Ασφάλεια πληροφοριακών συστημάτων στη Ναυτιλία ISO 27001

Εργασία στο μάθημα Ναυτιλιακή Πληροφορική (ΜΠ16 - INFS155)

Γάκης Βασίλειος (ΑΕΜ 00246)
Μυριδάκης Ηλίας (ΑΕΜ 00195)

Επιβλέπων
Ιωάννης Φιλιππόπουλος

Η ΠΛΗΡΟΦΟΡΙΚΗ ΣΤΗ ΝΑΥΤΙΛΙΑ ΚΑΙ Η ΑΝΑΓΚΑΙΟΤΗΤΑ ΤΗΣ ΑΣΦΑΛΕΙΑΣ

ΟΡΙΣΜΟΙ

- ΝΑΥΤΙΛΙΑ (Τεχνική – Οικονομική έννοια)
- ΝΑΥΤΙΛΙΑΚΗ ΕΠΙΧΕΙΡΗΣΗ (Δομή – Περιβάλλον λειτουργίας)

ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ (Information Systems - IS)

Τα Συστατικά Μέρη Ενός Πληροφοριακού Συστήματος

- Οι Άνθρωποι (People)
- Οι Διαδικασίες (Procedures)
- Τα Δεδομένα (Data)
- Το Λογισμικό (Software)
- Ο Υλικός Εξοπλισμός (Hardware)
- Το Δίκτυο Επικοινωνιών (Network of Communications)

ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ ΣΤΗ ΝΑΥΤΙΛΙΑ

Πληροφοριακό Σύστημα σε μια ναυτιλιακή

- Δυσκολίες στην υιοθέτηση νέων τεχνολογιών
- Οι σύγχρονες ανάγκες των Ναυτιλιακών Εταιρειών
- Πλεονεκτήματα και προοπτικές υιοθέτησης σύγχρονων πληροφοριακών συστημάτων

ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ ΣΤΗ ΝΑΥΤΙΛΙΑ

Πλεονεκτήματα και προοπτικές υιοθέτησης σύγχρονων πληροφοριακών συστημάτων

- Μειώνουν το κόστος λειτουργίας τους
- Απλοποιούν και αυτοματοποιούν τις διαδικασίες τους
- Βελτιώνουν σημαντικά την ποιότητα των υπηρεσιών που παρέχουν
- Αυξάνουν την ασφάλεια της ναυσιπλοΐας

ΑΝΑΛΥΣΗ ΚΙΝΔΥΝΩΝ ΣΤΑ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

Τα Είδη των Κινδύνων

- Ως προς την προέλευσή τους
- Ως προς τη φύση τους

Οι Κατηγορίες των Κινδύνων

- Οι Φυσικές Απειλές (Natural Threats)
- Οι Ανθρώπινες Απειλές (Human Threats)
- Οι Κίνδυνοι Τεχνολογίας (Dangers of Technology)
- Οι Επιχειρησιακοί Κίνδυνοι (Dangers Operational)

ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΣΤΗ ΝΑΥΤΙΛΙΑ

Αναγκαιότητα της ασφάλειας

- Ασφαλή πλεύση ενός πλοίου
  - Κυβερνοαπειλή
  - Πειρατεία
- Κόστος από άμεσες οικονομικές απώλειες

ΣΧΕΔΙΑΣΜΟΣ ΣΥΣΤΗΜΑΤΟΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΣΤΗ ΝΑΥΤΙΛΙΑ

ΜΕΘΟΔΟΙ ΑΣΦΑΛΕΙΑΣ

Είδη απειλής στην ασφάλεια του Π.Σ.

- Διακοπή (interruption)
- Παρεμπόδιση (interception)
- Τροποποίηση (modification
- Πλαστοποίηση (fabricate)

ΣΧΕΔΙΑΣΜΟΣ ΣΥΣΤΗΜΑΤΟΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΣΤΗ ΝΑΥΤΙΛΙΑ

ΜΕΘΟΔΟΛΟΓΙΑ ΥΛΟΠΟΙΗΣΗΣ

Φάση 1η «Καταγραφή υφιστάμενης κατάστασης»

- Δεδομένα (Data assets)
- Υπηρεσίες (End User Services)
- Υλικά Στοιχεία
- Τοποθεσίες
- Λογισμικό (software)

ΣΧΕΔΙΑΣΜΟΣ ΣΥΣΤΗΜΑΤΟΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΣΤΗ ΝΑΥΤΙΛΙΑ

ΜΕΘΟΔΟΛΟΓΙΑ ΥΛΟΠΟΙΗΣΗΣ

Φάση 2η «Ανάλυση επικινδυνότητας»

- Η αναγνώριση των απειλών
- Η αναγνώριση των επιμέρους ευπαθειών
- Η αναγνώριση των πιθανών κατηγοριών απωλειών
- Η εκτίμηση της πιθανότητας να συμβεί μια απώλεια

ΣΧΕΔΙΑΣΜΟΣ ΣΥΣΤΗΜΑΤΟΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΣΤΗ ΝΑΥΤΙΛΙΑ

ΜΕΘΟΔΟΛΟΓΙΑ ΥΛΟΠΟΙΗΣΗΣ

Φάση 3η «Πολιτική Ασφαλείας»

- Χαρακτηριστικά της πολιτικής ασφαλείας
  - Αποτελείται από τμήματα
  - Να είναι απόλυτα σαφής
  - Δεν πρέπει να τροποποιείται συχνά
- Σχέδιο ασφάλειας

ΣΧΕΔΙΑΣΜΟΣ ΣΥΣΤΗΜΑΤΟΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΣΤΗ ΝΑΥΤΙΛΙΑ

ΜΕΘΟΔΟΛΟΓΙΑ ΥΛΟΠΟΙΗΣΗΣ

Φάση 4η «Καθορισμός Μέτρων Ασφαλείας»

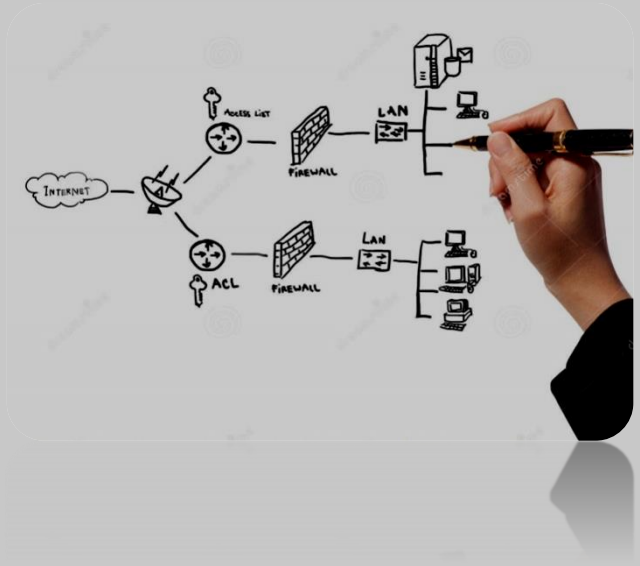
- Μέτρα Ασφαλείας
  - Οργανωτικά μέτρα ασφαλείας
  - Τεχνικά μέτρα ασφαλείας
  - Μέτρα φυσικής ασφαλείας
- Πλάνο υλοποίησης των μέτρων ασφαλείας

ΣΧΕΔΙΑΣΜΟΣ ΣΥΣΤΗΜΑΤΟΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΣΤΗ ΝΑΥΤΙΛΙΑ

ΜΕΘΟΔΟΛΟΓΙΑ ΥΛΟΠΟΙΗΣΗΣ

Φάση 5η «Σχέδιο έκτακτης ανάγκης»

- Περιπτώσεις δυσλειτουργίας
- Περιπτώσεις ολικής καταστροφής



ΣΧΕΔΙΑΣΜΟΣ ΣΥΣΤΗΜΑΤΟΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΣΤΗ ΝΑΥΤΙΛΙΑ

ΣΧΕΔΙΟ ΑΝΑΚΑΜΨΗΣ ΑΠΟ ΚΑΤΑΣΤΡΟΦΕΣ

- Ελαχιστοποίηση διακοπών της κανονικής λειτουργίας
- Περιορισμός της έκτασης των ζημιών και καταστροφών
- Δυνατότητα ομαλής υποβάθμισης
- Εγκατάσταση εναλλακτικών μέσων λειτουργίας εκ των προτέρων
- Εκπαίδευση, εξάσκηση και εξοικείωση του ανθρώπινου δυναμικού με διαδικασίες έκτακτης ανάγκης
- Δυνατότητα ταχείας και ομαλής αποκατάστασης της λειτουργίας
- Ελαχιστοποίηση των οικονομικών επιπτώσεων

ΚΥΡΙΟΤΕΡΑ ΠΡΟΤΥΠΑ ΠΟΛΙΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ

ITIL®

ISM³

COBIT® 5

AN ISACA® FRAMEWORK

ΚΥΡΙΟΤΕΡΑ ΠΡΟΤΥΠΑ ΠΟΛΙΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ

ISO/IEC 27001 – Πρότυπο Διαχείρισης Ασφάλειας Πληροφοριακών Συστημάτων
Οκτώβριος 2005 International Organization for Standardization

IT Infrastructure Library (ITIL) - Συλλογή από βιβλία, οπού το καθένα καλύπτει μια συγκεκριμένη πρακτική διαχείρισης του IT (CCTA GB) (1989)

CORBIT - Σύνολο βέλτιστων πρακτικών (πλαίσιο) για την τεχνολογία της διαχείρισης των πληροφοριών
ISACA και IT Governance Institute (ITGI) (1996)

ISM3 (Information Security Management Maturity) - Πλαίσιο για την Διαχείριση Ασφάλειας Πληροφοριακών Συστημάτων. (μέσα δεκαετίας ‘90)

ISO 27001
Ασφάλεια πληροφοριών

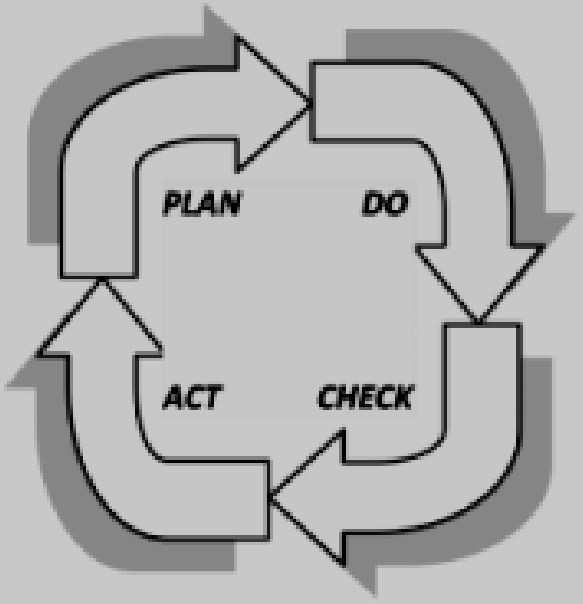
Τρίγωνο C-I-A (C-I-A triad)

- Εμπιστευτικότητα
- Διαθεσιμότητα
- Ακεραιότητα

ISO 27001
Ασφάλεια πληροφοριών

PDCA

- Σχεδιασμός
- Εφαρμογή
- Έλεγχος
- Ενέργειες



ISO 27001
Ασφάλεια πληροφοριών

Η πιστοποίηση του ISO/IEC 27001 περιέχει διεργασίες τριών επιπέδων

Επίπεδο 1

Είναι το προπαρασκευαστικό στάδιο οπού γίνεται μια ανασκόπηση του υπάρχοντος συστήματος ασφάλειας πληροφοριών.

Επίπεδο 2

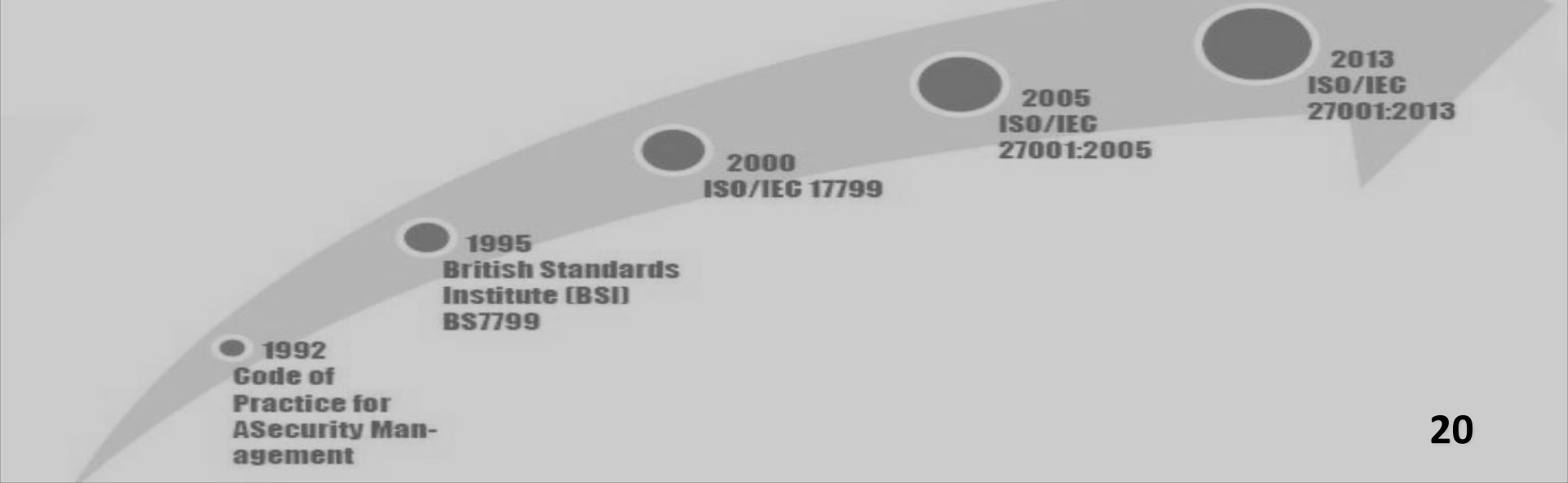
Στο επίπεδο 2 γίνεται μια ποιο λεπτομερής και επίσημη παρακολούθηση και έλεγχος των συστημάτων ασφάλειας πληροφοριακών συστημάτων.

Επίπεδο 3

Σε αυτό το επίπεδο εμπεριέχονται συνεχόμενες εκθέσεις και έλεγχοι για την επιβεβαίωση ότι ο οργανισμός συνεχίζει να είναι εναρμονισμένος με το πρότυπο

ISO 27001
Εξέλιξη του προτύπου

ISO (International Organization for Standardization/Διεθνής Οργανισμός Τυποποίησης)
IEC (International Electrotechnical Commission/Διεθνής Ηλεκτροτεχνική Επιτροπή)



ISO 27001

Εφαρμογή σε Ναυτιλιακή Εταιρία / Οργανισμό

- Γενικές Απαιτήσεις
- Απαιτήσεις Τεκμηρίωσης
- Ευθύνη της Διοίκησης
- Εσωτερικές Επιθεωρήσεις του ISMS
- Ανασκόπηση του ISMS από τη Διοίκηση
- Βελτίωση του ISMS

* ISMS (Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών)

ISO 27001

Εφαρμογή σε Ναυτιλιακή Εταιρία / Οργανισμό

Γενικές Απαιτήσεις

- Καθιέρωση του ISMS
  - Risk Assessment (Εκτίμηση κινδύνων)
  - Potential risk treatment (Πιθανή «θεραπεία» κινδύνων)
  - Create risk management plan (Σχέδιο διαχείρισης κινδύνων)
- Εφαρμογή και λειτουργία του ISMS
- Παρακολούθηση και επανεξέταση του ISMS
- Συντήρηση και βελτίωση ISMS

ISO 27001

Εφαρμογή σε Ναυτιλιακή Εταιρία / Οργανισμό
Γενικές Απαιτήσεις / Καθιέρωση του ISMS

- Risk Assessment (Εκτίμηση κινδύνων)

Κάθε ενδεχόμενος κίνδυνος διαβαθμίζεται

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

ISO 27001

Εφαρμογή σε Ναυτιλιακή Εταιρία / Οργανισμό
Γενικές Απαιτήσεις / Καθιέρωση του ISMS

Potential risk treatment

(Πιθανή «θεραπεία» κινδύνων)

Να προσδιορίσει και να αξιολογήσει τις εναλλακτικές επιλογές για την αντιμετώπιση των κινδύνων.

ISO 27001

Εφαρμογή σε Ναυτιλιακή Εταιρία / Οργανισμό
Γενικές Απαιτήσεις / Καθιέρωση του ISMS

Πιθανές ενέργειες περιλαμβάνουν:

- Εφαρμογή κατάλληλων ελέγχων (Μείωση κινδύνου).
- 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 (Αποδοχή).
- Αποφυγή των κινδύνων (Αποφυγή).
- Μεταφορά των κινδύνων που συνδέονται με την επιχείρηση σε άλλα μέρη (π.χ. ασφαλιστές, προμηθευτές) (Μεταβίβαση).

ISO 27001

Εφαρμογή σε Ναυτιλιακή Εταιρία / Οργανισμό
Γενικές Απαιτήσεις / Καθιέρωση του ISMS

Create risk management plan
(Σχέδιο διαχείρισης κινδύνων)

- Να επιλέξει στόχους ελέγχων και τους ελέγχους για την αντιμετώπιση των κινδύνων.
- Να λάβει την έγκριση της διοίκησης όσον αφορά τους προτεινόμενους εναπομένοντες κινδύνους.
- Να λάβει την άδεια της διοίκησης για την υλοποίηση και τη λειτουργία του ISMS.
- Να συντάξει μια Δήλωση Εφαρμοσιμότητας.

ISO 27001

Εφαρμογή σε Ναυτιλιακή Εταιρία / Οργανισμό

Απαιτήσεις Τεκμηρίωσης (1/2)

- Τεκμηριωμένες δηλώσεις της πολιτικής και των στόχων του ISMS.
- Το πεδίο εφαρμογής του ISMS.
- Τις διαδικασίες και τους ελέγχους για την υποστήριξη του ISMS.
- Περιγραφή της μεθοδολογίας αξιολόγησης κινδύνου.
- Την έκθεση αξιολόγησης των κινδύνων.
- Το σχέδιο «θεράπευσης» κινδύνου.

ISO 27001

Εφαρμογή σε Ναυτιλιακή Εταιρία / Οργανισμό

Απαιτήσεις Τεκμηρίωσης (2/2)

- 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.
- Τα αρχεία που απαιτούνται από το προκείμενο Διεθνές Πρότυπο
- Τη Δήλωση Εφαρμοσιμότητας

ISO 27001

Εφαρμογή σε Ναυτιλιακή Εταιρία / Οργανισμό

Ευθύνη της Διοίκησης

Δέσμευση Διοίκησης

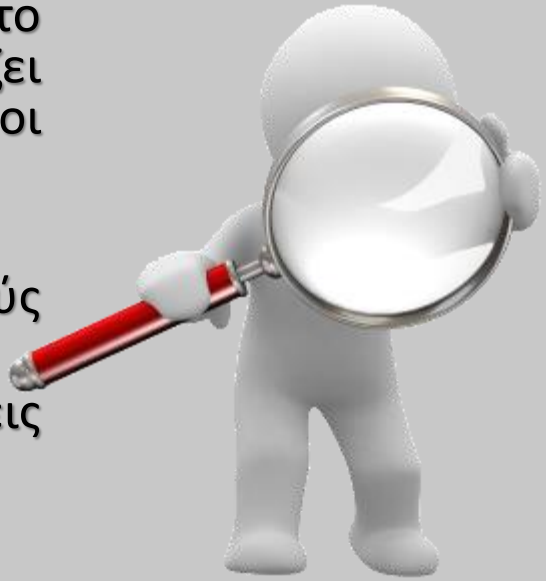
Παροχή των πόρων

ISO 27001

Εφαρμογή σε Ναυτιλιακή Εταιρία / Οργανισμό

Εσωτερικές Επιθεωρήσεις 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:



- Συμμορφώνονται με τις απαιτήσεις του παρόντος διεθνούς προτύπου και τη σχετική νομοθεσία ή κανονισμούς
- Συμμορφώνονται με τις προσδιορισμένες απαιτήσεις ασφάλειας των πληροφοριών
- Εφαρμόζονται αποτελεσματικά και να διατηρούνται
- Εκτελούνται όπως αναμένεται

ISO 27001

Εφαρμογή σε Ναυτιλιακή Εταιρία / Οργανισμό
Ανασκόπηση του ISMS από τη Διοίκηση

Εφαρμογή Απαιτήσεων

Εισερχόμενα Ανασκοπήσεων

Εξερχόμενα Ανασκοπήσεων

ISO 27001

Εφαρμογή σε Ναυτιλιακή Εταιρία / Οργανισμό

Βελτίωση του ISMS

Συνεχής βελτίωση

Διορθωτικές Ενέργειες

Προληπτικές ενέργειες

ISO 27001

Εφαρμογή σε Ναυτιλιακή Εταιρία / Οργανισμό

Παραδείγματα Εφαρμογής

Κίνδυνος : Εξάντληση χρόνου ζωής εξοπλισμού

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

Έλεγχος : A.11.2.4 Equipment maintenance

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

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

ISO 27001

Εφαρμογή σε Ναυτιλιακή Εταιρία / Οργανισμό

Παραδείγματα Εφαρμογής

Αιτιολόγηση :

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

.

ISO 27001

Εφαρμογή σε Ναυτιλιακή Εταιρία / Οργανισμό

Παραδείγματα Εφαρμογής

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

Στόχος ελέγχου : Να αποτρέψει μη εξουσιοδοτημένη πρόσβαση ή ανεπανόρθωτη ζημιά στις κρίσιμες ναυτιλιακές πληροφορίες του οργανισμού.

Έλεγχος : A.11.1.4 Protecting against external and environmenta threats

-Έλεγχος ύπαρξης πυροσβεστήρων & ανιχνευτών καπνού

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

-Έλεγχος ύπαρξης ασφάλισης σε περίπτωση πυρκαγιάς, πλημμύρας κλπ

ISO 27001

Εφαρμογή σε Ναυτιλιακή Εταιρία / Οργανισμό

Παραδείγματα Εφαρμογής

Αιτιολόγηση :

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

.

ISO 27001

Εφαρμογή σε Ναυτιλιακή Εταιρία / Οργανισμό

Παραδείγματα Εφαρμογής

Κίνδυνος : Μη συγχρονισμός ρολογιών συστήματος

Στόχος ελέγχου : Να διασφαλιστεί η αξιοπιστία των κρίσιμων ναυτιλιακών πληροφοριών

Έλεγχος : A.12.4.4 Clock synchronization

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

ISO 27001

Εφαρμογή σε Ναυτιλιακή Εταιρία / Οργανισμό

Παραδείγματα Εφαρμογής

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.

.

Ασφάλεια πληροφοριακών συστημάτων στη Ναυτιλία ISO 27001

ΑΝΑΚΕΦΑΛΑΙΩΣΗ

Το ISO/IEC 27001 είναι το μόνο διεθνές πρότυπο που μπορεί να επιθεωρηθεί και το οποίο καθορίζει τις απαιτήσεις για ένα Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ-ISMS).

Το πρότυπο είναι σχεδιασμένο έτσι ώστε να διασφαλίζει την επιλογή επαρκών και ισορροπημένων ελέγχων ασφάλειας. Αυτή η επιλογή βοηθά τον ναυτιλιακό οργανισμό/εταιρία να προστατεύσει τα περιουσιακά του στοιχεία πληροφοριών και να τον εμπιστεύονται τα ενδιαφερόμενα μέρη και ιδιαίτερα οι πελάτες του.

Ασφάλεια πληροφοριακών συστημάτων στη Ναυτιλία ISO 27001

Ευχαριστούμε!

Γάκης Βασίλειος (ΑΕΜ 00246)
Μυριδάκης Ηλίας (ΑΕΜ 00195)

Επιβλέπων
Ιωάννης Φιλιππόπουλος