρακτήρα σχετικά με τεχνικά, νομικά ή αμιγώς διοικητικά θέματα, τότε δεν θα ενταχθεί στο Εγχειρίδιο Αεροναυτικών Πληροφοριών AIP, αλλά θα δοθεί εντολή για έκδοση ενός Δελτίου Αεροναυτικών Πληροφοριών AIC (αναφέρεται στο ΠΑΡΑΡΤΗΜΑ Ι)

Σε αντίθετη περίπτωση, το επόμενο βήμα είναι να κρίνει το αρμόδιο Τμήμα εάν η αλλαγή έχει μόνιμο ή προσωρινό χαρακτήρα.

Εάν είναι *μόνιμη αλλαγή* διακρίνουμε τρείς πιθανές περιπτώσεις.

- *Μόνιμη αλλά όχι επιχειρησιακά σημαντική*

  πρέπει να καταγραφεί σε ένα Ενδιάμεσο Έντυπο «Διόρθωση AIP»

- *Μόνιμη και επιχειρησιακά σημαντική αλλά χωρίς άμεση συνέπεια*

  πρέπει να καταγραφεί σε ένα Ενδιάμεσο Έντυπο «Διόρθωση AIRAC AIP»

- *Μόνιμη και επιχειρησιακά σημαντική με άμεση συνέπεια*

  πρέπει να καταγραφεί αμέσως σε ένα Ενδιάμεσο Έντυπο «Αεροναυτική Αγγελία NOTAM». Στη συνέχεια ακυρώνεται η Αεροναυτική Αγγελία NOTAM και καταγράφεται σε ένα Ενδιάμεσο Έντυπο «Διόρθωση AIRAC AIP»

Εάν είναι *προσωρινή αλλαγή μακράς διάρκειας* διακρίνουμε τρείς πιθανές περιπτώσεις.

- *Προσωρινή μακράς διάρκειας αλλά όχι επιχειρησιακά σημαντική*

  πρέπει να καταγραφεί σε ένα Ενδιάμεσο Έντυπο «Συμπλήρωση πληροφορία AIP»

- *Προσωρινή μακράς διάρκειας και επιχειρησιακά σημαντική αλλά χωρίς άμεση συνέπεια*

πρέπει να καταγραφεί σε ένα Ενδιάμεσο Έντυπο «Συμπλήρωση AIRAC AIP»

- *Προσωρινή μακράς διάρκειας και επιχειρησιακά σημαντική με άμεση συνέπεια*

πρέπει να καταγραφεί αμέσως σε ένα Ενδιάμεσο Έντυπο «Αεροναυτική Αγγελία NOTAM». Στη συνέχεια ακυρώνεται η Αεροναυτική Αγγελία NOTAM και καταγράφεται σε ένα Ενδιάμεσο Έντυπο «Συμπλήρωση AIRAC AIP»

Εάν είναι *προσωρινή αλλαγή μικρής διάρκειας* διακρίνουμε τέσσερεις πιθανές περιπτώσεις.

- *Προσωρινή μικρής διάρκειας δίχως εκτεταμένο κείμενο ή γραφικά*

  Πρέπει να καταγραφεί σε ένα Ενδιάμεσο Έντυπο «Αεροναυτικής Αγγελίας NOTAM»

- *Προσωρινή μικρής διάρκειας αλλά όχι επιχειρησιακά σημαντική*

  πρέπει να καταγραφεί σε ένα Ενδιάμεσο Έντυπο «Συμπλήρωση AIP»

- *Προσωρινή μικρής διάρκειας και επιχειρησιακά σημαντική αλλά χωρίς άμεση συνέπεια*

  πρέπει να καταγραφεί σε ένα Ενδιάμεσο Έντυπο «Συμπλήρωση AIRAC AIP»

- *Προσωρινή μικρής διάρκειας και επιχειρησιακά σημαντική με άμεση συνέπεια*

  πρέπει να καταγραφεί αμέσως σε ένα Ενδιάμεσο Έντυπο «Αεροναυτική Αγγελία NOTAM». Στη συνέχεια ακυρώνεται η Αεροναυτική Αγγελία NOTAM και καταγράφεται σε ένα Ενδιάμεσο Έντυπο «Συμπλήρωση AIRAC AIP»

Εφόσον εκδοθεί τελικά η «Διόρθωση AIRAC AIP» ή η «Συμπλήρωση AIRAC AIP» στη συνέχεια εκδίδεται πάντα και μια «Αεροναυτική Αγγελία NOTAM ενεργοποίησης», η οποία χρησιμεύει ως υπενθύμιση στους υπεύθυνους για την ενημέρωση του Εγχειριδίου Αεροναυτικών Πληροφοριών AIP (αναλύεται στο ΠΑΡΑΡΤΗΜΑ Ι).

Εξειδικευμένη Οδηγία ΙΙΙ
Εφαρμογή eAIP.wiz@rd

Η εφαρμογή **eAIP.wiz@rd** παρέχει στο χρήστη ένα ολοκληρωμένο σύστημα διαχείρισης της ποιότητας για τη συλλογή αεροναυτικών πληροφοριών, την επεξεργασία τους και τελικά την έκδοση του Εγχειριδίου AIP, των Διορθώσεων του AIP (AIP Amendments) και των Συμπληρώσεων του AIP (AIP Supplements).

Η εφαρμογή έχει υιοθετήσει τη λογική του «Υποδειγματικού Μοντέλου Παρουσίασης & Ανταλλαγής Αεροναυτικών Πληροφοριών-AICM/AIXM (Aeronautical Information Conceptual/Exchange Model) με τέτοιον τρόπο ώστε αεροναυτικές πληροφορίες που αποτελούν στατικά δεδομένα να έχουν συγκεντρωθεί σε διάφορες εγγραφές σε βάσεις δεδομένων. Εντός αυτών των βάσεων ο χρήστης μπορεί εύκολα να πλοηγηθεί και να εντοπίσει τις πληροφορίες αυτές, δίχως να χρειάζεται να διαθέτει εκτενή γνώση του Μοντέλου AICM/AIXM.

Η διεπαφή του χρήστη είναι κατασκευασμένη σύμφωνα με την καθιερωμένη δομή του «Εγχειριδίου Αεροναυτικών Πληροφοριών AIP», όπως αυτή καθορίζεται από το Διεθνή Οργανισμό Πολιτικής Αεροπορίας-ICAO (International Civil Aviation Organization) στο Παράρτημα 15 (Annex 15) και επιτρέπει την εύκολη είσοδο των αεροναυτικών πληροφοριών ανάλογα με τη σειρά που αυτές εισάγονται και στο Εγχειρίδιο Αεροναυτικών Πληροφοριών AIP.

Χαρακτηριστικά & Λειτουργικότητα Εφαρμογής

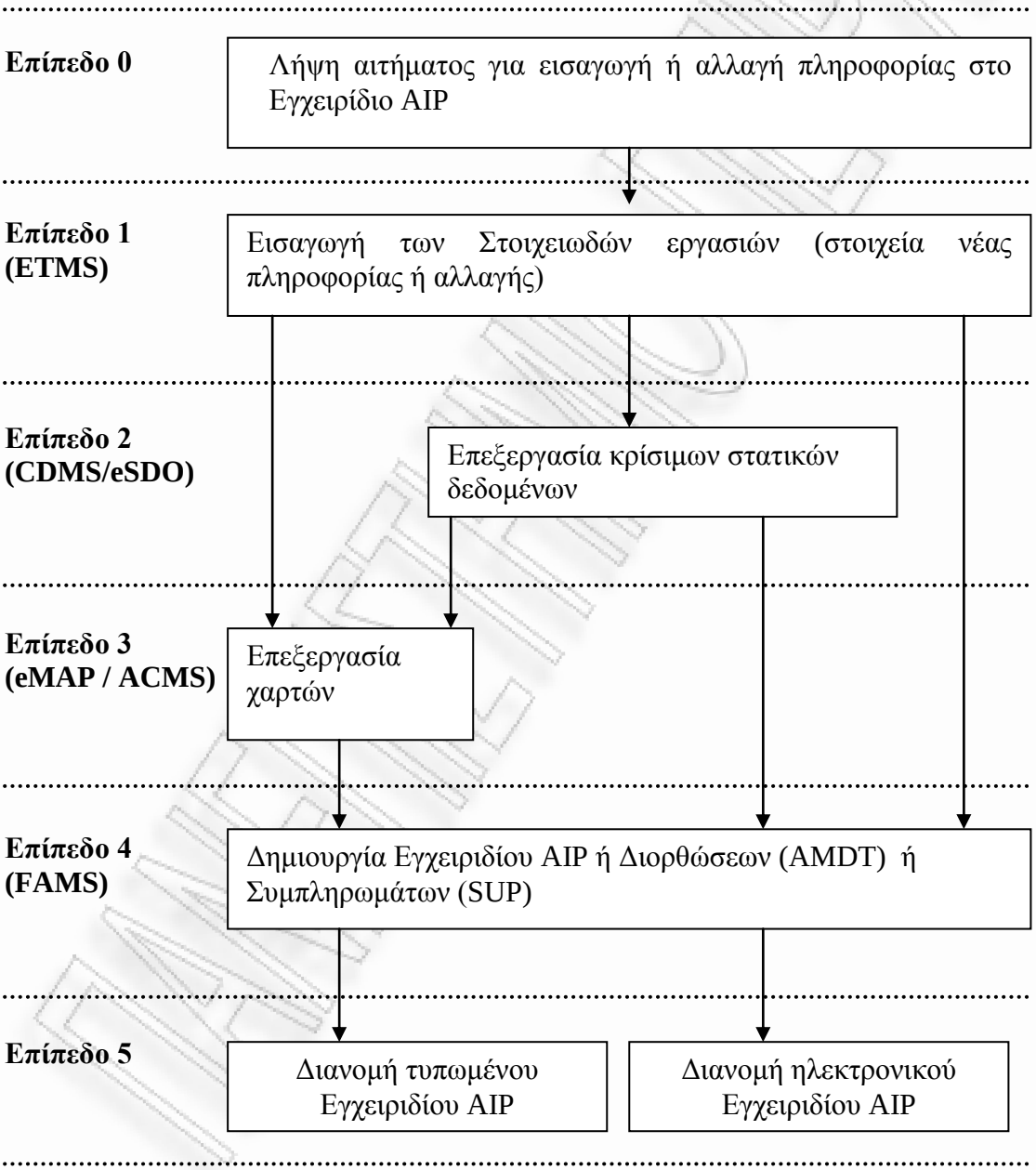
Τα ακόλουθα αποτελούν χαρακτηριστικά του συστήματος :

- διαμόρφωση ροής εργασιών
- διαχείριση δεδομένων
- διαχείριση αλλαγών
- δημιουργία εγγράφων
- διαχείριση εγγράφων
- υποστήριξη πολλών γλωσσών
- διαχείριση Αεροναυτικών Αγγελιών-NOTAM

Εφαρμογή eAIP.wiz@rd – Επίπεδα Συστήματος - Ροή Δεδομένων

Το παρακάτω σχήμα απεικονίζει τη λειτουργία της εφαρμογής. Η εφαρμογή διαχωρίζει τη ροή των εργασιών σε πέντε επίπεδα.

Τα επίπεδα 0 και 5 υλοποιούνται χειρωνακτικά ενώ τα επίπεδα 1 έως και 4 είναι αυτοματοποιημένα.



Εφαρμογή eAIP.wiz@rd – Υπο συστήματος (modules)

Η εφαρμογή **eAIP.wiz@rd** έχει στη διάθεσή της τέσσερα υποπρογράμματα (modules) προκειμένου τα επίπεδα 1-4 να είναι αυτοματοποιημένα. Τα υποπρογράμματα αυτά είναι ενσωματωμένα μέσα στην ίδια την εφαρμογή και σκοπός τους είναι το καθένα από αυτά να αναλαμβάνει την άρτια διεξαγωγή του επιπέδου εργασίας που του αντιστοιχεί.

Τα εν λόγω υποπρογράμματα (modules) είναι τα ακόλουθα :

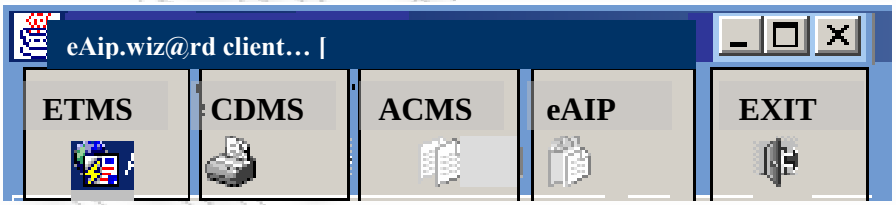
Επίπεδο 1: **ETMS**-Σύστημα Διαχείρισης Στοιχειωδών Εργασιών (Elementary Tasks Management System)

Επίπεδο 2: **CDMS**- Σύστημα Διαχείρισης Κρίσιμων Στατικών Δεδομένων (Critical Data Management System)
eSDO- νέα γενιά του CDMS (Static Data Operation)

Επίπεδο 3: **eMAP** - Σύστημα Χαρτών
ACMS- Σύστημα Διαχείρισης Αεροναυτικών Χαρτών (Aeronautical Charts Management System)

Επίπεδο 4: **FAMS**- Σύστημα Διαχείρισης του Πλαισίου Δημιουργίας του Εγχειριδίου AIP
eAIP (Frame-Maker AIP Management System)

Το κάθε υποπρόγραμμα (module) της εφαρμογής **eAIP.wiz@rd**, ξεκινάει με το πάτημα του αντίστοιχου εικονιδίου στη γραμμή εργαλείων (toolbar) της εφαρμογής.



Τότε το παράθυρο διαλόγου (dialog window) του εκάστοτε υποπρογράμματος, που ο χρήστης έχει επιλέξει, εμφανίζεται στην επιφάνεια εργασίας (desktop).

*Εφαρμογή **eAIP.wiz@rd** – Σύντομη επισκόπηση*

Επίπεδο 0:
Το Τμήμα Εγχειριδίων Αεροναυτικών Πληροφοριών AIP (E1/A) της Διεύθυνσης Αεροναυτικών Εκδόσεων (E1) παραλαμβάνει τα ενδιάμεσα έγγραφα και το αίτημα για εισαγωγή ή αλλαγή πληροφορίας.

Ένας μοναδικός αριθμός ορίζεται στα ανεπεξέργαστα δεδομένα που παρελήφθησαν προκειμένου να εισαχθούν στο σύστημα. Τα δεδομένα αυτά προσδιορίζονται και σημειώνονται με την ημερομηνία παραλαβής, την ημερομηνία αποδοχής και την αναγνώριση ενός χρήστη του συστήματος ως υπεύθυνου για την επεξεργασία τους.

Δημιουργείται έτσι μια φόρμα με τίτλο «Αίτηση για έκδοση αεροναυτικών πληροφοριών-Αλλαγή στο Εγχειρίδιο AIP», η οποία αποτελεί εισερχόμενο για το επίπεδο 1.

Επίπεδο 1 (ETMS) :
Ο χρήστης αποφασίζει ποιά στοιχεία του αιτήματος για αλλαγή των πληροφοριών του Εγχειριδίου AIP θα αντιμετωπιστούν ως ένα ανεξάρτητο μέρος και από τώρα και στο εξής θα ονομάζεται **εργασία (task)**. Μία τέτοια εργασία, χρησιμεύει ως σημείο εισόδου για την περαιτέρω επεξεργασία των δεδομένων στα επόμενα επίπεδα.

Οι **εργασίες** αυτές αποθηκεύονται στη **Βάση Δεδομένων εργασιών (task database)**. Αυτή η βάση δεδομένων περιλαμβάνει μια λίστα με τις εργασίες, τις σημειώσεις για αυτές και τη σημερινή τους κατάσταση.

Επίπεδο 2 (CDMS/eSDO) :
Τα ακόλουθα είναι κρίσιμα στατικά δεδομένα :

1.Δεδομένα Αεροδρομίων/ Ελικοδρομίων (Aerodrome/heliport data)
2.Δεδομένα Βοήθειας Πλοήγησης (Navigation data)
3.Δεδομένα Διαδικασίας (Procedure data)
4.Δεδομένα Εναέριου Χώρου (Airspace data)
5.Δεδομένα Οργανισμού (Organization data)
6.Δεδομένα Καθορισμένων Σημείων (Designated point data)
7.Δεδομένα Αεροδιαδρόμων (Routes data)
8.Δεδομένα Εμποδίων (Obstacle data)

Όλα τα κρίσιμα στατικά δεδομένα είναι αποθηκευμένα στην Βάση Δεδομένων στατικών δεδομένων (static data database), αυτός είναι και ο λόγος που η βάση αυτή αποτελεί την πηγή των στατικών στοιχείων για τα επόμενα επίπεδα 3 και 4.

Κατά τη διεκπεραίωση μιας εργασίας (task) τα στατικά δεδομένα επεξεργάζονται στο επίπεδο 2. Συνεπώς η Βάση αυτή τροποποιείται από τον χρήστη σε αυτό το επίπεδο.

Κάθε στοιχείο σε αυτή τη Βάση δεδομένων επισημαίνεται με την ημερομηνία της εισαγωγής του, την περίοδο ισχύος του, τα στοιχεία του χρήστη και μια σύνδεση με την εργασία εξαιτίας της οποίας το συγκεκριμένο στοιχείο προστέθηκε στη βάση δεδομένων.

Επίπεδο 3 (eMAP / ACMS) :
Το Σύστημα Διαχείρισης Αεροναυτικών Χαρτών (ACMS) το οποίο επιτρέπει την εργασία με τους αεροναυτικούς χάρτες, αποτελεί το τρίτο επίπεδο του συστήματος.

Παρέχει εργαλεία για την προσθήκη των νέων εκδόσεων των αεροναυτικών χαρτών στη Βάση δεδομένων αεροναυτικών χαρτών, την τροποποίηση των παλιών ή την ολοκληρωτική διαγραφή τους.

Προκειμένου να φέρει εις πέρας τις τρείς παραπάνω λειτουργίες (εισαγωγή, τροποποίηση, διαγραφή) συνεργάζεται με το υπάρχον σύστημα χρησιμοποιώντας τα στοιχεία της Βάσης δεδομένων εργασιών και της Βάση στατικών δεδομένων ως εισερχόμενα.

Στο τέλος, οι χάρτες μπορούν αποθηκεύονται με μορφή γραφήματος στη Βάση δεδομένων αεροναυτικών χαρτών.

Επίπεδο 4 (FAMS / eAIP) :
Το επίπεδο αυτό υποστηρίζει τη δημιουργία του Εγχειριδίου AIP καθώς και την ενσωμάτωση σε αυτό των όποιων αλλαγών.

Σε συνδυασμό με τα άλλα υποπρογράμματα παρέχει συνδέσεις στη Βάση δεδομένων εργασιών, στη Βάση δεδομένων στατικών δεδομένων και στη Βάση δεδομένων αεροναυτικών χαρτών.

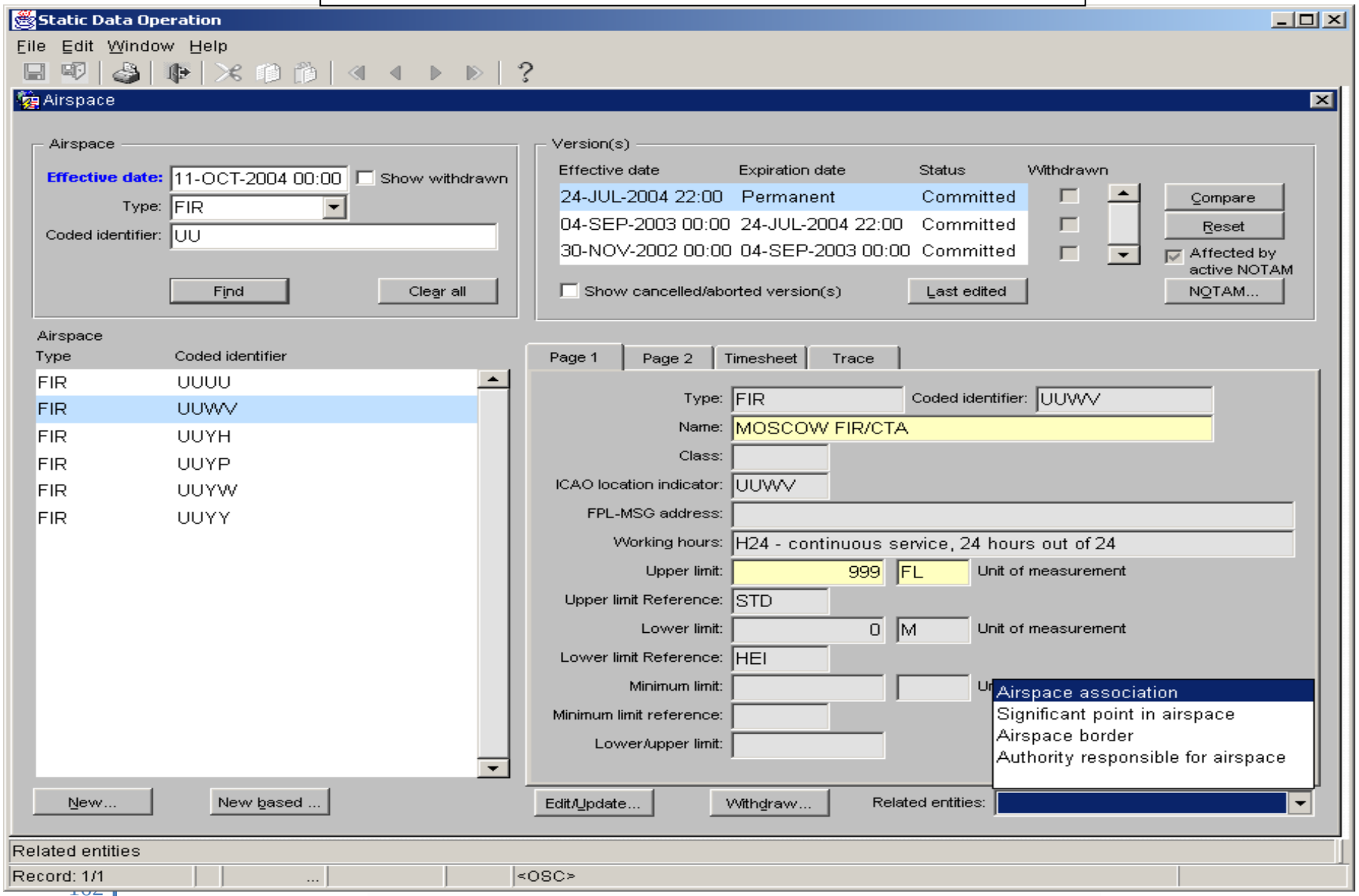
Επίσης :
- επιτρέπει τον εντοπισμό της προέλευσης των αλλαγών στις πληροφορίες των εγγράφων του Εγχειριδίου AIP
- προβλέπει τη μορφοποίηση σελίδων AIP σε μορφή pdf αρχείου, ώστε να δύναται να τυπωθούν ή να αποθηκευτούν σε CD-ROM καθώς και σε μορφή SGML/XML αρχείου, ώστε να είναι δυνατή μια ηλεκτρονική δημοσίευση του Εγχειριδίου AIP

Επίπεδο 5 :
Το Εγχειρίδιο αποστέλλεται στους συνδρομητές με κάποιον από τους εξής τρόπους :

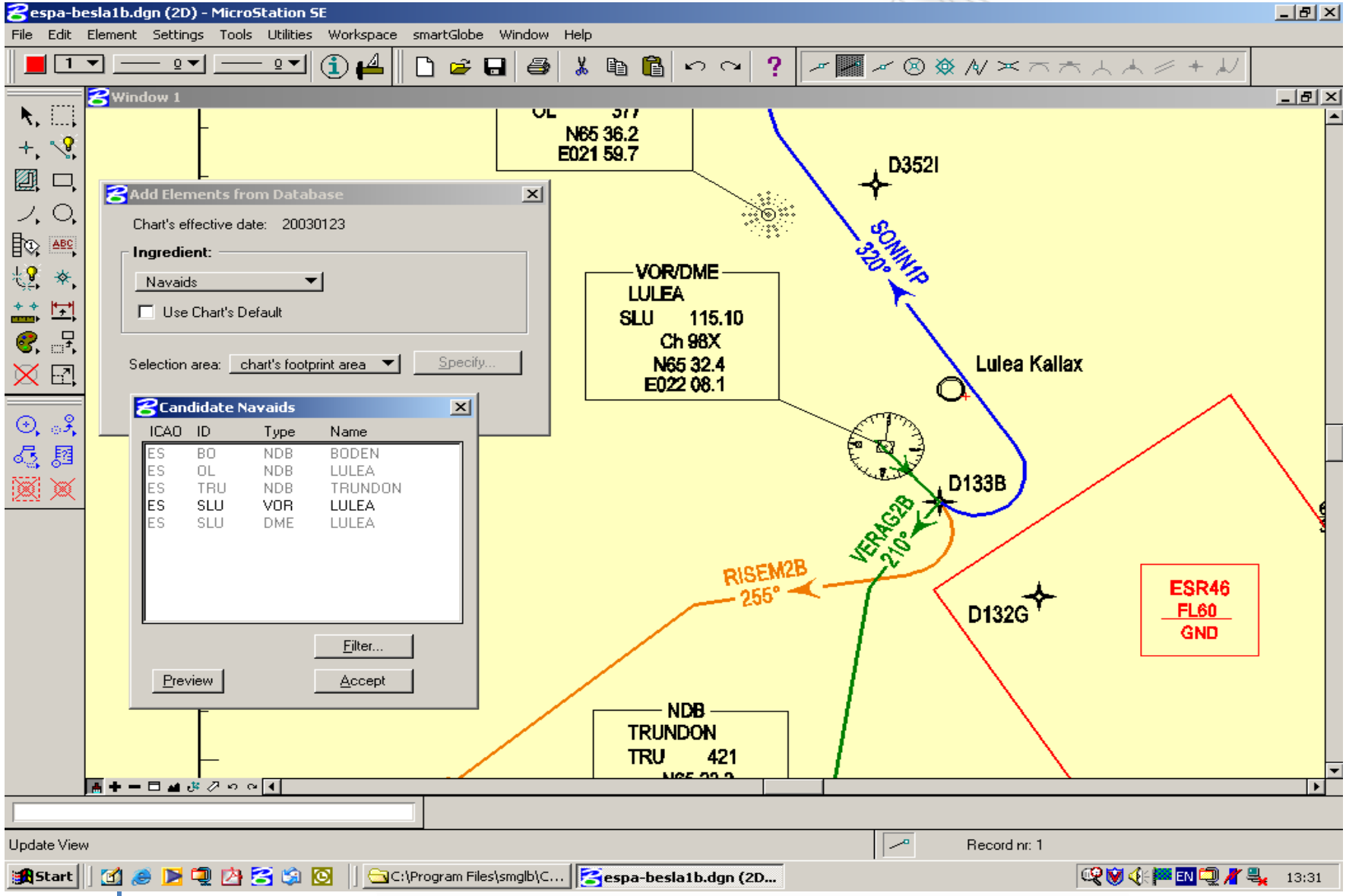
- εκτυπωμένο
- σε ηλεκτρονική μορφή μέσω εσωτερικού δικτύου (intranet)
- σε ηλεκτρονική μορφή μέσω Διαδικτύου (internet)
- σε CD-ROM

Οι παρακάτω εικόνες αποτελούν ένα παράδειγμα της εφαρμογής **eAIP.wiz@rd** σε λειτουργία.

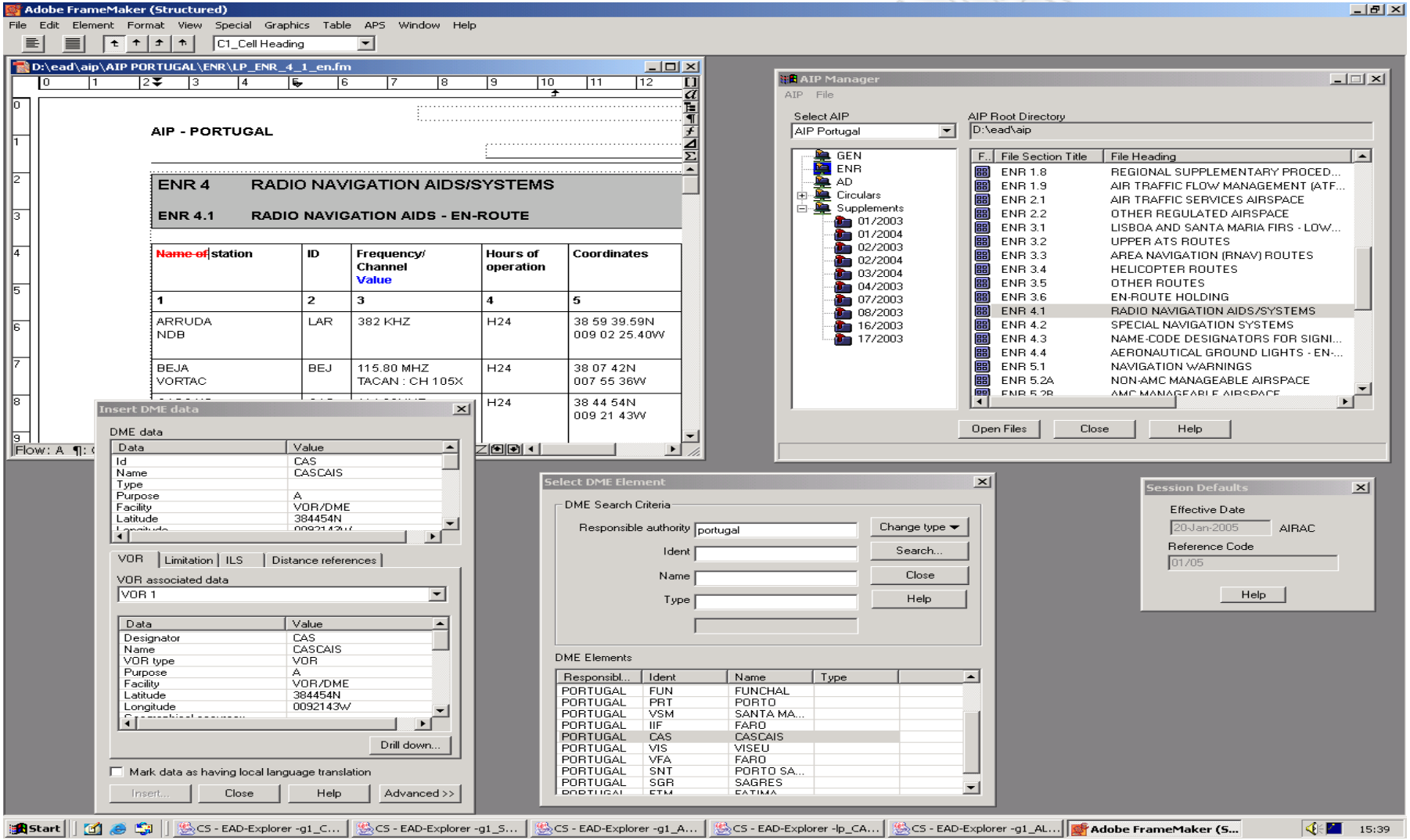
Επίπεδο 2 : «Επεξεργασία Κρίσιμων Στατικών Δεδομένων» (CDMS/ eSDO)



Επίπεδο 3 : «Επεξεργασία Αεροναυτικών Χαρτών» (eMAP / ACMS)



Επίπεδο 4 : «Διαχείρισης του Πλαισίου Δημιουργίας του Εγχειριδίου AIP» (FAMS/ eAIP)



Εξειδικευμένη Οδηγία IV
Τυπογραφείο Υ.Π.Α

Το Τυπογραφείο της Υ.Π.Α έχει την ευθύνη και μέριμνα για την :

- προμήθεια του χαρτιού της αναγκαίας και ικανής ποσότητας σε ετήσια βάση, για την έκδοση του Εγχειριδίου Αεροναυτικών Πληροφοριών AIP Ελλάδος και των μηνιαίων ενημερώσεων (Διορθώσεις-Amendments, Συμπληρώσεις-Supplements).

- άριστη εκτύπωση των αποστελλόμενων σελίδων AIP.

Εξειδικευμένη Οδηγία V
Λογιστικό & Εφοδιαστικό Κέντρο (ΛΕΚ) της Υ.Π.Α

Το Τμήμα Εγχειριδίων Αεροναυτικών Πληροφοριών AIP (Ε1/Α), το οποίο υπάγεται στη Διεύθυνση Αεροναυτικών Εκδόσεων (Ε1), είναι υποχρεωμένο να παρέχει τις Αεροναυτικές Εκδόσεις σε τιμές, που να καλύπτουν το ελάχιστο κόστος, σύμφωνα με τις εισηγήσεις του Διεθνούς Οργανισμού Πολιτικής Αεροπορίας (ICAO).

Η Διεύθυνση Εναέριας Κυκλοφορίας (Δ4) προσδιορίζει το ελάχιστο κόστος των Αεροναυτικών Εκδόσεων και το γνωστοποιεί στη Διεύθυνση Οικονομικού & Εφοδιασμού (Δ11).

Οι τιμές πώλησης των Αεροναυτικών Εκδόσεων καθορίζονται με απόφαση του Διοικητού της Υ.Π.Α μετά από σχετική εισήγηση των αρμοδίων Διευθύνσεων Δ4 και Δ11. Στην ίδια απόφαση καθορίζεται το ύψος της ετήσιας συνδρομής ενδιαφερομένων εσωτερικού και εξωτερικού για τα εξής :

- Εγχειρίδιο Αεροναυτικών Πληροφοριών AIP
- Διορθώσεις στο Εγχειρίδιο
- Συμπληρώσεις στο Εγχειρίδιο

Το Λογιστικό & Εφοδιαστικό Κέντρο (ΛΕΚ) εκδίδει μηχανογραφικά Τιμολόγιο (για συνδρομητές εξωτερικού) ή Χρηματική Εντολή (για συνδρομητές εσωτερικού) στο όνομα του υπόχρεου προς πληρωμή και αποστέλλεται στη διεύθυνση :

1. του υπόχρεου
2. ή του εκπροσώπου, ο οποίος έχει αναλάβει την ευθύνη της αποστολής των τιμολογίων στον υπόχρεο οπότε αναγράφεται στο τιμολόγιο «με φροντίδα»

Η Χρηματική Εντολή ή αντίστοιχα το Τιμολόγιο αποστέλλονται ταχυδρομικά, συστημένα με απόδειξη παραλαβής, ώστε να αποδεικνύεται η επίδοση τους στον παραλήπτη αν αυτό απαιτηθεί.

Εξειδικευμένη Οδηγία VI

Ετήσια Συνδρομή «Εγχειριδίου Αεροναυτικών Πληροφοριών-AIP»

Κάθε υποψήφιος συνδρομητής, εσωτερικού ή εξωτερικού, κάνει τα εξής :

- Προπληρώνει για όλους τους υπόλοιπους μήνες του τρέχοντος χρόνου με έναρξη την 1^{η} του επόμενου μήνα της ημερομηνίας διάθεσης οπότε ακολουθείται η διαδικασία ετήσιας συνδρομής.

- Αποστέλλει αντίγραφο του αποδεικτικού κατάθεσης του αναλογούντος ποσού στον Ειδικό Λογαριασμό της Υ.Π.Α. που τηρείται στην Τράπεζα της Ελλάδος-ΤΜΗΜΑ ΣΧΕΣΕΩΝ ΜΕ ΤΟ ΔΗΜΟΣΙΟ.

Η ετήσια συνδρομή καλύπτει χρονικό διάστημα από 1^{ης} Ιανουαρίου κάθε έτους μέχρι 31 Δεκεμβρίου του αυτού έτους και προκαταβάλλεται για τη διάθεση :

- Εγχειριδίου Αεροναυτικών Πληροφοριών AIP Τόμος I, Τόμος II
- Διορθώσεων Εγχειριδίου Αεροναυτικών Πληροφοριών AIP
- Συμπληρώσεων Εγχειριδίου Αεροναυτικών Πληροφοριών AIP

Η προθεσμία πληρωμής δεν πρέπει να υπερβαίνει την 10^{η} Δεκεμβρίου του εκάστοτε έτους. Εάν ο συνδρομητής δεν έχει εξοφλήσει τις οφειλές του εντός των προβλεπόμενων προθεσμιών πληρωμής, τότε το Τμήμα (Ε1/Α) αποστέλλει σε αυτόν πρόσκληση εξόφλησης οφειλών μετά των αναλογούντων τόκων υπερημερίας και με τη ειδοποίηση ότι πέραν του τριμήνου ακολουθεί διαγραφή αυτού.

Εάν δεν εξοφλήσει ούτε τότε :

- διακόπτει τη συνδρομή λόγω οφειλών
- εγγράφει τον πρώην συνδρομητή σε κατάσταση διαγραφομένων συνδρομητών λόγω οφειλών
- ενημερώνει το Λογιστικό & Εφοδιαστικό Κέντρο (ΛΕΚ)

Ο συνδρομητής μπορεί μέχρι και την 31 Οκτωβρίου του προηγούμενου έτους να υποβάλλει «Αίτηση διακοπής συνδρομής» προς το Τμήμα (Ε1/Α) που υποβάλλεται και μέσω ηλεκτρονικού ταχυδρομείου και αποδεικνύεται με το πρωτόκολλο που τηρεί το Τμήμα (Ε1/Α).

7.1.3. ΠΑΡΑΡΤΗΜΑ ΙΙΙ - ΣΧΕΔΙΟ ΜΕΙΩΣΗΣ ΚΙΝΔΥΝΟΥ (RISK TREATMENT PLAN)

(Εγχειρίδιο Διαχείρισης της Ασφάλειας Υπηρεσιών Ελέγχου Εναέριας Κυκλοφορίας-Safety Management Manual, Υπηρεσία Πολιτικής Αεροπορίας)

Μη συμμόρφωση με τις απαιτήσεις του προτύπου ενδέχεται να καταλήξει σε συμβάν. Συμβάν ορίζεται οτιδήποτε σχετίζεται με την αεροναυτική πληροφορία και επηρεάζει ή θα μπορούσε να επηρεάσει την ασφάλεια της.

Εφόσον το ISO/IEC 27001:2005 ορίζει ως ασφάλεια πληροφοριών τη διατήρηση και προστασία των ακόλουθων τριών βασικών ιδιοτήτων της πληροφορίας, της εμπιστευτικότητας, της ακεραιότητας, της διαθεσιμότητας αλλά και δύο πρόσθετων, της εγκυρότητας και της αυθεντικότητας, συμβάν τότε θεωρείται οτιδήποτε πλήττει μία ή και όλες εξ αυτών των ιδιοτήτων.

Τα συμβάντα που αφορούν την αεροναυτική πληροφορία και θα μπορούσαν να προκύψουν από μη συμμόρφωση με τις απαιτήσεις του προτύπου και κατά συνέπεια μη ορθή εφαρμογή της «Δήλωσης Εφαρμοσιμότητας» που αποτελεί βασική απαίτηση του προτύπου, άρα και των ελέγχων που αυτή περιλαμβάνει, είναι τα ακόλουθα :

- Βλάβη συστήματος
- Εξάντληση χρόνου ζωής εξοπλισμού
- Φυσική καταστροφή (σεισμός, τσουνάμι)
- Ξαφνική καταστροφή (μπλάκ-ουτ)
- Ατύχημα (πυρκαγιά)
- Τρομοκρατική ενέργεια (9/11)
- Ιοί
- Απώλεια εντύπου
- Λανθασμένη καταχώρηση
- Παράλειψη καταχώρησης
- Παράνομη πρόσβαση
- Αλλαγή διαδικασίας δίχως έγκαιρη ενημέρωση προσωπικού

Ο οργανισμός έχει διατυπώσει ένα «Σχέδιο Μείωσης Κινδύνου» το οποίο προσδιορίζει τη διαδικασία διαχείρισης μη συμμορφώσεων, τις ευθύνες και τις προτεραιότητες για την αντιμετώπιση τους.

Τη στιγμή του εντοπισμού μιας μη συμμόρφωσης ή ενός συμβάντος που προέκυψε από μη συμμόρφωση, με ευθύνη των Διευθυντών των μονάδων λαμβάνονται τα άμεσα διορθωτικά μέτρα και εκδίδεται μια Αναφορά ασφαλείας προς τη Διοίκηση.

Ο οργανισμός διαθέτει ένα σύστημα αναφορών στο οποίο περιγράφονται λεπτομέρειες για τα παρακάτω :

- ✓ ποιά περιστατικά πρέπει να αναφέρονται
- ✓ πότε και πώς πρέπει να γίνονται οι αναφορές
- ✓ ποιό θα είναι το περιεχόμενο και ο τύπος των αναφορών
- ✓ ποιοί έχουν την αρμοδιότητα για διερεύνηση και ανάλυση περιστατικών ασφαλείας
- ✓ πώς γίνεται η διασπορά των πληροφοριών για τα περιστατικά ασφαλείας πληροφοριών

Στο συντομότερο δυνατό χρόνο με ευθύνη πάλι των Διευθυντών των μονάδων που έλαβε χώρα η μη συμμόρφωση συγκεντρώνονται τα σχετικά στοιχεία όπως, ηλεκτρονικά αρχεία καταγραφής του συστήματος, συμπληρωμένα έντυπα, αναφορές των εμπλεκομένων και άλλα. Στη συνέχεια ξεκινά η ανάλυση τους από τους Διευθυντές των εμπλεκόμενων μονάδων με στόχο:

- Τον έλεγχο της αποτελεσματικότητας των άμεσων μέτρων που λήφθηκαν.
- Την κατάταξη της μη συμμόρφωσης ανάλογα με το βαθμό σοβαρότητάς της.
- Την αναγνώριση παραγόντων που την προκάλεσαν.
- Την υποβολή προτάσεων για διορθωτικά μέτρα ώστε να εξαλειφθούν οι παράγοντες που οδήγησαν στη μη συμμόρφωση.
- Τη λήψη διορθωτικών μέτρων
- Την επαλήθευση των διορθωτικών μέτρων και της εξάλειψης των μη συμμορφώσεων
- Τη σύνταξη και αποστολή ενημερωτικού σημειώματος για τη μη συμμόρφωση προς το προσωπικό. Τα ενημερωτικά σημειώματα είναι αποταυτοποιημένα επειδή ενδιαφέρον έχει η διασπορά της πληροφορίας για τους παράγοντες που οδήγησαν στη μη συμμόρφωση και όχι για τους εμπλεκόμενους σε αυτήν.

Προτεραιότητες για την Αντιμετώπιση Μη Συμμορφώσεων

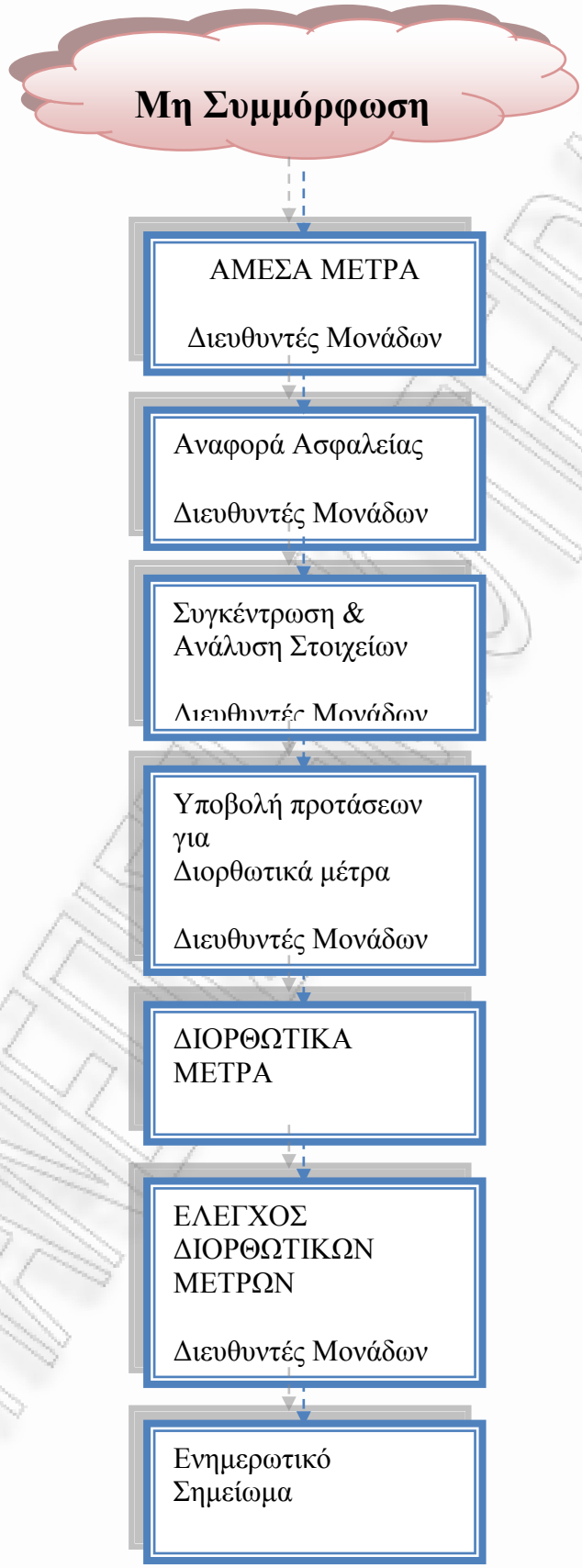
Ο κίνδυνος διαβαθμίζεται όσον αφορά τη σοβαρότητα και τη ρεαλιστική πιθανότητα εμφάνισής της :

Επίπεδο Κινδύνου	Προτεραιότητα Αντιμετώπισης
3 Μείζονος Σημασίας	Πρέπει να ληφθούν άμεσα μέτρα για να μειωθεί ο κίνδυνος
2 Σοβαρή	Πρέπει να ενημερωθεί ο Διευθυντής μέχρι το τέλος της εργάσιμης ημέρας
1 Μη Συμμόρφωση Ρουτίνας	Πρέπει να ληφθούν μέτρα με την πρώτη δυνατή ευκαιρία

Ιδιαίτερη σημασία αποδίδεται στη διαχείριση μιας «Μείζονος Σημασίας Μη Συμμορφώσεως». Μείζονος Σημασίας μη συμμόρφωση θεωρείται εκείνη η οποία οδήγησε σε μείζων συμβάν κατά το οποίο η ζημιά έχει ήδη γίνει.

Οι εργαζόμενοι γενικά όταν προβαίνουν στην αντιμετώπιση μιας μη συμμόρφωσης πρέπει να διασφαλίζουν ότι ο κίνδυνος ελαχιστοποιήθηκε στο κατώτερο δυνατό επίπεδο.

Διαδικασία Διαχείρισης Μη Συμμορφώσεων



7.1.4. ΠΑΡΑΡΤΗΜΑ IV - ΕΝΤΥΠΑ

- ΕΝΤΥΠΟ Δ.1.1
  «ΥΠΗΡΕΣΙΑΚΟ ΣΗΜΕΙΩΜΑ ΑΝΑΘΕΣΗΣ ΣΥΓΚΕΝΤΡΩΣΗΣ Η ΑΛΛΑΓΗΣ ΠΛΗΟΦΟΡΙΩΝ»
- ΕΝΤΥΠΟ Δ.1.2
  «ΕΝΔΙΑΜΕΣΟ ΕΝΤΥΠΟ ΔΙΟΡΘΩΣΗΣ AIP»
- ΕΝΤΥΠΟ Δ.1.3
  «ΕΝΔΙΑΜΕΣΟ ΕΝΤΥΠΟ ΔΙΟΡΘΩΣΗΣ AIRAC AIP»
- ΕΝΤΥΠΟ Δ.1.4
  «ΕΝΔΙΑΜΕΣΟ ΕΝΤΥΠΟ ΣΥΜΠΛΗΡΩΣΗΣ AIP»
- ΕΝΤΥΠΟ Δ.1.5
  «ΕΝΔΙΑΜΕΣΟ ΕΝΤΥΠΟ ΣΥΜΠΛΗΡΩΣΗΣ AIRAC AIP SUPPLEMENT»
- ΕΝΤΥΠΟ Δ.1.6
  «ΕΝΔΙΑΜΕΣΟ ΕΝΤΥΠΟ ΑΕΡΟΝΑΥΤΙΚΗ ΑΓΓΕΛΙΑ NOTAM»
- ΕΝΤΥΠΟ Δ.2.1
  «ΥΠΗΡΕΣΙΑΚΟ ΣΗΜΕΙΩΜΑ ΛΑΝΘΑΣΜΕΝΗΣ ΚΑΤΑΧΩΡΗΣΗΣ ΠΛΗΡΟΦΟΡΙΩΝ»
- ΕΝΤΥΠΟ Δ.2.2
  «ΤΕΛΙΚΟ ΕΝΤΥΠΟ ΔΙΟΡΘΩΣΗΣ AIP AMENDMENT»
- ΕΝΤΥΠΟ Δ.2.3
  «ΤΕΛΙΚΟ ΕΝΤΥΠΟ ΔΙΟΡΘΩΣΗΣ AIRAC AIP AMENDMENT»
- ΕΝΤΥΠΟ Δ.2.4
  «ΤΕΛΙΚΟ ΕΝΤΥΠΟ ΣΥΜΠΛΗΡΩΣΗΣ AIP SUPPLEMENT»
- ΕΝΤΥΠΟ Δ.2.5
  «ΤΕΛΙΚΟ ΕΝΤΥΠΟ ΣΥΜΠΛΗΡΩΣΗΣ AIRAC AIP SUPPLEMENT»
- ΕΝΤΥΠΟ Δ.2.6
  «ΤΕΛΙΚΟ ΕΝΤΥΠΟ ΑΕΡΟΝΑΥΤΙΚΗ ΑΓΓΕΛΙΑ NOTAM»
- ΕΝΤΥΠΟ Δ.3.1
  «ΥΠΗΡΕΣΙΑΚΟ ΣΗΜΕΙΩΜΑ ΑΝΑΘΕΣΗΣ ΕΚΔΟΣΗΣ ΑΕΡΟΝΑΥΤΙΚΩΝ ΕΚΔΟΣΕΩΝ»
- ΕΝΤΥΠΟ Δ.3.2
  «ΑΙΤΗΣΗ ΧΟΡΗΓΗΣΗΣ ΑΕΡΟΝΑΥΤΙΚΩΝ ΕΚΔΟΣΕΩΝ»
- ΕΝΤΥΠΟ Δ.3.3
  «ΑΙΤΗΣΗ ΧΟΡΗΓΗΣΗΣ ΑΕΡΟΝΑΥΤΙΚΩΝ ΕΚΔΟΣΕΩΝ» (ΑΓΓΛΙΚΑ)
- ΕΝΤΥΠΟ Δ.3.4

«ΕΓΚΡΙΣΗ ΔΙΑΘΕΣΗΣ ΑΕΡΟΝΑΥΤΙΚΩΝ ΕΚΔΟΣΕΩΝ»

- ΕΝΤΥΠΟ Δ.3.5
  «ΑΠΟΔΕΙΚΤΙΚΟ ΠΑΡΑΛΑΒΗΣ ΑΕΡΟΝΑΥΤΙΚΩΝ ΕΚΔΟΣΕΩΝ»

- ΕΝΤΥΠΟ Δ.3.6
  «ΕΝΤΥΠΟ ΔΙΑΘΕΣΗΣ ΑΕΡΟΝΑΥΤΙΚΩΝ ΕΚΔΟΣΕΩΝ»

- ΕΝΤΥΠΟ 6.1
  «ΕΝΤΥΠΟ ΕΤΗΣΙΟ ΠΡΟΓΡΑΜΜΑ ΕΠΙΘΕΩΡΗΣΕΩΝ»

- ΕΝΤΥΠΟ 6.2
  «ΕΝΤΥΠΟ ΑΝΑΦΟΡΑ ΕΠΙΘΕΩΡΗΣΗΣ»

- ΕΝΤΥΠΟ 7
  «ΕΝΤΥΠΟ ΠΡΑΚΤΙΚΑ ΑΝΑΣΚΟΠΗΣΗΣ»

- ΕΝΤΥΠΟ 8.1
  «ΕΝΤΥΠΟ ΑΝΑΦΟΡΑΣ ΒΛΑΒΩΝ, ΣΥΜΒΑΝΤΩΝ & ΑΤΥΧΗΜΑΤΩΝ»

- ΕΝΤΥΠΟ 8.2
  «ΕΝΤΥΠΟ ΔΙΟΡΘΩΤΙΚΕΣ & ΠΡΟΛΗΠΤΙΚΕΣ ΕΝΕΡΓΕΙΕΣ»

ΥΠΗΡΕΣΙΑ ΠΟΛΙΤΙΚΗΣ ΑΕΡΟΠΟΡΙΑΣ

ΕΝΤΥΠΟ Δ.1.1

ΥΠΗΡΕΣΙΑΚΟ ΣΗΜΕΙΩΜΑ ΑΝΑΘΕΣΗΣ ΣΥΓΚΕΝΤΡΩΣΗΣ Ή ΑΛΛΑΓΗΣ ΠΛΗΡΟΦΟΡΙΩΝ

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΜΕΤΑΦΟΡΩΝ & ΕΠΙΚΟΙΝΩΝΙΩΝ
ΥΠΗΡΕΣΙΑ ΠΟΛΙΤΙΚΗΣ ΑΕΡΟΠΟΡΙΑΣ
ΓΕΝΙΚΗ ΔΙΕΥΘΥΝΣΗ
Δ/ΝΣΗ ΑΕΡΟΛΙΜΕΝΩΝ (Δ3)
Δ/ΝΣΗ ΕΝΑΕΡΙΑΣ ΚΥΚΛΟΦΟΡΙΑΣ (Δ4)
Δ/ΝΣΗ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ (Δ5)
Δ/ΝΣΗ ΗΛ.ΣΥΣΤΗΜΑΤΩΝ ΑΕΡΟΝΑΥΤΙΛΙΑΣ (Δ6)

Αθήνα

ΑΡ.ΠΡΩΤ:

ΠΡΟΣ:

- Τμήμα Αεροδρομίων & Ελικοδρομίων
- Τμήμα Διαδικασιών ΕναέριαςΚυκλοφορίας Τμήμα Διαχείρισης Φάσματος Συχνοτήτων &Τμήμα Επικοινωνιών και Ραδιοβοηθημάτων

ΘΕΜΑ: Συγκέντρωση ή αλλαγή Αεροναυτικών Πληροφοριών

(σημειώνεται η αντίστοιχη ανάθεση, το αντίστοιχο Τμήμα και ενδιάμεσο έντυπο)

Αναθέτουμε :

1. τη συγκέντρωση Αεροναυτικών Πληροφοριών στο :
   I. Τμήμα Αεροδρομίων & Ελικοδρομίων
   II. Τμήμα Διαδικασιών Εναέριας Κυκλοφορίας
   III. Τμήμα Διαχείρισης Φάσματος Συχνοτήτων & Τμήμα Επικοινωνιών και Ραδιοβοηθημάτων

ή

2. την αλλαγή υφιστάμενων Αεροναυτικών Πληροφοριών στο :

Ενδιάμεσο Έντυπο	Τμήμα Αεροδρομίων & Ελικοδρομίων	Τμήμα Διδικασιών Εναέριας Κυκλοφορίας	Τμήμα Διαχείρισης Φάσματος Συχνοτήτων & Τμήμα Επικοινωνιών & Ραδιοβοηθημάτων
Διόρθωση AIP			
Διόρθωση AIRAC AIP			
Συμπλήρωση AIP			
Συμπλήρωση AIRAC AIP			
Αεροναυτική Αγγελία NOTAM			

Με Εντολή Διοικητή
Ο Διευθυντής

ΥΠΗΡΕΣΙΑ ΠΟΛΙΤΙΚΗΣ ΑΕΡΟΠΟΡΙΑΣ

ΕΝΤΥΠΟ Δ.1.2

ΕΝΔΙΑΜΕΣΟ ΕΝΤΥΠΟ «ΔΙΟΡΘΩΣΗ AIP AMENDMENT»

AIP AMENDMENT

Phone:+302109972480
FAX: +302109750757
AFTN: LGGGYNYP Email: e1a@hcaa.gr

GREECE
MINISTRY OF TRANSPORT AND COMMUNICATION
CIVIL AVIATION AUTHORITY
AERONAUTICAL INFORMATION SERVICE DIVISION
P.O BOX 70360 GR 166 10 GLYFADA GREECE

(ΑΛΛΑΓΕΣ)

1. .....
2. .....
3. .....
4. .....
5. .....

ΥΠΗΡΕΣΙΑ ΠΟΛΙΤΙΚΗΣ ΑΕΡΟΠΟΡΙΑΣ

ΕΝΤΥΠΟ Δ.1.3

ΕΝΔΙΑΜΕΣΟ ΕΝΤΥΠΟ «ΔΙΟΡΘΩΣΗ AIRAC AIP AMENDMENT»

AIRAC AIP AMENDMENT

Phone:+302109972480
FAX: +302109750757
AFTN: LGGGYNYP Email: e1a@hcaa.gr

GREECE
MINISTRY OF TRANSPORT AND COMMUNICATION
CIVIL AVIATION AUTHORITY
AERONAUTICAL INFORMATION SERVICE DIVISION
P.O BOX 70360 GR 166 10 GLYFADA GREECE

Effective Date:

(ΑΛΛΑΓΕΣ)

1. ……
2. ……
3. ……
4. ……
5. ……

ΥΠΗΡΕΣΙΑ ΠΟΛΙΤΙΚΗΣ ΑΕΡΟΠΟΡΙΑΣ

ΕΝΤΥΠΟ Δ.1.4

ΕΝΔΙΑΜΕΣΟ ΕΝΤΥΠΟ «ΣΥΜΠΛΗΡΩΣΗ AIP SUPPLEMENT»

AIP SUPPLEMENT

Phone:+302109972480
FAX: +302109750757
AFTN: LGGGYNYP Email: e1a@hcaa.gr

GREECE
MINISTRY OF TRANSPORT AND COMMUNICATION
CIVIL AVIATION AUTHORITY
AERONAUTICAL INFORMATION SERVICE DIVISION
P.O BOX 70360 GR 166 10 GLYFADA GREECE

(ΚΕΙΜΕΝΟ ΠΟΥ ΠΡΟΚΕΙΤΑΙ ΝΑ ΠΡΟΣΤΕΘΕΙ ΣΤΟ ΕΓΧΕΙΡΙΔΙΟ)

ΥΠΗΡΕΣΙΑ ΠΟΛΙΤΙΚΗΣ ΑΕΡΟΠΟΡΙΑΣ

ΕΝΤΥΠΟ Δ.1.5

ΕΝΔΙΑΜΕΣΟ ΕΝΤΥΠΟ «ΣΥΜΠΛΗΡΩΣΗ AIRAC AIP SUPPLEMENT»

AIRAC AIP SUPPLEMENT

Phone:+302109972480
FAX: +302109750757
AFTN: LGGGYNYP Email: e1a@hcaa.gr

GREECE
MINISTRY OF TRANSPORT AND COMMUNICATION
CIVIL AVIATION AUTHORITY
AERONAUTICAL INFORMATION SERVICE DIVISION
P.O BOX 70360 GR 166 10 GLYFADA GREECE

Effective Date:

(ΚΕΙΜΕΝΟ ΠΟΥ ΠΡΟΚΕΙΤΑΙ ΝΑ ΠΡΟΣΤΕΘΕΙ ΣΤΟ ΕΓΧΕΙΡΙΔΙΟ)

ΥΠΗΡΕΣΙΑ ΠΟΛΙΤΙΚΗΣ ΑΕΡΟΠΟΡΙΑΣ

ΕΝΤΥΠΟ Δ.1.6

ΕΝΔΙΑΜΕΣΟ ΕΝΤΥΠΟ «ΑΕΡΟΝΑΥΤΙΚΗ ΑΓΓΕΛΙΑ NOTAM»

NOTAM

Phone:+302109972480
FAX: +302109750757
AFTN: LGGGYNYP Email: e1a@hcaa.gr

GREECE
MINISTRY OF TRANSPORT AND COMMUNICATION
CIVIL AVIATION AUTHORITY
AERONAUTICAL INFORMATION SERVICE DIVISION
P.O BOX 70360 GR 166 10 GLYFADA GREECE

(ΚΕΙΜΕΝΟ ΑΕΡΟΝΑΥΤΙΚΗΣ ΑΓΓΕΛΙΑΣ)

ΥΠΗΡΕΣΙΑ ΠΟΛΙΤΙΚΗΣ ΑΕΡΟΠΟΡΙΑΣ

ΕΝΤΥΠΟ Δ.2.1

ΥΠΗΡΕΣΙΑΚΟ ΣΗΜΕΙΩΜΑ ΛΑΝΘΑΣΜΕΝΗΣ ΚΑΤΑΧΩΡΗΣΗΣ ΠΛΗΡΟΦΟΡΙΩΝ

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΜΕΤΑΦΟΡΩΝ & ΕΠΙΚΟΙΝΩΝΙΩΝ
ΥΠΗΡΕΣΙΑ ΠΟΛΙΤΙΚΗΣ ΑΕΡΟΠΟΡΙΑΣ
ΥΠΗΡΕΣΙΑ ΕΛΕΓΧΟΥ ΠΕΡΙΟΧΗΣ
Δ/ΝΣΗ ΑΕΡΟΝΑΥΤΙΚΩΝ ΕΚΔΟΣΕΩΝ (Ε1)
ΤΜΗΜΑ(Ε1/Α)

Αθήνα

ΑΡ.ΠΡΩΤ:

ΠΡΟΣ:

- Δ/νση Αερολιμένων (Δ3)
- Δ/νσηΕναέριαςΚυκλοφορίας (Δ4)
- Δ/νση Τηλεπικοινωνιών(Δ5)

& Δ/νση Ηλ.Συστημάτων Αεροναυτιλίας (Δ6)

ΘΕΜΑ: Διόρθωση λανθασμένης καταχώρησης Αεροναυτικών Πληροφοριών

Αναθέτουμε :
την διόρθωση της λανθασμένης καταχώρησης Αεροναυτικών Πληροφοριών που εντοπίστηκε σε ορισμένα από τα παρακάτω ενδιάμεσα έντυπα :

Στοιχεία Λανθασμένης Καταχώρησης

- Ενδιάμεσο Έντυπο «Διόρθωση AIP»……
- Ενδιάμεσο Έντυπο «Διόρθωση AIRAC AIP»……
- Ενδιάμεσο Έντυπο «Συμπλήρωση AIP»……
- Ενδιάμεσο Έντυπο «Συμπλήρωση AIRAC AIP»……..
- Ενδιάμεσο Έντυπο «Αεροναυτικής Αγγελίας NOTAM»……..

Με Εντολή Διοικητή
Ο Διευθυντής

ΣΥΝΗΜΜΕΝΑ
Έγγραφα στα οποία διαπιστώθηκε η λανθασμένη καταχώρηση σε έντυπη μορφή & σε αρχείο pdf

ΥΠΗΡΕΣΙΑ ΠΟΛΙΤΙΚΗΣ ΑΕΡΟΠΟΡΙΑΣ

ΕΝΤΥΠΟ Δ.2.2

ΤΕΛΙΚΟ ΕΝΤΥΠΟ «ΔΙΟΡΘΩΣΗ AIP AMENDMENT»

AIP AMENDMENT

Phone:+302109972480
FAX: +302109750757
AFTN: LGGGYNYP Email: e1a@hcaa.gr

GREECE
MINISTRY OF TRANSPORT AND COMMUNICATION
CIVIL AVIATION AUTHORITY
AERONAUTICAL INFORMATION SERVICE DIVISION
P.O BOX 70360 GR 166 10 GLYFADA GREECE

VOLUME

(ΑΛΛΑΓΕΣ)

1. …….
2. …….
3. …….
4. …….
5. …….

ΥΠΗΡΕΣΙΑ ΠΟΛΙΤΙΚΗΣ ΑΕΡΟΠΟΡΙΑΣ

ΕΝΤΥΠΟ Δ.2.3

ΤΕΛΙΚΟ ΕΝΤΥΠΟ «ΔΙΟΡΘΩΣΗ AIRAC AIP AMENDMENT»

AIRAC AIP AMENDMENT

Phone:+302109972480
FAX: +302109750757
AFTN: LGGGYNYP Email: e1a@hcaa.gr

GREECE
MINISTRY OF TRANSPORT AND COMMUNICATION
CIVIL AVIATION AUTHORITY
AERONAUTICAL INFORMATION SERVICE DIVISION
P.O BOX 70360 GR 166 10 GLYFADA GREECE

Effective Date:

VOLUME

(ΑΛΛΑΓΕΣ)

1. ……..
2. ……..
3. ……
4. ……
5. ……

ΥΠΗΡΕΣΙΑ ΠΟΛΙΤΙΚΗΣ ΑΕΡΟΠΟΡΙΑΣ

ΕΝΤΥΠΟ Δ.2.4

ΤΕΛΙΚΟ ΕΝΤΥΠΟ «ΣΥΜΠΛΗΡΩΣΗ AIP SUPPLEMENT»

AIP SUPPLEMENT

Phone:+302109972480
FAX: +302109750757
AFTN: LGGGYNYP Email: e1a@hcaa.gr

GREECE
MINISTRY OF TRANSPORT AND COMMUNICATION
CIVIL AVIATION AUTHORITY
AERONAUTICAL INFORMATION SERVICE DIVISION
P.O BOX 70360 GR 166 10 GLYFADA GREECE

(ΠΕΡΙΓΡΑΦΗ ΚΕΙΜΕΝΟΥ ΠΟΥ ΠΡΟΚΕΙΤΑΙ ΝΑ ΠΡΟΣΤΕΘΕΙ ΣΤΟ ΕΓΧΕΙΡΙΔΙΟ)

Επισυνάπτονται σελίδες με το κείμενο αναλυτικά

NOTES:

ΥΠΗΡΕΣΙΑ ΠΟΛΙΤΙΚΗΣ ΑΕΡΟΠΟΡΙΑΣ

ΕΝΤΥΠΟ Δ.2.5

ΤΕΛΙΚΟ ΕΝΤΥΠΟ «ΣΥΜΠΛΗΡΩΣΗ AIRAC AIP SUPPLEMENT»

AIRAC AIP SUPPLEMENT

Phone:+302109972480
FAX: +302109750757
AFTN: LGGGYNYP Email: e1a@hcaa.gr

GREECE
MINISTRY OF TRANSPORT AND COMMUNICATION
CIVIL AVIATION AUTHORITY
AERONAUTICAL INFORMATION SERVICE DIVISION
P.O BOX 70360 GR 166 10 GLYFADA GREECE

Effective Date:

(ΠΕΡΙΓΡΑΦΗ ΚΕΙΜΕΝΟ ΠΟΥ ΠΡΟΚΕΙΤΑΙ ΝΑ ΠΡΟΣΤΕΘΕΙ ΣΤΟ ΕΓΧΕΙΡΙΔΙΟ)

Επιυνάπτονται σελίδες με το κείμενο αναλυτικά

NOTE:

ΥΠΗΡΕΣΙΑ ΠΟΛΙΤΙΚΗΣ ΑΕΡΟΠΟΡΙΑΣ

ΕΝΤΥΠΟ Δ.2.6

ΤΕΛΙΚΟ ΕΝΤΥΠΟ «ΑΕΡΟΝΑΥΤΙΚΗ ΑΓΓΕΛΙΑ NOTAM»

NOTAM

Phone:+302109972480
FAX: +302109750757
AFTN: LGGGYNYP Email: e1a@hcaa.gr

GREECE
MINISTRY OF TRANSPORT AND COMMUNICATION
CIVIL AVIATION AUTHORITY
AERONAUTICAL INFORMATION SERVICE DIVISION
P.O BOX 70360 GR 166 10 GLYFADA GREECE

(ΚΕΙΜΕΝΟ ΑΕΡΟΝΑΥΤΙΚΗΣ ΑΓΓΕΛΙΑΣ)

ΥΠΗΡΕΣΙΑ ΠΟΛΙΤΙΚΗΣ ΑΕΡΟΠΟΡΙΑΣ

ΕΝΤΥΠΟ Δ.3.1

ΥΠΗΡΕΣΙΑΚΟ ΣΗΜΕΙΩΜΑ ΑΝΑΘΕΣΗΣ ΕΚΔΟΣΗΣ ΑΕΡΟΝΑΥΤΙΚΩΝ ΕΚΔΟΣΕΩΝ

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΜΕΤΑΦΟΡΩΝ & ΕΠΙΚΟΙΝΩΝΙΩΝ
ΥΠΗΡΕΣΙΑ ΠΟΛΙΤΙΚΗΣ ΑΕΡΟΠΟΡΙΑΣ
ΥΠΗΡΕΣΙΑ ΕΛΕΓΧΟΥ ΠΕΡΙΟΧΗΣ
Δ/ΝΣΗ ΑΕΡΟΝΑΥΤΙΚΩΝ ΕΚΔΟΣΕΩΝ (Ε1)
ΤΜΗΜΑ(Ε1/Α)

Αθήνα

Αθήνα

ΑΡ.ΠΡΩΤ:

ΠΡΟΣ: Δ/ΝΣΗ ΔΙΟΙΚΗΤΟΥ (Δ9)/
Τυπογραφείο Υ.Π.Α

ΘΕΜΑ: Ανάθεση έκδοσης Αεροναυτικών Εκδόσεων

Αναθέτουμε :

1. την άριστη εκτύπωση των αιτούμενων Αεροναυτικών Εκδόσεων :
   - AIP Τόμος Ι……
   - AIP Τόμος ΙΙ……
   - Διορθώσεις AIP……..
   - Συμπληρώσεις AIP……..

2. τη διάθεση ντοσιέ πλαστικού καλύμματος για :
   - AIP Ελλάδος Τόμος Ι……..
   - AIP Ελλάδος Τόμος ΙΙ……

Με Εντολή Διοικητή
Ο Διευθυντής

ΣΥΝΗΜΜΕΝΑ
Αιτούμενα έγγραφα σε αρχείο pdf

ΥΠΗΡΕΣΙΑ ΠΟΛΙΤΙΚΗΣ ΑΕΡΟΠΟΡΙΑΣ

ΕΝΤΥΠΟ Δ.3.2

ΑΙΤΗΣΗ ΧΟΡΗΓΗΣΗΣ ΑΕΡΟΝΑΥΤΙΚΩΝ ΕΚΔΟΣΕΩΝ

ΕΠΩΝΥΜΟ:
ΟΝΟΜΑ:
Δ/ΝΣΗ ΚΑΤΟΙΚΙΑΣ:
ΟΔΟΣ ΑΡΙΘΜΟΣ:
Τ.Κ ΣΥΝΟΙΚΙΑ:
ΠΟΛΗ:

Δ/ΝΣΗ ΕΠΑΓΓΕΛΜΑΤΙΚΗΣ ΣΤΕΓΗΣ
ΟΔΟΣ ΑΡΙΘΜΟΣ:
Τ.Κ ΣΥΝΟΙΚΙΑ:
ΠΟΛΗ:

ΘΕΜΑ: Χορήγηση…….
…….

Ελληνικό,…….
Συνημμένα: Απόδειξη Κατάθεσης
Νο:……
Ποσού:……..€

Παρελήφθησαν από……

ΠΡΟΣ

Υπηρεσία Ελέγχου Περιοχής (ΥΕΠ)
Δ/νση Αεροναυτικών Εκδόσεων (Ε1)
Τμήμα Εγχειριδίων Αεροναυτικών Πληροφοριών (Ε1/Α)

Παρακαλώ όπως μου χορηγήσετε:

- ΕΑΠ (AIP) Τόμος Ι
- ΕΑΠ (AIP) Τόμος ΙΙ
- Πλαστικό κάλυμμα
- Διορθώσεις του ΕΑΠ (AIP)
- Συμπληρώσεις του ΕΑΠ (AIP)

(Κυκλώνονται οι αντίστοιχες εκδόσεις)

ΥΠΗΡΕΣΙΑ ΠΟΛΙΤΙΚΗΣ ΑΕΡΟΠΟΡΙΑΣ

ΕΝΤΥΠΟ Δ.3.3

SUBSCRIPTION TO AIP PUBLICATION
ΑΙΤΗΣΗ ΧΟΡΗΓΗΣΗΣ ΑΕΡΟΝΑΥΤΙΚΩΝ ΕΚΔΟΣΕΩΝ (αγγλικά)

ORDER FORM (Please circle the appropriate case)

- NEW SUBSCRIPTION
- RENEWAL
- REVISED ADDRESS

RETURN TO

For new subscribers or revised addresses:

MINISTRY OF TRANSPORT & COMMUNICATIONS

CIVIL AVIATION AUTHORITY

AERONAUTICAL INFORMATION SERVICE DIVISION

GREECE

For renewals and invoices:

MINISTRY OF TRANSPORT & COMMUNICATIONS

CIVIL AVIATION AUTHORITY

ACCOUNTING & SUPPLY CENTER (LEK)

GREECE

NUMBER OF COPIES REQUIRED

1. ANNUAL SUBSCRIPTION To AIP Publication	**On payment**	**Free of charge**
a. AIP GREECE	……..	……
b. AIP GREECE Amendments	……..	……..
c. AIP GREECE Supplements	……..	……

2. SUBSCRIPTION TITLE/ADDRESS Please indicate below the correct address

In case of revised address the previous one must be mentioned too.

Indicate Below/

Publication must be sent to	**Bills must be sent to**
……	……
……	……

ΥΠΗΡΕΣΙΑ ΠΟΛΙΤΙΚΗΣ ΑΕΡΟΠΟΡΙΑΣ

ΕΝΤΥΠΟ Δ.3.4

ΕΓΚΡΙΣΗ ΔΙΑΘΕΣΗΣ ΑΕΡΟΝΑΥΤΙΚΩΝ ΕΚΔΟΣΕΩΝ

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΜΕΤΑΦΟΡΩΝ & ΕΠΙΚΟΙΝΩΝΙΩΝ
ΥΠΗΡΕΣΙΑ ΠΟΛΙΤΙΚΗΣ ΑΕΡΟΠΟΡΙΑΣ
ΥΠΗΡΕΣΙΑ ΕΛΕΓΧΟΥ ΠΕΡΙΟΧΗΣ
Δ/ΝΣΗ ΑΕΡΟΝΑΥΤΙΚΩΝ ΕΚΔΟΣΕΩΝ (Ε1)
ΤΜΗΜΑ(Ε1/Α)

Αθήνα

Αριθμ.Πρωτ.ΥΕΠ/Ε1

ΠΡΟΣ : ΟΠΩΣ Ο Π.Δ

ΘΕΜΑ: Έγκριση διάθεσης Αεροναυτικών Εκδόσεων

ΑΠΟΦΑΣΗ
Ο ΥΠΟΥΡΓΟΣ

Έχοντας υπόψη :

1. Το Ν.Δ. 714/70 "Περί Οργανώσεως της Υ.Π.Α." όπως τροποποιήθηκε με το 1340/83 & το Π.Δ. 56/89 "Περί Οργανισμού της Υ.Π.Α." όπως τροποποιήθηκε μεταγενέστερα.
2. Την Δ10/Α/11898/822/28.3.91 απόφαση κ.Υπουργού Μεταφορών και Επικοινωνιών "Περί μεταβίβασης αρμοδιοτήτων και δικαιώματος υπογραφής και λοιπά",(ΦΕΚ 242/Β/19.4.91).
3. Την ΜΟΔ 72 "Περί διαδικασίας διαθέσεως και αποστολής εκδόσεων Αεροναυτικών χαρτών και Αεροναυτικών πληροφοριών".
4. Τον Κανονισμό Διοικήσεως Υλικού.
5. Το σχετικό απόθεμα που υπάρχει στις αποθήκες του Λ.Ε.Κ.
6. Τις διαδικασίες που ισχύουν για τη διαχείριση και διάθεση του υλικού.
7. Την αίτηση που υποβλήθηκε από τ……με αριθμό πρωτοκόλλου……και ημερομηνία……

Αποφασίζουμε :

3. Εγκρίνουμε τη διάθεση των αιτούμενων Αεροναυτικών Εκδόσεων…….

4. Η διαχειριστική τακτοποίηση να γίνει βάσει της παρούσας και της σχετικής απόδειξης αποστολής του ταχυδρομείου.

Με Εντολή Διοικητή
Ο Διευθυντής

ΣΥΝΗΜΜΕΝΑ
Αντίγραφο της αίτησης

ΠΙΝΑΚΑΣ ΔΙΑΝΟΜΗΣ

ΔΩΡΕΑΝ ΧΟΡΗΓΗΣΗ
Ι.ΑΠΟΔΕΚΤΕΣ ΓΙΑ ΚΟΙΝΟΠΟΙΗΣΗ
Λ.Ε.Κ

ΙΙ.ΕΣΩΤΕΡΙΚΗ ΔΙΑΝΟΜΗ
ΥΕΠ/Ε1/Α

ΕΠΙ ΠΛΗΡΩΜΗ ΧΟΡΗΓΗΣΗ
Ι.ΑΠΟΔΕΚΤΕΣ ΓΙΑ ΕΝΕΡΓΕΙΑ
Λ.Ε.Κ

ΙΙ.ΕΣΩΤΕΡΙΚΗ ΔΙΑΝΟΜΗ
ΥΕΠ/Ε1/Α

ΥΠΗΡΕΣΙΑ ΠΟΛΙΤΙΚΗΣ ΑΕΡΟΠΟΡΙΑΣ

ΕΝΤΥΠΟ Δ.3.5

ΑΠΟΔΕΙΚΤΙΚΟ ΠΑΡΑΛΑΒΗΣ ΑΕΡΟΝΑΥΤΙΚΩΝ ΕΚΔΟΣΕΩΝ

Ο κάτωθι υπογεγραμμένος……

βεβαιώνω ότι παρέλαβα από την Υπηρεσία Ελέγχου Περιοχής/Διεύθυνση Αεροναυτικών Εκδόσεων (Ε1) / Τμήμα Εγχειριδίων Αεροναυτικών Πληροφοριών (Α), ΥΕΠ/Ε1/Α, τα παρακάτω αντίτυπα Αεροναυτικών Εκδόσεων :

AIP ΤΟΜΟΣ Ι ΤΕΜΑΧΙΑ……..

AIP ΤΟΜΟΣ ΙΙ ΤΕΜΑΧΙΑ……..

Στον ανωτέρο αριθμό περιλαμβάνονται :

- ΚΑΛΥΜΜΑΤΑ
- ΠΕΡΙΕΧΟΜΕΝΟ
- ΚΑΛΥΜΜΑΤΑ & ΠΕΡΙΕΧΟΜΕΝΟ

Ο ΠΑΡΑΛΑΒ (ΩΝ/ΟΥΣΑ)

……
(Ονοματεπώνυμο ολογράφως)

ΥΠΗΡΕΣΙΑ ΠΟΛΙΤΙΚΗΣ ΑΕΡΟΠΟΡΙΑΣ

ΕΝΤΥΠΟ Δ.3.6

ΕΝΤΥΠΟ ΔΙΑΘΕΣΗΣ ΑΕΡΟΝΑΥΤΙΚΩΝ ΕΚΔΟΣΕΩΝ

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΜΕΤΑΦΟΡΩΝ & ΕΠΙΚΟΙΝΩΝΙΩΝ
ΥΠΗΡΕΣΙΑ ΠΟΛΙΤΙΚΗΣ ΑΕΡΟΠΟΡΙΑΣ
ΥΠΗΡΕΣΙΑ ΕΛΕΓΧΟΥ ΠΕΡΙΟΧΗΣ
Δ/ΝΣΗ ΑΕΡΟΝΑΥΤΙΚΩΝ ΕΚΔΟΣΕΩΝ (Ε1)
ΤΜΗΜΑ(Ε1/Α)

Αθήνα

ΑΡ.ΠΡΩΤ:

ΠΡΟΣ: ΛΕΚ

ΘΕΜΑ: Διάθεση Αεροναυτικών Εκδόσεων

1. Σας γνωρίζουμε ότι σύμφωνα με την ΜΟΔ 72 διαθέσαμε με πληρωμή, δωρεάν στον

Επάγγελμα:

Εκδίδουσα Αρχή:

Όνομα/Επώνυμο:
Αριθμός ταυτότητας/διαβατηρίου:
Διεύθυνση: Χώρα: Πόλη: Τ.Κ:
Επαγγ.Διεύθυνση: Χώρα: Πόλη: Τ.Κ:

- AIP Τόμος I — τιμή μονάδας:.....τεμ. .....αξίας.....€
- AIP Τόμος II
- Διορθώσεις AIP (Amendments) — τιμή μονάδας:.....τεμ. .....αξίας.....€
- Συμπληρώσεις AIP(Supplements) — τιμή μονάδας:.....τεμ. .....αξίας.....€

2. Το ποσό της Απόδειξης Κατάθεσης καλύπτει την απαιτούμενη αξία

- των Αεροναυτικών εκδόσεων
- ετήσια συνδρομή των εκδόσεων

(κυκλώνονται οι αντίστοιχες εκδόσεις)

Συνημμένα:

- φωτοαντίγραφο της αίτησης
- απόδειξη κατάθεσης No..... αξίας:.....€
- φωτοαντίγραφο του αποδεικτικού παραλαβής

Με Εντολή Διοικητή
Ο Διευθυντής

ΥΠΗΡΕΣΙΑ ΠΟΛΙΤΙΚΗΣ ΑΕΡΟΠΟΡΙΑΣ **ΕΝΤΥΠΟ 6.1 :** **ΕΤΗΣΙΟ ΠΡΟΓΡΑΜΜΑ ΕΠΙΘΕΩΡΗΣΕΩΝ**	**ΕΤΟΣ : ……**												
	Ιανουάριος	**Φεβρουάριος**	**Μάρτιος**	**Απρίλιος**	**Μάιος**	**Ιούνιος**	**Ιούλιος**	**Αύγουστος**	**Σεπτέμβριος**	**Οκτώβριος**	**Νοέμβριος**	**Δεκέμβριος**	**ΠΑΡΑΤΗΡΗΣΕΙΣ**
Δ/νση Αερολιμένων (Δ3) : ***Τμήμα Αεροδρομίων & Ελικοδρομίων***													
Δ/νση Εναέριας Κυκλοφορίας (Δ4) : ***Τμήμα Διαδικασιών Εναέριας Κυκλοφορίας***													
Δ/νση Τηλεπικοινωνιών (Δ5) : **Τμήμα Διαχείρισης Φάσματος Συχνοτήτων**													
Δ/νση Ηλ.Συστημάτων Αεροναυτιλίας (Δ6) : **Τμήμα Επικοινωνιών & Ραδιοβοηθημάτων**													

ΥΠΗΡΕΣΙΑ ΠΟΛΙΤΙΚΗΣ ΑΕΡΟΠΟΡΙΑΣ

ΕΝΤΥΠΟ 6.2

ΑΝΑΦΟΡΑ ΕΠΙΘΕΩΡΗΣΗΣ

ΗΜΕΡΟΜΗΝΙΑ:

ΔΙΕΥΘΥΝΣΗ/ ΤΜΗΜΑ ΠΡΟΣ ΕΠΙΘΕΩΡΗΣΗ:

ΕΠΙΘΕΩΡΗΤΗΣ:

ΣΥΜΠΕΡΑΣΜΑΤΑ ΕΠΙΘΕΩΡΗΣΗΣ

ΜΗ ΣΥΜΜΟΡΦΩΣΕΙΣ:

ΠΑΡΑΤΗΡΗΣΕΙΣ:

ΟΙ ΕΠΙΘΕΩΡΗΤΕΣ:
ΟΙ ΕΠΙΘΕΩΡΟΥΜΕΝΟΙ:

ΥΠΗΡΕΣΙΑ ΠΟΛΙΤΙΚΗΣ ΑΕΡΟΠΟΡΙΑΣ **ΕΝΤΥΠΟ 7**	ΠΡΑΚΤΙΚΑ ΑΝΑΣΚΟΠΗΣΗΣ		
ΠΕΡΙΟΔΟΣ:	**ΗΜΕΡΟΜΗΝΙΑ ΑΝΑΣΚΟΠΗΣΗΣ : __/__/200_**		
ΣΥΜΜΕΤΕΧΟΝΤΕΣ			
Ονοματεπώνυμο	**Θέση**	**Υπογραφή**	**Παρατηρήσεις**
	Διοικητής		
	Υποδιοικητής		
	Γενικός Διευθυντής Αεροναυτιλίας		
	Υπεύθυνος Ασφάλειας Πληροφοριών		
	Διευθυντής Αερολιμένων (Δ/νση Δ3)		
	Διευθυντής Εναέριας Κυκλοφορίας (Δ/νση Δ4)		
	Διευθυντής Τηλεπικοινωνιών (Δ/νση Δ5)		
	Διευθυντής Ηλ.Συστημάτων Αεροναυτιλίας (Δ/νση Δ6)		
	Διευθυντής Αεροναυτικών Εκδόσεων (Δ/νση Ε1)		
	Εξωτερικός Σύμβουλος (27001)		

ΕΙΣΕΡΧΟΜΕΝΑ	ΑΞΙΟΛΟΓΗΣΗ ΕΙΣΕΡΧΟΜΕΝΩΝ (καταγραφή αποτελεσμάτων και σύγκριση με την τρέχουσα κατάσταση)	ΥΠΕΥΘΥΝΟΙ, ΗΜΕΡΟΜΗΝΙΑ ΥΛΟΠΟΙΗΣΗΣ
1. Απαιτήσεις των προτύπων ISO 27001:2005		
2. Πολιτική Ποιότητας		
3. Συμμόρφωση με τη Νομοθεσία		
4. Αποτελέσματα εξωτερικών επιθεωρήσεων		
5. Αποτελέσματα εσωτερικών επιθεωρήσεων		
6. Αποτελέσματα προηγούμενων ανασκοπήσεων		
7. Ανατροφοδότηση από ενδιαφερόμενα μέρη		
8. Νέες τεχνικές, συστήματα ή διαδικασίες		
9. Αναφορές Ασφαλείας, Διορθωτικές και προληπτικές ενέργειες		
10. Αναφορές Ενδεχόμενων Κινδύνων (τρωτά σημεία και απειλές)		
11. Αξιολόγηση προηγούμενων στόχων - Αποτελέσματα ανάλυσης δεικτών		
12. Αλλαγές συνθηκών, περιλαμβανομένων των εξελίξεων σε νομικές και κανονιστικές απαιτήσεις καθώς και σε συμβατικές υποχρεώσεις		

13. Εκπαίδευση προσωπικού και αξιολόγησή της		
14. Συστάσεις για βελτίωση		

ΕΞΕΡΧΟΜΕΝΑ	ΑΞΙΟΛΟΓΗΣΗ ΕΞΕΡΧΟΜΕΝΩΝ (καταγραφή αποτελεσμάτων και σύγκριση με την τρέχουσα κατάσταση)	ΥΠΕΥΘΥΝΟΙ ΗΜΕΡΟΜΗΝΙΑ ΥΛΟΠΟΙΗΣΗΣ
1. Βελτίωση του συστήματος ISMS		
2. Στόχοι στους δείκτες		
3. Γενικά – Άλλοι στόχοι ➢ Ανανέωση Σχεδίου Εκτίμησης Κινδύνων ➢ Ανανέωση Σχεδίου Θεράπευσης Κινδύνων ➢ Τροποποίηση διαδικασιών & ελέγχων, που επηρεάζουν την ασφάλεια αεροναυτικών πληροφοριών ➢ Επιχειρηματικές Απαιτήσεις ➢ Απαιτήσεις Ασφάλειας ➢ Συμβατικές Υποχρεώσεις ➢ Νέα δεδομένα (νέες απαιτήσεις, νέες τεχνολογίες) ➢ Νέα νομοθεσία ➢ Αλλαγές στον οργανισμό που επηρεάζουν την Διαχείριση Αεροναυτικών Πληροφοριών ➢ Νέες ευκαιρίες για βελτίωση ➢ Ανάγκες σε πόρους ➢ Προγραμματισμός για σεμινάρια		
4. Επόμενες διορθωτικές και προληπτικές *ενέργειες*		

ΥΠΗΡΕΣΙΑ ΠΟΛΙΤΙΚΗΣ ΑΕΡΟΠΟΡΙΑΣ

ΕΝΤΥΠΟ 8.1

ΕΝΤΥΠΟ ΑΝΑΦΟΡΑΣ ΜΗ ΣΥΜΜΟΡΦΩΣΕΩΝ, ΒΛΑΒΩΝ, ΣΥΜΒΑΝΤΩΝ & ΑΤΥΧΗΜΑΤΩΝ

Αριθμός Έκθεσης: …/…
Σύντομη Περιγραφή:
Ημερομηνία Βλάβης / Συμβάντος / Ατυχήματος:
Σημασία:
Πιθανότητα επανάληψης:
Αναφέρθηκε από:

ΑΝΑΣΚΟΠΗΣΗ ΚΑΙ ΑΝΑΛΥΣΗ

Σχετικές αναφορές: 1.
2.
3.

Περιγραφή Βλάβης / Συμβάντος / Ατυχήματος

Άμεσες Αιτίες

Βασικές (Υποκείμενες) Αιτίες

Άμεσες Ενέργειες
-
-
-
-
-

Προτεινόμενες Διορθωτικές Ενέργειες
-
-

Υπεύθυνοι για follow-up
-

Ο αναφέρων Υπεύθυνος Ασφάλειας Πληροφοριών Γενικός Διευθυντής

ΥΠΗΡΕΣΙΑ ΠΟΛΙΤΙΚΗΣ ΑΕΡΟΠΟΡΙΑΣ

ΕΝΤΥΠΟ 8.2

ΔΙΟΡΘΩΤΙΚΕΣ & ΠΡΟΛΗΠΤΙΚΕΣ ΕΝΕΡΓΕΙΕΣ

ΔΙΕΥΘΥΝΣΗ: **ΤΜΗΜΑ:**

ΠΕΡΙΓΡΑΦΗ:

☐ **ΜΗ ΣΥΜΜΟΡΦΩΣΗΣ**

☐ **ΠΑΡΑΤΗΡΗΣΗΣ**

……

……

ΑΙΤΙΑ:……

Υπεύθυνος:…… Ημερομηνία: …/…/….

ΠΕΡΙΓΡΑΦΗ ΠΡΟΤΕΙΝΟΜΕΝΗΣ:

☐ **ΔΙΟΡΘΩΤΙΚΗΣ ΕΝΕΡΓΕΙΑΣ**

☐ **ΠΡΟΛΗΠΤΙΚΗΣ ΕΝΕΡΓΕΙΑΣ**

……

……..……...

Υπεύθυνος Υλοποίησης: ……Χρονικό Πλαίσιο Υλοποίησης έως: ……/……/……

Ημερομηνία Υλοποίησης : ……/……/……

ΕΠΑΛΗΘΕΥΣΗ ΔΙΟΡΘΩΤΙΚΗΣ ΕΝΕΡΓΕΙΑΣ

Πραγματοποιήθηκε ; ΝΑΙ □ ΟΧΙ □

Αποτελεσματικά ; ΝΑΙ □ ΟΧΙ □

Υπεύθυνος Επαλήθευσης: …… Ημ/ναι Επαλήθευσης:…/…./…..

Βιβλιογραφία

Ελληνική Βιβλιογραφία

1. Δερβιτσιώτης Κ.Ν. & Λαγοδήμος Α.Γ. (2007). *Ανταγωνιστικότητα των Επιχειρήσεων ανάλυση - βελτίωση-στρατηγικές* (2η έκδ.). Οικονομική Βιβλιοθήκη, Αθήνα.

2. Κάτσικας Σ. (2001). *Ασφάλεια Υπολογιστών* (τόμος Α). Ελληνικό Ανοικτό Πανεπιστήμιο, Πάτρα.

3. Λαγοδήμος Α.Γ. (2007). *Συστήματα Διασφάλισης Ποιότητας* (Σημειώσεις). Πανεπιστήμιο Πειραιώς, Πειραιάς.

Ξενόγλωσση Βιβλιογραφία

1. Arnason S.T. & Willett K.D. (2007). *How to Achieve 27001 Certification: An Example of Applied Compliance Management.* Auerbach Publications, New York.

2. Ashenden D. (2008). Information Security Management: A human challenge. *Information Security Technical Report* 13(4), 195-201.

3. Boehmer W. (2009). Cost-Benefit Trade-Off Analysis of an ISMS Based on ISO 27001. *Availability, Reliability and Security. ARES apos; 09. International Conference* 16(19), 392- 399.

4. Boehmer W. (2008). Appraisal of the Effectiveness and Efficiency of an Information Security Management System Based on ISO 27001. *Emerging Security Information, Systems and Technologies. SECURWARE apos;08. Second International Conference* 25(31), 224-231.

5. Broderick J.S. (2006). ISMS, security standards and security regulations. *Information Security Technical Report* 11(1), 26-31.

6. Calder A. & Watkins S. (2006). *International IT Governance: An Executive Guide to ISO 17799/ISO 27001* (1st ed.). Kogan Page Publishers, London.

7. Calder A. (2006). *Information Security Based on ISO 27001/ISO 17799: A Management Guide* (1st ed.). Van Haren Publishing, Zaltbommel.

8. Calder A. & Watkins S. (2006). IT under scrutiny: ISO 27001 for information security management. *Management Reviews, Quality World (UK)* 32(3), 38-43.

9. Coulson C.T. (1997). *The Future of the Organisation: Achieving Excellence through Business Transformation.* Kogan Page Publishers, London.

10. Dey. M. (2007). Information security management - A practical approach. *AFRICON* 26(28), 1-6.

11. Endorf C.F. (2002). *Secured Computing: A SSCP Study Guide* (1st ed.). Endorf Technical Research, Victoria.

12. Farn K.J., Lin S.K. & Lo C.C. (2008). A study on e-Taiwan information system security classification and implementation. *Computer Standards & Interfaces* 30(1/2), 1-7.

13. Freeman E.H. (2007). Holistic Information Security: ISO 27001 & Due Care. *Information Systems Security* 16(5), 291-294.

14. Harris S. (2007). *CISSP All-in-One Exam Guide* (4th ed.). McGraw-Hill Publishing, New York.

15. Humphreys T. & Plate A. (2005). *Guide to the Implementation and Auditing of ISMS Controls Based on ISO/IEC 27001.* BSI British Standards Institution, London.

16. Humphreys E. (2007). *Implementing the ISO/IEC 27001 Information Security Management System Standard.* Artech House, Norwood.

17. Humphreys E. (2008). Information security management standards: compliance, governance & risk management. *Information Security Technical Report* 13(4), 247-255.

18. Kenning M.J. (2001). Security Management standard-ISO 17799/BS 7799. *BT Technology Journal* 19(3), 132-135.

19. Khosrow-Pour M. (2004). *Innovations through information technology*. Idea Group Inc (IGI), London.

20. Layton P.T. (2006). *Information Security: Design, Implementation, Measurement, and Compliance.* CRC Press LLC, Florida.

21. Overill R.E. (2008). ISMS insider intrusion prevention & detection. *Information Security Technical Report* 13(4), 216-219.

22. Peltier T.R. (2002). *Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management*. CRC Press LLC, Florida.

23. Siponen M. & Willison R. (2009). Information Security Management Standards: Problems & Solutions. *Information & Management* 46(5), 267-270.

24. Stewart J.M., Tittel E. & Chapple M. (2005). *CISSP: Certified Information Systems Security Professional Study Guide.* John Wiley and Sons Publishing, Indianapolis, Indiana.

25. Sungho K., Sangsoo J., Jaeil L. & Sangkyun K. (2007). Common defects in information security management system of Korean companies. *The Journal of Systems & Software* 80(10), 1631-1638.

26. Van Bon J. & Verheijen T. (2006). *Frameworks for I.T Management: An Introduction.* Van Haren Publishing, Zaltbommel.

27. Von Solms B. & Von Solms R., (2004). The 10 deadly sins of information security management. *Computers & Security* 23(5), 371-376.

28. Zeithaml V.A., Parasuraman A. & Berry L.L. (1990). *Delivering Quality Service-SERVQUALmodel*. Free Press, New York.

Οργανισμοί

1. ISO/IEC 27000:2005 *Information technology - Security techniques - Information security management systems - Overview and vocabulary,* Ελληνικός Οργανισμός Τυποποίησης (ΕΛΟΤ).

2. ISO/IEC 27001:2005 *Information technology-Security techniques-Information security management systems- Requirements,* Ελληνικός Οργανισμός Τυποποίησης (ΕΛΟΤ).

3. ISO/IEC 27002:2007 *Information technology - Security techniques - Code of practice for information security management,* Ελληνικός Οργανισμός Τυποποίησης (ΕΛΟΤ).

4. ISO/IEC 27006:2007 *Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems*, Ελληνικός Οργανισμός Τυποποίησης (ΕΛΟΤ).

5. Εγχειρίδιο Αεροναυτικών Πληροφοριών-AIP (Aeronautical Information Publication), Υπηρεσία Πολιτικής Αεροπορίας (Υ.Π.Α).

6. Εγχειρίδιο Διαχείρισης της Ασφάλειας Υπηρεσιών Ελέγχου Εναέριας Κυκλοφορίας (Safety Management Manual), Υπηρεσία Πολιτικής Αεροπορίας (Υ.Π.Α).