ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ **Η**ΛΕΚΤΡΟΛΟΓΩΝ **Μ**ΗΧΑΝΙΚΩΝ ΚΑΙ **Μ**ΗΧΑΝΙΚΩΝ **Υ**ΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ **Η**ΛΕΚΤΡΙΚΩΝ **Β**ΙΟΜΗΧΑΝΙΚΩΝ **Δ**ΙΑΤΑΞΕΩΝ ΚΑΙ **Σ**ΥΣΤΗΜΑΤΩΝ **Α**ΠΟΦΑΣΕΩΝ

ΕΠΙΣΚΟΠΗΣΗ ΠΡΟΤΥΠΩΝ ISO 9001 ΚΑΙ ISO 27001- ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ ΤΗΣ ΕΤΑΙΡΕΙΑΣ VODAFONE

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Χρήστος Ν. Θεοδωρόπουλος

Επιβλέπων: Δημήτριος Ασκούνης

Καθηγητής Ε.Μ.Π.

Αθήνα, Οκτώβριος 2020

ΣΥΓΚΡΙΣΗ ΠΡΟΤΥΠΩΝ ISO 9001 ΚΑΙ ISO 27001-ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ ΤΗΣ ΕΤΑΙΡΕΙΑΣ VODAFONE

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ **Η**ΛΕΚΤΡΟΛΟΓΩΝ **Μ**ΗΧΑΝΙΚΩΝ ΚΑΙ **Μ**ΗΧΑΝΙΚΩΝ **Υ**ΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ **Η**ΛΕΚΤΡΙΚΩΝ **Β**ΙΟΜΗΧΑΝΙΚΩΝ **Δ**ΙΑΤΑΞΕΩΝ ΚΑΙ **Σ**ΥΣΤΗΜΑΤΩΝ **Α**ΠΟΦΑΣΕΩΝ

ΕΠΙΣΚΟΠΗΣΗ ΠΡΟΤΥΠΩΝ ISO 9001 ΚΑΙ ISO 27001-ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ ΤΗΣ ΕΤΑΙΡΕΙΑΣ VODAFONE

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Χρήστος Ν. Θεοδωρόπουλος

Επιβλέπων: Δημήτριος Ασκούνης

Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 27η Οκτωβρίου 2020.

.....	.....	.....
Δημήτριος Ασκούνης	Ιωάννης Ψαρράς	Χρυσόστομος Δούκας
Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.	Επίκουρος Καθηγητής Ε.Μ.Π.

Αθήνα, Οκτώβριος 2020

…….

Χρήστος Ν. Θεοδωρόπουλος

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Copyright © Χρήστος Ν. Θεοδωρόπουλος, 2020

Με επιφύλαξη παντός δικαιώματος. All rights reserved.

Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας εργασίας, εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μμήνυμα. Ερωτήματα που αφορούν τη χρήση της εργασίας για κερδοσκοπικό σκοπό πρέπει να απευθύνονται προς τον συγγραφέα.

Οι απόψεις και τα συμπεράσματα που περιέχονται σε αυτό το έγγραφο εκφράζουν τον συγγραφέα και δεν πρέπει να ερμηνευθεί ότι αντιπροσωπεύουν τις επίσημές θέσεις του Εθνικού Μετσόβιου Πολυτεχνείου.

Πρόλογος-Ευχαριστίες

Έναυσμα για αυτή τη διπλωματική αποτέλεσε το σεμινάριο <<ISO 9001:2015 - ΕΠΙΘΕΩΡΗΤΗΣ / ΕΠΙΚΕΦΑΛΗΣ ΕΠΙΘΕΩΡΗΤΗΣ ΣΥΣΤΗΜΑΤΩΝ ΔΙΑΧΕΙΡΙΣΗΣ ΠΟΙΟΤΗΤΑΣ>> που παρακολούθησα κατά τη διάρκεια της πρακτικής μου άσκησης στην ΤÜV HELLAS (TÜV NORD). Θερμές ευχαριστίες στους κύριους Σάββα Πελτέκη και Δημήτριο Γουρνάκη που μου έδωσαν αυτή την ευκαιρία.

Επίσης θα ήθελα να ευχαριστήσω τον επιβλέποντα της εργασίας και καθηγητή του ΕΜΠ κύριο Δημήτριο Ασκούνη που μου έδωσε την δυνατότητα να ασχοληθώ με ένα θέμα που σχετίζεται με τα ενδιαφέροντα μου.

Επιπλέον θα ήθελα να ευχαριστήσω θερμά τον κ. Κανάρη Μπούνα , υποψήφιο διδάκτορα ΕΜΠ , για την αρωγή του στη διαμόρφωση του θέματος και την καθοδήγηση κατά τη διάρκεια της συγγραφής της διπλωματικής μου εργασίας.

Ακόμη οφείλω να ευχαριστήσω και όλους τους συμφοιτητές μου που με βοήθησαν κατά τη διάρκεια των σπουδών μου. Ειδική αναφορά θέλω να κάνω στους φίλους και συμφοιτητές μου Γιάννη, Θοδωρή και Ελένη που με στήριξαν από την αρχή μέχρι το τέλος των σπουδών μου.

Τέλος τη μεγαλύτερη ευγνωμοσύνη την οφείλω στους γονείς μου, Νίκο και Αντωνία, που φρόντισαν να μη στερηθώ τίποτα κατά τη διάρκεια των σπουδών μου και στις αδερφές μου, Χρυσάνθη, Γεωργία, Φωτεινή που είναι δίπλα μου όλα αυτά τα χρόνια .

Αθήνα, Οκτώβριος 2020

Χρήστος Ν.Θεοδωρόπουλος

Περίληψη

Σκοπός της συγκεκριμένης εργασίας είναι να αναλύσει δύο πολύ σημαντικά πρότυπα ISO για μια επιχείρηση και να τα συγκρίνει. Το ISO 9001 που αφορά το *Σύστημα Διαχείρισης Ποιότητας* και το ISO 27001 που αφορά το *Σύστημα Ασφάλειας Πληροφοριών*. Τα δύο αυτά πρότυπα ανήκουν στον ίδιο οργανισμό, ISO και τα κοινά σημεία που έχουν καθιστούν πολύ εύκολη την εφαρμογή του ενός σε μια επιχείρηση, όταν ήδη έχει υιοθετήσει ένα από τα δύο. Η δομή της εργασίας χωρίζεται σε επτά κεφάλαια. Στο πρώτο κεφάλαιο γίνεται μια σύντομη αναφορά στη ποιότητα και τα συστήματα διαχείρισης της ενώ το δεύτερο κεφάλαιο αναφέρεται στην ασφάλεια των πληροφορίων. Στο τρίτο κεφάλαιο γίνεται μια εισαγωγή στα πρότυπα ISO και τις διαδικασίες πιστοποίησης. Στο τέταρτο κεφάλαιο αναλύεται το ISO 9001, τα χαρακτηριστικά του και οι αναθεωρήσεις του, ενώ το πέμπτο κεφάλαιο ασχολείται με τον ίδιο τρόπο για το ISO 27001. Ακολουθεί το έκτο κεφάλαιο όπου δίνονται τα κοινά σημεία μεταξύ των δύο προτύπων καθώς και τα βήματα που πρέπει να ακολουθηθούν, όταν μια επιχείρηση διαθέτει ήδη το ένα πρότυπο και θέλει να ενσωματώσει και το άλλο. Το έβδομο κεφάλαιο περιλαμβάνει μελέτη περίπτωσης εταιρείας που κατέχει και τα δύο πρότυπα, στη περίπτωση μας είναι η Vodafone Ελλάδος. Η εργασία τελειώνει με τα απαραίτητα συμπεράσματα και τον επίλογο.

Λέξεις Κλειδιά

Ποιότητα, ασφάλεια πληροφοριών, πληροφοριακό σύστημα, πρότυπα ISO, ISO 9001, ISO 27001, αξιοπιστία, εμπιστοσύνη πελατών.

Abstract

The purpose of this thesis is to analyze two very important ISO standards for a company and try to compare them. The first is the ISO 9001 concerning the Quality Management System and the second one is the ISO 27001 concerning the Information Security System. These two standards belong to the same organization, ISO and the common points that have made it very easy to implement one of them in a company, when it has already adopted one of these. The structure of the thesis is divided into six chapters. The first chapter provides a brief overview of quality and its management systems, while the second chapter provides some points about information safety. The third chapter makes an introduction to ISO standards and certification procedures. The fourth chapter analyzes ISO 9001, its features and its revisions while the fifth chapter deals in the same way with ISO 27001. In the sixth chapter the commonalities between the two standards are given as well as the steps to be followed when a company already has one standard and wants to integrate the other. The seventh chapter includes a case study of a company that holds both standards, in our case Vodafone Greece. The work ends with the necessary conclusions and the epilogue.

Keywords

Quality, information security, information system, ISO, ISO 9001, ISO 27001 standards, reliability, customer trust.

Περιεχόμενα

Πίνακας Σχημάτων

Λίστα Πινάκων

Εισαγωγή

Σκοπός κάθε επιχείρησης είναι να μπορεί να παράγει ποιοτικά προϊόντα και υπηρεσίες τα οποία θα καλύπτουν τις ανάγκες και τις απαιτήσεις των καταναλωτών. Όταν συμβαίνει αυτό, η επιχείρηση αυτομάτως αποκτά καλή φήμη και ξεκινά μια σχέση εμπιστοσύνης ανάμεσα σε εκείνη και τους πελάτες της. Συμβαίνει αυτό που επιθυμούν τα στελέχη της διοίκησης της επιχείρησης, δημιουργείται ένα πιστό πελατολόγιο που ξεκινά να αγαπά την επιχείρηση και ότι αυτή προσφέρει. Για να επιτευχθεί όμως αυτός ο σκοπός η επιχείρηση πρέπει να έχει ένα σωστό πλάνο, μια σωστή οργάνωση και να τηρεί κάποιες προϋποθέσεις.

Από τις πιο σημαντικές προϋποθέσεις που τίθενται τόσο από το εσωτερικό περιβάλλον της επιχείρησης όσο και από το εξωτερικό είναι η παρεχόμενη ποιότητα στα προϊόντα και τις υπηρεσίες της όσο και η ασφάλεια των δεδομένων που κατέχει. Για να μπορέσει μια επιχείρηση να αποδείξει πως τηρεί ένα συγκεκριμένο πλάνο άλλα και όλες τις απαραίτητες προϋποθέσεις που θέτουν οι κανονισμοί και οι νόμοι πρέπει να τηρεί κάποια ορισμένα πρότυπα μέσω πιστοποιήσεων. Γεγονός, που τα παλαιότερα χρόνια αντιμετωπιζόταν περισσότερα στο εσωτερικό κάθε χώρας τα τελευταία χρόνια γίνεται όλο και περισσότερο διεθνές. Εμφανίζεται η τάση οι επιχειρήσεις να επιθυμούν την εφαρμογή συγκεκριμένων προδιαγραφών όπως εκείνες δίνονται μέσω των διεθνών προτύπων και καθορίζουν τις λειτουργίες της επιχείρησης. Τα πρότυπα αυτά πιστοποιούν πως οι επιχειρήσεις τηρούν τις προδιαγραφές σε κάθε τομέα διότι υπάρχουν πολλοί τομείς στους οποίους μπορεί να πιστοποιηθεί μια επιχείρηση (ποιότητα, περιβάλλον, συνθήκες εργασίας και υγιεινής κλπ). Τα πρότυπα αυτά μπορούν να εκδοθούν από διάφορους φορείς όπως η Ευρωπαϊκή Ένωση, εθνικοί μικρότεροι φορείς προτύπων, όπως ο ΕΛΟΤ στην Ελλάδα ή ο γνωστότερος όλων διεθνής οργανισμός έκδοσης προτύπων ISO.

Η επιχείρηση δεν αρκεί μόνο να υποστηρίζει πως ακολουθεί τους κανονισμούς των διαφόρων προτύπων, το επόμενο βήμα είναι να πιστοποιηθεί και με αυτό το πρότυπο. Ο λόγος που συμβαίνει αυτό είναι πως κατά την διάρκεια της διαδικασίας πιστοποίησης η επιχείρηση περνά από έλεγχο από φορείς πιστοποίησης, οι οποίοι

αποφασίζουν αν εκείνη τηρεί τα κριτήρια για να της απονεμηθεί η πιστοποίηση ή πρέπει να προβεί σε αλλαγές και να δοκιμάσει εκ νέου.

Ένα από τα πιο σημαντικά πρότυπα που υιοθετούν σχεδόν όλοι οι οργανισμοί είναι το ISO 9001. Το πρότυπο αυτό αφορά την ποιότητα σε μία επιχείρηση και την διαχείριση των συστημάτων ποιότητας της. Εξετάζει πόσο οργανωμένα μπορεί να λειτουργήσει από τα υψηλότερα επίπεδα ηγεσίας μέχρι και την παραγωγή, ώστε να παραδώσει στους τελικούς πελάτες το προϊόν και την υπηρεσία που επιθυμούν. Ουσιαστικά πρόκειται για ένα σύνολο εγγράφων που περιέχουν τους κανόνες που πρέπει να διέπουν την επιχείρηση. Τα οφέλη για μια επιχείρηση είναι πολλά το σημαντικότερο από τα οποία είναι η ώθηση για συνεχή ποιοτική βελτίωση.

Ένα πρότυπο που χρησιμοποιείται πολύ από τις εταιρείες είναι το ISO 27001, που αφορά στη διαχείριση της ασφάλειας των πληροφοριών που κατέχει μια επιχείρηση. Οι απαιτήσεις του είναι γενικές, αφορούν όλους τους τύπους επιχειρήσεων και μπορεί πολύ εύκολα να εφαρμοστεί σε καθεμία από αυτές. Οι πληροφορίες και τα δεδομένα που κατέχει μια επιχείρηση από τους πελάτες της αποτελούν πολύ ευαίσθητο θέμα και χρειάζεται ιδιαίτερη προσοχή στη διαχείριση τους. Το εν λόγω πρότυπο με την εφαρμογή του ωφελεί την επιχείρηση καθώς την βοηθά να αντιμετωπίσει κινδύνους υποκλοπής και να ασφαλίσει τις πληροφορίες της. Ταυτόχρονα, όταν ένας οργανισμός κατέχει μια τέτοια πιστοποίηση αυτομάτως κερδίζει και την εμπιστοσύνη των πελατών του.

Τα τελευταία χρόνια πολλές είναι οι επιχειρήσεις που δεν παραμένουν μόνο σε ένα τύπο πιστοποιήσεων αλλά επιδιώκουν πιστοποιήσεις από διάφορες κατηγορίες προτύπων. Επειδή το ISO 9001 έχει κοινά σημεία με το ISO 27001 είναι συχνό το φαινόμενο του συνδυασμού αυτών των δύο προτύπων.

Σε κάθε περίπτωση οι επιχειρήσεις αντιλαμβάνονται πόσο σημαντική είναι η διασφάλιση της ποιότητας και της ασφάλειας των στοιχείων που έχουν στη κατοχή τους καθώς και οι πιστοποιήσεις που πρέπει να κατέχουν ως ένα σημάδι σωστού επαγγελματισμού και εύρυθμης λειτουργίας.

Κεφάλαιο 1^{ο}: Ποιότητα

1.1 Τι είναι ποιότητα

Πολύ συχνά όταν καλούμαστε να πάρουμε μια αγοραστική απόφαση για ένα προϊόν ή μια υπηρεσία αναφερόμαστε στην ποιότητα του. Κάθε επιχείρηση ενδιαφέρεται για την ποιότητα των εκροών που παράγει και κάθε καταναλωτής ανησυχεί για την ποιότητα των αγαθών που αποκτά. Πρόκειται για μια λέξη που από διαφορετικές οπτικές γωνίες αποκτά και ξεχωριστή σημασία. Ένας βασικός ορισμός είναι εκείνος που δίνει το λεξιλόγιο ISO (θα αναφερθούμε στα ISO στη συνέχεια) το 1986 (ΕΛΟΤ ΕΝ ISO 8402:1994, 1994): «*Ποιότητα είναι το σύνολο των ιδιοτήτων και χαρακτηριστικών ενός προϊόντος ή μιας υπηρεσίας που συμβάλουν στην ικανότητά του να ικανοποιεί εκφρασμένες ή υπονοούμενες ανάγκες*». Ένας πιο απλός ορισμός που χρησιμοποιείται στη καθημερινότητα μας είναι αυτός που αντιμετωπίζει την ποιότητα ως την ικανοποίηση των προσδοκιών που έχει ο καταναλωτής από ένα προϊόν ή υπηρεσία. Από την πλευρά της επιχείρησης, ποιότητα θεωρείται η ικανοποίηση των προδιαγραφών που έχουν τεθεί για το προϊόν ή υπηρεσία (ΤΕΧΝΙΚΟ ΕΠΙΜΕΛΗΤΗΡΙΟ ΕΛΛΑΔΟΣ).

Στη διεθνή βιβλιογραφία συναντάμε αρκετούς ορισμούς για την ποιότητα σύμφωνα με τις μελέτες που έκανε κάθε ερευνητής. Μερικές από τις πιο κύριες είναι οι εξής:

- Ως ποιότητα ορίζεται η συμμόρφωση του προϊόντος/υπηρεσίας με το σκοπό για τον οποίο προορίζεται-Joseph M. Juran, 1950 (Dr.Moyassar I. Ahmed, 2010).

- Ποιότητα είναι οι αναμενόμενες επιθυμίες που έχει ο πελάτης-David Garvin, 1988 (David A. Garvin, 1988).

- Η ποιότητα δεν αφορά μόνο στη διαφοροποίηση της ανταγωνιστικότητας, αποτελεί ένα από τα χαρακτηριστικά εκείνα με τα οποία μια επιχείρηση εισέρχεται στην αγορά-Richard Sullivan, 1996 (Mukherjee, 2003)

Όπως βλέπουμε από τους παραπάνω ορισμούς η ίδια λέξη ερμηνεύεται διαφορετικά από τον καθένα, άρα αποτελεί μια σχετική έννοια που μπορεί να χρησιμοποιηθεί σε πολλά και διαφορετικά πλαίσια ανάλογα με τις επιδιώξεις του καταναλωτή ή της επιχείρησης.

1.1.1 Εμφάνιση ποιότητας στην επιχείρηση

Υπάρχουν διαφορετικές όψεις της ποιότητας σε μια επιχείρηση και μπορεί να εντοπιστεί σε διαφορετικές διαδικασίες. Μια από αυτές τις όψεις της ποιότητας συναντάμε στη διαδικασία σχεδίασης και θέσπιση των προδιαγραφών των προϊόντων ή υπηρεσιών που έχει η επιχείρηση. Σε αυτή την περίπτωση η όψη της, εξαρτάται από το τμήμα της αγοράς στο οποίοι απευθύνονται τα προϊόντα/υπηρεσίες της επιχείρησης. Παράλληλα συνδέεται και με τις απαιτήσεις του πελάτη και στο βαθμό που μπορεί να τις ικανοποιήσει. Οι απαιτήσεις αυτές είναι ανάγκες του πελάτη αλλά και προσδοκίες για την ικανοποίηση των αναγκών που θα επιφέρει η αγορά του προϊόντος ή της υπηρεσίας. Η παραγωγική διαδικασία σχετίζεται και αυτή με την ποιότητα. Κατά την διαδικασία παραγωγής μεγάλο ρόλο έχει η αποτελεσματικότητα που διαθέτουν οι υπεύθυνοι του τομέα παραγωγής στο να ταιριάξουν προδιαγραφές του προϊόντος με τις δυνατότητες της διαδικασίας παραγωγής. Η ποιότητα φαίνεται με την δυνατότητα που έχει η παραγωγική διαδικασία να παράγει τα προϊόντα σύμφωνα με τα πρότυπα. Στο τομέα της παραγωγικής διαδικασίας ωστόσο δεν γίνεται αντιληπτή τόσο στη σχεδίαση του προϊόντος, όσο στο τρόπο που τηρεί τις απαιτήσεις των προτύπων. Πέρα από τα προϊόντα/υπηρεσίες και τις διαδικασίες παραγωγής την συναντάμε και αλλού, στο σύνολο δηλαδή όλων των επιχειρησιακών λειτουργιών. Η επιχειρησιακή λειτουργία αποτελείται από το σύνολο της επιχείρησης και των λειτουργιών που λαμβάνουν μέρος, ώστε να υπάρχει ομαλό κλίμα συνεργασίας στο εσωτερικό της. Όταν σε ένα κατάστημα το προσωπικό είναι ευγενικό με τους πελάτες και εξυπηρετικό ή όταν σε μια επιχείρηση οι συνεργάτες έχουν κλίμα αλληλοϋποστήριξης και συνεργασίας μεταξύ τους είναι και αυτό ένα στοιχείο της. Ο γενικός κανόνας είναι πως όταν μια επιχείρηση με τις σχέσεις που χτίζει στο εσωτερικό της χαρακτηρίζεται από ποιότητα τότε είναι σε θέση αυτήν την ποιότητα να την μεταφέρει και στο εξωτερικό της, προς τους πελάτες της. Δεν αρκεί μόνο να υιοθετεί ένα πρότυπο από την επιχείρηση και να ακολουθηθεί πιστά αν μέσω των

εσωτερικών καθημερινών διαδικασιών στο περιβάλλον της έχει χαθεί προηγουμένως η ποιότητα.

1.1.2 Αντίληψη ποιότητας από πελάτη

Όταν μια επιχείρηση έχει εξασφαλίσει την ποιότητα μέσω των διεργασιών και τον προτύπων που έχει συμπεριλάβει αυτό είναι ένα πρώτο βήμα. Χρειάζεται ωστόσο η ποιότητα αυτή να γίνει αντιληπτή και από τον πελάτη ώστε να έχει αποτέλεσμα η πιστοποίηση που έλαβε η επιχείρηση. Ο πελάτης μπορεί μέσα από κάποια συγκεκριμένα στοιχεία να αντιληφθεί την ύπαρξη ή μη ποιότητας στα προϊόντα και τις υπηρεσίες που του παρέχονται. Τα στοιχεία είναι:

- Χαρακτηριστικά προϊόντος ή υπηρεσίας που θεωρούνται βασικά. Τα χαρακτηριστικά αυτά ικανοποιούν τις βασικές ανάγκες των αγοραστών αλλά και της ομάδας που βρίσκεται στο τομέα της παραγωγής.

- Δευτερεύοντα χαρακτηριστικά. Τα χαρακτηριστικά εκείνα που διευκολύνουν στη χρήση του αρχικού προϊόντος. Μπορεί να είναι μια συσκευασία, δικλείδες ασφαλείας για μια υπηρεσία κα.

- Αξιοπιστία προϊόντος/υπηρεσίας. Η αξιοπιστία αποτελεί ένα από τα βασικότερα στοιχεία στο οποίο δίνουν έμφαση οι πελάτες. Εάν ένα προϊόν δεν εμφανίσει βλάβη ή μια υπηρεσία τηρεί όλες τις προδιαγραφές χαρακτηρίζεται ως αξιόπιστη. Η αξιοπιστία οδηγεί τους πελάτες να γίνουν πιο πιστοί απέναντι στην επιχείρηση.

- Ποιότητα παραγωγής. Στη ποιότητα παραγωγής αναφερόμαστε από την πλευρά που την αντιλαμβάνεται ο παραγωγός. Η ποιότητα παραγωγής συνδέεται άμεσα με το ποσοστό των μονάδων που παράγονται και οι οποίες τηρούν τις καθορισμένες προδιαγραφές ποιότητας.

- Διάρκεια ζωής προϊόντος. Αναφερόμαστε στην αναμενόμενη διάρκεια ζωής του προϊόντος κατά την οποία το προϊόν/υπηρεσία δεν εμφανίζει προβλήματα.

- Ποιότητα εξυπηρέτησης μετά την πώληση. Από τις πιο σημαντικές μορφές ποιότητας αποτελεί η ποιότητα της παρεχόμενης εξυπηρέτησης μετά την πώληση. Είναι ένας από τους καθοριστικούς λόγους για τους οποίους μια επιχείρηση αποκτά πιστούς πελάτες και ξεχωρίζει ανάμεσα στις άλλες.

- Αισθητικά χαρακτηριστικά. Χαρακτηριστικά που αφορούν τα βασικά και δευτερεύοντα χαρακτηριστικά στοιχεία της ποιότητας.

- Υποκειμενική αντίληψη της ποιότητας. Είναι αρκετά δύσκολο για τον καταναλωτή να αντιληφθεί την αντικειμενική διάσταση της ποιότητας. Αυτό που μπορεί να διακρίνει είναι η φήμη της, πόσο ανταγωνιστική είναι, η εικόνα για τα προϊόντα της, δηλαδή όλα εκείνα τα στοιχεία που είναι η εξωτερική εικόνα της επιχείρησης και ως την αντιλαμβάνεται κάθε άτομο που δεν διαθέτει εμπειρία στα θέματα πιστοποιήσεων και παραγωγής. (Σπύρος Γκούμας & Κατερίνα Τέφα, 2018).

1.2 Διαχείριση ποιότητας

Συχνά οι διαδικασίες που έχουν να κάνουν με την ποιότητα αναφέρονται στις διαδικασίες με τις οποίες πραγματοποιείται η παραγωγή των προϊόντων. Οι πελάτες έχουν ολοένα και περισσότερες απαιτήσεις σε αγαθά τα οποία πλέον δεν είναι απλά αλλά πολλά από αυτά τείνουν να έχουν μια πολυπλοκότητα. Με βάση το ανταγωνιστικό περιβάλλον μιας επιχείρησης, τις σχέσεις τις με τους προμηθευτές της άλλα και την οργάνωση που επικρατεί στο εσωτερικό της ήταν αναγκαίο να υπάρχει ένας κανονισμός, ένα πρότυπο που να θέτει κάποιους κανονισμούς σχετικά με τις προδιαγραφές του προϊόντος ή της υπηρεσίας που δημιουργεί η επιχείρηση.

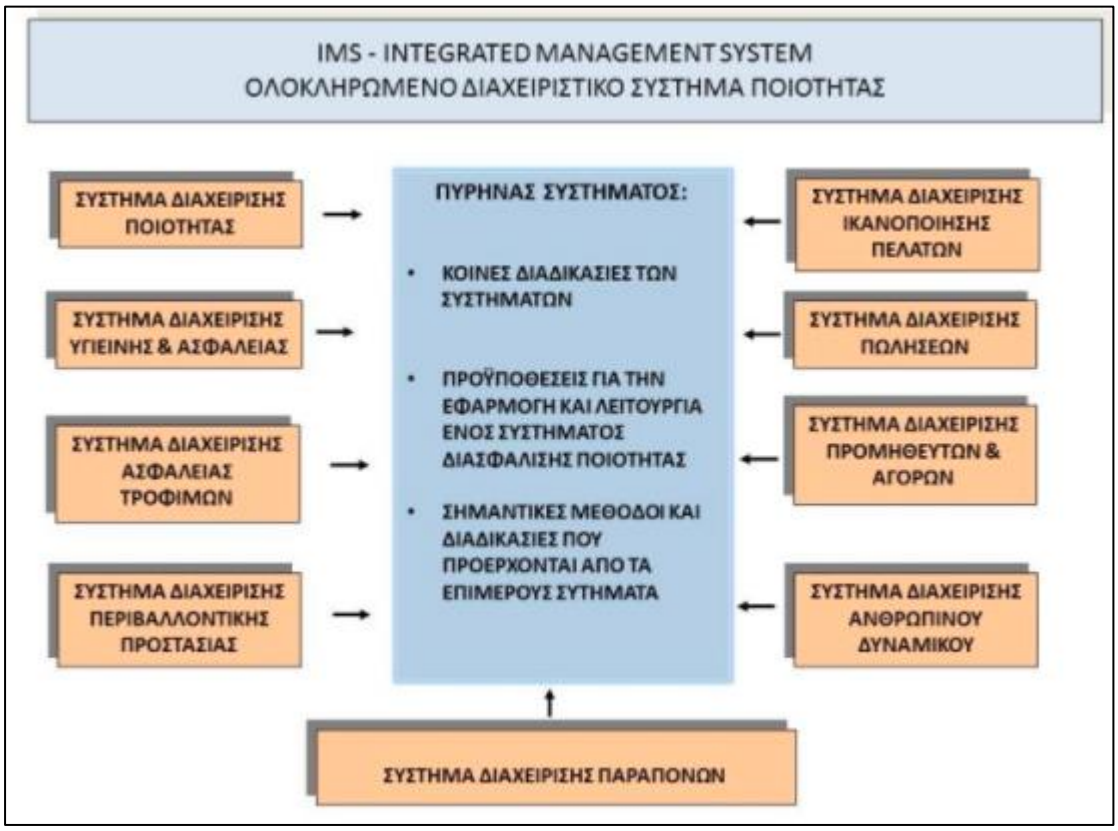
Όταν αναφερόμαστε σε διαχείριση ποιότητας, δεν είναι ένας τυπικός έλεγχος που αφορά κατά πόσο ένα προϊόν τηρεί τα χαρακτηριστικά που πρέπει για παράδειγμα εάν ένας υπολογιστής έχει κατασκευαστεί σωστά. Η διαχείριση ποιότητας είναι ουσιαστικά η διαχείριση του τρόπου με τον οποίο μια επιχείρηση έχει οργάνωση εσωτερική και εξωτερική αλλά και ο τρόπος με τον οποίο λειτουργεί σαν σύνολο, συντονίζοντας μεταξύ τους όλα τα επιμέρους τμήματα τους. Επομένως, ορίζεται ως «*το σύνολο των προγραμματισμένων ή συστηματικών ενεργειών ή διαδικασιών που είναι απαραίτητες για να εξασφαλίσουν ότι ένα προϊόν ή υπηρεσία θα πληροί ορισμένες*

προδιαγραφές.». Γι'αυτό το λόγο υπάρχουν και οι πιστοποιήσεις ISO οι οποίες βεβαιώνουν πως η επιχείρηση λειτουργεί σωστά, έχει ποιότητα στα παραγόμενα προϊόντα της, προστατεύει με ορθό τρόπο τις πληροφορίες των εργαζομένων και των πελατών της, είναι φιλική προς το περιβάλλον κα (SnežanaTopalović, 2014).

1.2.1 Σύστημα διαχείρισης ποιότητας

Το σύστημα διαχείρισης ποιότητας δεν είναι ουσιαστικά μονάχα ένα πράγμα, ένα απλό σύστημα ή πρόγραμμα. Αποτελείται από την οργάνωση, τους πόρους και το προσωπικό που απαιτείται έτσι ώστε να πραγματοποιηθεί η διαχείριση ποιότητας. Μεγάλο ρόλο έχει η διεύθυνση ποιότητας η οποία αναλαμβάνει τις ευθύνες για την σωστή οργάνωση πόρων και ανθρώπων στο θέμα της ποιότητας. Ας μην ξεχνάμε πως στόχος ενός συστήματος ποιότητας είναι να καταφέρει να ενοποιήσει όλα τα στοιχεία που μπορεί να επηρεάσουν την παρεχόμενη ποσότητα στα προϊόντα και τις υπηρεσίες που παράγει η επιχείρηση.

Πολλές φορές η σχετική με την ποιότητα βιβλιογραφία αναφέρεται στο Ολοκληρωμένο Διαχειριστικό Σύστημα Ποιότητας (Integrated Management System) γνωστό ως IMS. Πρόκειται για την ανάπτυξη ενός μεγάλου συστήματος που εμπεριέχει τα πρότυπα των Συστημάτων Διαχείρισης Ποιότητας (ISO 9001), Περιβάλλοντος (ISO 14001) και Ασφάλειας Τροφίμων (HACCP ή ISO 22000). Ο λόγος που δημιουργήθηκε ήταν τα κοινά σημεία των παραπάνω προτύπων. Το μεγάλο πλεονέκτημα αυτής της προσέγγισης είναι η παροχή ενός ενιαίου συνόλου τεκμηρίωσης διαδικασιών και διεργασιών που έχει ως σκοπό την αύξηση της αποτελεσματικότητας, τη μείωση του συνολικού αριθμού διαδικασιών καθώς και την επίτευξη οικονομίας κλίμακας. Πέρα από αυτό συμβάλλει στη μείωση πολλαπλών καταχωρίσεων και αρχείων και οδηγεί προς την εξάλειψη των περιττών ενεργειών. Τα αποτελέσμα είναι εξοικονόμηση οικονομικών και μη πόρων με ταυτόχρονη αύξηση της προστιθέμενης αξίας. Οι φορείς πιστοποιήσεις έχουν εκδώσει στοιχεία στα οποία φαίνεται πως με την υιοθέτηση αυτού του μοντέλου το κόστος πιστοποίησης μπορεί να μειωθεί κατά ένα ποσοστό της τάξης του 40%. Ανάλογα με το σύστημα στο οποίο απευθύνεται η επιχείρηση και τις ανάγκες που θέλει να καλύψει έχει την δυνατότητα να δημιουργήσει ένα IMS. Αυτό φαίνεται καλύτερα μέσω της **Εικόνας 1.**



Εικόνα 1:Ολοκληρωμένο Διαχειριστικό Σύστημα Ποιότητας(IMS) ***(****Πηγή: (Excellence & Lean, 2016))*

Με την εφαρμογή στην επιχείρηση ενός συστήματος διαχείρισης ποιότητας πολλά είναι τα πλεονεκτήματα που προκύπτουν:

- **Ικανοποιούνται οι απαιτήσεις των πελατών.** Το συγκεκριμένο στοιχείο είναι πολύ σημαντικό ώστε να μπορεί να υπάρξει εμπιστοσύνη από μέρος των πελατών προς την επιχείρηση. Με αυτό το βασικό βήμα η επιχείρηση αποκτά καλή φήμη που την οδηγεί σε περισσότερους πελάτες, πώληση προϊόντων/υπηρεσιών και κατά επέκταση σε περισσότερα κέρδη.

- **Ικανοποιούνται οι απαιτήσεις των οργανισμών.** Ένα άλλο σημαντικό στοιχείο είναι οι διεργασίες που λαμβάνουν χώρα σε μια επιχείρηση να είναι σύμφωνες με τους κανονισμούς και τους νόμους που ισχύουν σε κάθε περίπτωση. Επίσης, η παραγωγή των προϊόντων να γίνεται με τον πιο αποτελεσματικό και με λιγότερα κόστη τρόπο ώστε να υπάρξει χώρος για

ανάπτυξη και περαιτέρω επέκταση της επιχείρησης (Excellence & Lean, 2016).

Κεφάλαιο 2^{ο}: Ασφάλεια

2.1 Ασφάλεια πληροφοριών

.Η ασφάλεια σαν όρος σημαίνει την προστασία από τυχόν κινδύνους ή απειλές (The free dictionary, n.d.). Η ασφάλεια των πληροφοριών είτε αυτές είναι σε ψηφιακή μορφή (πχ βάση δεδομένων σε κάποιο υπολογιστή), είτε σε φυσική (πχ μια λίστα ονομάτων σε ένα γραφείο) αποτελεί ένα σημαντικό ζήτημα για μια επιχείρηση. Όσον αφορά το ηλεκτρονικό επιχειρείν και το ψηφιακό κόσμο η ασφάλεια των πληροφοριών στα πληροφοριακά συστήματα είναι το πιο βασικό θεμέλιο της επιχείρησης, καθώς η υποκλοπή πληροφοριών από έναν οργανισμό μπορεί να επηρεάσει κρίσιμα εθνικές και παγκόσμιες υποδομές. Οι επιχειρήσεις με την εξέλιξη της τεχνολογίας χρησιμοποιούν προηγμένες μεθόδους, ώστε να αποθηκεύουν τα δεδομένα τους, όπως για παράδειγμα βάσεις δεδομένων τις οποίες μετά διαμοιράζονται μέσω του διαδικτύου. Από την άλλη πλευρά βρίσκονται κακόβουλοι χρήστες οι οποίοι με τις γνώσεις πληροφορικής που διαθέτουν μπορούν να εισέλθουν στα πληροφοριακά συστήματα των επιχειρήσεων και να αλλοιώσουν ή να κλέψουν τα δεδομένα τους ή ακόμα να τις εξαπατήσουν μέσω του διαδικτύου. Αντιλαμβανόμαστε πως είναι πλέον υψίστης σημασία για μια επιχείρηση να τηρεί την συνθήκη για ασφάλεια των πληροφοριών που έχει. Αυτός ο παράγοντας σε συνδυασμό με άλλες παραμέτρους λειτουργίας όπως η διασφάλιση ποιότητας και εσωτερικής οργάνωσης εξασφαλίζει την ομαλή λειτουργία ενός οργανισμού, ενώ ταυτόχρονα αποτελεί και στοιχείο εμπιστοσύνης για τους πελάτες. Ας μην ξεχνάμε πως περίπου το 80% των σημερινών επιχειρήσεων στηρίζεται κατά βάση στη πληροφορική και αποθηκεύει όλα του τα δεδομένα ηλεκτρονικά σε ψηφιακή μορφή (Kwo-Shing Hong, Yen-Ping Chi, Louis R Chao, & Jih-Hsing Tang, 2013).

2.1.1 Ασφάλεια και πληροφοριακά συστήματα

Με τον όρο πληροφοριακό σύστημα εννοούμε το σύνολο των ανθρώπων αλλά και του λογισμικού, του λοιπού υλικού, των διαδικασιών και των δεδομένων που αλληλοεπιδρούν συνεχώς μεταξύ τους ώστε να μπορούν να διαχειριστούν και να επεξεργαστούν την πληροφορία που λαμβάνουν από το περιβάλλον τους. Οι

οργανισμοί σήμερα όπως έχουμε δει επενδύουν στα πληροφοριακά συστήματα για να συγκεντρώσουν όσο το δυνατό μεγαλύτερο όγκο πληροφοριών που να μπορούν στη συνέχεια να επεξεργαστούν. Η διασφάλιση πως υπάρχει εμπιστευτικότητας και ακεραιότητα για τις διαθέσιμες πληροφορίες σημαντική, ανεξάρτητα του κατά πόσον οι πληροφορίες αποτελούν το αντικείμενο επεξεργασίας και διαχείρισης ή ανταλλάσσονται μεταξύ των συνεργαζόμενων οργανισμών (Παπαθεωδόρου Χρήστος).

Πολλές είναι οι μεμονωμένες λύσεις που υιοθετούνται από τον εκάστοτε οργανισμό. Οι λύσεις αυτές προσφέρουν προστασία μόνο στο πεδίο για το οποίο εφαρμόζονται και δεν αφορούν το πληροφοριακό σύστημα στο σύνολο του. Ένα από τα πιο επίκαιρα παραδείγματα είναι αυτό της χρήσης τείχους προστασίας «firewall», το οποίο ελέγχει τις πληροφορίες που εισέρχονται και εξέρχονται από και προς το δίκτυο και δίνει ένα ρυθμό ασφάλειας ,ωστόσο δεν μπορεί να εντοπίσει κακόβουλα προγράμματα. Για την εύρεση και αντιμετώπιση τέτοιων προγραμμάτων πολύ συχνά χρησιμοποιούνται λογισμικά προστασίας, που κατά κύριο λόγο αφορούν τη χρήση στο διαδίκτυο και έχουν ως σκοπό να εξουδετερώνουν κακόβουλα προγράμματα για το πληροφοριακό σύστημα. Τα λογισμικά αυτά ονομάζονται στο χώρο της πληροφορικής «antivirus». Παρότι κάθε μία από αυτές τις λύσεις μπορεί να είναι αποτελεσματική στο πεδίο που την αφορά αυτό δεν σημαίνει πως παρέχει ασφάλεια στην ολότητα του πληροφοριακού συστήματος. Γι΄αυτό το λόγο συχνά απαιτείται να δημιουργηθεί ένα πλαίσιο που θα ορίζει ποιες είναι οι προϋποθέσεις για την ασφάλεια του πληροφοριακού συστήματος ενός οργανισμού και ποιες είναι οι δράσεις που πρέπει να λαμβάνονται. Προχωράμε δηλαδή προς την θέσπιση των προτύπων (standards) που αναγνωρίζονται από όλους τους οργανισμούς και έχουν νομική υπόσταση (Blyth M., 2008).

2.2 Συστήματα διαχείρισης ασφάλειας

Η πληροφορία που κατέχει ένας οργανισμός είναι πολλές φορές δείκτης ανάπτυξης γι' αυτόν και γι'αυτό πρέπει να προστατεύεται. Οι παρακάτω συγκεκριμένοι παράγοντες διαδραματίζουν σημαντικό ρόλο ως προς την ασφάλεια των πληροφοριών σε ένα πληροφοριακό σύστημα:

- Η πολιτική ασφάλειας των πληροφοριών.

- Η υποστήριξη της διοίκησης της επιχείρησης στο έργο της ασφάλειας των πληροφοριών.
- Η κατανόηση των απαιτήσεων της ασφάλειας με μελέτη του αντίστοιχου σχεδίου.
- Η εφαρμογή των διαδικασιών εκείνων που κρίνονται ως αποτελεσματικές για την αντιμετώπιση επικίνδυνων γεγονότων.
- Η παροχή εκπαίδευσης και κατάρτισης στο προσωπικό.
- Η υλοποίηση ενός συστήματος μέτρησης που να μπορεί να αξιολογήσει την απόδοση του συστήματος διαχείρισης της ασφάλειας πληροφοριών και να προτείνει προτάσεις για βελτιώσεις (Blyth M., 2008).

Το πεδίο στο οποίο εστιάζει ένα σύστημα Διαχείρισης Ασφάλειας πληροφοριών είναι στις διαδικασίες που συμβαίνουν στο εσωτερικό του οργανισμού. Από τις πιο διαδεδομένες μεθόδους για τον έλεγχο και τη βελτίωση των διαδικασιών κατά την ανάπτυξη ενός Συστήματος Διαχείρισης της Ασφάλειας Πληροφοριών (π.χ. σύμφωνα με το πρότυπο ISO/IEC 27001) είναι η μέθοδος *Plan-Do-Check-Act* (PDCA) που θα δούμε αναλυτικότερα σε επόμενο κεφάλαιο. Το σύστημα διαχείρισης ασφαλείας είναι ουσιαστικά μια ενιαία διεργασία που έχει ως σκοπό να δέχεται ως εισροές τις απαιτήσεις ασφαλείας του οργανισμού και να δίνει ως εκροές την διαχείριση της ασφάλειας των πληροφοριών (Sennewald, 2011).

Κεφάλαιο 3^{ο} : Εισαγωγή στο ISO

3.1. ISO: Ορισμός και ετυμολογική προέλευση

Ο ISO είναι ένας διεθνής μη κυβερνητικός οργανισμός, με έδρα την Γενεύη, ο οποίος ιδρύθηκε το 1947. Ασχολείται με την τυποποίηση του τρόπου λειτουργίας οργανισμών και επιχειρήσεων καθώς και με τον τρόπο που παράγουν και εμπορεύονται τα προϊόντων και των υπηρεσιών που έχουν δημιουργήσει. Ουσιαστικά πρόκειται για μια παγκόσμια ομοσπονδία εθνικών επιτροπών Προτύπων (Standards) που αποτελείται από περισσότερες από 140 χώρες. Αποστολή τους είναι η ανάπτυξη της τυποποίησης των σχετικών δραστηριοτήτων με σκοπό την διευκόλυνση της διεθνούς ανταλλαγής αγαθών και υπηρεσιών, καθώς επίσης και η ανάπτυξη συνεργασίας στους τομείς της πνευματικής, επιστημονικής τεχνολογικής και οικονομικής δραστηριότητας. Με λίγα λόγια το ISO δεν καθιερώνει μόνο πρότυπα απόδοσης αλλά καθορίζει και τις διαδικασίες με τις οποίες πληρούνται τα πρότυπα διαχείρισης ποιότητας (Walker Rhet H & W. Johnson Lester, 2009).

Πολλοί τείνουν να συσχετίζουν το ISO με τα αρχικά των λέξεων ***International Organization of Standardization*****.** Ωστόσο υπάρχει και μια διαφορετική άποψη σύμφωνα με την οποία η λέξη έχει τις ρίζες της στην ελληνική γλώσσα. Επομένως, αν αναζητήσουμε την ετυμολογική προέλευση της λέξης θα πρέπει να μελετήσουμε το ελληνικό λεξιλόγιο. Η λέξη προέρχεται από την ελληνική λέξη «ίσος» που έχει την έννοια του ισοδύναμου, κάποιου που έχει τα ίδια δικαιώματα με κάποιον άλλον Πρόκειται για την ρίζα του προθέματος ίσος- που συναντάμε πολύ συχνά στην ελληνική γλώσσα, για παράδειγμα ισόνομος ή ισότητα (Γ. Μπαμπινιώτης, 2004). Άλλωστε γι' αυτό ακριβώς το λόγο χρησιμοποιείται το ακρωνύμιο ISO, ώστε να αποφεύγονται διάφορες παρερμηνείες στις γλώσσες των διάφορων χωρών που το χρησιμοποιούν. Στις μέρες μας η εξάπλωση των προτύπων του ISO είναι πολύ μεγάλη και γι' αυτό το λόγο κάποιες φορές η ονομασία αυτή χρησιμοποιείται για να περιγράψει προϊόντα που ακολουθούν κάποιο πρότυπο. Για παράδειγμα:

- Οι εικόνες οπτικών δίσκων (CD image) χρησιμοποιούν την κατάληξη αρχείου .iso. Αυτή η κίνηση δηλώνει πως χρησιμοποιούν το πρότυπα συστήματος αρχείων ISO 9660 έναντι άλλων. Αυτός είναι και ο λόγος που πολλές φορές οι εικόνες των οπτικών δίσκων αναφέρονται ως «ISO». Οι υπολογιστές που

διαθέτουν οδηγούς CD-ROM μπορούν να διαβάσουν CD που χρησιμοποιούν αυτό το πρότυπο. Επιπλέον και τα DVD-ROM χρησιμοποιούν επίσης το σύστημα αρχείων ISO 9660.

- Στη ταχύτητα των φιλμ συναντάται συχνά ένα νούμερο ISO. Το νούμερο αυτό αφορά στην ευαισθησία στο φως των φωτογραφικών φιλμ και μετριέται βάση αυτού του νούμερου.

3.2 Πιστοποιήσεις και διεθνείς συνεργασίες

Ο οργανισμός ISO παράγει πιστοποιήσεις, τις λεγόμενες «πιστοποιήσεις ISO». Οι πιστοποιήσεις αυτές δεν μπορούν να θεωρηθούν άδειες απαγόρευσης ή άσκησης μιας δραστηριότητας. Πρόκειται για βεβαίωση πως η επιχείρηση που την κατέχει τηρεί βασικούς κανόνες στη διασφάλιση της ποιότητας των προϊόντων ή των υπηρεσιών αντίστοιχα, την παραγωγή τους, την διανομή τους κλπ. Για να μπορεί η επιχείρηση να πιστοποιείται με ISO πρέπει ουσιαστικά να τηρεί τους κανόνες αυτούς. Όταν ο καταναλωτής-πελάτης αλλά και οι συνεργάτες μιας επιχείρησης γνωρίζει πως εκείνη κατέχει μια τέτοια πιστοποίηση τότε δείχνουν μεγαλύτερη εμπιστοσύνη. Οι πιο κοινοί τύποι τέτοιων πιστοποιήσεων είναι το ISO 9001 και 14001 (IHS Markit, n.d.).

Τα μέλη που αποτελούν το ISO χωρίζονται σε τρεις κατηγορίες:

1. Η επιτροπή: Εδώ αναφερόμαστε στην εθνική επιτροπή κάθε χώρας που αντιπροσωπεύει την τυποποίηση της.
2. Μέλος-ανταποκριτής: Πρόκειται για μια οργάνωση μιας χώρας η οποία δεν έχει αναπτύξει ακόμα την δραστηριότητα της με βάση τα εθνικά Standards.
3. Συνδρομητικά μέλη: Πρόκειται για μέλη από χώρες που έχουν πολύ μικρές οικονομίες.

Ο ISO συνεργάζεται με πληθώρα οργανισμών σε παγκόσμιο επίπεδο. Τα μέλη των οργανισμών αυτών προσανατολίζονται αρκετές φορές σε διαφορετικά ενδιαφέροντα. Κάποια από τα μέλη του ανήκουν σε τοπικούς οργανισμούς τυποποίησης, οι οποίοι έχουν αναγνωριστεί από τον ISO, εκπροσωπώντας διάφορες περιοχές. Μιλώντας με νούμερα ο συγκεκριμένος οργανισμός συνεργάζεται με παραπάνω από 600 διεθνείς και τοπικούς οργανισμούς (Roxanne Oclarino, 2020). Η Παγκόσμια Συνεργασία Προτυποποίησης (World Standards Cooperation - WSC) ιδρύθηκε μέσω μιας τέτοιας

συνεργασίας. Συγκεκριμένα Ο ISO συνεργάστηκε με τη Διεθνή Ηλεκτροτεχνική Επιτροπή (Electrotechnical Commission - IEC) και τη Διεθνή Ένωση Τηλεπικοινωνιών (International Telecommunication Union - ITU) ώστε να ενισχύσει και να προωθήσει την διεθνή τυποποίηση. Επιπλέον σε διεθνές επίπεδο συνεργάζεται με τον Παγκόσμιο Οργανισμό Εμπορίου (World Trade Organization - WTO), τον Οργανισμό Ηνωμένων Εθνών (United Nations Organization) και με άλλους οργανισμούς των Ηνωμένων Εθνών που στηρίζουν τις αναπτυσσόμενες χώρες (ISO, n.d.).

Οι ανάγκες για πιστοποιήσεις ISO συχνά προέρχονται από τον βιομηχανικό τομέα. Υπάρχουν ορισμένες φάσεις από τις οποίες πρέπει να περάσει η επιχείρηση ώστε να αποκτήσει την τελική πιστοποίηση. Η επιχείρηση-οργανισμός απευθύνει την ανάγκη πιστοποίησης στην εθνική επιτροπή μέλος της χώρας του. Η επιτροπή με την σειρά της προτείνει το θέμα στην οργάνωση ISO. Μετά αναμένεται να αναγνωριστεί και να συμφωνηθεί επίσημα η ανάγκη για το διεθνές Πρότυπο ISO. Έτσι *η πρώτη φάση* περιλαμβάνει τον καθορισμό της τεχνικής θεώρησης του μελλοντικού προτύπου. Γι' αυτό το λόγο δημιουργούνται ομάδες εργασίας που αποτελούνται από ειδικούς τεχνικούς που προέρχονται από χώρες που ενδιαφέρονται για την εν λόγω πιστοποίηση. Όταν υπάρξει συμφωνία σχετικά με τις τεχνικές πλευρές που οφείλει να καλύψει το πρότυπο, είναι το σημάδι έναρξης της δεύτερης φάσης. Στη *δεύτερη φάση* λαμβάνει μέρος η κοινή συναίνεση. Οι χώρες δηλαδή διαπραγματεύονται με λεπτομέρεια τις προδιαγραφές του προτύπου. Έπειτα είναι η στιγμή για την *τελική φάση*. Κατά την διάρκεια αυτής της φάσης έχουμε την επίσημη έγκριση του τελικού προσχεδίου του Διεθνούς Προτύπου. Είναι σημαντικό να τονίσουμε πως υπάρχει όρος με συγκεκριμένα κριτήρια αποδοχής για να φτάσουμε στην αποδοχή του τελικού προτύπου: πρέπει να εγκριθεί από τα 2/3 των μελών που αποτελούν την επιτροπή ISO αλλά και να υπάρχει έγκριση του 75% των μελών που παίρνουν μέρος στη ψηφοφορία. Αφού τελειώσει και αυτή η φάση το κείμενο που συμφωνήθηκε εκδίδεται πλέον ως Διεθνές Πρότυπο ISO. Βέβαια πολλά από τα Standards χρειάζονται περιοδική επανεξέταση για να διαπιστωθεί εάν ισχύουν οι αρχικοί κανόνες και οδηγίες. Το ISO μέχρι και στις μέρες μας έχει εκδώσει **12000 Διεθνή Standards.** Τα κείμενα αυτά παρουσιάζονται σε πάνω από 300.000 σελίδες τόσο στα Αγγλικά όσο και στα Γαλλικά. Οι ορολογίες σαφώς παρέχονται και σε άλλες

γλώσσες ανάλογα την χώρα που απευθύνεται. Επίσημες γλώσσες είναι τα Αγγλικά, τα Γαλλικά και τα Ρωσικά (Ανθής Δημήτρης, n.d.).

3.3 Πρότυπα ISO (ISO Standards)

Στη προηγούμενη ενότητα έγινε λόγος για πρότυπα του ISO. Τα πρότυπα αποτελούν οδηγίες για την παραγωγική διαδικασία ενός προϊόντος, τον τρόπο διανομής προϊόντων, τον τρόπο δημιουργίας υπηρεσιών και άλλων παρόμοιων δραστηριοτήτων. Βασίζονται στις γνώσεις θεωρητικές και πρακτικές των ειδημόνων σε κάθε τομέα ώστε να μπορέσει η επιχείρηση να πετύχει υψηλά επίπεδα απόδοσης. Οι ειδικοί αυτοί μπορεί να είναι ο γενικός διευθυντής μιας επιχείρησης, ο προμηθευτής της, ο εργαζόμενος στη μονάδα παραγωγής κλπ. Τα Διεθνή Πρότυπα (*International Standards*) είναι συμφωνίες που έχουν τεκμηριωθεί μέσω εγγράφων που περιέχουν τεχνικές προδιαγραφές για να μπορέσουν να χρησιμοποιηθούν ως κανόνες, οδηγίες για την χρήση προϊόντων και υπηρεσιών. Με αυτό τον τρόπο γνωρίζουμε ως καταναλωτές ότι υπάρχει αξιοπιστία, αποτελεσματικότητα και ασφάλεια στα προϊόντα και τις υπηρεσίες που χρησιμοποιούμε.

Ανάλογα με τις διάφορες κατηγορίες επιχειρήσεων και οργανισμών έχουν δημιουργηθεί και τα ανάλογα πρότυπα:

- **Πρότυπα διαχείρισης ποιότητας (*Quality management standards*):** Πρότυπα που συμβάλουν στη βελτίωση της εργασίας και απομακρύνουν κινδύνους, απειλές και αποτυχίες. Σε αυτήν την κατηγορία συναντάτε το ISO 9001 που βοηθά στη δημιουργία ποιοτικών προϊόντων και την εξάλειψη πιθανών κινδύνων. Μπορεί να χρησιμοποιηθεί από οποιαδήποτε επιχείρηση ανεξάρτητα από το μέγεθος τους και το πεδίο στο οποίο δραστηριοποιούνται Δημιουργείται έτσι μια μεγάλη οικογένεια τέτοιων προτύπων όπως τα *ISO 9000:2015, ISO 9001:2015, ISO 9004:2018.*
- **Πρότυπα διαχείρισης περιβάλλοντος (*Environmental management standards*):** Πρόκειται για την οικογένεια των ISO 14000 που βοηθά στην υιοθέτηση καλύτερων πρακτικών από τις επιχειρήσεις για να φέρουν εις πέρας τις

περιβαλλοντικές τους ευθύνες. Σε αυτήν την κατηγορία συναντάμε τα ISO 14001: 2015, ISO14004:2016, ISO 14005:2019.

- **Πρότυπα υγιεινής και ασφάλειας:** Το κύριο πρότυπο αυτής της οικογένειας είναι το ISO 45001. Αφορά στην ασφάλεια των ζωών των εργαζομένων, σε ένα εργατικό περιβάλλον όπου οι κίνδυνοι είναι εξαλειμμένοι δημιουργώντας καλύτερες εργασιακές συνθήκες. Αρκεί να σκεφτούμε πως κάθε μέρα τουλάχιστον 7.600 εργαζόμενοι στο πλανήτη χάνουν την ζωή τους από εργατικό ατύχημα ή επιδημίες για να καταλάβουμε την σημαντικότητα του συγκεκριμένου προτύπου. Η προσέγγιση του είναι ίδια με εκείνη των ISO 14001 και ISO 9001. Η τελευταία έκδοση του προτύπου είναι το ISO 45001:2018.
- **Πρότυπα διαχείρισης ενέργειας (Energy management standards):** Είναι πρότυπα που αφορούν στο περιορισμό της κατανάλωσης ενέργειας. Ουσιαστικά βοηθά την επιχείρηση να βελτιώσει την χρήση ενέργειας μέσω της ανάπτυξης συστημάτων διαχείρισης της. Το ISO εδώ είναι το ISO 50001.
- **Πρότυπα διαχείρισης τροφίμων (Food management system):** Οι επιχειρήσεις που πραγματεύονται την δημιουργία και εμπορία τροφίμων πρέπει να είναι πολλοί προσεκτικοί σχετικά με την ασφάλεια και ποιότητα των προϊόντων τους καθώς και την υγεία των καταναλωτών τους. Το πιο γνωστό ISO αυτής της κατηγορίας είναι το ISO 22000. Το πρότυπο αυτό βοηθά της επιχειρήσεις να εντοπίσουν πιθανές επικίνδυνες ουσίες στα τρόφιμα και να διατηρήσουν τα προϊόντα τους ασφαλή. Μέσω αυτής της λειτουργίας δημιουργείται μια παγκόσμια αλυσίδα εφοδιασμού τροφίμων που συμβάλλουν στη πιο αποτελεσματική και ευκολότερη εξαγωγή των τροφίμων εκτός συνόρων. Πλέον οι άνθρωποι εμπιστεύονται τα τρόφιμα που καταφτάνουν σπίτι τους. Πολλές φορές για να είναι ορθότερη η χρήση του συγκεκριμένου προτύπου συνδυάζεται με το ISO 9001. Σε αυτήν την κατηγορία ανήκουν τα ISO 22000:2018 και ISO/TS 22003:2013.
- **Πρότυπα διαχείρισης ασφάλειας πληροφοριών (Information Security Management):** Το πιο διαδεδομένο πρότυπο αυτής της κατηγορίας είναι το ISO/IEC 27001 που σκοπό του έχει να παρέχει τις προϋποθέσεις για ένα σύστημα ασφάλειας και διαχείρισης πληροφοριών. Με την υιοθέτηση του οι επιχειρήσεις μπορούν να χειρίζονται καλύτερα τα δεδομένα των υπαλλήλων τους και

οικονομικές πληροφορίες της επιχείρησης με πλήρη ασφάλεια (International Organization for Standardization, 2015).

3.3.1 Διάρκεια ζωής του προτύπου

Τα πρότυπα δεν είναι μια απλή έκδοση ενός εγγράφου άλλα όταν ζητηθεί η έκδοση τους από μια επιχείρηση πρέπει να περάσουν από κάποιες καθορισμένες φάσεις. Οι φάσεις αυτές είναι οι ακόλουθες επτά:

1. **Καταγραφή ανάγκης του κατασκευαστή και του χρήστη.** Ανάλυση βάση του τομέα που απευθύνεται το πρότυπο της καταλληλόλητας του αλλά και της τεχνοοικονομικής σκοπιμότητας που εξυπηρετεί. Δίνεται έμφαση στα πλεονεκτήματα που μπορεί να φέρει το πρότυπο στο τομέα καθώς και αν υπάρχει η απαραίτητη γνώση που απαιτεί το πρότυπο.
2. **Συλλογικός προγραμματισμός.** Προγραμματισμός βάση των καταγεγραμμένων αναγκών και των προτεραιοτήτων που καθορίζουν οι συμμετέχοντες. Απόφαση για το οριστικό πρόγραμμα που θα χρησιμοποιηθεί.
3. **Σχεδιασμός της αρχικής μορφής του προτύπου από τα ενδιαφερόμενη μέρη.** Σε αυτήν την φάση παρουσιάζεται η σχεδιασμένη πρώτη μορφή του προτύπου. Την παρουσίαση αναλαμβάνουν οι ειδικοί όπως μπορεί να είναι χρήστες, καταναλωτές, οι αντιπρόσωποι μιας επιχείρησης κλπ. Όλα αυτά τα μέρη συμμετέχουν σε ειδικές επιτροπές που ασχολούνται με την τυποποίηση.
4. **Ομοφωνία εμπειρογνωμόνων σχετικά με το αρχικό πρότυπο.** Αυτή η φάση είναι ιδιαιτέρως καθοριστική καθώς εδώ συγκεντρώνονται οι ειδικοί εμπειρογνώμονες και αποφασίζουν σχετικά με το αρχικό πρότυπο που έχει κατατεθεί από τα ενδιαφερόμενα μέρη.
5. **Φάση νομιμοποίησης.** Πρόκειται για ένα ευρύ συμβούλιο που μπορεί να είναι σε διεθνές ή εθνικό επίπεδο. Το συμβούλιο αυτό δίνεται μέσω ενός δημόσιου ερωτηματολογίου που εμπλέκει τους οικονομικούς συμμετέχοντες ώστε να διαπιστωθεί πως το αρχικό πρότυπο είναι συμβατό με τις απαιτήσεις των μερών και δεν υπάρχουν αντιρρήσεις. Εξετάζονται τα αποτελέσματα και οι διάφορες παρατηρήσεις που μπορεί να δημιουργήθηκαν. Σε αυτή την φάση περιλαμβάνεται και η οριστικοποίηση του αρχικού προτύπου.
6. **Επικύρωση κειμένου.** Κατά την έκτη φάση επικυρώνεται το κείμενο που θα δημοσιευτεί ως πρότυπο. Είναι η προτελευταία φάση της όλης διαδικασίας.

7. **Τελική ανασκόπηση:** Σε όλα τα πρότυπα πραγματοποιείται τακτική ανασκόπηση που αφορά την σχετικότητα της εφαρμογής των προτύπων από τον οργανισμό τυποποίησης. Στη συγκεκριμένη φάση πραγματοποιείται και ο χρονικός προσδιορισμός ο οποίος δίνεται σε ένα πρότυπο ώστε να προσαρμοστεί στις ανάγκες του εκάστοτε οργανισμού. Είναι η λεγόμενη φάση της αναθεώρησης. Μετά από την αναθεώρηση υπάρχουν τρείς επιλογές για το πρότυπο: να επιβεβαιωθεί χωρίς πραγματοποίηση κάποιας αλλαγής, να προχωρήσει σε μια διαδικασία διασκευής ή να καταργηθεί εντελώς.

Πιο συγκεκριμένα, ο Οργανισμός ISO προκειμένου να διαμορφώσει τα πρότυπα του αναθέτει την διαδικασία αυτή σε μια επιτροπή ειδικών που αποκαλείται Τεχνική Επιτροπή. Η επιτροπή αυτή απαρτίζεται από ειδικούς-μέλη που προέρχονται από όλες τις χώρες που συμμετέχουν στον οργανισμό. Να τονίσουμε πως κάθε τέτοια επιτροπή δεν είναι μόνη της αλλά αποτελείται από ένα ικανό αριθμό υποεπιτροπών, οι οποίες διαιρούνται ακόμα σε ομάδες εργασίας ώστε να υπάρξει σαφής συντονισμός προσπαθειών για να αναπτυχθεί ένα Διεθνές Πρότυπο ISO (Roger Atkinson, 1999).

3.4. Οφέλη για τις επιχειρήσεις από την χρήση του ISO

Με την απόκτηση μιας πιστοποίησης ISO τα οφέλη μιας επιχείρησης είναι αρκετά αλλά συγκεκριμένα. Κυρίως έχουν να κάνουν με την βελτίωση της αποτελεσματικότητας της επιχείρησης και της παραγωγικότητας. Παράλληλα ενισχύεται το ηθικό των υπαλλήλων και βελτιώνεται η ικανοποίηση των πελατών.

Σύμφωνα με την *Rowda Mohamud*, σύμβουλο επιχειρήσεων που έχει υποστηρίξει πολλές επιχειρήσεις στο Τορόντο να αποκτήσουν πιστοποιήσεις ISO, υπάρχουν πέντε σημεία-κλειδιά που αποκτούν οι επιχειρήσεις από τις πιστοποιήσεις αυτές. Πιο συγκεκριμένα:

1. **Προσδιορισμός των πιθανών απειλών και ευκαιριών**. Για να μπορέσει μια επιχείρηση να αποφύγει κινδύνους, η καλύτερη στρατηγική είναι να τους προβλέψει. Η λύση εδώ βρίσκεται με την πιστοποίηση ISO 9001. Βάση αυτού του ISO δημιουργείται ένας πίνακας με τις πιθανές απειλές που θεωρεί η κάθε επιχείρηση ότι αντιμετωπίζει και σχεδιάζει ένα τρόπο ώστε να μπορέσει να τις αντιμετωπίσει. Για να γίνει αυτό, εξετάζεται το ιστορικό της επιχείρησης, ποια προβλήματα είχαν προκύψει στο παρελθόν ώστε να αποτραπεί η επανεμφάνιση

τους στο μέλλον. Πέρα από αυτό το κομμάτι, ζητείται από την επιχείρηση να εστιάσει και στο θετικό κομμάτι, να εντοπίσει πιθανές ευκαιρίες στην αγορά. Έπειτα πρέπει να σκεφτεί τρόπους ώστε να τις εκμεταλλευτεί με αποτελεσματικό τρόπο.

2. **Αποτροπή επανάληψης των ίδιων προβλημάτων**. Είναι πολύ συχνό το φαινόμενο οι επιχειρήσεις να υποπίπτουν σε σφάλματα του παρελθόντος. Αυτό συμβαίνει διότι δεν έχουν κρατήσει ένα ιστορικό με τα λάθη που είχαν συμβεί στο παρελθόν. Μία από τις προϋποθέσεις που θέτουν τα ISO είναι η δημιουργία ενός ιστορικού με όσα προβλήματα προκύπτουν στην επιχείρηση, να εντοπιστούν οι βαθύτερες αιτίες και να υπάρξουν λύσεις μακράς διαρκείας. Ο κύριος στόχος αυτού του βήματος είναι: λιγότερες σπατάλες πόρων, καλύτερη ποιότητα, χαμηλότερα κόστη.
3. **Ενίσχυση του marketing και των πωλήσεων της επιχείρησης**. Η κατοχή πιστοποίησης ISO από μια επιχείρηση αποτελεί ένα γεγονός που μπορεί να διαφημιστεί και να προωθηθεί έτσι προς τα έξω, προς τους συνεργάτες αλλά και τους πελάτες η αξιοπιστία του οργανισμού. Αυτός είναι ο λόγος που οι πιστοποιήσεις διαφημίζονται από τις επιχειρήσεις στα sites τους και στις διαφημιστικές τους καμπάνιες. Αποτελεί λοιπόν ένα νέο τρόπο διαφήμισης για την επιχείρηση που την βοηθά να αυξήσει τις πωλήσεις της. Μάλιστα για να επιτευχθεί μια συνεργασία μεταξύ μεγάλων επιχειρήσεων η κατοχή ISO είναι από τις βασικές προϋποθέσεις. Αλλά και στη περίπτωση που μια επιχείρηση θέλει να εισέλθει σε μια νέα, ξένη αγορά και πάλι απαιτείται η κατοχή πιστοποίησης ISO. Το πιο συχνό στοιχείο που πρέπει να κατέχουν οι επιχειρήσεις είναι το ISO 9001 και οποιοδήποτε συγκεκριμένο ISO απαιτεί κάθε βιομηχανία.
4. **Βελτίωση του ηθικού των υπαλλήλων**. Όταν η επιχείρηση έχει αφοσιωθεί και έχει δεσμευτεί να παράγει προϊόντα και υπηρεσίες μεγάλης αξίας χωρίς να κατασπαταλά πόρους τότε αυτομάτως βελτιώνεται και το ηθικό του ανθρώπινου δυναμικού της. Τα ISO έχουν ως σκοπό να μειώσουν πιθανά προβλήματα και να συντονίσουν τις διαδικασίες βάση κανόνων για την εξαγωγή ποιοτικών προϊόντων και υπηρεσιών. Όταν αυτό το στοιχείο λείπει από μια επιχείρηση τότε δημιουργείται σύγχυση μεταξύ των υπαλλήλων που δεν γνωρίζουν ποιο σκοπό εξυπηρετούν. Όταν υπάρχει οργάνωση, όταν είναι συγκεκριμένα τα εργαλεία, οι κανόνες και ο τρόπος λειτουργίας της επιχείρησης στους υπαλλήλους τότε και οι ίδιοι θα αισθάνονται καλύτερα και θα αποδίδουν περισσότερο.

5. **Βελτίωση του ελέγχου της επιχείρησης**. Αυτό που απαιτούν τα διάφορης κατηγορίας ISO είναι ο έλεγχος, η μέτρηση και η ανάλυση της αποτελεσματικότητας του συστήματος που έχει κάθε επιχείρηση. Αυτός είναι ένας τρόπος δημιουργίας μετρητών απόδοσης, ώστε να αντιληφθεί η επιχείρηση το επίπεδο αποτελεσματικότητας στο οποίο βρίσκεται και να βελτιώσει ενδεχόμενες αδυναμίες της (Sirdeshmukh D., Singh J., & B., 2002).

3.5. Κόστος πιστοποιήσεων και αποσβέσεις

Το κόστος ενός Συστήματος Διαχείρισης Ποιότητας μπορεί να ξεκινήσει από τα 1600€ και να φτάσει μέχρι και τα 3.000€. Το ποσό έχει να κάνει με την πολυπλοκότητα της επιχείρησης. Για ένα έτος μια πιστοποίηση ISO κοστίζει 800€ - 1.000€ βάση του φορέα που έχει επιλέξει. Επομένως, γίνεται εύκολα κατανοητό πως οι πιστοποιήσεις αυτές δεν απευθύνονται σε επιχειρήσεις χαμηλού τζίρου. Οι μεγαλύτερες επιχειρήσεις μπορούν να αποσβέσουν αυτό το κόστος με τους κάτωθι τρόπους:

1. Από την καλύτερη λειτουργία (μείωση κόστους, αποδοτικότερη εργασία, καλύτερα προϊόντα κλπ)
2. Από προσέλκυση νέων πελατών λόγω της πιστοποίησης.
3. Από την είσοδο σε νέες αγορές λόγω της πιστοποίησης.
4. Από τη συμμετοχή σε διαγωνισμούς που θέτουν την πιστοποίηση ή προϋπόθεση συμμετοχής (Κουτσογιάννη Λογιστικό Γραφείο, 2016) .

Κεφάλαιο 4^{ο}: Μελέτη του ISO 9001

4.1 Ορισμός του ISO 9001

Τα πρότυπα ISO όπως είδαμε και στη προηγούμενη ενότητα είναι μια μεγάλη οικογένεια προτύπων. Το ISO 9001 ανήκει στην οικογένεια των προτύπων ISO 9000, η οποία περιλαμβάνει τα ISO 9000, ISO 9001, ISO 9004 και ISO 19011. Το ISO 9000 περιγράφει τις έννοιες που θεωρούνται βασικές και την γλώσσα που χρησιμοποιείται έτσι ώστε να μπορέσουν να υιοθετήσουν οι οργανισμοί το πρότυπο ISO 9001. Το πρότυπο αυτό αποτελεί το πιο δημοφιλές στα συστήματα ποιότητας και καθορίζει τις βασικές απαιτήσεις για ένα τέτοιο σύστημα διαχείρισης. Πρόκειται για διεθνές αναγνωρισμένο πρότυπο στην εφαρμογή της διαχείρισης ποιότητας. Είναι ενδεικτικό πως μόνο το 2013, εκδόθηκαν 1.138,155 πιστοποιητικά ISO 9001 σε 187 χώρες. Ένας αριθμός που αντιστοιχούσε στα τρία τέταρτα όλων των προτύπων ISO που εκδόθηκαν.

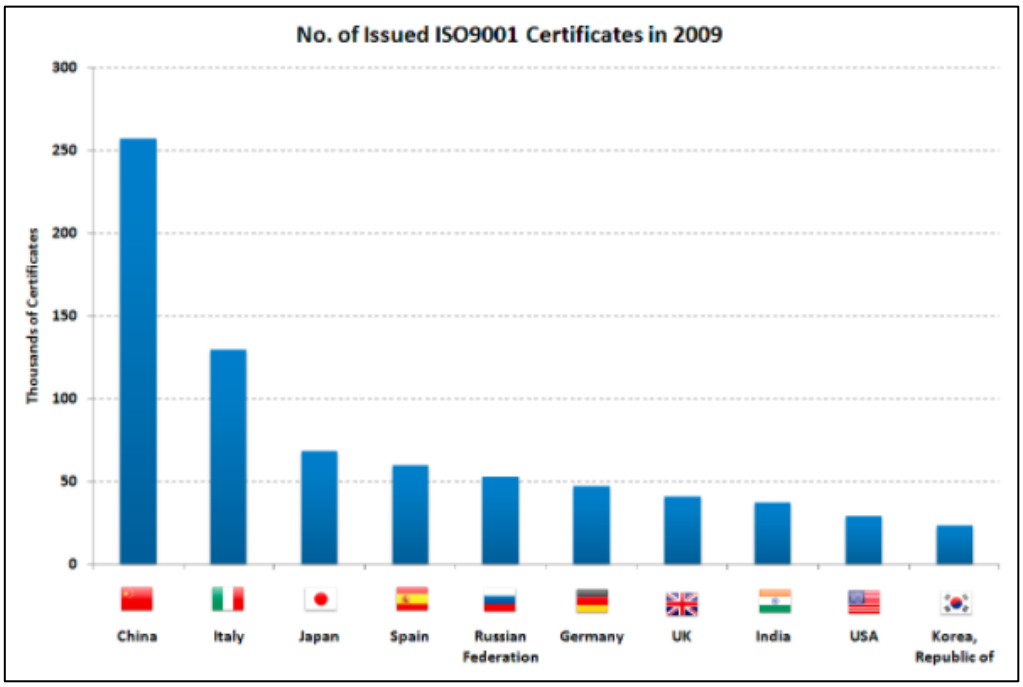
Όλα τα παραπάνω πρότυπα που ανήκουν στην οικογένεια ISO 9000 έχουν γραφτεί με την σειρά που διατάχτηκαν έτσι ώστε από κοινού να μπορούν να γίνει η χρησιμοποίησή τους. Πιο συγκεκριμένα, το πρότυπο ISO 9000:2000 εμπεριέχει τις βασικές αρχές για το σύστημα διαχείρισης ποιότητας, το ISO 9001: 2000 καθορίζει τις βασικές απαιτήσεις του συστήματος. Με την σειρά του το ISO 9004:2000 έχει περισσότερο υποστηρικτό ρόλο καθώς παρέχει οδηγίες για την βελτίωση του συστήματος με βάση μακροπρόθεσμους στόχους. Τέλος, το ISO 19011 επικεντρώνεται στον έλεγχο των συστημάτων διαχείρισης της ποιότητας και των συστημάτων περιβαλλοντικής διαχείρισης. Επειδή ζούμε σε ένα κόσμο που οι επιχειρήσεις διαμορφώνονται συνεχώς εκ νέου, αλλάζουν και αναπτύσσονται το ίδιο συμβαίνει και με το ISO 9001. Κάθε πέντε χρόνια στο περίπου το πρότυπο εξετάζεται εκ νέου και ενημερώνεται, ώστε να ανταποκρίνεται στις μεταβαλλόμενες συνθήκες που επικρατούν στο περιβάλλον της αγοράς και των επιχειρήσεων. Για πρώτη φορά εμφανίστηκε το 1987 και έκτοτε έχει αλλάξει, όπως είναι φυσικό, πολλές φορές.

4.1.1 Ιστορική αναδρομή

Το 1987 εκδίδεται για πρώτη φορά η σειρά των προτύπων ποιότητα ISO 9000. Η σειρά αυτή συμπεριελάμβανε τα τρία ακόλουθα πρότυπα διαχείρισης ποιότητας ISO 9001, ISO 9002 και ISO 9003. Το πρότυπο ISO 9001:1987 ήταν εκείνο που καθόριζε το μοντέλο για τη διαχείριση της ποιότητας στο σχεδιασμό, την ανάπτυξη, την παραγωγή, την εγκατάσταση και τη συντήρηση. Η έκδοση του βασιζόταν σε ένα στρατιωτικό Πρότυπο της Βρετανίας και των Η.Π.Α το οποίο περιείχε τρία διαφορετικά συστήματα διαχείρισης ποιότητας σύμφωνα πάντα με τις επιχειρηματικές δραστηριότητες του προς πιστοποίηση οργανισμού. Έτσι το πρότυπο ISO 9002:1987 ήταν το μοντέλο διαχείρισης της ποιότητας τόσο στην παραγωγή, όσο και στην εγκατάσταση και τη συντήρηση. Η διαφορά του με το ISO 9001 ήταν πως δεν μπορούσε να καλύψει την έκδοση νέων προϊόντων. Τέλος, το ISO 9003:1987 ήταν το πρότυπο διαχείρισης ποιότητας στην τελική επιθεώρηση και δοκιμή. Ωστόσο, δεν χρησιμοποιήθηκε ποτέ. Έπειτα ήταν η στιγμή για την δεύτερη έκδοση της σειράς ISO 9000, ουσιαστικά την πρώτη αναθεώρηση του προτύπου το έτος 1994. Αυτήν την περίοδο η σειρά αυτή τόνισε περισσότερο την σημασία και την σπουδαιότητα των προληπτικών ενεργειών και της διασφάλισης της ποιότητας πέραν του ποιοτικού ελέγχου. Η τρίτη έκδοση, το 2000, είναι ενοποιημένη καθώς συνδυάζει τα πρότυπα ISO 9001, 9002 και 9003 σε ένα πρότυπο, το γνωστό ISO 9001:2000. Πρόκειται για μια πιο ριζική αναθεώρηση βασισμένη σε σύγχρονες μεθόδους διαχείρισης ποιότητας. Αυτή η έκδοση χρησιμοποίησε μια ευρύτερη έννοια της διαχείρισης της ποιότητας και η βελτίωση της ικανοποίησης των πελατών έγινε μια από τις μετρήσεις απόδοσης. Δόθηκε περαιτέρω βαρύτητα στην ικανοποίηση του πελάτη για πρώτη φορά και φάνηκε πως η συνεχή βελτίωση της ποιότητας είναι το ζητούμενο. Επιπλέον, επικεντρώθηκε στην προσέγγιση της διαδικασίας και στην ενεργό συμμετοχή της διοίκησης. Το ISO 9001:2008 είναι βασικά το ίδιο με την προηγούμενη έκδοση του αλλά περιέχει περισσότερη σαφήνεια ως προς τις διαδικασίες. Σημαντικές αλλαγές δεν υπήρξαν. Παρατηρήθηκε πως το ISO 9001:2008 είχε κοινά με το πρότυπο ISO 140001 που αφορά στη περιβαλλοντική διαχείριση. Βέβαια υπάρχει και η νέα έκδοση του προτύπου, το ISO 9001:2015. Με τους νέους κανονισμούς που περιέχει κάνει πιο εύκολη την προσαρμογή του στις επιχειρήσεις που ασχολούνται με τον τομέα των υπηρεσιών (Basak Manders, Vries, & Knut, 2016).

4.2 Επιχειρήσεις και ISO 9001

Το συγκεκριμένο πρότυπο είναι πολύ σημαντικό για τις επιχειρήσεις διότι της βοηθά να προλαμβάνουν κινδύνους, μειώνοντας τις πιθανές απώλειες από την ποιότητα των προϊόντων και των υπηρεσιών τους. Παράλληλα περιορίζουν με αυτόν τον τρόπο την αύξηση του κόστους παραγωγής. Ένα άλλο θετικό στοιχείο αυτού του προτύπου είναι ότι παρέχει προτάσεις και βελτιώσεις για την επιχείρηση σε μακροπρόθεσμο ορίζοντα, δίνοντας το αίσθημα της ασφάλειας στη διοίκηση της. Εκτός από την ποιότητα στο χώρο εργασίας παρέχει και οδηγίες για αποφυγή εργασιακών ατυχημάτων, τονίζοντας την σημαντικότητα της ασφάλειας στον εργασιακό χώρο. Οι αποζημιώσεις και ο χαμένος παραγωγικός εργασιακός χρόνος αντιστοιχεί σε μεγάλη απώλεια για οποιαδήποτε επιχείρηση και γι' αυτό υπάρχουν διαδικασίες πρόληψής τέτοιων θεμάτων (Juan José Tarí, José Francisco Molina-Azorín, & Iñaki Heras, 2012). Βέβαια, το γεγονός αυτό είναι και ένας από τους λόγους που ολοένα και περισσότεροι οργανισμοί θέλουν να αποκτήσουν την πιστοποίηση ISO 9001. Ενδεικτικά παρατίθεται η **Εικόνα 2**, που απεικονίζει τον αριθμό των πιστοποιήσεων που εκδόθηκαν ανά χώρα παγκοσμίως για το έτος 2009.



Εικόνα 2: **Αριθμός πιστοποιήσεων προτύπων ISO 9001 ανά χώρα για το 2009.** (Abbas Ahmed, 2011) .

Σύμφωνα με τον ISO στην έρευνα του για πιστοποιήσεις το 2009 ενώ οι χώρες της Ευρώπης στο σύνολο τους είχαν λάβει τις περισσότερες πιστοποιήσεις, η Κίνα είχε τις περισσότερες πιστοποιήσεις (257,076) ξεπερνώντας τις υπόλοιπες 9 χώρες της από τις 10 κορυφαίες για το συγκεκριμένο πρότυπο. Η Ιταλία, δεύτερη στη κατάταξη είχε τις μισές περίπου πιστοποιήσεις (130,066) σε σχέση με την Κίνα. Η Κίνα κατόρθωσε από τρίτη στη κατάταξη να ανέλθει στη πρώτη θέση από το 2000 και έπειτα, ενώ άλλες χώρες όπως η Τσεχία εκτοπίστηκαν εντελώς (Abbas Ahmed, 2011).

4.3 ISO 9001:2000

Για να μπορέσει να αντιληφθεί μια επιχείρηση πως λειτουργούν τα πρότυπα αυτά και τα συστήματα διαχείρισης ποιότητας χρειάζεται πρώτα να κατανοήσει τις αρχές αυτών των προτύπων. Όλα τα πρότυπα που εμπεριέχονται στην οικογένεια των ISO 9000 ισχύουν 8 βασικές αρχές. Οι αρχές αυτές ισχύουν τόσο για τις μικρές όσο και για τις μεγαλύτερες επιχειρήσεις και μπορούν να υιοθετηθούν εύκολα. Αυτό έγινε βάση της αναθεώρησης του προτύπου το 2000.

4.3.1 Βασικές αρχές ISO 9001:2000

1. Πελατοκεντρική οργάνωση. Η πρώτη αρχή του συστήματος έχει να κάνει με το κατά πόσο το πρότυπο εστιάζει στο πελάτη. Με την αναθεώρηση του το 2000 το ISO 9001 απαιτεί όλη η εταιρεία να έχει προσανατολιστεί ως προς τον πελάτη. Για να συμβεί αυτό η εταιρεία χρειάζεται καθιέρωση διαδικασιών που θα την βοηθήσουν να να αντιληφθεί τις ανάγκες του πελάτη. Ταυτόχρονα, χρειάζεται και ένας μηχανισμός πρόβλεψης των ενδεχόμενων απαιτήσεων τους. Η επιχείρηση πρέπει σε κάθε περίπτωση να είναι ένα βήμα μπροστά. Αυτό που αποζητούν οι πελάτες είναι η ποιότητα και η επιχείρηση πρέπει να στοχεύει σε αυτήν βάση των κανονισμών που εμπεριέχει το διεθνές πρότυπο. Το συγκεκριμένο ISO έχει σαν αρχή του ότι η εταιρεία δεν σταματά την προσπάθεια της ως προς την ποιότητα των προϊόντων και των υπηρεσιών της ακόμα και όταν έχει καταφέρει να ικανοποιήσει τους πελάτες της. Για να μπορέσει να δημιουργήσει μια βάση με ικανοποιημένους πελάτες πρέπει να μην σταματά ποτέ την προσπάθεια της, ώστε να προβλέπει και να προλαβαίνει τις προσδοκίες τους.

2. Ευθύνη διοίκησης. Σαν δεύτερη αρχή για ένα σύστημα διαχείρισης ποιότητας έρχεται η ευθύνη που έχουν τα άτομα της διοίκησης. Η εταιρεία θα πρέπει να αντιλαμβάνεται ποιες είναι οι ανάγκες και οι απαιτήσεις των πελατών, να εξετάζει κάθε περίπτωση ξεχωριστά και τα πορίσματα που εξάγει να φαίνονται μέσω των προϊόντων και των υπηρεσιών που παράγει και παρέχει στους πελάτες της. Πολύ σημαντικό ρόλο εδώ έχουν οι διαδικασίες που λαμβάνουν μέρος σε όλη αυτήν την προσπάθεια. Η πολιτική ποιότητας που θα ακολουθήσει η επιχείρηση είναι και αυτή μια ευθύνη της διοίκησης. Οι στόχοι που θέτει η διοίκηση πρέπει να είναι ρεαλιστικοί και σύμφωνα με με τα δεδομένα στα οποία μπορεί να κινηθεί. Το πρότυπο προτείνει συνεχές ανασκοπήσεις στο σύστημα για να ελέγχονται οι λειτουργίες της επιχείρησης, η πορεία των στόχων αλλά και η επικοινωνία με τους πελάτες.

3. Συμμετοχή προσωπικού. Η τρίτη αρχή είναι εξίσου σημαντική και έχει να κάνει με το ποσοστό συμμετοχής του προσωπικού τόσο στη λειτουργία, όσο και στο τρόπο διαχείρισης του συστήματος. Για να πραγματοποιηθεί αυτό, όπως γίνεται εύκολα αντιληπτό πρέπει το προσωπικό να είναι κατάλληλα καταρτισμένο και εκπαιδευμένο ώστε να μπορέσει να ανταπεξέλθει. Κρίνεται απαραίτητη η συνεχής εκπαίδευση και επιμόρφωση του προσωπικού σε σχέση με το αντικείμενο της εργασίας αλλά και ζητήματα που απασχολούν το εσωτερικό και το εξωτερικό της επιχείρησης. Ταυτόχρονα χρειάζονται και κάποιες επιβραβεύσεις για τις επιδόσεις του προσωπικού. Είναι ένας τρόπος να εκτιμά η επιχείρηση την αποφυγή λαθών από τους εργαζομένους της.

4.Προσέγγιση βάση διεργασιών. Η τέταρτη αρχή βασίζεται στις διεργασίες. Οι διεργασίες στο εσωτερικό μιας επιχείρησης πρέπει κατά κάποιον τρόπο να συνδέονται μεταξύ τους και να δίνουν απαντήσεις σε ζητήματα που προκύπτουν. Θεμελιώδης ερωτήσεις που βοηθούν την επιχείρηση να αναπτυχθεί είναι:

- Ποιος είναι ο στόχος της επιχείρησης;
- Ποιοι οι πόροι που πρέπει να χρησιμοποιηθούν;
- Ποιοι οι καθοριστικοί για το τελικό αποτέλεσμα παράγοντες;
- Πως προχωρά η διεργασίας;
- Ποιος είναι ο λόγος για τον οποίο διεξάγεται η διεργασία;

- Πως κινείται η διεργασία;
- Πως μπορεί να βελτιωθεί;

Αυτές είναι οι ερωτήσεις που καλείται να απαντήσει το σύστημα διαχείρισης ποιότητας.

5. Προσέγγιση συστήματος διοίκησης. Με αυτήν την αρχή εννοείται ο διαχωρισμός των αρμοδιοτήτων μεταξύ των διαφόρων τμημάτων μιας επιχείρησης. Πέρα από το διαχωρισμό υπάρχει ειδική μέριμνα για τον τρόπο επικοινωνίας και συνεργασίας μεταξύ των διαφόρων τμημάτων. Ο τρόπος με τον οποίο το σύστημα διαχείρισης ποιότητας θα προσεγγίσει την λειτουργία και την επικοινωνία των τμημάτων, είναι καθοριστικός για την αποτελεσματικότητα της επιχείρησης.

6. Προσέγγιση δεδομένων και γεγονότων. Εδώ γίνεται η προσπάθεια του να προσεγγιστούν τα δεδομένα και τα γεγονότα, κατά την διάρκεια λήψης των διαφόρων αποφάσεων της επιχείρησης. Τα δεδομένα που είναι κρίσιμο να καθοριστούν είναι:

- Η ικανοποίηση ή όχι του πελάτη από το τελικό αποτέλεσμα.
- Τα κριτήρια με τα οποία το προϊόν/υπηρεσία κατάφερε ή δεν κατάφερε να συναντήσει τις προσδοκίες του πελάτη.
- Ο κατάλογος των χαρακτηριστικών των προϊόντων και των υπηρεσιών που παρέχονται.
- Τι συμβαίνει στο εξωτερικό περιβάλλον, η σχέση της επιχείρησης με τον ανταγωνισμό της αγοράς.

7. Διαρκής βελτίωση. Είναι η πιο ρητή αρχή της αναθεώρησης του ISO 9001:2000. Η αρχή αυτή δεν υπήρχε στο παλιό πρότυπο. Η επιχείρηση οφείλει να θέτει στο εσωτερικό της ερωτήματα τέτοια σχετικά με την απόδοση και την λειτουργία της που θα την ωθούν να είναι καλύτερη. Για να το καταφέρει αυτό θα πρέπει να εντοπίσει πιθανά σφάλματα και παραλείψεις και να τα διορθώσει. Παράλληλα, θα πρέπει να έχει προβλέψει ενδεχόμενες απειλές. Για να μετρηθούν οι αποδόσεις μιας επιχείρησης το πρότυπο ορίζει κάποιες συγκεκριμένες εφαρμογές: εφαρμογή δειγματοληψίας της αποδοχής, εφαρμογή τεχνικών που λειτουργούν στο στατιστικό έλεγχο καθώς και εφαρμογή τεχνικών βελτίωσης της ποιότητας.

8. Σχέση πελάτη-προμηθευτή. Η όγδοη και τελευταία αρχή είναι αυτή της σχέσης μεταξύ του πελάτη και του προμηθευτή. Ουσιαστικά πρόκειται για την σχέση που

πρέπει να έχει η επιχείρηση με τους διάφορους προμηθευτές της, η οποία οφείλει να είναι επωφελής και για τα δύο μέρη. Το ISO 9001:2000 ορίζει πως η επιχείρηση θα πρέπει να επιλέγει τους προμηθευτές της βάση κριτηρίων και όχι άκριτα. Ακόμα, πρέπει να έχει συγκεκριμενοποιήσει τους στόχους της, βραχυπρόθεσμους και μακροπρόθεσμους, ώστε να τους γνωστοποιήσει στους προμηθευτές της για να κινηθούν ανάλογα. Οφείλει ακόμα να διατηρεί τα κανάλια επικοινωνίας. Τέλος, να καθορίζει στόχους βελτίωσης και για τον προμηθευτή, χρησιμοποιώντας μεθόδους που είδαμε στην έβδομη αρχή, όπως η εφαρμογή της δειγματοληψίας της αποδοχής (Thandapani, K., S.R. Devadasan, C.G. Sreenivasa, & R. Murugesh, 2011).

4.4 ISO 9001:2008

Το ISO 9001:2008 πρόκειται για μία νεότερη αναθεώρηση. Η συγκεκριμένη πιστοποίηση είναι η πιο ευρέως διαδεδομένη στο χώρο των επιχειρήσεων. Η έκδοση αυτή του προτύπου παρουσιάζει μικρές διαφορές με εκείνη του 2000.

Το ISO 9001:2008 καθορίζει απαιτήσεις για την επιχείρηση εκείνη που θέλει να βελτιώσει τον τρόπο με τον οποίο λειτουργεί και να γίνει παραγωγικότερη και αποδοτικότερη. Το συγκεκριμένο ISO απευθύνεται σε επιχειρήσεις και εταιρείες που:

1. Προσπαθούν να αποδείξουν την δυνατότητα τους, να παρέχουν στους πελάτες τους ποιοτικά προϊόντα που μπορούν να καλύψουν τις ανάγκες των πελατών τους, βάση της νομοθεσίας και των κανόνων.
2. Έχουν ως στόχο τους να ικανοποιήσουν τους πελάτες τους. Αυτό το επιτυγχάνουν μέσω της αποτελεσματικής εφαρμογής των διαδικασιών που βελτιώνουν το σύστημα τους. Στοχεύουν πάντα να προσαρμόζονται στις απαιτήσεις τόσο του πελάτη όσο και του κανονιστικού πλαισίου.

Γενικά, μπορούμε να ισχυριστούμε πως το ISO 9001:2008 έχει γενικές αρχές που μπορούν να προσαρμοστούν σε οποιοδήποτε είδος οργανισμού και επιχείρησης.

4.4.1 Αλλαγές IS0 9001:2008 σε σύγκριση με το ISO 9001:2000

Η αναθεωρημένη έκδοση του ISO δεν εμπεριέχει σημαντικές αλλαγές από την προηγούμενη έκδοση του, ωστόσο έχει ακολουθήσει μια διαφορετική προσέγγιση σε διάφορους τομείς. Για παράδειγμα, στο ISO 9001:2008 συμπεριλαμβάνονται εκτός

από τα βασικά αρχεία και άλλα αρχεία που αφορούν στη λειτουργία και τον έλεγχο του συστήματος. Επιπλέον, διασαφηνίζει ποιος πρέπει να είναι ο υπεύθυνος για αυτό το πρότυπο: μέλος της διαχείρισης του οργανισμού. Όσον αφορά τις ευθύνες που προκύπτουν καθώς και τις αρμοδιότητες το ISO 9001:2008 θεωρεί πως όλο το προσωπικό που έχει άμεση ή έμμεση επαφή με το σύστημα διαχείρισης ποιότητας αποκτά ευθύνη. Βέβαια οι ευθύνες αυτές είναι καθορισμένες και παρέχεται ειδική εκπαίδευση γι' αυτό το λόγο στα άτομα αυτά. Μια καινοτομία του πρότυπου αυτού είναι η προσέγγιση του ως προς την εξωτερική ανάθεση σε τρίτα μέρη. Σύμφωνα με τα παραπάνω το πρότυπο θεωρεί πως ακόμα και όταν γίνεται εξωτερική ανάθεση εργασιών σε τρίτους για καλύτερα αποτελέσματα, ο αρχικός οργανισμός έχει την ευθύνη πως οι διεργασίες γίνονται βάση των απαιτήσεων και προτιμήσεων των πελατών. Μια άλλη σημαντική προσθήκη, η οποία δεν υπήρχε στη παλαιότερη έκδοση, είναι πως στις υποδομές ενσωματώθηκαν και τα συστήματα πληροφορικής. Στο τομέα των απαιτήσεων των πελατών υπάρχει μια επίσης σημαντική τροποποίηση: περιλαμβάνονται έννοιες, όπως οι διατάξεις εγγύησης και οι συμπληρωματικές υπηρεσίες (για παράδειγμα, η ανακύκλωση συσκευασιών μετά την κατανάλωση) ,έτσι ώστε να γίνει αντιληπτή η έννοια της «μετά της παράδοσης» απαίτησης των πελατών για την εταιρεία. Τέλος, το ISO 9001:2008 εμπεριέχει και την έννοια της αποδέσμευσης. Τα προϊόντα και οι υπηρεσίες αποδεσμεύονται προς τους πελάτες. Ουσιαστικά υποδεικνύει την ανάγκη τήρησης αρχείων για τον υπεύθυνο κάθε προϊόντος και τα κριτήρια που πρέπει να ικανοποιούνται ώστε να γίνει πραγματικότητα η αποδέσμευση ως προς τους πελάτες (Saleh Ali Husseini, Al-shami, Soo-Fen, & Saif, 2018).

4.5 ISO 9001:2015

Στις 15 Σεπτεμβρίου του 2015 ο οργανισμός ISO εκδίδει την έκδοση ISO 9001:2015 που αποτελεί αναθεώρηση του προτύπου του ISO 9001:2008. Η τελική έκδοση πραγματοποιήθηκε στις 23 Σεπτεμβρίου του ίδιου έτους. Η έκδοση αυτή θα παραμείνει σταθερή για τουλάχιστον 10 χρόνια και εμπεριέχει πολλές διαφορές από τις προηγούμενες.

4.5.1 Οι κύριες αλλαγές του ISO 9001:2015

Γενικά υπάρχουν διαφορετικά είδη προτύπων για διαφορετικά θέματα, όπως για παράδειγμα το ISO 140001 που αφορά την περιβαλλοντική διαχείριση ή το ISO 50001 που έχει να κάνει με την διαχείριση της ενέργειας. Το ISO 9001:2015 φέρνει μια καινοτομία, που ονομάζεται «***Νέα Δομή Προτύπων***» (*High Level Structure*). Η διάσταση αυτή προσπαθεί να φέρει σε επαφή τα κοινά στοιχεία των διαφόρων προτύπων. Επειδή υπάρχουν τόσο διαφορετικές κατηγορίες μεταξύ τους, η «ένωση» αυτή δεν είναι εύκολη, ωστόσο εφαρμόζεται πλέον μια ενιαία δομή στα κεφάλαια, στην ορολογία, στα διάφορα κείμενα των προτύπων ώστε να οδηγηθούμε σε αυτήν την κατεύθυνση. Στο **Πίνακα 1** μπορούμε να δούμε πότε θα πραγματοποιηθεί/πραγματοποιήθηκε αυτή η μετάβαση των προτύπων σε μία ενιαία δομή.

Πρότυπο	Έχει ήδη γίνει η μετάβαση στη Νέα Δομή Προτύπων	Μετάβαση το 2015	Μετάβαση το 2016	Μετάβαση το 2017
ISO 27001	X			
ISO 9001		X		
ISO 14001		X		
ISO 45001 (BS OHSAS 18001)			X	
ISO 22000				X
ISO 22301				
ISO/TS 16949			X	
ISO 50001				X
ISO 13485				

Πίνακας 1: Μετάβαση προτύπων ISO στην Νέα Δομή Προτύπων. (Πηγή: (TÜV HELLAS (TÜV NORD), 2016), σελ 8.)

Με το πρότυπο αυτό εισάγεται μια νέα μορφή ανάλυσης: η ***ανάλυση με βάση την διακινδύνευση*** (*Risk-Based Thinking*). Βασικό στοιχείο στο σημερινό μεταβαλλόμενο περιβάλλον που δραστηριοποιούνται οι επιχειρήσεις είναι να καταφέρνουν να εντοπίζουν τις απειλές και να τις αντιμετωπίζουν με το καλύτερο δυνατό τρόπο. Γι' αυτό το λόγο το πρότυπο αυτό υιοθετεί μεταξύ άλλων την εν λόγω ανάλυση. Πέρα από τον εντοπισμό των απειλών βοηθά και στην ανακάλυψη ευκαιριών. Από τα μεγαλύτερα πλεονεκτήματα της ανάλυσης αυτής είναι πως ο οργανισμός γλυτώνει ουσιαστικά το κόστος προληπτικών ενεργειών.

Θα μπορούσαμε να χαρακτηρίσουμε το ISO 9001:2015 ως το λιγότερο γραφειοκρατικό. Σε αυτήν την έκδοση του προτύπου έχουν καταργηθεί έξι συνολικά διαδικασίες τεκμηρίωσης. Δεν δίνεται βαρύτητα σε έγγραφα και λοιπά αρχεία καθώς προτεραιότητα έχουν ***οι πληροφορίες που μπορούν να τεκμηριωθούν***. Κάθε

οργανισμός, ως διαφορετική οντότητα αποφασίζει μόνος του για το ποια είναι η πληροφορία εκείνη που χρειάζεται να τεκμηριωθεί.

Ένα από τα πιο σημαντικά χαρακτηριστικά αυτής της αναθεώρησης του ISO 9001 είναι η ευχέρεια με την οποία καταφέρνει να συμβαδίζει με την εποχή που διανύουμε. Οι υπηρεσίες βρίσκονται σε έναν ολοένα και πιο ανεπτυγμένο κλάδο και το πρότυπο εστιάζει στο γεγονός αυτό. Πλέον, δεν γίνεται λόγος μόνο για *προϊόντα* αλλά στα κείμενα των ISO συναντάμε τους όρους ***προϊόντα και υπηρεσίες***.

Η βασικότερη έννοια του ISO 9001:2015 είναι αυτή των λεγόμενων «***ενδιαφερομένων μερών***». Σίγουρα η έννοια αυτή υπήρχε και στις παλαιότερες εκδόσεις αλλά είναι άλλο ένα σημείο που η συγκεκριμένη έκδοση αποφασίζει να δώσει έμφαση. Ο οργανισμός παύει να λαμβάνει υπόψη του μόνο τις απαιτήσεις τις νομοθεσίας και των πελατών του. Ξεκινά σε αυτές να συγκαταλέγει τις σχέσεις με τους εργαζόμενους, τα μεσαία διοικητικά στελέχη, τους συνεργάτες, τους προμηθευτές τους καθώς και όλα τα άλλα μέρη που μπορεί σχετίζονται με το σύστημα διαχείρισης ποιότητας από συγγενείς οργανισμούς μέχρι την τοπική οικονομία, προσδίδοντας στην εταιρεία ένα πιο φιλικό προφίλ προς όλα τα ενδιαφερόμενα μέρη.

Η ανάθεση ρόλων και αρμοδιοτήτων έχει αλλάξει ήδη από την προηγούμενη έκδοση, το ISO 9001:2008. Αυτό που συμβαίνει με την τωρινή έκδοση είναι ότι καθιστά πιο σαφή την ευθύνη και την δέσμευση που έχει πλέον η διοίκηση της επιχείρησης. Γι' αυτό το ρόλο του συντονιστή των συστημάτων διαχείρισης ποιότητας αναλαμβάνει μέρος του οργανισμού και όχι μόνο της διοίκησης. Η διοίκηση πλέον έχει μεγαλύτερες αρμοδιότητες. Πρέπει να υπερασπίζεται τον ηγετικό της ρόλο, να φροντίζει για την σωστή επικοινωνία των ενδιαφερόμενων μερών και να κάνει πράξη τον στρατηγικό σχεδιασμό.

Στην εποχή μας, οι επιχειρήσεις γίνονται ολοένα και περισσότερο πελατοκεντρικές. Με την ίδια λογική το ISO 9001:2015 δίνει ***έμφαση στην ικανοποίηση του πελάτη***. Το πρότυπο λοιπόν θέτει βασικές διαδικασίες που πρέπει να ακολουθεί ο οργανισμός ώστε να μετρά εισερχόμενα και εξερχόμενα δεδομένα που σχετίζονται με τον πελάτη. Η επιχείρηση ξέροντας τις ανάγκες του πελάτη βελτιώνει την ποιότητα των εκροών της και γίνεται καλύτερη (TÜV HELLAS (TÜV NORD), 2016).

4.5.2 Σύγκριση ISO 9001:2015 με το ISO 9001:2008

Αν συγκρίνουμε τις δύο τελευταίες χρονολογικά αναθεωρήσεις του προτύπου ISO 9001 θα βρούμε αρκετές διαφορές:

- Σαν κείμενο το ISO 9001:2015 περιέχει περισσότερα στοιχεία και κεφάλαια από το ISO 9001:2008.
- Η έκδοση του 2008 βασίζεται περισσότερο στο πελάτη και την ποιότητα, ενώ εκείνη του 2015 εισάγει την έννοια του κινδύνου και των απειλών και την προσέγγιση που πρέπει να ακολουθούν οι οργανισμοί ώστε να τους επιλύουν.
- Το ISO 9001:2015 δίνει έμφαση στη διαχείριση των πληροφοριών που μπορούν να τεκμηριωθούν ενώ το ISO 9001:2008 είναι περισσότερο γραφειοκρατικό.
- Το ISO 9001:2008 εστιάζει στην ευθύνη της διαχείρισης, ενώ αντιθέτως η έκδοση του 2015 στην ηγεσία και τον σχεδιασμό διαδικασιών.
- Το ISO 9001:2008 μετρά, αξιολογεί και βελτιώνει ενώ το ISO 9001:2015 αξιολογεί την απόδοση ως ξεχωριστή διαδικασία και έπειτα προχωρά προς την βελτίωση.
- Το ISO 9001:2008 περιέχει περισσότερη τυποποίηση ενώ το ISO 9001:2015 μπορεί να γίνει δεκτό από κάθε εταιρεία λόγω της ευελιξίας που διαθέτει (Stojanovic Strahinja, advisera, n.d.).

4.6 Πλεονεκτήματα της χρήσης ISO 9001

Στη διεθνή βιβλιογραφία συναντάμε πολλές μελέτες που αναλύουν τις πιστοποιήσεις ISO 9001 και συγκεντρώνουν τα πλεονεκτήματα που μπορεί να προκύψουν για έναν οργανισμό, όταν κατέχει πιστοποίηση από αυτό το πρότυπο. Μερικά από τα πιο συνήθη πλεονεκτήματα που αναφέρονται είναι:

- Βελτίωση των αποδόσεων της επιχείρησης και των προϊόντων/υπηρεσιών της.
- Βελτίωση της διαδικασίας εργασίας.
- Εμπνευσμένη καθοδήγηση.
- Μείωση λαθών και σφαλμάτων.
- Αύξηση ικανοποίησης πελατών.
- Καλύτερη εξυπηρέτηση πελατών.
- Καλύτερη ενδοεπιχειρησιακή επικοινωνία.

- Μετρήσεις αναφορικά με τις προτιμήσεις των πελατών.
- Καλύτερη εικόνα προς την αγορά.

Υπάρχει μια τάση τα οφέλη από την χρήση του ISO 9001 να χωρίζονται σε εξωτερικά και εσωτερικά. Σαν εσωτερικά οφέλη ορίζονται: η βελτίωση της ποιότητας των προϊόντων και των υπηρεσιών, η μείωση των λαθών στη παραγωγή, η μείωση των εργατικών ατυχημάτων, η βελτίωση της παραγωγικότητας και της αποτελεσματικότητας, μείωση όλων των μορφών εσωτερικού κόστους, το κερδος, η βελτίωση του περιβάλλοντος εργασίας και η καλύτερη εξυπηρέτηση των πελατών. Σαν εξωτερικά οφέλη ορίζονται τα ακόλουθα: η αυξημένη ικανοποίηση του πελάτη, η καλύτερη επικοινωνία με τους προμηθευτές, το άνοιγμα στις διεθνείς αγορές, η αύξηση του μεριδίου αγοράς καθώς και η βελτίωση της εικόνας του οργανισμού στην αγορά (Staines A., 2000).

Κεφάλαιο 5^{ο}: Μελέτη του ISO 27001

5.1. Περιγραφή του ISO 27001

Το ISO 27001 γνωστό και ως IEC 27001 είναι ένα διεθνές πρότυπο που ασχολείται με την ασφάλεια των πληροφοριών που ανταλλάσσουν, αποθηκεύουν, επεξεργάζονται και γενικά διαχειρίζονται τα συστήματα του οργανισμού. Έχει πιστοποιηθεί τόσο από τον οργανισμό ISO όσο και από την IEC (International Electrotechnical Commission). Ανήκει στην ίδια οικογένεια με τα ISO 27000 και 27002. Αυτό που κάνει στην ουσία το συγκεκριμένο πρότυπο είναι να παρέχει όλες τις απαραίτητες κατευθυντήριες γραμμές και τους ελέγχους στην επιχείρηση έτσι ώστε εκείνη να έχει ένα επαρκές σύστημα ελέγχου και ασφάλειας για τις πληροφορίες της. Αφορά επιχειρήσεις κερδοσκοπικές ή μη, κυβερνητικές και εμπορικές οργανώσεις. Για πρώτη φορά το πρότυπο αυτό εκδόθηκε τον Οκτώβριο του 2005, όταν οι επιχειρήσεις άρχισαν να αντιλαμβάνονται πόσο σημαντικός είναι ο τομέας της ασφάλειας των πληροφοριακών τους συστημάτων. Η αναθεώρηση του πραγματοποιήθηκε το 2013. Υπάρχει και μια Ευρωπαϊκή αναθεώρηση του προτύπου που έγινε το 2017. Η πιστοποίηση του προτύπου ISO 27001 είναι εξαιρετικής σημασίας για την επιχείρηση διότι επιβεβαιώνει πως εμπεριέχει όλα τα γνωστά και αναγνωρισμένα πρότυπα ασφάλειας. Το γεγονός αυτό έχει σαν αποτέλεσμα να αποκτηθεί η εμπιστοσύνη των πελατών της καθώς βλέπουν πως η εταιρεία που εμπιστεύονται φροντίζει για την ασφάλεια των δεδομένων τους.

5.1.1 Ιστορική αναδρομή του ISO 27001

Παρα το γεγονός πως το ISO 27001 εκδόθηκε το 2005, το συναντάμε σε διαφορετικές μορφές από την δεκαετία του ’90. Πράγματι, το 1993 ένας επαγγελματικός οργανισμός από την Βρετανία, γνωστός ως National Computing Center (NCC), προχώρησε στην έκδοση ενός αρχείου με τίτλο: «*PD 0003 A Code of Practice for Information Security Management*» το οποίο είχε σχέση με την ασφάλεια στα πληροφοριακά συστήματα που ανταλλάσσουν πληροφορίες. Το Ινστιτούτο Προτύπων της Βρετανίας (BSI) υιοθέτησε το παραπάνω για να μπορέσει να εκδώσει τελικά το 1995 ένα διεθνές πρότυπο, το BS 7799-1 IT—Security techniques— Code of practice for information security management. Ουσιαστικά αυτό το πρότυπο έθεσε

τις γενικές αρχές για ένα μελλοντικό πρότυπο, πιο ολοκληρωμένο. Στη συνέχεια, ακολούθησε ένα συμπληρωματικό μέρος του πρώτου, το BS 7799-2 Information security management systems—Specification with guidance for use. Με αυτήν την προσθήκη πλέον οι επιχειρήσεις μπορούσαν να πιστοποιήσουν την πρόοδο τους στο τομέα της ασφάλειας. Ο ISO χρησιμοποίησε τις αρχές αυτού του προτύπου, το εναρμόνισε με άλλα υφιστάμενα πρότυπα όπως το ISO 9001 για να δημιουργήσει το 2005 το πρότυπο ISO 27001. Με την δημιουργία του τα προηγούμενα πρότυπα αποσύρθηκαν. Ωστόσο το ISO/IEC 27001 περιέχει το Παράρτημα A (*Annex A*), στο οποίο εμπεριέχονται τα σημεία ελέγχου από παλαιότερες εκδόσεις. Οι επιχειρήσεις πλέον πιστοποιούνται για τον τρόπο που διαχειρίζονται τις πληροφορίες που κατέχουν στα συστήματα τους μέσω αυτού του προτύπου που ισχύει για όλες τις χώρες (Georg Disterer, 2013).

5.1.2 Το πρότυπο BS 7799

Το πρότυπο BS 7799:1995 ήταν ένα πρότυπο που εκδόθηκε στην Βρετανία από το BSI Group το 1995 ως κώδικας πρακτικής για την διαχείριση ασφάλειας των πληροφοριών. Το συγκεκριμένο πρότυπο γράφτηκε και εκδόθηκε από το κυβερνητικό τμήμα που αφορούσε το εμπόριο και την βιομηχανία και αποτελούταν από πολλά και διαφορετικά μέρη.

Το πρώτο μέρος περιείχε τις καλύτερες πρακτικές για την διαχείριση ασφάλειας των πληροφοριών αναθεωρήθηκε το 1999 και αποτέλεσε το BS 7799-1:1999. Ο τίτλος του ήταν: *Κώδικας Πρακτικής για διαχείριση ασφάλειας πληροφοριών-Οδηγίες και Συστάσεις*. Ο σκοπός του ήταν να παρέχει οδηγίες σχετικά με την πιο αποτελεσματική πρακτική που μπορούσε να ακολουθήσει ένας οργανισμός στο τομέα που αφορά την διαχείριση της ασφάλειας των πληροφοριών. Ένα δεύτερο μέρος του ίδιου προτύπου που αφορούσε γενικές οδηγίες εκδόθηκε τον ίδιο χρόνο ως BS 7799-2:1999 και προστέθηκε στο πρότυπο. Ο σκοπός του δεύτερου μέρους ήταν ουσιαστικά να είναι ένα μέτρο παρακολούθησης και ένας τρόπος μέτρησης του πρώτου μέρους ενώ ταυτόχρονα θα αποτελούσε και το σημείο αναφοράς για την συγκεκριμένη πιστοποίηση. Ο τίτλος του ήταν: *Συστήματα διαχείρισης ασφάλεια πληροφοριών-Προδιαγραφές με οδηγίες χρήσης*. Αφορούσε τις απαιτήσεις που πρέπει να

ικανοποιούνται από την επιχείρηση στο θέμα της ασφάλειας των πληροφοριών ώστε να καταφέρει να λάβει την ανάλογη πιστοποίηση.

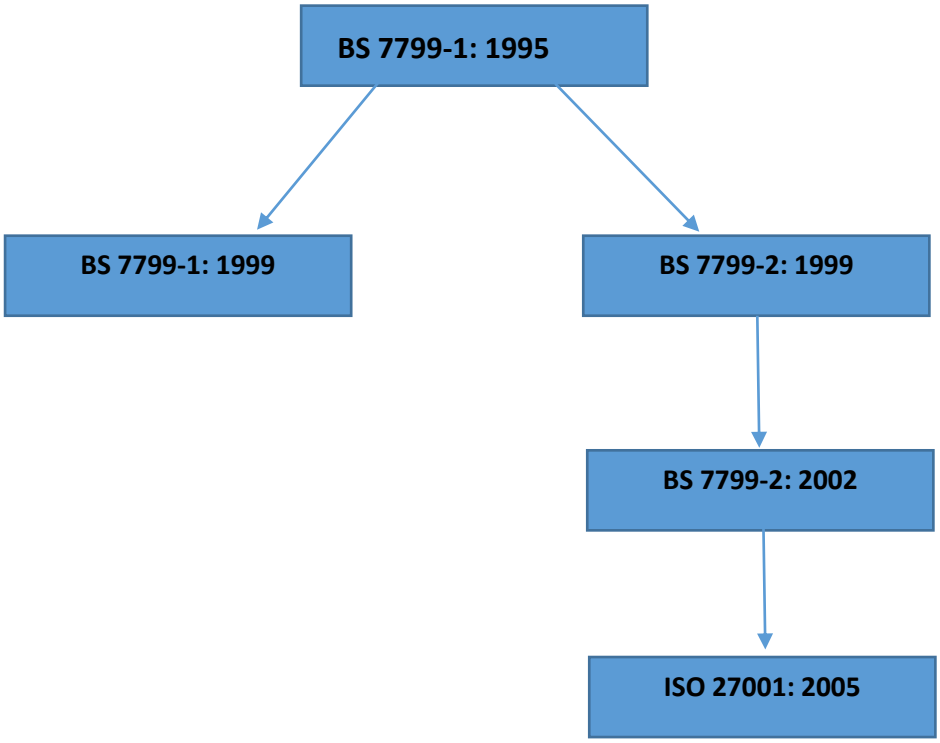
Το σημείο σύνδεσης των δύο προτύπων ήταν πως οι λίστες ελέγχων των δύο μερών ευθυγραμμίζονται μεταξύ τους. Επίσης το δεύτερο μέρος απαιτούσε από το χρήστη να προσπαθήσει να βρει μια λεπτομερή καθοδήγηση που αφορούσε την εφαρμογή των ελέγχων του BS 7799-1:1999.

Το τελευταίο και τρίτο μέρος BS 7799-3 εκδόθηκε το 2005. Αφορά στην ανάλυση κινδύνου και την διαχείριση του και ευθυγραμμίζεται σε αρκετά σημεία με το ISO/IEC 27001.

5.1.3 Από το BS 7799-2:1999 στο ISO/IEC 27001:2005

Για να μπορέσει το πρότυπο BS 7799-2:1999 να συσχετιστεί με τα υπόλοιπα πρότυπα που αφορούσαν την ποιότητα, το 2002 εισήγαγε το μοντέλο διασφάλισης ποιότητας "PDCA" του Demming και έτσι κατάφερε να συσχετιστεί με πρότυπο όπως αυτό της διασφάλισης ποιότητας ISO 9000.

Τρία χρόνια αργότερα το Νοέμβριο του 2005, υιοθετείται το ISO/IEC 27001:2005 που ως διεθνές πρότυπο και αντικαθιστά το BS 7799-2:1999. Ο τίτλος του νέου προτύπου είναι Τεχνολογία πληροφοριών-Τεχνικές ασφάλειας-Συστήματα διαχείρισης ασφάλειας πληροφοριών. Το νέο πρότυπο πληροί όλα τα κριτήρια έτσι ώστε να μπορέσει ένας οργανισμός να λάβει την πιστοποίηση για ασφάλεια στο τομέα των δεδομένων και των υπηρεσιών (Dey.M, 2007). Στο **Διάγραμμα 1** που ακολουθεί γίνεται μια προσπάθεια να παρουσιαστεί η ιστορική εξέλιξη που ακολουθήθηκε από το αρχικό πρότυπο μέχρι και το διεθνές πρότυπο ISO 27001:2005.



Διάγραμμα 1: Ιστορική εξέλιξη του ISO 27001:2005

5.1.4 Η οικογένεια των ISO 27000

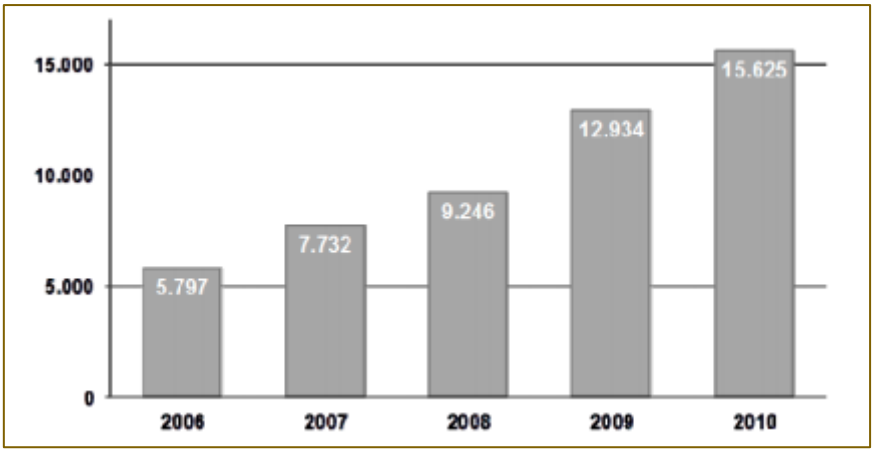
Το πρότυπο ISO 27001 είναι ένα κομμάτι μιας μεγάλης κατηγορίας προτύπων που έχουν να κάνουν με την ασφάλεια των πληροφοριακών συστημάτων, την οικογένεια του ISO 27000. Η οικογένεια αυτή αποτελείται από 69 πρότυπα καθένα από τα οποία έχει να προσθέσει το δικό του κομμάτι, την δική του πτυχή στο τομέα της ασφάλειας των πληροφοριών και των δεδομένων. Τα πιο σημαντικά από αυτά είναι 6, μεταξύ των οποίων και το ISO 27001 που μας ενδιαφέρει σε αυτήν την εργασία. Από το σύνολο αυτών των 6, 2 από αυτά είναι *Τύπου Α* κάτι που σημαίνει πως περιέχουν απαιτήσεις για την πιστοποίηση ενώ τα υπόλοιπα 4 λογίζονται ως *Τύπου Β*, δηλαδή πως παρέχουν γενικές οδηγίες και κατευθυντήριες γραμμές. Στο **Πίνακα 2** μπορούμε να δούμε αυτά τα 6 πρότυπα και πως διαχωρίζονται στις κατηγορίες. Το σημαντικό στοιχείο είναι πως το ISO 27001 είναι *Τύπου Α* κάτι που σημαίνει πως περιέχει απαιτήσεις. Ίδιου τύπου άλλωστε είναι και το ISO 27552 που βρίσκεται ακόμα υπό έκδοση (itgovernance, 2020).

Πρότυπο ISO	Τίτλος	Τύπος	Έκδοση
27001	Τεχνικές ασφάλειας-Διοίκηση Ασφάλειας Πληροφοριακών Συστημάτων	**A**	2013
27003	Τεχνικές ασφάλειας-Διοίκηση Ασφάλειας Πληροφοριακών Συστημάτων	**B**	2017
27010	Διοίκηση Ασφάλειας για διακλαδικές και οργανωτικές διαβιβάσεις	**B**	2016
27013	Οδηγίες για την εφαρμογή των ISO 27001 και 27000	**B**	2015
27014	Τεχνικές ασφάλειας σε Κυβερνητικό επίπεδο	**B**	2013
27552	Τεχνικές ασφάλειας για βελτίωση της ασφάλειας απορρήτου στις τακτικές του ISO 27001	**A**	Δεν έχει εκδοθεί

Πίνακας 2: Τα 6 πιο σημαντικά ISO της οικογένειας ISO 27000. (Πηγή: (itgovernance, 2020)).

5.2 ISO 27001: Η παγκόσμια διάδοση

Το συγκεκριμένο πρότυπο γνωρίζει μεγάλη διάδοση. Το τέλος του 2010 είχαν εκδοθεί σε όλο τον κόσμο 15.625 πιστοποιήσεις. Η μεγαλύτερη διάδοση του συνέβη την τριετία 2006-2010. Σύμφωνα με έρευνες το πρότυπο οφείλει αυτή την διάδοση του στη δυνατότητα που δίνει στις επιχειρήσεις να μετατρέψουν τις παλαιότερες εκδόσεις των προτύπων που ακολουθούσαν στη μορφή του συγκεκριμένου. Στην **Εικόνα 3** μπορούμε να δούμε πως κινήθηκε ο αριθμός την συγκεκριμένη χρονική περίοδο για την οποία υπάρχουν τα στοιχεία. Η πορεία που ακολουθούν οι πιστοποιήσεις είναι αυξητική καθώς ολοένα και περισσότερες επιχειρήσεις σπεύδουν να πιστοποιηθούν με το συγκεκριμένο πρότυπο ώστε να ακολουθούν το γράμμα του νόμου και να έχουν αφοσιωμένους πελάτες.



Εικόνα 3: Αριθμός πιστοποιήσεων ISO 27001 την περίοδο 2006-2010. (Πηγή: (Georg Disterer, 2013)

Ενδιαφέρον παρουσιάζει η κατανομή των πιστοποιήσεων ανά γεωγραφική περιοχή. 7.000 περίπου πιστοποιήσεις αφορούσαν την Ιαπωνία. Αυτό το γεγονός προκλήθηκε από τις νομικές αρχές της χώρας που στις περισσότερες περιπτώσεις των επιχειρήσεων ζητούν να υπάρχει πιστοποίηση των συστημάτων ασφαλείας μέσω τέτοιων προτύπων. Πέρα από την Ιαπωνία, οι περισσότερες πιστοποιήσεις ISO 27001 δόθηκαν στις χώρες της Ασίας. Η εξήγηση αυτού του φαινομένου είναι απλή. Πολλές χώρες της Ευρώπης αλλά και της Βόρειας Αμερικής προσπαθούν να μειώσουν το κόστους τους αναθέτοντας σε τρίτα μέρη την διαχείριση των πληροφοριακών τους συστημάτων. Πολλές επιχειρήσεις πληροφορικής στην Ασία, που δεν είναι ιδιαιτέρως γνωστές στο Δυτικό κόσμο, προσπαθούν να εκμεταλλευτούν αυτήν την ευκαιρία. Για να αποκτήσουν αναγνωρισιμότητα και να κάνουν τις επιχειρήσεις της Δύσης να τις εμπιστευτούν στρέφονται στη διεκδίκηση πιστοποιήσεων του ISO 27001. Υπάρχει ακόμα ένα ενδιαφέρον στοιχείο στην έρευνα της (Deloitte, 2020). Μόνο 329 τέτοιες πιστοποιήσεις εκδόθηκαν για επιχειρήσεις και οργανισμούς της Βόρειας Αμερικής. Πράγματι, υπάρχει μια φιλοσοφία στο επιχειρηματικό κόσμο της άλλης πλευράς του πλανήτη που δεν στηρίζει την αξιοπιστία των επιχειρήσεων του μέσω αυτών των προτύπων. Σε αντίθεση, στην Ευρώπη μόνο το Ηνωμένο Βασίλειο είχε φτάσει τις 1.157 πιστοποιήσεις. Ο αριθμός αυτός είναι αρκετά μεγάλος και αποτελεί απόρροια του γεγονότος πως στην Αγγλία ξεκίνησαν οι πρώιμες μορφές που οδήγησαν έπειτα στην γέννηση του ISO 27001.

5.2.1 Διάδοση του ISO 27001:2013

Το IS0 27001:2013 αποτελεί την πρώτη αναθεώρηση του συγκεκριμένου τύπου ISO. Σε έρευνα που πραγματοποιήθηκε από τον ίδιο τον οργανισμό ISO για το έτος 2018 μετρήθηκαν οι πιστοποιήσεις για το πρότυπο ασφάλειας των πληροφοριακών συστημάτων σε 25 χώρες από όλον τον κόσμο. Στην **Εικόνα 4** φαίνονται αυτά τα αποτελέσματα.

ISO 27001:2013					
Country		Valid Certification	Country		Valid Certification
1	China	7,199	16	Israel	439
2	Japan	5,093	17	Korea (Republic of)	353
3	United Kingdom of Great Britain and Northern Ireland	2,444	18	Bulgaria	339
4	India	2,161	19	Malaysia	276
5	Germany	1,057	20	Australia	264
6	Italy	1,041	21	Greece	240
7	United States of America	911	22	Thailand	239
8	Taiwan, Province of China	827	23	France	223
9	Netherlands	788	24	Serbia	223
10	Spain	726	25	Mexico	218
11	Turkey	707			
12	Poland	700			
13	Romania	585			
14	Czech Republic	543			
15	Hungary	484			

Εικόνα 4: Αριθμός πιστοποιήσεων έκδοσης ISO 27001:2013 σε 25 χώρες του κόσμου (Πηγή: (ISO - International Organisation for Standardisation, 2019))

Σε σύγκριση με την προηγούμενη έρευνα του απλού ISO 27001 βλέπουμε πως η Ιαπωνία είναι σταθερά σε υψηλή θέση αλλά έχει παραδώσει τα πρωτεία στη Κίνα. Ένα σημάδι πως οι Κινέζοι έχουν επενδύσει στο τομέα της πληροφορικής και θέλουν να εξασφαλίσουν την εμπιστοσύνη των διεθνών πελατών τους, γι αυτό και έχουν τις περισσότερες πιστοποιήσεις (7,199). Το Ηνωμένο Βασίλειο, όπως έχουμε δει ξανά, λόγω της ιδιαίτερης ιστορίας του με το συγκεκριμένο πρότυπο βρίσκεται στη τρίτη θέση. Με λιγότερες πιστοποιήσεις από τις χώρες της Ασίας, μόλις 911, οι Ηνωμένες Πολιτείες Αμερικής καταφέρνουν να κατακτήσουν την έβδομη θέση. Ο αριθμός είναι σαφώς μεγαλύτερος από τις 329 πιστοποιήσεις της περιόδου 2006-2010 που μπορεί να ερμηνευθεί βάση δύο στοιχείων: α) ο αριθμός θα μπορούσε να είναι ακόμα μεγαλύτερος αλλά οι Αμερικανικές επιχειρήσεις επενδύουν στο τομέα των πληροφοριών σε αναθέσεις σε τρίτους, κυρίως αναδυόμενων επιχειρήσεων της

Ανατολής β) ξεκινά μια στροφή των Αμερικανικών επιχειρήσεων στα πρότυπα ISO. Ένα άλλο ενδιαφέρον στοιχείο είναι πως η Ελλάδα βρίσκεται στη 21^{η} θέση με 264 πιστοποιήσεις ξεπερνώντας την Γαλλία που κατέχει την 23^{η} θέση (ISO - International Organisation for Standardisation, 2019).

5.3 Το περιεχόμενο του ISO 27001

Το ISO 27001 είναι γενικό από την άποψη πως απευθύνεται σε επιχειρήσεις οποιοδήποτε τύπου και μεγέθους. Στις σελίδες του περιγράφονται όλες εκείνες οι προϋποθέσεις που πρέπει να τηρεί μια επιχείρηση ώστε να καταφέρει να αποκτήσει την πιστοποίηση. Το πιο σημαντικό σημείο του προτύπου αποτελεί η προϋπόθεση για τον σχεδιασμό, την εκτέλεση, την λειτουργία και την συνεχή επίβλεψη και βελτίωση της διαδικασίας που έχει ως στόχο της τα πληροφοριακά συστήματα διαχείρισης ασφάλειας. Ουσιαστικά, πρόκειται για ένα κύκλο (μέθοδο management) που στη διεθνή βιβλιογραφία ονομάζεται *PDCA* από τα αρχικά των λέων *Plan* (*Σχεδιάζω*), Do (*Κάνω*), *Check* (*Ελέγχω*), *Act* (*Ενεργώ*). Ο κύκλος αυτός στη διαδικασία της πιστοποίησης για το ISO 27001 έχει ως εξής:

Plan-Καθιέρωση του συστήματος διαχείρισης ασφάλειας των πληροφοριών:

- Προσδιορισμός των σημαντικών πληροφοριών που κατέχει ο οργανισμός και πως αυτές συνδέονται με τις προϋποθέσεις ασφάλειας.
- Εκτίμηση των ρίσκων ασφαλείας που υπάρχουν στις πληροφορίες.
- Επιλογή τρόπων διαχείρισης των κινδύνων που μπορεί να προκύψουν χωρίς να το αναμένει η επιχείρηση.

Do-Εκτέλεση και λειτουργία του συστήματος:

- Εκτέλεση ελέγχου.
- Διαχείριση λειτουργιών.

Check-Έλεγχος και ανασκόπηση του συστήματος:

- Έλεγχος της εκτέλεσης.
- Εκτίμηση της εκτέλεσης.

Act-Διατήρηση και βελτίωση του συστήματος:

- Διόρθωση δράσεων όπου το απαιτούν.
- Προληπτικές ενέργειες.

Ο κύκλος αυτός λοιπόν επαναλαμβάνεται συνεχώς ώστε να εντοπίζονται οι πιθανοί κίνδυνοι και να αντιμετωπίζονται αποτελεσματικά την στιγμή που πρέπει. Συγκεκριμένα υπάρχουν 39 στόχοι ελέγχου που πρέπει να επιτύχει μια επιχείρηση και 134 μετρικές για διαχείριση ασφάλειας. Για παράδειγμα, στο χώρο της ασφάλειας των Ανθρωπίνων Πόρων ένας από τους στόχους ελέγχου είναι να εξασφαλιστεί πως οι εργαζόμενοι, οι εργολάβοι καθώς και τα τρίτα μέρη αντιλαμβάνονται πλήρως τις αρμοδιότητες τους, είναι ικανοί για τους ρόλους που τους έχουν ανατεθεί και περιορίζουν στα όρια του δυνατού την πιθανότητα κλοπής και απάτης. Οι κυριότερες κατηγορίες στις οποίες εφαρμόζεται το πρότυπο αυτό είναι:

- Πολιτική ασφάλειας.
- Οργάνωση ασφάλειας της πληροφορίας.
- Διαχείριση περιουσιακών στοιχείων.
- Ασφάλεια τομέα Ανθρώπινων Πόρων.
- Φυσική και περιβαλλοντική ασφάλεια.
- Διοίκηση λειτουργιών και επικοινωνίας.
- Αξιολόγηση ελέγχου.
- Απόκτηση, ανάπτυξη και συντήρηση πληροφοριακών συστημάτων.
- Ασφάλεια πληροφοριών και διαχείριση συμβάντων.
- Διαχείριση επιχείρησης.
- Συμμόρφωση.

Αξίζει να σημειωθεί πως όλοι αυτοί οι στόχοι αναπτύσσονται περαιτέρω μέσω του ISO 27002. Στο **Πίνακα 2** παρουσιάζονται όλοι αυτοί οι στόχοι και τα αντικείμενα τους.

Θέμα	**Αντικείμενο Ελέγχου**
Πολιτική ασφάλειας	Παροχή κατευθυντήριων γραμμών στη διοίκηση και υποστήριξη στο τομέα ασφάλειας των πληροφοριών όπως ορίζει το καταστατικό της εταιρείας και οι κανονισμοί εκτός αυτής.
Οργάνωση ασφάλειας πληροφορίας	Διαχείριση της ασφάλειας μέσα στην επιχείρηση. Διατήρηση της ασφάλειας των πληροφορίων που έχει η επιχείρηση όταν επικοινωνεί και ανταλλάσσει στοιχεία με τρίτα μέρη.
Διαχείριση περιουσιακών στοιχείων	Η επιτυχία και η διατήρηση της προστασίας των περιουσιακών στοιχείων της επιχείρησης. Επιπλέον, η εξασφάλιση του γεγονότος πως οι πληροφορίες προστατεύονται επαρκώς.
Ασφάλεια τομέα ανθρωπίνων πόρων	Εξασφάλιση πως οι εργαζόμενοι, εργοδότες και τρίτα μέρη γνωρίζουν για τις απειλές που διατρέχουν τις πληροφορίες τους, ποιες είναι οι δικές τους ευθύνες αλλά και τα δικαιώματα τους.
Ασφάλεια φυσική και περιβαλλοντική	Η απαγόρευση της φυσικής εισόδου χωρίς ταυτοποίηση στα πληροφοριακά συστήματα της επιχείρησης και η παρεμπόδιση δημιουργίας ζημιών. Επίσης, η απαγόρευση κλοπής στοιχείων της επιχείρησης ή διακοπής της εύρυθμης λειτουργίας της.
Διοίκηση λειτουργιών και επικοινωνίας	Περιορισμός εμφάνισης σφαλμάτων στα πληροφοριακά συστήματα. Επιβεβαίωση πως οι πληροφορίες προστατεύονται επαρκώς. Διατήρηση της προσβασιμότητας στις πληροφορίες από τα μέλη της επιχείρησης αλλά και τους πελάτες που τους αφορούν. Η διατήρηση ασφάλειας στα ηλεκτρονικά συστήματα και η ανίχνευση απειλών από κακόβουλα

	λογισμικά. Η ανακάλυψη προσπαθειών πρόσβασης στο σύστημα τρίτων μερών που δεν ανήκουν στους πιστοποιημένους χρήστες των συστημάτων ή πελατών της επιχείρησης.
Αξιολόγηση ελέγχου	Να υπάρχει έλεγχος στις πληροφορίες, να υπάρχει πρόσβαση μόνο σε πιστοποιημένους χρήστες και να απαγορεύεται στους μη πιστοποιημένους. Να αποτρέψει την πρόσβαση σε μη πιστοποιημένους χρήστες στις πληροφορίες ή τις προσπάθειες τους να κλέψουν ή να προκαλέσουν αλλοίωση στα δεδομένα αυτά. Να αποτρέψει στα άτομα αυτά να ελέγχουν τα συστήματα πληροφοριών. Να υπάρχει εξασφάλιση πως οι πληροφορίες που διαμοιράζονται μέσω κινητών υπολογιστών και γενικώς καταστάσεων τηλεργασίας δεν πρόκειται να αντιμετωπίσουν απειλές ως προς τα δεδομένα προσωπικού χαρακτήρα.
Απόκτηση, ανάπτυξη και συντήρηση πληροφοριακών συστημάτων	Να υπάρχει διασφάλιση πως η ασφάλεια των πληροφοριών είναι κομμάτι του συστήματος πληροφοριών της εταιρείας. Να περιοριστούν απώλειες, αλλοιώσεις, μη γνωστές τροποποιήσεις πληροφοριών στις εφαρμογές. Να εξασφαλιστεί η αυθεντικότητα και η εμπιστευτικότητα όσον αφορά τα δεδομένα με χρήση δεδομένων κρυπτογράφησης. Να περιοριστούν στο όριο του δυνατού απειλές και ρίσκα που προέρχονται από τυχόν τεχνικά σφάλματα κατά την δημοσίευση των πληροφοριών.
Ασφάλεια πληροφοριών και διαχείριση συμβάντων	Εξασφάλιση πως όποιο συμβάν έχει σχέση με διαρροή πληροφοριών σε τρίτα μέρη ή αλλοιώσεις αυτών κοινοποιείται στα πληροφοριακά συστήματα του οργανισμού έτσι ώστε να γίνουν οι κατάλληλες διορθωτικές κινήσεις.
Διαχείριση επιχείρησης	Αντιμετώπιση τυχόν διακοπών που μπορεί να συμβούν στις διαδικασίες της επιχείρησης καθώς και

	αποτυχίες των συστημάτων πληροφορίας ώστε να μην υπάρξει επανάληψη τους.
Συμμόρφωση	Αποφυγή από μεριάς της επιχείρησης παραβιάσεων των νόμων και των κανονισμών αλλά και των απαιτήσεων ασφάλειας. Συμμόρφωση με τις πολιτικές και τα πρότυπα ασφάλειας. Μεγιστοποίηση της αποτελεσματικότητας και ελαχιστοποίηση παρεμβολών κατά την διαδικασία ελέγχου των πληροφοριακών συστημάτων.

Πίνακας 3: Οι στόχοι των ελέγχων του ISO 27001.

Μέσω του πίνακα βλέπουμε πως πολλοί από τους στόχους είτε επιτελούν την ίδια διαδικασία, είτε είναι αλληλοσυμπληρούμενοι. Εξετάζουν εξονυχιστικά κάθε λεπτομέρεια ώστε να παρέχουν την μέγιστη δυνατή ασφάλεια στα δεδομένα των πληροφοριακών συστημάτων της επιχείρησης.

Για να μπορέσει μέλος της επιχείρησης να εφαρμόσει αυτούς του στόχους και ελέγχους χρειάζεται η απαραίτητη εκπαίδευση. Η συμβατότητα των πράξεων με τις κατευθυντήριες γραμμές του προτύπου πρέπει να ελέγχεται συνεχώς, επομένως το άτομο που ασκεί τον έλεγχο καθίσταται σαφές πως πρέπει να είναι κατάλληλα εκπαιδευμένο όσον αφορά τους στόχους που πρέπει να ελέγχει. Πέρα από τον έλεγχο τα άτομα αυτά θα κληθούν να βελτιώσουν τους στόχους. Έπειτα πρέπει να είναι προσεχτικοί ώστε να παρατηρούν που μπορεί να προκύψουν κίνδυνοι και να προσπαθήσουν να τους αποφύγουν. Ανάμεσα στα άλλα καθήκοντα τους είναι: η υιοθέτηση μιας πολιτικής ασφάλειας για τον οργανισμό, ο καθορισμός ρόλων και αρμοδιοτήτων για το κάθε μέλος της επιχείρησης ξεχωριστά, η πρόσληψη καινούργιου προσωπικού και η παροχή κατάλληλης εκπαίδευσης και τέλος οι αποφάσεις που πρέπει να παρθούν σε καταστάσεις κινδύνου (ISO 27001, 2005).

5.4 Διαδικασία πιστοποίησης

Στη προσπάθεια της η επιχείρηση να αποδείξει πως το πληροφοριακό της σύστημα είναι συμβατό με το ISO 27001 πρέπει να υποβληθεί σε μια διαδικασία πιστοποίησης. Κανένας οργανισμός δεν κατέχει οποιοδήποτε πρότυπο ISO εάν πρώτα δεν έχει πραγματοποιηθεί η πιστοποίηση. Την διαδικασία αυτή εκτελεί ένας αναγνωρισμένος οργανισμό για αυτήν την περίπτωση (*Registered Certification Bodies- RCB*). Ο ISO παρέχει στους πελάτες τους μια λίστα με τέτοιους οργανισμούς ώστε να μπορέσουν να επιλέξουν. Για να ξεκινήσει η διαδικασία πιστοποίησης η επιχείρηση που θέλει να αποκτήσει την πιστοποίηση πρέπει να υποβάλλει αίτηση στον αντίστοιχο οργανισμό που έχει επιλέξει από την λίστα. Η πρώτη κίνηση που κάνει ένα RCB αφού επιλεγεί είναι να δει σε ποια έκταση η επιχείρηση που ήρθε σε επαφή μαζί του πληροί ήδη κάποιες από τις προϋποθέσεις του προτύπου. Έπειτα ακολουθεί η διαδικασία συμμόρφωσης των υπόλοιπων στοιχείων της επιχείρησης σύμφωνα με τις προϋποθέσεις και τους στόχους που θέτει το ISO 27001. Σε αρκετές περιπτώσεις μπορεί να κληθούν και εμπειρογνώμονες, ώστε να υπάρχει σιγουριά πως οι πληροφορίες της επιχείρησης θα καλύπτονται από την μέγιστη δυνατή ασφάλεια.

Η πρώτη φάση περιλαμβάνει τον έλεγχο όλων των εγγράφων που είναι απαραίτητα για την πιστοποίηση από το RCB. Τα έγγραφα αυτά είναι συνήθως η πολιτική ασφάλειας, κανόνες διαχείρισης της επιχείρησης, περιγραφές των διαδικασιών που εκτελούνται, εκτιμήσεις επικινδυνότητας για την επιχείρηση, οι ορισμοί των διαδικασιών που έχουν σχέση με την ασφάλεια καθώς και οι οδηγίες εφαρμογής τους. Η διαδικασία αυτή είναι πολύ σημαντική καθώς τα έγγραφα θα αποσταλούν στον οργανισμό πιστοποίησης. Αφού οι ελεγκτές από την πλευρά του οργανισμού πιστοποίησης πραγματοποιήσουν τον έλεγχο των εγγράφων ξεκινά η δεύτερη φάση. Οι ελεγκτές αυτήν την φορά επισκέπτονται το φυσικό χώρο της επιχείρησης για επιτόπιο έλεγχο. Κατά την διάρκεια της επίσκεψης μπορούν να αντιληφθούν σε ποιον βαθμό η επιχείρηση ακολουθεί τους κανόνες ασφαλείας που ορίζει το πρότυπο. Έπειτα συντάσσουν μια έκθεση σύμφωνα με την οποία θα αποφασιστεί εάν ο έλεγχος ήταν επιτυχής ή όχι. Στη περίπτωση που η απάντηση είναι θετική ο ISO ετοιμάζει το Πιστοποιητικό του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών ISO 27001 και το παραδίδει στην εταιρεία που εκδήλωσε το ενδιαφέρον. Οι αναθεωρήσεις του προτύπου ανάλογα με το αίτημα που έχει κάνει η επιχείρηση, πραγματοποιούνται μία με δύο φορές το χρόνο. Το συγκεκριμένο πρότυπο διαρκεί για τρία έτη. Όταν

περάσουν τα τρία έτη είναι απαραίτητο να γίνουν μελέτες εκ νέου για την πιστοποίηση ενώ το πιστοποιητικό θα ανανεωθεί (Leal Rhand, 2018).

5.4.1 Παράδειγμα αίτησης για το ISO 27001

Σε αυτήν την ενότητα έχουμε την δυνατότητα να δούμε πως είναι δομημένη η αίτηση που οφείλει να υποβάλει μια επιχείρηση στην χώρα μας ώστε να περάσει τους απαραίτητους ελέγχους και να καταφέρει να πιστοποιηθεί με το ISO 27001. Η αίτηση υπήρχε σαν παράρτημα στην διαδικτυακή σελίδα της BQC (Business Quality Certification) που αποτελεί ένα φορέα πιστοποίησης. Όπως μπορούμε να δούμε από το **Πίνακα 3** η αίτηση χωρίζεται ουσιαστικά σε τρία μέρη:

1. Το πρώτο μέρος είναι γενικές πληροφορίες για τον οργανισμό. Η επωνυμία του οργανισμού, το όνομα του υπευθύνου για την διαχείρισης της ασφάλειας των πληροφοριών. Έπειτα αυτό το κομμάτι συνεχίζει με το αν εργάζονται άτομα απομακρυσμένα, ζητά πληροφορίες για τις εγκαταστάσεις και το είδος δραστηριοποίησης του οργανισμού.
2. Το δεύτερο μέρος γίνεται περισσότερο συγκεκριμένο. Εδώ γίνεται αναφορά για την δραστηριοποίηση και τον τρόπο οργάνωσης της επιχείρησης. Για παράδειγμα, αν ο τομέας στον οποίο ασκεί δραστηριότητα ο οργανισμός είναι τόσο κρίσιμος ώστε μια πιθανή απροσεξία να επηρεάσει όχι μόνο την επιχείρηση αυτή καθαυτή αλλά και την οικονομία ή την υγεία σε διεθνές επίπεδο. Αντιλαμβανόμαστε πως στόχος του ISO 27001 είναι όχι μόνο να προστατέψει την επιχείρηση απέναντι στους πελάτες της αλλά να φροντίσει για την έρρυθμη λειτουργία της απέναντι στο κράτος ώστε να μην προκύψουν αυστηρές συνέπειες σε περίπτωση εκδήλωσης κάποιου συμβάντος.
3. Στο τρίτο και τελευταίο μέρος γίνεται μια προσπάθεια μέτρησης των παραγόντων που σχετίζονται με το περιβάλλον πληροφορικής (IT) της επιχείρησης. Για παράδειγμα, πόσο συχνά χρησιμοποιεί ο οργανισμός πληροφοριακά συστήματα κατά την διάρκεια σημαντικών δραστηριοτήτων (BQC-Business Quality Certification, n.d.).

ΠΛΗΡΟΦΟΡΙΕΣ ΟΡΓΑΝΙΣΜΟΥ			
Επωνυμία Οργανισμού:			
Υπεύθυνος Διαχείρισης Ασφάλειας Πληροφοριών:			
Εργάζεται προσωπικό του Οργανισμού απομακρυσμένα; Αν ναι, πόσα άτομα;	Ναι ☐ Όχι ☐		
Υπάρχουν προσωρινές εγκαταστάσεις όπου δραστηριοποιείται ο Οργανισμός; Αν ναι, παρακαλώ αναφέρετε τοποθεσία και είδος δραστηριότητας:		Ναι ☐	Όχι ☐
Διαθέτει ο Οργανισμός επιπλέον εγκαταστάσεις (υποκαταστήματα); Αν ναι, παρακαλώ αναφέρετε τοποθεσία και αριθμό εργαζομένων:		Ναι ☐	Όχι ☐
Υλοποιείται μέρος του πεδίου δραστηριότητας που υπόκειται στην πιστοποίηση σε κάποια και όχι σε όλα τα ανωτέρω υποκαταστήματα; Αν ναι, σε ποια:		Ναι ☐	Όχι ☐
Υπάρχουν αρχεία του ΣΔΑΠ τα οποία, παρά το γεγονός ότι οι επιθεωρητές υπόκεινται σε κώδικα εμπιστευτικότητας, δεν μπορούν να διατεθούν προς ανασκόπηση στην ομάδα επιθεώρησης διότι περιέχουν εμπιστευτικές ή ευαίσθητες πληροφορίες; Αν ναι, παρακαλώ αναφέρετε:		Ναι ☐	Όχι ☐
ΔΡΑΣΤΗΡΙΟΠΟΙΗΣΗ ΚΑΙ ΟΡΓΑΝΩΣΗ ΤΟΥ ΟΡΓΑΝΙΣΜΟΥ			
Δραστηριοποιείται ο Οργανισμός σε αυστηρά νομοθετημένο ή κρίσιμο τομέα, τέτοιον ώστε μία αστοχία θα μπορούσε να επηρεάσει την ασφάλεια, την υγεία ή την οικονομία σε εθνικό επίπεδο;		Ναι ☐	Όχι ☐
Υπάρχουν πελάτες του Οργανισμού που δραστηριοποιούνται σε αυστηρά νομοθετημένο ή κρίσιμο τομέα, τέτοιον ώστε μία αστοχία θα μπορούσε να επηρεάσει την ασφάλεια, την υγεία ή την οικονομία σε εθνικό επίπεδο;		Ναι ☐	Όχι ☐
Εκτελεί μεγάλο μέρος των εργαζομένων του Οργανισμού την ίδια εργασία; Αν ναι, πόσα άτομα;		Ναι ☐	Όχι ☐
ΠΑΡΑΓΟΝΤΕΣ ΠΟΥ ΣΧΕΤΙΖΟΝΤΑΙ ΜΕ ΤΟ ΙΤ ΠΕΡΙΒΑΛΛΟΝ ΤΟΥ ΟΡΓΑΝΙΣΜΟΥ			
Ο Οργανισμός χρησιμοποιεί πλατφόρμες πληροφορικής, διακομιστές, λειτουργικά συστήματα, βάσεις δεδομένων, δίκτυα, κλπ.	☐	λίγες και όμοιες	
	☐	αρκετές διαφορετικές	
	☐	πολλές διαφορετικές	
Ο Οργανισμός εξαρτάται από υπεργολάβους/ προμηθευτές σε σημαντικές του δραστηριότητες.	☐	καθόλου ή λίγο	
	☐	μερικώς	
	☐	πλήρως	
Ο Οργανισμός χρησιμοποιεί πληροφοριακά συστήματα σε σημαντικές δραστηριότητες που ο ίδιος ή υπεργολάβοι του έχουν αναπτύξει.	☐	καθόλου ή λίγο	
	☐	μερικά	
	☐	εκτεταμένως	

Πίνακας 4: Παράδειγμα αίτησης για πιστοποίηση ISO 27001.

5.4.2 Μελέτη ανάλυσης κινδύνου (Risk analysis)

Για να μπορέσει να εφαρμοστεί σε μια εταιρεία/επιχείρηση το ISO 27001 είναι ανάγκη να εφαρμοστεί πρώτα μια μελέτη που θα μπορέσει να εντοπίσει τα αδύναμα σημεία της επιχείρησης, τις απειλές και τους κινδύνους από το περιβάλλον της εσωτερικό και εξωτερικό και να κάνει προβλέψεις για τις επιπτώσεις που θα έχουν αυτοί οι κίνδυνοι στην πορεία της. Γι'αυτό το λόγο είναι σημαντικό να εκπονηθεί εκ των προτέρων μια μελέτη ανάλυσης κινδύνων. Τα δύο σημαντικά στοιχεία της ανάλυσης κινδύνου είναι:

1. **Προσδιορισμός των απειλών:** απειλές από το ίδιο το σύστημα, τους εργαζομένους, τρίτα μέρη, κακόβουλα λογισμικά κλπ.
2. **Εκτίμηση πιθανού ρίσκου:** όταν έχουν εντοπιστεί οι απειλές και οι κίνδυνοι το επόμενο βήμα είναι να δούμε ποιες θα είναι οι συνέπειες από την εκδήλωση ενός τέτοιου συμβάντος στον οργανισμό της επιχείρησης. Η τιμή αυτού του ρίσκου μπορεί να υπολογιστεί με το παρακάτω τύπο:

$$\textbf{\textit{Τιμή κινδύνου}}: \textbf{\textit{Πιθανότητα εμφάνισης κινδύνου}} * \textbf{\textit{Κόστος κινδύνου}}$$

Με τον υπολογισμό αυτών των δύο στοιχείων μπορεί η επιχείρηση να συνεχίσει την ανάλυση της (Terje Aven, 2015).

Αυτός ο έλεγχος ξεκινά με μια λεπτομερή απογραφή των πληροφοριακών περιουσιακών στοιχείων που κατέχει η επιχείρηση που έκανε την αίτηση για την πιστοποίηση. Τα στοιχεία αυτά ταξινομούνται συνήθως στις ακόλουθες γενικές κατηγορίες:

- Άυλα δεδομένα/πληροφορίες: δεδομένα επιχείρησης, τεχνογνωσία, εξειδικεύσεις, πατέντες κλπ.
- Λογισμικό: οι διάφορες εφαρμογές που χρησιμοποιεί η επιχείρηση όπως για παράδειγμα το ERP σύστημα ή άλλες εφαρμογές του λογιστηρίου. Τα στοιχεία που αποθηκεύει το οικονομικό της τμήμα με την βοήθεια εφαρμογών (ονόματα και κωδικοί πελατών, στοιχεία προμηθευτών, στατιστικά πωλήσεων κα.).
- Εξοπλισμός: Οι ίδιοι οι υπολογιστές, επιτραπέζιοι ή κινητοί, τα routers, οι εξωτερικές μονάδες αποθήκευσης, τα usb sticks.

- Ανθρώπινο δυναμικό: Το πιο σημαντικό περιουσιακό στοιχείο μιας επιχείρησης. Εδώ μπορούμε να αντιληφθούμε τα άτομα και τις δυνατότητες τους στις οποίες βασίζεται η επιχείρηση. Ποιες είναι οι εξειδικεύσεις που κατέχουν, σε ποιους τομείς, πως μπορούν να βοηθήσουν την επιχείρηση, ποιο είναι το έργο της (insilico consulting, n.d.).

5.5. ISO 27001 και GDPR

Τον Μάιο του 2018 θεσπίστηκε ένας νέος κανονισμός για την προστασία των προσωπικών δεδομένων, ευρέως γνωστός *ως Γενικός Κανονισμός Προστασίας Δεδομένων* ή εν συντομία *GDPR*. Στο κανονισμό αυτό υπάρχουν πάρα πολλές αναφορές στα πρότυπα ISO. Μάλιστα ενθαρρύνεται η χρήση πολλών εξ αυτών με κυριότερο το ISO 27001, ώστε ο κάθε οργανισμός που έχει αυτήν την πιστοποίηση να μπορεί να εγγυηθεί για την ασφάλεια των δεδομένων των πελατών του. Υπάρχουν διάφορα στοιχεία όπως τα ορίζει ο κανονισμός όπου ο GDPR και το ISO 27001 τέμνονται όπως η κρυπτογράφηση των δεδομένων ή οι διαδικασίες τεχνικού ελέγχου.

5.5.1 Κρυπτογράφηση δεδομένων

Για το ISO 27001 η κρυπτογράφηση των δεδομένων αποτελεί ένα μέτρο πρόληψης των κινδύνων που ενδέχεται να αντιμετωπίσει μια επιχείρηση όσον αφορά τις πληροφορίες της. Πιο συγκεκριμένα, στο ISO 27001:2013 υπάρχει περιγραφή από μία σειρά 114 ελέγχων που μπορούν να χρησιμοποιηθούν από την επιχείρηση ώστε να μειωθούν οι κίνδυνοι στους οποίους εκτίθενται οι πληροφορίες τους. Με αυτό τον τρόπο η επιχείρηση προσδίδει στις πληροφορίες της εμπιστευτικότητα και διαθεσιμότητα καθώς μπορούν να διαβαστούν μόνο από τα μέλη που επιτρέπεται και τον πελάτη. Η κρυπτογράφηση των δεδομένων προσωπικού χαρακτήρα τα εξασφαλίζει όπως ορίζει και ο νόμος GDPR. Σφάλμα μπορεί να υπάρξει αν τα δεδομένα μπορεί να τα έχει η επιχείρηση στην διάθεση της αλλά όχι σε μορφή αναγνώσιμη, επομένως κάποιο τρίτο μέρος παραβίασε την ασφάλεια τους. Επίσης, κίνδυνος προκύπτει αν τα δεδομένα δεν μπορούν να είναι προσβάσιμα στα άτομα εκείνα που τα χρειάζονται για την εργασία τους.

5.5.2 Αξιολόγηση των κινδύνων

Βασική απαίτηση του ISO 27001 είναι τα μέλη της επιχείρησης να εφαρμόζουν μια εξονυχιστική σειρά ελέγχων έτσι ώστε να αντιμετωπίζουν τα αδύνατα σημεία της επιχείρησης αλλά και πιθανούς κινδύνους. Αφού προχωρήσουν με αυτήν την διαδικασία σε πρώτη φάση, έπειτα οι επιχειρήσεις είναι υποχρεωμένες να πάρουν κάποια μέτρα ώστε να διασφαλίσουν την εμπιστευτικότητα και τη μη διαρροή των πληροφοριών που κατέχουν.

5.5.3 Επιχειρησιακή συνέχεια

Με τον αριθμό τον ελέγχων που εφοδιάζει το ISO 27001 την επιχείρηση ο οργανισμός είναι σε θέση να προστατεύσει τις πληροφορίες του αν προκύψει κάποιος κίνδυνος και να περιορίσει την περίπτωση να δημιουργηθούν μεγάλες επιχειρηματικές καταστροφές. Ακόμη με αυτόν τον τρόπο μέσω των συνεχών ελέγχων για διαφόρους τομείς ακόμα και αν έχει συμβεί κάποιο επικίνδυνο περιστατικό περιορίζεται η επανάληψη τους.

5.5.4 Αξιολογήσεις και συνεχείς πιστοποιήσεις

Όπως γνωρίζουμε βασική προϋπόθεση για να αποκτήσει ένας οργανισμός την πιστοποίηση του ISO 27001 πρέπει να περάσει μια σειρά ελέγχων ώστε να διαπιστωθεί ότι τηρεί όλους τους κανόνες και της αρχές ασφάλειας. Γι' αυτό το λόγο απαιτείται από την επιχείρηση να ελέγχει και να ενημερώνει συνεχώς το πληροφοριακό της σύστημα ώστε να υπάρχει η διασφάλιση πως οι πληροφορίες που κατέχει δεν κινδυνεύουν (Παναγιώτης Καραλίβανος, 2017).

5.6 Αναθεωρήσεις ISO 27001

Υπάρχει μία αναθεώρηση του προτύπου ISO 27001 το 2013. Αν και φαίνεται σχετικά πρόσφατη, τόσο η σύσταση του προτύπου όσο και οι αναθεωρήσεις του είχαν μελετηθεί χρόνια πριν. Ανήκει στην οικογένεια προτύπων του ISO 27000. Δημιουργήθηκε ως εξέλιξη του προτύπου BS 7799-1:1997 Το ISO 27001:2013 αποτελεί λοιπόν το αναθεωρημένο πρότυπο διαχείρισης ασφάλεια των πληροφοριών. Η συγκεκριμένη αναθεώρηση εστιάζει ακόμα περισσότερο σε τρία συστατικά

στοιχεία για την ασφάλεια των δεδομένων: την εμπιστευτικότητα, την ετοιμότητα και την ακεραιότητα. Η έκδοση αυτή βοηθά την επιχείρηση να δεσμευτεί πιο σοβαρά απέναντι στους πελάτες της για την ασφάλεια των δεδομένων τους και την αντιμετώπιση πιθανών κινδύνων που υπάρχουν στο χώρο της ηλεκτρονικής ασφάλειας. Εμβαθύνει στο τομέα της απόδοσης του συστήματος που διαχειρίζεται την ασφάλεια των πληροφοριών που υπάρχουν στην εταιρεία. Η έκδοση του 2013 συμβάλει και άλλο στη προώθηση των ελέγχων ως μέτρο για την παροχή ασφάλειες στο τομέα των πληροφοριών.

5.6.1 Πλεονεκτήματα του ISO 27001

Τα πλεονεκτήματα του ISO 27001 είναι πολλά για μια επιχείρηση:

- Προστατεύει την επιχείρηση από τις ολοένα και περισσότερες διαδικτυακές απειλές.
- Αποδεικνύει πως ο οργανισμός δεσμεύεται να βελτιώνει συνεχώς την ασφάλεια του συστήματος του που διαχειρίζεται τις πληροφορίες.
- Αποδεικνύει πως ο οργανισμός είναι σε θέση να αντιμετωπίσει πιθανούς κινδύνους και απειλές αλλά και να τις αντιμετωπίσει αποτελεσματικά.
- Δείχνει την συμμόρφωση της επιχείρησης με τους κανόνες και τις νομοθεσίες που ορίζουν τα διάφορα πρότυπα αλλά και ο νέος νόμος για την προστασία των προσωπικών δεδομένων, ο GDPR.
- Βοηθά τους πελάτες να εμπιστευτούν στην εταιρεία τα προσωπικά τους δεδομένα.
- Είναι ένα σημάδι επιχειρηματικής συνέχειας.
- Παρέχει ανταγωνιστικό πλεονέκτημα για την εταιρεία σε σχέση με τους αντιπάλους της καθώς με την πιστοποίηση έχει κερδίσει μια σημαντική διάκριση σε σχέση με τις υπόλοιπες.
- Δεν προορίζεται μόνο για ένα συγκεκριμένο τύπο επιχειρήσεων. Ταυτόχρονα οι επιχειρήσεις δεν χρειάζεται να ανήκουν στο τομέα της πληροφορικής.
- Αυξάνει τις ευκαιρίες που μπορεί να «κυνηγήσει» η επιχείρηση στο δύσκολο μεταβαλλόμενο σύγχρονο περιβάλλον.
- Το πρότυπο ISO 27001:2013 παρέχει περισσότερα μέσα για να εξεταστούν οι κίνδυνοι που μπορεί να αντιμετωπίσει η εταιρεία (Γουσγούνης Ι. Νικόλαος, 2017).

5.7 Πιθανοί κίνδυνοι

Οι κίνδυνοι που διατρέχουν τα δεδομένα των χρηστών αλλά και των πελατών μιας επιχείρησης είναι αρκετοί. Η εξέλιξη της τεχνολογίας με τα ψηφιακά μέσα αποθήκευσης μπορεί να συντέλεσε στη δημιουργία μεγαλύτερου αποθηκευτικού χώρου και οργάνωσης ωστόσο συντέλεσε στο να γίνουν πιο ευάλωτες οι προσωπικές πληροφορίες των ατόμων απέναντι σε κινδύνους και απειλές. Κάποιοι από αυτούς τους κινδύνους είναι:

- Να μην πραγματοποιηθεί αποθήκευση ενός ψηφιακού εγγράφου στον υπολογιστή και μια διακοπή ρεύματος ή μια λάθος κίνηση του χρήστη να προκαλέσει την διαγραφή του. Τα δεδομένα θα χαθούν.
- Ένας υπάλληλος μπορεί να αφήσει ανοικτό τον υπολογιστή του χωρίς κωδικό πρόσβασης και κάποιος άλλος να αντιγράψει όλα τα αρχεία από τον υπολογιστή του με την βοήθεια ενός USB stick.
- Ιοί και κακόβουλα λογισμικά μπορούν να εισβάλουν στα αρχεία των πληροφοριακών συστημάτων και τα άτομα που χρησιμοποιούν αυτά τα λογισμικά να υποκλέψουν αρχεία πελατών της επιχείρησης.

Πέρα από τις απειλές που αντιμετωπίζει ο ψηφιακός κόσμος υποκλοπή και απώλεια στοιχείων μπορεί να συμβεί και στο φυσικό κόσμο. Για παράδειγμα, κάποιος να κλέψει ή να αντιγράψει αρχεία που έχει αφήσει εκτεθειμένα κάποιος υπάλληλος στο γραφείο του. Σε αυτά τα παραδείγματα, ο καθένας μπορεί να προσθέσει και άλλα βάση των δικών του εμπειριών στον εργασιακό χώρο.

5.8 Το ISO 27002

Το ISO 27001 χρησιμοποιείται τις περισσότερες φορές συνδυαστικά με το ISO 27002. Ο λόγος που συμβαίνει αυτό είναι πως το δεύτερο ISO είναι εκείνο που θέτει τους στόχους που πρέπει να επιτύχει ο εκάστοτε οργανισμός για να μπορεί να αποδείξει πως παρέχει ασφάλεια στις πληροφορίες τω πληροφοριακών του συστημάτων. Επιπλέον, έχει ρόλο περισσότερο συμβουλευτικό καθώς προτείνει ένα μεγάλο αριθμό ελέγχων που θα μπορούσε να χρησιμοποιήσει ο οργανισμός.

Οι πιστοποιήσεις ISO 27001 και ISO 27002 είναι συμπληρωματικές. Ουσιαστικά οι οδηγίες χρήσης που εμπεριέχει το πρότυπο δημοσιεύτηκαν το 2000. Ο τίτλος ήταν: "*Information technology—Security techniques—Code of practice for information security management*". Το 2007 υπήρξε αναθεώρηση, εισήλθε στην οικογένεια των ISO 27000 και έλαβε την επωνυμία ISO 27002. Η εξέλιξη αυτού του ISO συνέλαβε ώστε οι μέχρι τότε πρακτικές που επέβαλε το πρότυπο να γίνει μέθοδοι που θα μπορούσαν να αποδειχτούν μέσω της εφαρμογής τους. Η συνεχής βελτίωση του ISO 27002 βασίζεται ως επί το πλείστων στο ISO 27001. Το ιδιαίτερο στοιχείο αυτής της σχέσης είναι πως όλοι οι 39 έλεγχοι που εμπεριέχει το ISO 27001 αναλύονται μέσω του ISO 27002 (Harris S., 2007).

5.8.1 Διαφορές μεταξύ των δύο προτύπων

Πέρα από τα σημεία συμφωνίας και την συμπληρωματικότητα των δύο προτύπων ISO 27001 και 27002 υπάρχουν και δύο σημαντικές διαφορές. Το ISO 27001 παρέχει πιστοποίηση ενώ το 27002 υποστηρίζει το 27001. Επιπλέον, το ISO 27001 θέτει τις βασικές αρχές και τους ελέγχους που πρέπει να τηρηθούν ώστε να καταφέρει η επιχείρηση να πιστοποιείται με αυτό ενώ το ISO 27002 μπαίνει σε πιο πολύ λεπτομέρεια και δίνει κάποιες συμβουλές για την ενσωμάτωση ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών. Η ενσωμάτωση αυτών των μέτρων που προτείνει το 27002 δεν είναι υποχρεωτική για τη λήψη πιστοποίησης.

Κεφάλαιο 6^{ο}: Τομή των ISO 9001 και ISO 27001

6.1 Τα κοινά στοιχεία των δύο προτύπων

Όπως έχουμε δει στα παραπάνω κεφάλαια το ISO 9001 ασχολείται με την ποιότητα και την αντιμετώπιση των κινδύνων που αφορούν προϊόντα και υπηρεσίες ενώ το ISO 27001 με την διαχείριση της ασφάλειας των δεδομένων που υπάρχουν στα πληροφοριακά συστήματα της επιχείρησης. Οι οργανισμοί στις μέρες μας προσπαθούν να προλαβαίνουν όλες τις απαιτήσεις των πελατών τους και να είναι τυπικοί απέναντι τους. Γι' αυτό είναι συχνά το φαινόμενο πολλοί από αυτούς να προσπαθούν να αποκτούν και να συνδυάζουν πολλά πρότυπα ISO. Η γενικά τάση αυτή την στιγμή είναι να χρησιμοποιείται ο συνδυασμός του ISO 9001:2015 και εκείνου του ISO 27001:2013. Πρόκειται δηλαδή για τις τελευταίες αναθεωρήσεις των δύο ISO 9001 και ISO 27001 αντίστοιχα. Τα κοινά στοιχεία που αποτελούν την τομή των δύο αυτών προτύπων είναι τα παρακάτω:

- **Κοινό πεδίο ελέγχων:** Τα δύο πρότυπα στοχεύουν στη ποιότητα. Μπορεί βέβαια η σκοπιά τους να είναι διαφορετική καθώς το ένα εστιάζει στη ποιότητα αυτή καθαυτή (ISO 9001) και το άλλο στην ασφάλεια των πληροφοριών (ISO 27001) αλλά και τα δύο πρέπει να περάσουν μια σειρά εξωτερικών και εσωτερικών ελέγχων, να προσδιορίσουν διάφορα ζητήματα που αφορούν τον οργανισμό ώστε να φτάσουν στη πιστοποίηση. Οι διαδικασίες που ακολουθούνται και στα δύο είναι ίδιες, το περιεχόμενο αλλάζει.
- **Ηγεσία και υποστήριξη:** Η ηγεσία του οργανισμού και στις δύο περιπτώσεις ευθυγραμμίζει τις απαιτήσεις σε πόρους αλλά και σε ικανότητες από την πλευρά του προσωπικού με το τι θέλει να επιτύχει τελικά η επιχείρηση με την εφαρμογή των δύο πιστοποιήσεων.
- **Ενδιαφερόμενα μέρη:** Ο οργανισμός που θέλει τις πιστοποιήσεις αυτές είναι αναγκαίο να καθορίσει ποια είναι εκείνα τα ενδιαφερόμενα μέρη που θα λάβουν μέρος στη διαδικασία της πιστοποίησης. Οι απαιτήσεις που ορίζονται σε αυτό το κομμάτι είναι κοινές και για τα δύο πρότυπα
- **Αρμόδιες αρχές:** Κάθε αρμόδια αρχή επιτηρεί διαφορετικά πράγματα για τους διαφορετικούς τύπους ISO, δηλαδή άλλα στοιχεία θα ελέγξει για το πρότυπο ασφάλειας πληροφοριών και άλλα για εκείνο που ασχολείται με την ποιότητα στη

παραγωγή. Ωστόσο οι ρόλοι και οι αρμοδιότητες για τις αρχές αυτές ορίζονται στο ίδιο πλαίσιο και για τα δύο πρότυπα.

- **Προϋποθέσεις:** Υπάρχουν προϋποθέσεις που δεσμεύουν το κάθε πρότυπο και είναι ίδιες και για τα δύο στη περίπτωση μας. Αυτές είναι: η ικανότητα διαχείρισης της ποιότητας, η ασφάλεια, η ευαισθητοποίηση, η σωστή επικοινωνία, ο έλεγχος των εγγράφων και των αρχείων του συστήματος.
- **Διαχείριση εσωτερικού ελέγχου:** Οι απαιτήσεις που πρέπει να ελεγχθούν για το κάθε ISO είναι διαφορετικές όπως είναι φυσικό αφού καθένα βρίσκεται σε διαφορετικό πεδίο. Ωστόσο, ο τρόπος που πραγματοποιείται η διαχείριση του εσωτερικού ελέγχου είναι ο ίδιος.
- **Διορθωτικές ενέργειες:** Η πραγματοποίηση διορθωτικών ενεργειών είναι και πάλι ίδιες στις διαδικασίες και των δύο προτύπων.
- **Νέα δομή των προτύπων:** Γνωστό στη διεθνή βιβλιογραφία ως "*High Level Structure*" είναι μια προσπάθεια προς την ενοποίηση όχι μόνο των προτύπων που μελετάμε αλλά και όλων των προτύπων. Η προσπάθεια αυτή αφορά στη δημιουργία σχεδόν ίδιας διάρθρωσης των κεφαλαίων των οδηγιών των προτύπων, των κειμένων και της ορολογίας.
- **Συνεχής βελτίωση:** Τόσο το ISO 9001 όσο και το ISO 27001 βελτιώνονται συνεχώς μέσω των αναθεωρήσεων τους καθώς οι απαιτήσεις της αγοράς και των πελατών μεταβάλλονται στο σύγχρονο επιχειρησιακό περιβάλλον (Stojanovic Strahinja, Advisera, 2016).

Όπως βλέπουμε τα δύο πρότυπα ISO έχουν αρκετά κοινά σημεία που αφορούν κυρίως τις διαδικασίες ελέγχου, διοίκησης και ενδιαφερόμενων μερών. Το περιεχόμενο είναι το κύριο στοιχείο που τα διαφοροποιεί. Επίσης, αρχίζει να γίνεται μια προσπάθεια να ενοποιηθούν τα πρότυπα, η οποία αυτήν την στιγμή αφορά τον τρόπο γραφής και τα περιεχόμενα των εγχειριδίων των προτύπων. Σίγουρα ένα από τα πιο θετικά κοινά στοιχεία είναι η εξέλιξη και η ανάπτυξη των δύο προτύπων μέσω των διαρκών αναθεωρήσεων και βελτιώσεων τους.

6.2. Συνδυασμοί των προτύπων

Πλέον γνωρίζουμε πως τα κοινά σημεία μεταξύ του προτύπου ISO 9001 και του ISO 27001 είναι αρκετά. Πολλές επιχειρήσεις έχουν επιχειρήσει γι' αυτό το λόγο τον συνδυασμό των δύο. Ωστόσο, υπάρχουν επιχειρήσεις που διαθέτουν μόνο το ένα πρότυπο και θέλουν να ενσωματώσουν και το άλλο. Σε αυτήν την ενότητα θα μελετήσουμε δύο περιπτώσεις: α) μια επιχείρηση διαθέτει ISO 9001 και θέλει να ενσωματώσει το ISO 27001 β) μια επιχείρηση διαθέτει ISO 27001 και θέλει να ενσωματώσει και το ISO 9001.

6.2.1 Περίπτωση πρώτη: Ενσωμάτωση ISO 27001

Υπάρχουν περιπτώσεις που μια επιχείρηση μπορεί να διαθέτει το ISO 9001 και θέλει να ενσωματώσει και το ISO 27001. Σε αυτή την περίπτωση σε πρώτη φάση πρέπει να εντοπίσει τα κοινά σημεία των δύο προτύπων όπως τα είδαμε στη πρώτη ενότητα. Τα κοινά αυτά σημεία αφορούν:

- Τους σκοπούς και τις επιδιώξεις της επιχείρησης. Δηλαδή ποιο είναι το όραμα της επιχείρησης, ποιο το πλάνο της, ποιους σκοπούς θέλει να επιτύχει.

- Το σύστημα που αποθηκεύονται όλα τα έγγραφα και τα στοιχεία καθώς και η αποτελεσματικότητα του. Στις εταιρείες οτιδήποτε φυσικό στοιχείο αποθηκεύεται χαρακτηρίζεται από εκείνη την στιγμή από ένα μοναδικό κωδικό και ημερομηνία ώστε να μπορεί να βρεθεί και να αναθεωρηθεί σε οποιαδήποτε στιγμή χρειαστεί.

- Τις αναθεωρήσεις που πρέπει να γίνονται από τα ανώτατα μέλη της διοίκησης ανά τακτά χρονικά διαστήματα. Οι συνεδριάσεις των διοικητικών στελεχών για να υπάρξουν αναθεωρήσεις στο σύστημα ποιότητας μιας επιχείρησης πρέπει να γίνονται σε τακτά χρονικά διαστήματα και κατά την διάρκεια τους να υπάρχουν σημειώσεις και πρακτικά.

- Να δοθεί έμφαση στις διαδικασίες ελέγχων. Ένα χαρακτηριστικό όχι μόνο των δύο προτύπων που μελετάμε αλλά γενικότερα των ISO είναι να εντοπίζουν κενά στη διαδικασία ελέγχου και να προσπαθούν να τα γεφυρώσουν μέσα σε ορισμένα χρονοδιαγράμματα.

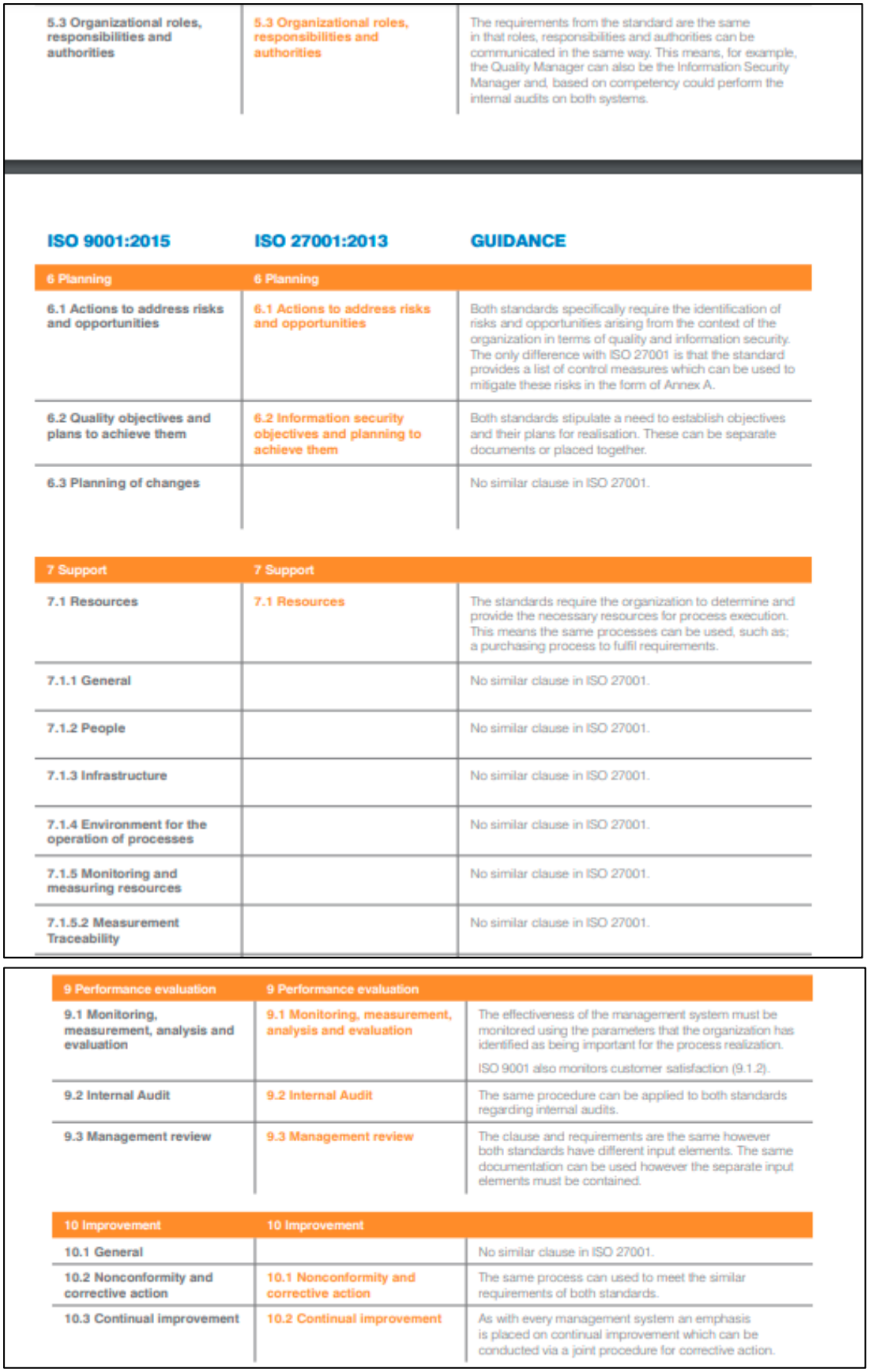
- Να υπάρχει προσδιορισμός των διορθωτικών πράξεων και πότε πρέπει αυτές να πραγματοποιηθούν.

Πέρα από τα κοινά σημεία στα οποία πρέπει να δοθεί έμφαση έτσι ώστε η επιχείρηση να μην δημιουργεί επαναλήψεις των ίδιων διαδικασιών, η δεύτερη φάση είναι να εντοπιστούν τα στοιχεία εκείνα τα οποία είναι τα επιπλέον που φέρνει με την προσαρμογή του το ISO 27001. Ουσιαστικά πρόκειται για τις δύο μεγάλες διαφορές των δύο προτύπων. Επομένως το ISO 27001 θα προσθέσει με την υιοθέτηση του δύο βασικά στοιχεία στο πληροφοριακό σύστημα:

1. **Εκτίμηση κινδύνου ασφάλειας πληροφοριών** (*Information security risk assessment*): Βασικό στοιχείο του οργανισμού είναι να μπορεί να αναπτύσσει μια μεθοδολογία που θα του επιτρέπει να κάνει ταυτοποίηση των ενδεχόμενων ρίσκων που συνδέονται με την ασφάλεια των πληροφορίων. Πέρα από την ταυτοποίηση η συγκεκριμένη διαδικασία βοηθά και στην εκτίμηση του κινδύνου και της ζημιάς που μπορεί να προκαλέσει το ρίσκο αυτό. Η προσοχή σε αυτό το σημείο εστιάζεται στο γεγονός πως αυτή η εκτίμηση κινδύνου δεν πρέπει σε καμία περίπτωση να συνδυάζεται με την αντίστοιχη του ISO 9001 καθώς μπορεί να έχει καταστροφικές συνέπειες ή να μην είναι το ίδιο παραγωγική.
2. **Αντιμετώπιση κινδύνου της ασφάλειας πληροφοριών:** Η διαδικασία αυτή δεν εμπεριέχεται στο ISO 9001. Επομένως, δεν μπορεί να γίνει συνδυαστικά και αφορά μόνο το ISO 27001. Άρα το εν λόγω ISO πρέπει να εφαρμόζει έναν ή ακόμα και περισσότερους από έναν ελέγχους ασφάλειας των πληροφοριών όπως δίνονται στο παράρτημα του (Zoé Hoy & Andrea Foley, 2014).

Οι γενικές διαφορές των δύο προτύπων φαίνονται στην **Εικόνα 5** όπως μελετήθηκαν από ένα άλλο φορέα πιστοποίησης, την *nqa* και αποτυπώθηκαν στην έκθεση της.

ISO 9001:2015	ISO 27001:2013	GUIDANCE
4 Context of the Organization	4 Context of the Organization	
4.1. Understanding the organization and its context	4.1. Understanding the organization and its context	Both standards require organizations to determine internal and external issues related to the suitability of the management system achieving its intended outcome.
4.2. Understanding the needs and expectations of interested parties	4.2. Understanding the needs and expectations of interested parties	Both standards require organizations to identify relevant interested parties as well as their needs and expectations.
4.3 Determining the scope of the quality management system	4.3 Determining the scope of the information security management system	The scope of the management system must be defined for both standards. The difference is that ISO 9001 requires products and services to be considered, and ISO 27001 requires consideration of interfaces and dependencies between the processes when defining the scope.
4.4. Quality management system and its processes	4.4. Information security management system	The requirements are exactly the same, each system must be established, implemented, documented, and continually improved.
5 Leadership	5 Leadership	
5.1 Leadership and commitment	5.1 Leadership and commitment	Both standards require management to implement policies, make provisions for resources, Continual Improvement assigning roles and responsibilities etc.
5.1.1 General		No similar clause in ISO 27001.
5.1.2 Customer focus		No similar clause in ISO 27001.
5.2 Policy	5.2 Policy	The requirements are very similar and could be met in a single document. Some policies are written as separate documents. If separate the policies should be compatible with each other.
5.2.1 Establishing the quality policy		No similar clause in ISO 27001.
5.2.2 Communicating the quality policy		No similar clause in ISO 27001.



5.3 Organizational roles, responsibilities and authorities	5.3 Organizational roles, responsibilities and authorities	The requirements from the standard are the same in that roles, responsibilities and authorities can be communicated in the same way. This means, for example, the Quality Manager can also be the Information Security Manager and, based on competency could perform the internal audits on both systems.

ISO 9001:2015	ISO 27001:2013	GUIDANCE
6 Planning	**6 Planning**	
6.1 Actions to address risks and opportunities	6.1 Actions to address risks and opportunities	Both standards specifically require the identification of risks and opportunities arising from the context of the organization in terms of quality and information security. The only difference with ISO 27001 is that the standard provides a list of control measures which can be used to mitigate these risks in the form of Annex A.
6.2 Quality objectives and plans to achieve them	6.2 Information security objectives and planning to achieve them	Both standards stipulate a need to establish objectives and their plans for realisation. These can be separate documents or placed together.
6.3 Planning of changes		No similar clause in ISO 27001.
7 Support	**7 Support**	
7.1 Resources	7.1 Resources	The standards require the organization to determine and provide the necessary resources for process execution. This means the same processes can be used, such as; a purchasing process to fulfil requirements.
7.1.1 General		No similar clause in ISO 27001.
7.1.2 People		No similar clause in ISO 27001.
7.1.3 Infrastructure		No similar clause in ISO 27001.
7.1.4 Environment for the operation of processes		No similar clause in ISO 27001.
7.1.5 Monitoring and measuring resources		No similar clause in ISO 27001.
7.1.5.2 Measurement Traceability		No similar clause in ISO 27001.

9 Performance evaluation	**9 Performance evaluation**	
9.1 Monitoring, measurement, analysis and evaluation	9.1 Monitoring, measurement, analysis and evaluation	The effectiveness of the management system must be monitored using the parameters that the organization has identified as being important for the process realization. ISO 9001 also monitors customer satisfaction (9.1.2).
9.2 Internal Audit	9.2 Internal Audit	The same procedure can be applied to both standards regarding internal audits.
9.3 Management review	9.3 Management review	The clause and requirements are the same however both standards have different input elements. The same documentation can be used however the separate input elements must be contained.
10 Improvement	**10 Improvement**	
10.1 General		No similar clause in ISO 27001.
10.2 Nonconformity and corrective action	10.1 Nonconformity and corrective action	The same process can used to meet the similar requirements of both standards.
10.3 Continual improvement	10.2 Continual improvement	As with every management system an emphasis is placed on continual improvement which can be conducted via a joint procedure for corrective action.

Εικόνα 5: Οι κυριότερες διαφορές ανάμεσα στα ISO 9001:2015 και ISO 27001: 2003 (Πηγή: (nqa)).

Αντιλαμβανόμαστε πως οι μεγαλύτερες διαφορές των δύο προτύπων εντοπίζονται στο τομέα της ηγεσίας αλλά και της υποστήριξης από την πλευρά των ανθρώπων, της δομής , του περιβάλλοντος που λαμβάνουν χώρο οι διαδικασίες κα.

Τα πλεονεκτήματα ωστόσο αυτής της περίπτωσης είναι αρκετά. Με την εισαγωγή του ISO 27001 πλέον η επιχείρηση είναι σύμφωνη με το νόμο GDPR για την προστασία των προσωπικών δεδομένων, κίνηση που αυξάνει την αξιοπιστία της επιχείρησης στα μάτια των πελατών. Επίσης είναι ένα δείγμα υπευθυνότητας της επιχείρησης και προς το εσωτερικό της πως λαμβάνει το θέμα της προστασίας των προσωπικών δεδομένων και των πληροφοριών σοβαρά με το να τις διασφαλίσει.

6.2.2 Περίπτωση δεύτερη: Ενσωμάτωση ISO 9001

Στο σημερινό επιχειρηματικό κόσμο είναι σύνηθες το φαινόμενο οι συνεργάτες επιχειρήσεων που διαθέτουν ήδη το ISO 27001 για την ασφάλεια των πληροφοριών τους να τους ωθούν και στη πιστοποίηση ISO 9001 προκειμένου να υπάρχει εξασφάλιση και για την ποιότητας των προϊόντων και των υπηρεσιών που παράγονται. Το γεγονός ότι η επιχείρηση διαθέτει ήδη το ISO 27001 είναι ένα πολύ θετικό στοιχείο που καθιστά ευκολότερη την υιοθέτηση του ISO 9001. Αυτό συμβαίνει διότι από την στιγμή που τα δύο πρότυπα έχουν κοινά στοιχεία, τότε απαιτείται μόνο προσθήκη κάποιων νέων στοιχείων και απαιτήσεων και όχι όλη η διαδικασία πιστοποίησης από την αρχή. Όπως είναι φυσικό μέσω αυτής της διαδικασίας η επιχείρηση γλυτώνει χρόνο και είναι πιο εύκολο να πιστοποιηθεί και στο δεύτερο πρότυπο.

Στη δεύτερη, λοιπόν περίπτωση μας θεωρούμε πως η επιχείρηση έχει ήδη το ISO 27001 και θέλει να εντάξει και το ISO 9001.

Τα πρότυπα ISO αποτελούν συστήματα διαχείρισης της ποιότητας. Τα σημεία 4 και 10 των ISO 9001 και 27001 περιγράφουν τις απαιτήσεις του κάθε συστήματος και έχουν κοινά σημεία. Επομένως η επιχείρηση για να εντάξει το ISO 9001 πρέπει να εστιάσει στα ακόλουθα:

- **Οργανωτική γνώση (*Organizational Knowledge*):** Το παράρτημα του ISO 27001 απαιτεί οι διαδικασίες που πραγματοποιούνται σε έναν οργανισμό να τεκμηριώνονται επαρκώς και να διατίθενται προς τα ενδιαφερόμενα μέρη που τις

χρειάζονται. Από την άλλη πλευρά το αντίστοιχο παράρτημα του ISO 9001 έχει σαν απαίτηση του όλοι οι οργανισμοί να καθορίζουν και να αποθηκεύουν την γνώση που είναι απαραίτητη για την προετοιμασία των διαδικασιών. Όσο η επιχείρηση ανταποκρίνεται στη συγκεκριμένη απαίτηση του ISO 27001 τόσο πιο έτοιμη είναι να υποδεχθεί το ISO 9001. Το επόμενο βήμα είναι οι οργανισμοί να είναι σίγουροι πως έχουν τεκμηριώσει όλες τις διαδικασίες που έχουν να κάνουν με την ποιότητα του παρεχόμενου προϊόντος.

- **Διαχείριση αλλαγών (*Change management*):** Βασικό στοιχείο και των δύο προτύπων είναι πως διαχειρίζονται τις αλλαγές. Κύριο χαρακτηριστικό αυτού του τομέα για το ISO 9001 είναι να υπάρχει σαφής ορισμός των απαιτήσεων που αφορούν τον σχεδιασμό αλλά και την επαλήθευση των αποτελεσμάτων των διαδικασιών που λαμβάνουν χώρα σε έναν οργανισμό. Από την πλευρά του το ISO 27001 περιέχει με λεπτομερή τρόπο τις απαιτήσεις για ένα ασφαλή περιβάλλον ανάπτυξης στον οργανισμό, σχολιασμούς τεχνικών και δοκιμές ασφαλείας. Στη περίπτωση αυτή για να εξασφαλιστεί η εφαρμογή του ISO 9001 οι οργανισμοί πρέπει να έχουν ένα μέτρο αξιολόγησης των απαιτήσεων που χρειάζονται για τα προϊόντα ενώ παράλληλα πρέπει να μπορούν να τις επαληθεύσουν. Επιπλέον, είναι καθοριστικό να υπάρχει στον οργανισμό η θέσπιση συγκεκριμένων διαδικασιών που θα επανεξετάζουν την ποιότητα των προϊόντων και θα μπορούν να τεκμηριώσουν με απλό τρόπο τα αποτελέσματα που θα προκύψουν από αυτήν την διαδικασία.

- **Διαχείριση προμηθευτών (*Vendor management*):** Ανάμεσα στις πιο σημαντικές απαιτήσεις που μπορεί να συναντήσει μια εταιρεία στο ISO 9001 είναι εκείνες που αφορούν τον προμηθευτή. Οι απαιτήσεις αυτές περιλαμβάνουν τον τρόπο αξιολόγησης του προμηθευτή πριν την διαδικασία επιλογής του καθώς και τον καθορισμό επικοινωνίας και απαιτήσεων για τους πόρους που θα δώσει ο προμηθευτής στον οργανισμό, μια σειρά ελέγχων που μπορούν να επιτρέψουν στην εκάστοτε εταιρεία να διασφαλίσει πως τηρούνται οι απαιτήσεις ποιότητα της και η καθιέρωση συνεχών ελέγχων ποιότητας στους προμηθευτές. Το θετικό στοιχείο με το ISO 27001 είναι πως, μέσω του προγράμματος του που αφορά την ασφάλεια σχετικά με τους προμηθευτές ,μπορεί να δώσει στις επιχειρήσεις τα εργαλεία εκείνα που θα τους χρειαστούν για να ενσωματώσουν και το ISO 9001.

Για να αποκτηθεί η πιστοποίηση του ISO 9001 οι διαδικασίες που θα ακολουθηθούν θα πρέπει να εστιάζουν στην εξέταση του προμηθευτή που έχει επιλέξει η επιχείρηση σχετικά με τις απαιτήσεις που έχει θέσει. Να επισημανθεί πως οι εσωτερικές διαδικασίες θα πρέπει να είναι εκείνες που θα καθορίζουν τα κριτήρια για τον έλεγχο πριν από την αποδοχή (Philip Bruney, 2020).

Γενικά όταν μια επιχείρηση έχει καταφέρει να ενσωματώσει και τα δύο πρότυπα στο εσωτερικό της και να κερδίσει τις ανάλογες πιστοποιήσεις έχει αρκετά πλεονεκτήματα. Αν θέλουμε να συνοψίσουμε τα πλεονεκτήματα με βάση τα στοιχεία που βρήκαμε στην ενότητα αυτή τότε αυτά είναι:

- Η γενικότερη βελτίωση στη διαδικασία πιστοποίησης.
- Εξοικονόμηση χρόνου και χρημάτων καθώς δεν χρειάζεται εάν υπάρχει ήδη το ένα από τα δύο ISO να γίνει η εξολοκλήρου η διαδικασία για την ενσωμάτωση του δεύτερου από την στιγμή που το ISO 9001 και το ISO 27001 έχουν μεταξύ τους πολλά κοινά σημεία.
- Αυξάνεται η εμπιστοσύνη των πελατών με όσες περισσότερες πιστοποιήσεις λαμβάνει η επιχείρηση.
- Η διαδικασία πιστοποίησης γίνεται πιο απλή καθώς η επιχείρηση πλέον αφού την έχει επαναλάβει την γνωρίζει καλά.

Κεφάλαιο 7^{ο}: Μελέτη περίπτωσης επιχείρησης

7.1 Γενικά στοιχεία

Στο κεφάλαιο αυτό θα ασχοληθούμε με την μελέτη περίπτωσης (case study) μιας επιχείρησης που χρησιμοποιεί και τα δυο πρότυπα ISO 9001 και 27001. Σκοπός αυτού του μέρους της διπλωματικής εργασίας είναι να αναλυθούν οι συνθήκες εκείνες που έκαναν απαραίτητη την υιοθέτηση των δύο προτύπων, τις απαιτήσεις για την απόκτηση των αναθεωρημένων πιστοποιήσεων καθώς και τα οφέλη στην επιχείρηση από την υιοθέτηση των προτύπων.

Η εταιρεία στην οποία θα εστιάσουμε ανήκει στο χώρο της τεχνολογίας και των τηλεπικοινωνιών. Πιο συγκεκριμένα θα μελετήσουμε την Vodafone Greece, που πρόκειται για την ελληνική θυγατρική της Βρετανικής πολυεθνικής εταιρείας Vodafone. Η έδρα της ελληνικής Vodafone βρίσκεται στο Χαλάνδρι, στην Αθήνα και ιδρύθηκε το 1992 στην Ελλάδα ως Panafon. Η εταιρεία πιστοποιείται συνεχώς με πρότυπα ISO και έχει κατορθώσει να πιστοποιηθεί με τις τελευταίες αναθεωρήσεις των προτύπων ISO 9001:2015 και ISO 27001:2013. Στις παρακάτω ενότητες θα παρουσιαστεί ο τρόπος που πραγματοποιήθηκε η έρευνα, τα στοιχεία που αποκτήθηκαν και τα συμπεράσματα που προέκυψαν.

7.2 Μεθοδολογία έρευνας

Η συγκεκριμένη εταιρεία αποτελεί και τη μελέτη περίπτωσης μας. Οι λόγοι που επιλέχθηκε είναι:

- Πρόκειται για μια μεγάλη εταιρεία, γνωστή στους περισσότερους από εμάς. Επομένως, η μελέτη της παρουσιάζει ενδιαφέρον
- Το αντικείμενο της που έχει σχέση με την τεχνολογία, την ψηφιακή εποχή, τις τηλεπικοινωνίες παρουσιάζει μεγάλο ενδιαφέρον σε σχέση με το πώς υιοθέτησε τα πρότυπα ISO που μελετάμε.
- Αποτελεί μια από τις εταιρείες που λόγω του αντικειμένου της, τόσο η ποιότητα των προϊόντων της όσο και η ασφάλεια των προσωπικών δεδομένων τόσων χιλιάδων πελατών της στην Ελλάδα είναι καθοριστικής σημασίας για την εξέλιξη της.
- Πρόκειται για μια από τις εταιρείες εκείνες που καταφέρνει να ηγηθεί του ανταγωνισμού της στο κλάδο της, έχει πιστούς πελάτες και κατάφερε να ανταπεξέλθει στην οικονομική κρίση.

Για να επιτευχθεί η έρευνα χρησιμοποιήθηκαν δευτερογενείς πηγές. Αναζήτηση πληροφοριών στο διαδίκτυο, επίσκεψη στον επίσημο ιστότοπο της εταιρείας, μελέτη των δελτίων τύπου και των πιστοποιήσεων που διαθέτει ελεύθερα στο κοινό της, σύγκριση των πληροφοριών που διαθέτει με τις ειδήσεις ειδησεογραφικών πρακτορείων και περιοδικών σχετικά με την τεχνολογία. Από όλες αυτές τις πληροφορίες χρησιμοποιήθηκαν οι πιο σημαντικές που αφορούν το σκοπό της εργασίας. Κάθε πληροφορία διασταυρώθηκε μέσω της σύγκρισης και με άλλες πηγές του διαδικτύου. Όσον αφορά τις πιστοποιήσεις είναι έγκυρες καθώς η Vodafone διαθέτει ελεύθερα τις πιστοποιήσεις της στο διαδίκτυο. Οι πιστοποιήσεις αυτές έχουν υπογραφή από εγκεκριμένα κέντρα πιστοποίησης.

7.3 Η εταιρεία

Όπως αναφέρθηκε και στην αρχή του κεφαλαίου η Vodafone Greece αποτελεί θυγατρική της αντίστοιχης εταιρείας στη Βρετανία. Στην Ελλάδα ιδρύθηκε το 1992 με την επωνυμία Panafon και η έδρα της βρίσκεται στο Χαλάνδρι, στην Αττική. Οι εταιρείες που συμμετείχαν στην ίδρυση της ήταν η γαλλική Telecom, η Intracom, η DataBank και φυσικά ο όμιλος Vodafone. Τον Ιανουάριο του 2002, δέκα χρόνια μετά

την ίδρυση της αλλάζει επωνυμία σε Vodafone. Έκτοτε ο όμιλος Vodafone αποτελεί βασικό μέτοχο της καθώς κατέχει το 99,8% των μετοχών της θυγατρικής της εδώ στην Ελλάδα. Όσον αφορά τον όμιλο Vodafone είναι ένας από τους ισχυρότερους στο πλανήτη καθώς έχει καταστήματα και στις 5 ηπείρους του πλανήτη με τους συνδρομητές της να ξεπερνούν τον αριθμό των 65 εκατομμυρίων. Στην Ελλάδα οι αντίστοιχοι συνδρομητές προσεγγίζουν τον αριθμό των 6 εκατομμυρίων. Στις στρατηγικές της κινήσεις, τον Ιούλιο του 2018 η εταιρεία απέκτησε όλες τις μετοχές της Cyta Hellas που αποτελούσε παράρτημα της στη Κύπρο. Τέλος, τον Απρίλιο του 2019 την απορρόφησε. Θυγατρική της αποτελεί και η Vodafone Αλβανίας.

Τα προϊόντα με τα οποία ασχολείται η εταιρεία είναι:

1. **Σταθερή τηλεφωνία**. Εδώ ανήκει η κατηγορία *Vodafone Home*. Πρόκειται ουσιαστικά για πάροχο ευρωζωνικών δικτύων στην Ελλάδα. Η εταιρεία αυτή ιδρύθηκε το 1993 με την επωνυμία Hellas on Line. Τον Ιούνιο του 2015 η Vodafone την εξαγόρασε και την πρόσθεσε στο δυναμικό της.

2. **Κινητή τηλεφωνία.** Στη κινητή τηλεφωνία η εταιρεία παρέχει πολλά και διαφορετικά πακέτα. Ξεχωρίζει το πακέτο καρτοκινητής CU που προσφέρει διάφορες ευκαιρίες επικοινωνίας σε ορισμένες ομάδες του ελληνικού πληθυσμού όπως για παράδειγμα οι φοιτητές. Από τον Οκτώβρη του 2012 η Vodafone προσφέρει στους συνδρομητές της πρόσβαση στο 4G δίκτυο της για μεγαλύτερη και πιο γρήγορη χρήση του διαδικτύου αλλά και τηλεφωνικών κλήσεων.

3. **Vodafone TV.** Η εταιρεία έχει επεκταθεί και στο τομέα της τηλεόρασης. Η συγκεκριμένη επιλογή είναι η συνδρομητική τηλεόραση της εταιρείας για τους πελάτες της.

4. **Internet.** Η εταιρεία είναι πάροχος internet τόσο μέσω της σταθερής τηλεφωνικής γραμμής όσο και με τα δεδομένα κινητής τηλεφωνίας. Προσφέρει μεγάλες ταχύτητες στο internet και αυτό είναι ευρέως γνωστό ως ένα από τα μεγαλύτερα πλεονεκτήματα της.

5. **Συσκευές τηλεφώνων και αξεσουάρ.** Τα φυσικά προϊόντα της επιχείρησης είναι η παροχή τηλεφωνικών συσκευών, κινητών τηλεφώνων, tablet, usb sticks,

συσκευών για το σπίτι όπως τηλεοράσεων ενώ έχει εισχωρήσει και στο τομέα των «έξυπνων» συσκευών. Πέρα από αυτά πουλά περιφερειακά αξεσουάρ και gadgets.

Η Vodafone παρουσιάζει πεδίο εφαρμογών στο σχεδιασμό, την ανάπτυξη και την συντήρηση των δικτύων κινητής αλλά και σταθερής τηλεφωνίας, στη παροχή, πώληση και επισκευή προϊόντων και υπηρεσιών στον ίδιο κλάδο. Επίσης, έχει την δυνατότητα να εγκαθιστά, να υποστηρίζει και να συντηρεί πληροφοριακά συστήματα ενώ παρέχει και υπηρεσίες μετά την πώληση. Διαθέτει τηλεφωνικό κέντρο που ασχολείται με παράπονα πελατών, την τεχνική τους υποστήριξη και την επίλυση απορίων.

Επίσης, διαθέτει το ίδρυμα Vodafone που έχει διάφορα προγράμματα κατά καιρούς για την υποστήριξη των μαθητών με καινοτόμες ιδέες (Generation Next), υποστήριξη επιστημόνων που έχουν ιδέες αλλά δεν μπορούν να τις εντάξουν στην αγορά και δεν έχουν χρηματοοικονομική υποστήριξη (World of Difference) και άλλα παρόμοια προγράμματα. (Vodafone.gr, 2020).

7.3.1 Το σκάνδαλο τον υποκλοπών

Γνωστό ως και το "Ελληνικό Watergate", ήταν ένα σκάνδαλο υποκλοπής κινητών τηλεφώνων που συνέβη το 2004 στην Ελλάδα. Υπολογίστηκε πως παραπάνω από 100 κινητά τηλέφωνα υπεκλάπησαν παράνομα στο δίκτυο της Vodafone Greece. Το σκάνδαλο αυτό πήρε μεγάλη έκταση καθώς τα κινητά τηλέφωνα αυτά αφορούσαν μέλη της ελληνικής κυβέρνησης και ανώτερους υπαλλήλους του δημόσιου τομέα. Ωστόσο το σκάνδαλο δεν αποκαλύφθηκε νωρίτερα από τον Μάρτη του 2005 έπειτα από έναν κανονικό έλεγχο που έκανε η Vodafone στα πλαίσια της στρατηγικής της. Εκεί αποκαλύφθηκε πως οι δράστες με χρήση κάποιον καρτοκινητών μπόρεσαν να υποκλέψουν συνομιλίες από αυτά τα 100 και παραπάνω κινητά τηλέφωνα. Το γεγονός αυτό κλυδώνισε την θέση της Vodafone ως την ασφάλεια που προσέφερε στους πελάτες της σχετικά με την ασφάλεια των προσωπικών τους δεδομένων και πληροφοριών (Κυριακίδου Ντίνα, 2006).

7.3.2 Οικονομική κατάσταση της Vodafone

Σύμφωνα με τα δελτία τύπου του οργανισμού αλλά και άλλες ειδησεογραφικές πηγές η Vodafone Greece ήταν όλα τα χρόνια από την ίδρυση της μέχρι τώρα κερδοφόρα. Κατά την διάρκεια της οικονομικής χρήσης 2017/2018 η εταιρεία παρουσίασε αύξηση του κύκλου εργασιών της κατά το ποσοστό του 2,7% που μεταφράζεται σε 874 εκατομμύρια. Να σημειωθεί πως το ποσό αυτό για την αμέσως προηγούμενη χρήση, δηλαδή του 2016/17 έφτανε τα 851 εκατομμύρια ευρώ (Vodafone annual report, 2019).

Με την ενσωμάτωση και της Cyta Hellas ο κύκλος εργασιών της εταιρείας για την χρήση 2018/19 αυξήθηκε κατά 3,0% σε σύγκριση με αυτήν του 2017/18 αγγίζοντας τα 897,9 εκατομμύρια ευρώ. Τα κέρδη προ φόρων για αυτήν την περίοδο ανήλθαν σε 55,2 εκατ. ευρώ ενώ την χρήση 2017/18 βρισκόντουσαν στο 37,2 εκατ. ευρώ επομένως η αύξηση ήταν αρκετή μεγάλή (Vodafone- Διοικητικό Συμβούλιο, 2019).

Όσον αφορά τα έσοδα από υπηρεσίες αυτά αυξήθηκαν κατά 6% κάτι που μπορεί να μεταφραστεί ως 488 εκατομμύρια ευρώ σε σύγκριση με την περίοδο της οικονομικής χρήσης του 2018 (Vodafone annual report, 2019).

Κατά την διάρκεια της περιόδου από τον Οκτώβριο του 2018 έως και το Σεπτέμβριο του 2019 μειώθηκε ο αριθμός των συνδρομητών που αφορούν την κινητή τηλεφωνία για την εταιρεία ενώ υπήρξε μείωση και 5.000 πελατών στο τομέα της σταθερής τηλεφωνίας. Αυτή η μείωση συνέβη διότι η Vodafone Greece αποφάσισε να προβεί σε εκκαθάριση τους πελατολογίου της, δηλαδή να διαγράψει από τα αρχεία της τους πελάτες που ήταν ανενεργοί. Με την διαγραφή αυτών των πελατών αυξήθηκε το μέσο έσοδο που αφορά την κινητή το οποίο έφτασε τα 9,3 ευρώ τον Ιούνιο το 2019, έφτασε τα 10 ευρώ τον Σεπτέμβρη του 2019, ενώ τον Σεπτέμβρη του 2018 βρισκόταν μόλις στα 9 ευρώ (Καθημερινή (ηλεκτρονική έκδοση), 2019).

Φαίνεται πως η εταιρεία κατόρθωσε ειδικά τα τελευταία χρόνια να αυξήσει τα έσοδα της, ενώ προχώρησε σε διαθρωτικές κινήσεις στο πελατολόγιο της ώστε να γνωρίζει ποιοι πελάτες της είναι ενεργοί και από ποιους μπορεί να αποκομίσει έσοδα.

7.4 Πολιτική ποιότητας Vodafone Greece

Η Vodafone Greece αναφέρεται στη πολιτική ποιότητας ως μια από τις βασικές επιλογές της στρατηγικής της. Για την ομάδα της Vodafone, η ποιότητα μεταφράζεται ως η δυνατότητα να υπερβούν τις απαιτήσεις και τις προσδοκίες που έχουν οι πελάτες από την επιχείρηση. Βέβαια δεν εστιάζουν μόνο στους πελάτες αλλά και τους ανθρώπους που απασχολούν. Αυτή η υπέρβαση συμβαίνει μέσω της συνεχής βελτίωσης των διεργασιών που λαμβάνουν χώρα αλλά και των συστημάτων που χρησιμοποιεί η εταιρεία. Η εταιρεία αναφέρει πως έχει δεσμευτεί σε τρία συγκεκριμένα στοιχεία που υπαγορεύει η πολιτική της. Τα στοιχεία αυτά είναι:

1. Να αφουγκράζεται η εταιρεία τις ανάγκες των πελατών της. Πέρα από αυτό το βασικό βήμα να κρατά τις υποσχέσεις που την δεσμεύουν απέναντι τους με τρόπο συστηματικό που έχει σαν κύριο χαρακτηριστικό την συνέπεια.

2. Η ανάπτυξη ποσοτικών και ποιοτικών δεικτών ώστε να μπορεί μέσω αυτών να έχει η εταιρεία μια ολοκληρωμένη εικόνα των λειτουργιών και των διαδικασιών της. Όσον αφορά τους δείκτες ποιότητας αυτοί αφορούν τους τελικούς χρήστες, τις ευρυζωνικές υπηρεσίες, την ποιότητα της σταθερής τηλεφωνίας, το χρόνο απόκρισης που αφορά τις υπηρεσίες πληροφοριών καταλόγου, δείκτες που μετρούν την ποιότητα των σταθερών ευρυζωνικών υπηρεσιών και τέλος δείκτη ποιότητας για υπηρεσίες συστημάτων των κινητών επικοινωνιών για κάθε έτος.

3. Η διασφάλιση πως η Vodafone έχει συμμορφωθεί με το Σύστημα Διαχείρισης Ποιότητας και η συνεχής προσπάθεια για την βελτίωση της αποτελεσματικότητα του συστήματος αυτού.

Κύριο πυλώνα για την πολιτική ποιότητας της εταιρείας αποτελεί η συνεχής αξιολόγηση. Στην εταιρεία η αξιολόγηση αφορά τα προϊόντα και τις υπηρεσίες που διαθέτει στην αγορά, τις επιχειρηματικές δραστηριότητες που ασκεί αλλά και τις διαδικασίες λειτουργίας και τέλος την αξιολόγηση της εμπειρίας του πελάτη. Πιο αναλυτικά για την κάθε αξιολόγηση ξεχωριστά δίνονται οι παρακάτω διευκρινήσεις:

Αξιολόγηση προϊόντων και υπηρεσιών:

- Συνεχής αξιολόγηση από την στιγμή του σχεδιασμού μέχρι και την στιγμή που γίνονται διαθέσιμα στο εμπόριο. Με αυτό τον τρόπο εξασφαλίζεται πως πληρούν όλες τις απαιτήσεις.
- Αξιολόγηση βάση πελατοκεντρικών δεικτών προσομοίωσης των υπηρεσιών του τηλεπικοινωνιακού δικτύου.
- Μέλος της ομάδας εργασίας *Network & Service Quality* του Ομίλου της Vodafone που είναι επιφορτισμένη με την ευθύνη για το σωστό σχεδιασμό, την εισαγωγή αλλά και την μέτρηση των δεικτών που μετρούν την ποιότητα των υπηρεσιών της εταιρείας προς τους πελάτες.
- Αξιολόγηση προμηθευτών και συνεργατών. Καθορισμός από κοινού προγράμματος για βελτίωση των παραγόμενων αγαθών.

Αξιολόγηση επιχειρηματικών δραστηριοτήτων και διαδικασιών λειτουργίας:

- Ανάπτυξη εταιρικού μοντέλου διεργασιών που συμβάλει στην απεικόνιση των επιχειρηματικών δραστηριοτήτων δίνοντας έμφαση στις πιο βασικές από αυτές. Σε αυτό το μοντέλο καθορίζονται οι αλληλοσυσχετίσεις και οι αλληλεπιδράσεις των διεργασιών αυτών.
- Παρακολούθηση ποιοτικών και ποσοτικών δεικτών απόδοσης των εταιρικών δραστηριοτήτων και διεργασιών με ταυτόχρονη βελτίωση πιθανών λαθών με ενεργό συμμετοχή των εργαζομένων της εταιρείας στο σύνολο τους.

Αξιολόγηση εμπειρίας πελάτη:

- Στόχευση στη ποιότητα που έχει για τον πελάτη η εμπειρία με την επιχείρηση. Παρακολούθηση και αξιολόγηση διεργασιών που αφορούν πώληση προϊόντων και υπηρεσιών αλλά και την γενικότερη εξυπηρέτηση των πελατών. Για να γίνει αντιληπτό κάποιο λάθος σε αυτήν την διαδικασία δίνεται έμφαση στα παράπονα που κάνουν οι πελάτες κατά καιρούς.

- Συνεχή εκπαίδευση και ενημέρωση του προσωπικού σε θέματα ποιότητας ώστε να παρέχει την καλύτερη δυνατή εκπαίδευση όταν έρχεται σε επαφή με τον πελάτη.
- Συντονισμός, ανάπτυξη και συνεχής βελτίωση του Συστήματος Διαχείρισης της Ποιότητας βάση των κριτηρίων του ISO 9001:2008 (Vodafone, 2020).

7.5. Ιστορικό πιστοποιήσεων της Vodafone Greece

Σύμφωνα με την ίδια την εταιρεία διαθέτει 20 χρόνια πιστοποιήσεων στο ενεργητικό της. Η Vodafone είναι από τις λίγες εταιρείες που διαθέτει Ολοκληρωμένο Σύστημα Διαχείρισης και η πρώτη που έλαβε πολλές από τις πιστοποιήσεις. Η πρώτη πιστοποίηση έγινε το 1996, αφορούσε το Σύστημα Διαχείρισης Ποιότητας (ISO 9001) και αργότερα ακολούθησε η πιστοποίηση του προτύπου Διαχείρισης Ασφάλειας Δεδομένων και Πληροφοριών (ISO 27001). Ακολούθησαν οι πιστοποιήσεις για Περιβαλλοντική Διαχείριση (ISO 14001), Υγεία & Ασφάλεια στην Εργασία (OHSAS 18001), Διαχείριση Επιχειρησιακής Συνέχειας (ISO 22301) και Ενεργειακή Διαχείριση (ISO 50001). Μάλιστα το Νοέμβριο του 2016 πιστοποιήθηκε για το Σύστημα Διαχείρισης Ενέργειας (ISO 50001:2011). Όλες αυτές οι πιστοποιήσεις δίνουν στην εταιρεία την δυνατότητα να εξασφαλίσει την παροχή υψηλής ποιότητας στα προϊόντα και τις υπηρεσίες της.

Η ιστορική αναδρομή σύμφωνα με την πολιτική ποιότητας για την επιχείρηση έχεις ως εξής:

- Η τότε Panafon πιστοποιείται το 1996 με το πρότυπο ISO 9001:1994.
- Το 1999 πραγματοποιείται πιστοποίηση του ολοκληρωμένου πλέον συστήματος διαχείρισης της εταιρείας. Το σύστημα είχε επιμέρους τμήματα: διαχείρισης ποιότητας, διαχείριση περιβάλλοντος, υγιεινή και ασφάλεια των εργαζομένων, ασφάλεια πληροφοριών και δεδομένων της επιχείρησης και των πελατών.
- Το 2002 η εταιρεία πιστοποιείται όσον αφορά τα καταστήματα της με ISO 9001:2000 για την πώληση αλλά και την εξυπηρέτηση των πελατών από τους υπαλλήλους μετά την πώληση των προϊόντων και των υπηρεσιών στους τομείς της κινητής τηλεφωνίας αλλά και του διαδικτύου.

- Το 2009 πιστοποιείται στον χώρο των τηλεπικοινωνιών και ασύρματων επικοινωνιών, του Εργαστηρίου Μετρήσεων Ηλεκτρομαγνητικών Πεδίων στο Περιβάλλον σύμφωνα με τις απαιτήσεις που ορίζει το πρότυπο ΕΛΟΤ EN ISO/ IEC 17025.
- Το 2010 είναι η χρονιά που η εταιρεία πιστοποιείται για το σύστημα διαχείρισης της επιχειρησιακής συνέχειας στην εταιρεία σύμφωνα με το πρότυπο BS 25999-2:2007.
- Το 2012 έρχεται άλλη μια πιστοποίηση που αφορά την επιχειρησιακή συνέχεια αυτήν την φορά βάση του προτύπου ISO 22301:2012.
- Το 2016 πραγματοποιείται πιστοποίηση για το Σύστημα Διαχείρισης Ενέργειας που αφορά το δίκτυο σταθερής αλλά και κινητής, κτήρια γραφείων και τα ιδιόκτητα καταστήματα. Η πιστοποίηση ήταν σύμφωνη με το πρότυπο ISO 50001:2011 (Vodafone-Ανασκόπηση, 2020).

Γενικά μέσω της ιστορικής αναδρομής μπορούμε να αντιληφθούμε πως η Vodafone Greece επενδύει στις πιστοποιήσεις για να παρέχει ποιοτικά προϊόντα, να εξασφαλίζει σωστές συνθήκες εργασίας για τους εργαζομένους της αλλά και να δημιουργεί σχέση εμπιστοσύνης και αξιοπιστίας με τους πελάτες της. Βέβαια η εργασία μας θα εστιάσει στις πιστοποιήσεις που αφορούν τα πρότυπα ISO 9001 και IS0 27001.

7.6. Vodafone και ISO 9001

7.6.1 ISO 9001:1994-Panafon

Όπως είδαμε από την ιστορική αναδρομή στις πιστοποιήσεις της εταιρείας, το 1994 ήρθε η πρώτη πιστοποίηση για την Panafon με το πρότυπο ISO 9001:1994. Το πρότυπο αυτό παρείχε πιστοποίηση για το Σύστημα Διαχείρισης Ποιότητας για το σύνολο των δραστηριοτήτων που ασκούσε η επιχείρηση εκείνη την εποχή. Η πιστοποίηση αυτή ήταν η πρώτη που δόθηκε σε εταιρεία στην Ελλάδα και κατέστησε την Vodafone πρωτοπόρο.

7.6.2 ISO 9001:2000-Vodafone

Το 2002 η εταιρεία αποκτά την πιστοποίηση ISO 9001:2000 για την πώληση και την εξυπηρέτηση των πελατών από τον Ελληνικό Οργανισμό Τυποποίησης (ΕΛΟΤ) και αυτή η πιστοποίηση ήταν η πρώτη που δόθηκε σε αλυσίδα καταστημάτων λιανικής πώλησης. Για να μπορέσει να διασφαλίσει η Vodafone πως μπορεί να επιτευχθεί η παραπάνω πιστοποίηση έπρεπε να εξασφαλίσει πως όλα τα σημεία πώλησης και εξυπηρέτησης πελατών στη χώρα:

- ✓ Παρέχουν υψηλό επίπεδο εξυπηρέτησης που είναι το ίδιο για όλα τα καταστήματα
- ✓ Ακολουθούν κοινές διαδικασίες ως προς την πώληση των προϊόντων και την εξυπηρέτηση των πελατών μετά την πώληση.
- ✓ Εφαρμόζουν πρακτικές που έχουν στο κέντρο τους το πελάτη και αφοσιώνονται σε αυτόν.

Δεδομένου ότι η Vodafone βασίζεται σε πολλούς επιχειρηματίες ανά τόπους, οι οποίοι εκείνη την εποχή εμπιστεύονταν το σήμα της και συμμετείχαν ως συνεργάτες στο franchising ανοίγοντας το δικό τους κατάστημα, η πιστοποίηση αυτή ενίσχυσε την σχέση μεταξύ των δύο. Η πιστοποίηση του ISO 9001:2000 έφερε την δέσμευση τόσο της Vodafone όσο και του κάθε συνεργάτη ατομικά στα παρακάτω συγκεκριμένα σημεία που υπαγορεύει το σύστημα διαχείρισης ποιότητας:

- Τήρηση των δεσμεύσεων και των υποσχέσεων απέναντι στους πελάτες με συνεχή και συστηματικό τρόπο.
- Εγγύηση προς τους πελάτες για συνεχή εξυπηρέτηση υψηλού επιπέδου όπως και παροχή υπηρεσιών.
- Μελέτη των αναγκών των πελατών και ικανοποίηση τους με τις κατάλληλες προσαρμογές στα προϊόντα και τις υπηρεσίες.
- Συνεχής και αποτελεσματική βελτίωση.

Για να δοθεί η πιστοποίηση μελετήθηκαν κατά πόσο ήταν πλήρης η εξυπηρέτηση του πελάτη, πως διαχειριζόντουσαν τα διάφορα καταστήματα τα αιτήματα των πελατών, η σωστή επικοινωνία και η ενημέρωση μεταξύ των καταστημάτων, πως γίνεται η μέτρηση ποσοτικών και ποιοτικών χαρακτηριστικών, ο τρόπος που γίνονται η παραγγελία και τέλος το γενικότερο κλίμα που επικρατεί στα καταστήματα μεταξύ των συναδέλφων αλλά και οι σχέσεις εργοδότη-υπαλλήλου.

Μέσω αυτής της πιστοποίησης τα οφέλη για την Vodafone ήταν τα ακόλουθα:

- Ενίσχυση της αξιοπιστίας της στη σχέση με τους πελάτες της.
- Μήνυμα στους ανταγωνιστές πως πρωτοπορεί.
- Ενίσχυση της σχέσης της κεντρικής εταιρείας με τα κατά τόπους καταστήματα.
- Ενίσχυση του ονόματος της στην ελληνική αγορά, που ξεκίνησε να γίνεται συνώνυμο της ποιότητας στις τηλεπικοινωνίες και τις υπόλοιπες υπηρεσίες που παρέχει.
- Έχει την δυνατότητα να γνωρίζει πως όλα τα καταστήματα της στην Ελλάδα ακολουθούν την ίδια πελατοκεντρική προσέγγιση και τρόπους εξυπηρέτησης (Vodafone annual, 2007).

7.6.3 ISO 9001:2015-Vodafone

Έπειτα από χρόνια και ενώ η εταιρεία έχει ήδη στο ενεργητικό της την πιστοποίηση που αφορά την ποιότητα ISO 9001:2000 πιστοποιείται έπειτα από χρόνια και με την αναθεωρημένη έκδοση του το ISO 9001:2015. Οι λόγοι που η Vodafone κινήθηκε προς την κατεύθυνση για μια ακόμα τέτοιου είδος πιστοποίησης είναι οι παρακάτω:

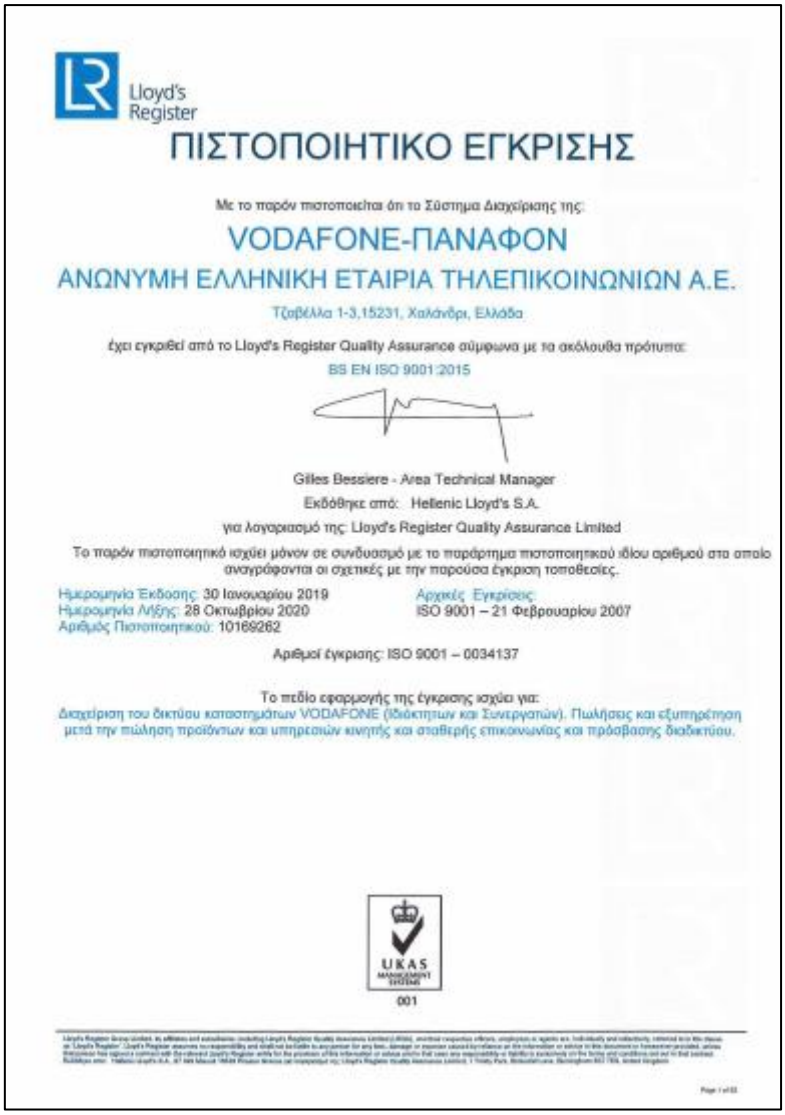
- Από την στιγμή που διαθέτει πολλές και διαφορετικές όπως είδαμε πιστοποιήσεις θέλει να εκμεταλλευτεί το πλεονέκτημα της νεότερης έκδοσης του ISO 9001 που έχει ως στόχο την ενοποίηση όλων των πιστοποιήσεων με κοινή γλώσσα και ορολογία.
- Η στρατηγική της να βελτιώνεται συνεχώς και να κερδίζει συνεχώς την εμπιστοσύνη των πελατών της την οδήγησε στο να αναθεωρήσει τα πρότυπα της όσον αφορά την ποιότητα των προϊόντων και των υπηρεσιών της.
- Η αναθεωρημένη έκδοση του ISO 9001 μειώνει τις πολλές απαιτήσεις που πρέπει να τηρεί μια εταιρεία για να πιστοποιηθεί δίνοντας βαρύτητα στο πελάτη. Το στοιχείο αυτό ταιριάζει στη πελατοκεντρική πολιτική της εταιρείας.
- Να εστιάσει η εταιρεία σε μια διαδικασία ελέγχου ποιότητας που βασίζεται στο κύκλο: Σχεδιάζω – Ενεργώ – Ελέγχω – Βελτιώνω.

- Όλες οι εταιρείες με παλαιότερες εκδόσεις ISO 9001 έπρεπε μέσα σε ένα χρονικό διάστημα 3 ετών από την έκδοση του ISO 9001:2015 να ακολουθήσουν αυτό το πρότυπο.

Τα οφέλη από την χρήση του ISO 9001: 2015 είναι αδιαμφισβήτητα πολλά για την Vodafone:

- Περαιτέρω ενίσχυση της φήμης της εταιρείας με ταυτόχρονη εξασφάλιση της εμπιστοσύνης τους.
- Δημιουργία ευκαιριών ώστε να διεισδύσει και σε νέες αγορές.
- Αύξηση της ικανοποίησης των πελατών από την εξυπηρέτηση. Η Vodafone έχει κερδίσει πολλές φορές βραβεία για την εξυπηρέτηση που παρέχει στους πελάτες της.
- Περαιτέρω εκπαίδευση και ευαισθητοποίηση όσον αφορά τους εργαζόμενους σε θέματα ποιότητας.
- Μείωση του κόστους της παραγωγής καθώς βελτιώνεται και άλλο η εικόνα της επιχείρησης.
- Μείωση της γραφειοκρατίας.

Στην **Εικόνα 6** φαίνεται το πιστοποιητικό που έλαβε η Vodafone για τα καταστήματα της σύμφωνα με τις απαιτήσεις του προτύπου ISO 9001-2015. Το πιστοποιητικό αυτό αφορά στο τρόπο εξυπηρέτησης των πελατών τόσο κατά την διαδικασία αγοράς ενός προϊόντος όσο και μετά από αυτό καθώς και την σχέση του δικτύου καταστημάτων της Vodafone μεταξύ της κεντρικής εταιρείας και του γενικότερου franchise της στην Ελλάδα.



Lloyd's Register

ΠΙΣΤΟΠΟΙΗΤΙΚΟ ΕΓΚΡΙΣΗΣ

Με το παρόν πιστοποιείται ότι το Σύστημα Διαχείρισης της:

VODAFONE-ΠΑΝΑΦΟΝ

ΑΝΩΝΥΜΗ ΕΛΛΗΝΙΚΗ ΕΤΑΙΡΙΑ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ Α.Ε.

Τζαβέλλα 1-3,15231, Χαλάνδρι, Ελλάδα

έχει εγκριθεί από το Lloyd's Register Quality Assurance σύμφωνα με τα ακόλουθα πρότυπα:

BS EN ISO 9001:2015

Gilles Bessiere - Area Technical Manager

Εκδόθηκε από: Hellenic Lloyd's S.A.

για λογαριασμό της: Lloyd's Register Quality Assurance Limited

Το παρόν πιστοποιητικό ισχύει μόνον σε συνδυασμό με το παράρτημα πιστοποιητικού ίδιου αριθμού στο οποίο αναγράφονται οι σχετικές με την παρούσα έγκριση τοποθεσίες.

Ημερομηνία Έκδοσης: 30 Ιανουαρίου 2019
Ημερομηνία Λήξης: 28 Οκτωβρίου 2020
Αριθμός Πιστοποιητικού: 10169262

Αρχικές Εγκρίσεις:
ISO 9001 – 21 Φεβρουαρίου 2007

Αριθμοί έγκρισης: ISO 9001 – 0034137

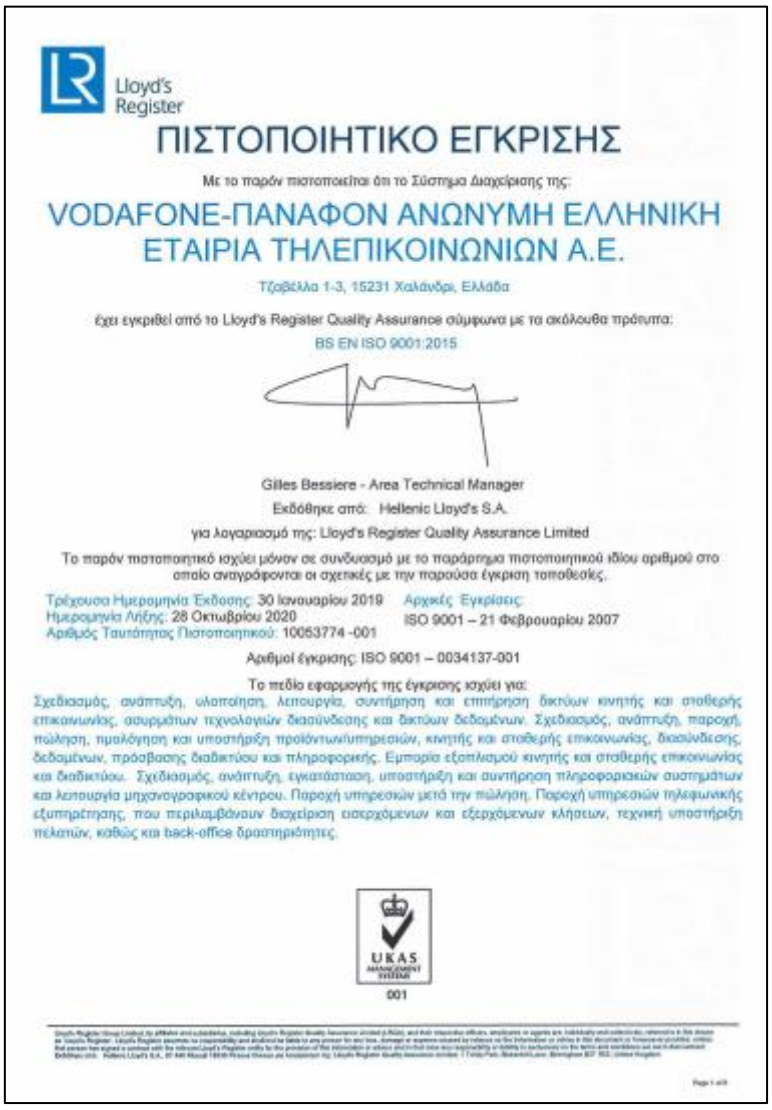
Το πεδίο εφαρμογής της έγκρισης ισχύει για:
Διαχείριση του δικτύου καταστημάτων VODAFONE (Ιδιόκτητων και Συνεργατών). Πωλήσεις και εξυπηρέτηση μετά την πώληση προϊόντων και υπηρεσιών κινητής και σταθερής επικοινωνίας και πρόσβασης διαδικτύου.

UKAS MANAGEMENT SYSTEMS
001

Εικόνα 6: Πιστοποιητικό ISO 9001:2015 για την Vodafone-Καταστήματα *(Πηγή:* (Vodafone, 2020)*)*

Το πιστοποιητικό αυτό εκδόθηκε τον Ιανουάριο του 2019 και έχει ισχύ μέχρι και τον Οκτώβρη του 2020. Αυτό σημαίνει πως πρέπει να ξαναγίνει για τα συγκεκριμένα θέματα έλεγχος στη Vodafone ώστε να εξασφαλιστεί εκ νέου πως τηρεί τις κατάλληλες προϋποθέσεις για να κατέχει την πιστοποίηση ISO 9001:2015.

Πέρα από το δίκτυο των καταστημάτων της, η εταιρεία έλαβε και την γενικότερη πιστοποίηση ISO 9001:2015 για τις εργασίες και τις διαδικασίες που επιτελεί όπως φαίνεται στην **Εικόνα 7.**



Lloyd's Register

ΠΙΣΤΟΠΟΙΗΤΙΚΟ ΕΓΚΡΙΣΗΣ

Με το παρόν πιστοποιείται ότι το Σύστημα Διαχείρισης της:

VODAFONE-ΠΑΝΑΦΟΝ ΑΝΩΝΥΜΗ ΕΛΛΗΝΙΚΗ ΕΤΑΙΡΙΑ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ Α.Ε.

Τζαβέλλα 1-3, 15231 Χαλάνδρι, Ελλάδα

έχει εγκριθεί από το Lloyd's Register Quality Assurance σύμφωνα με τα ακόλουθα πρότυπα:

BS EN ISO 9001:2015

Giles Bessiere - Area Technical Manager

Εκδόθηκε από: Hellenic Lloyd's S.A.

για λογαριασμό της: Lloyd's Register Quality Assurance Limited

Το παρόν πιστοποιητικό ισχύει μόνον σε συνδυασμό με το παράρτημα πιστοποιητικού ιδίου αριθμού στο οποίο αναγράφονται οι σχετικές με την παρούσα έγκριση τοποθεσίες.

Τρέχουσα Ημερομηνία Έκδοσης: 30 Ιανουαρίου 2019
Ημερομηνία Λήξης: 28 Οκτωβρίου 2020
Αριθμός Ταυτότητας Πιστοποιητικού: 10053774 -001

Αρχικές Εγκρίσεις:
ISO 9001 – 21 Φεβρουαρίου 2007

Αριθμοί έγκρισης: ISO 9001 – 0034137-001

Το πεδίο εφαρμογής της έγκρισης ισχύει για:

Σχεδιασμός, ανάπτυξη, υλοποίηση, λειτουργία, συντήρηση και επιτήρηση δικτύων κινητής και σταθερής επικοινωνίας, ασυρμάτων τεχνολογιών δικασύνδεσης και δικτύων δεδομένων. Σχεδιασμός, ανάπτυξη, παροχή, πώληση, τιμολόγηση και υποστήριξη προϊόντων/υπηρεσιών, κινητής και σταθερής επικοινωνίας, δικασύνδεσης, δεδομένων, πρόσβασης διαδικτύου και πληροφορικής. Εμπορία εξοπλισμού κινητής και σταθερής επικοινωνίας και διαδικτύου. Σχεδιασμός, ανάπτυξη, εγκατάσταση, υποστήριξη και συντήρηση πληροφοριακών συστημάτων και λειτουργία μηχανογραφικού κέντρου. Παροχή υπηρεσιών μετά την πώληση. Παροχή υπηρεσιών τηλεφωνικής εξυπηρέτησης, που περιλαμβάναν διαχείριση εισερχόμενων και εξερχόμενων κλήσεων, τεχνική υποστήριξη πελατών, καθώς και back-office δραστηριότητες.

UKAS MANAGEMENT SYSTEMS
001

Εικόνα 7: Πιστοποιητικό ISO 9001:2015 για την Vodafone-Διαδικασίες *(Πηγή:* (Vodafone, 2020)*)*

Όπως μπορούμε να δούμε η εταιρεία εδώ πιστοποιείται για τον σχεδιασμό, την ανάπτυξη, την υλοποίηση, την λειτουργία, την συντήρηση και την επιτήρηση:

- Των δικτύων κινητής και σταθερής τηλεφωνίας.
- Των τεχνολογιών ασύρματων διασυνδέσεων και δικτύων δεδομένων.
- Τιμολόγησης και υποστηρικτικών διαδικασιών.
- Εμπορίας εξοπλισμού και προϊόντων.
- Πληροφοριακών κέντρων καθώς και κέντρων μηχανογράφησης.

Επίσης και εδώ γίνεται αναφορά στην εξυπηρέτηση των πελατών πριν και μετά την πώληση των προϊόντων καθώς και ένα καινούργιο στοιχείο που αποτελεί η εξυπηρέτηση μέσω κλήσεων στο τηλεφωνικό κέντρο της εταιρείας. Όλα αυτά απαρτίζουν την ποιότητα με κέντρο πάντα τον χρήστη. Η εφαρμογή αυτών των συστημάτων πιστοποιείται όπως φαίνεται από το 2007 και έπειτα από τον αναγνωρισμένο φορέα πιστοποίησης Lloyd's Register Quality Insurance (Vodafone, 2020).

7.7 Vodafone και ISO 27001

Η εταιρεία όπως είναι φυσιολογικό ασχολείται με μεγάλο όγκο πληροφοριών και προσωπικών δεδομένων τα οποία πρέπει να προστατεύει. Για να μπορέσει να πείσει πως κατέχει αυτήν την δυνατότητα τους πελάτες αλλά και τους συνεργάτες της κινήθηκε στα Συστήματα Διαχείρισης Ασφάλειας Δεδομένων και Πληροφορίων.

7.7.1 Vodafone και BS 7799

Ήδη από το 1999 η Vodafone ήταν το πρώτο ελληνικό δίκτυο που κατάφερε να πιστοποιηθεί για το Σύστημα Διαχείρισης Ασφάλειας Δεδομένων και Πληροφορίων. Η πρωτιά αυτή κινήθηκε σε ευρωπαϊκό επίπεδο καθώς ήταν μία από τις πρώτες χώρες και στην Ευρώπη. Η πιστοποίηση που έλαβε ήταν το BS-7799 παλαιότερη εκδοχή αυτού που γνωρίζουμε σήμερα ως ISO 27001.

Με το πρότυπο αυτό η Panafon-Vodafone μπόρεσε:

- Να εξασφαλίσει την ασφάλεια κατά την διάρκεια του σχεδιασμού των προϊόντων και των υπηρεσιών της.
- Να ενισχύσει την αξιοπιστία του τηλεφωνικού της κέντρου.
- Να κερδίσει την εμπιστοσύνη τον ολοένα και αυξανόμενων πελατών της, πως οι πληροφορίες τους είναι ασφαλής όταν χρησιμοποιούν τα κινητά τους.
- Να διαφοροποιηθεί σε σχέση με τους ανταγωνιστές της. Έδειξε πως η ασφάλεια που εγγυάται έχει μελετηθεί, έχει τηρήσει όλες τις απαραίτητες προϋποθέσεις και απαιτήσεις ενός μεγάλου οργανισμού πιστοποίησης και πλέον είναι επισήμως πιστοποιημένη για την επιχείρηση.

- ❖ Πέρα από τους ιδιώτες πελάτες κατάφερε να εξασφαλίσει την εμπιστοσύνη πολλών εταιρικών πελατών που όπως είναι φυσικό αναζητούσαν ασφάλεια και παροχή διαφορετικών ωφελειών στους πελάτες τους (Vodafone-Panafon, 2001).

7.7.2 Vodafone και ISO 27001

Τον Ιούνιο του 2007 η Vodafone επιτυγχάνει να πιστοποιηθεί με την νεότερη εκδοχή του BS-7799, το ISO 27001. Έτσι το παλαιότερο πρότυπο αντικαταστάθηκε με το νεότερο.

Το ISO 27001 προϋπέθετε:

- Υλοποίηση 133 μηχανισμών που αφορούν την ασφάλεια και οργανωτικά μέτρα που έχουν σχέση με την Ασφάλεια των Πληροφοριών.
- Έμφαση στον έλεγχο του Συστήματος Διαχείρισης Επιχειρησιακής Συνέχειας (*Business Continuity Management*), το οποίο διασφαλίζει την επιχειρησιακή λειτουργία της Vodafone.

Χάρη στο συγκεκριμένο πρότυπο η Vodafone μπόρεσε να επανακτήσει την εμπιστοσύνη των πελατών της ύστερα από το γεγονός της υποκλοπής των τηλεφωνικών κλήσεων που είχε ανακαλυφθεί. Η πιστοποίηση ενός οργανισμού για ασφάλεια των πληροφοριών και των δεδομένων δείχνει πως είχε βελτιώσει όσα κενά υπήρξαν στη λειτουργία της. Οι κατάλληλες διαδικασίες και έλεγχοι είναι εκείνοι που εφαρμόζονται σύμφωνα με τα διεθνή πρότυπα ώστε να αποφευχθούν απειλές και εξωτερικοί κίνδυνοι στης πληροφορίες που παρείχαν οι πελάτες και οι συνεργάτες της εταιρείας, σε αυτήν. Επιπλέον, χάρη στο Σύστημα Διαχείρισης Επιχειρησιακής Συνέχειας κατάφερε να διασφαλίσει πως η λειτουργία της θα είναι έρρυθμη ανεξάρτητα από οποιασδήποτε συνθήκες μπορεί να συντρέχουν ή κάποιων απρόσμενων γεγονότων (Vodafone annual, 2007).

Σύμφωνα με το φορέα πιστοποίησης Lloyd’s Register, προτού γίνει η πιστοποίηση υπήρξε διαγνωστική επιθεώρηση του συστήματος της για να εκτιμηθεί εάν είναι έτοιμη για μια τέτοια αξιολόγηση. Είναι η γνωστή *gap analysis*. Σε περίπτωση που κάποιο στοιχείο δεν ήταν κατάλληλο ή ήθελε βελτίωση η εταιρεία μπορούσε να το βελτιώσει με βάση παρατηρήσεις από την έκθεση που είχε στα χέρια της έπειτα από αυτήν την ανάλυση (Lloyd's Register, 2020).

7.7.3 Vodafone και ISO 27001:2013

Ειδικά σε πιστοποιήσεις που αφορούν την ασφάλεια των δεδομένων και των πληροφοριών κάθε επιχείρηση πρέπει να δώσει ιδιαίτερη βάση και να κάνει όσο πιο συχνά γίνεται αναθεωρήσεις. Αυτό ήταν άλλωστε και το σκεπτικό της Vodafone η οποία έκανε προσπάθεια πιστοποίησης για την αναθεώρηση του ISO 27001, το ISO 27001:2013.

Με την κίνηση της αυτή η Vodafone κατάφερε να ωφεληθεί στους παρακάτω τομείς:

- Τονώσει την εικόνα της για την εταιρική της υπευθυνότητα καθώς εξασφαλίζει περαιτέρω την ασφάλεια των δεδομένων και των πληροφοριών που διαθέτει στα συστήματα της.
- Δείξει πως σέβεται τα προσωπικά δεδομένα, διότι η καινούργια αναθεώρηση του ISO 27001: 2013 είναι συμβατή με το νόμο περί προστασίας των προσωπικών δεδομένων GDPR. Έτσι με αυτή την πράξη κινείται μέσω παγκόσμιων αποδεκτών κανόνων για τα προσωπικά δεδομένα και τις πληροφορίες.
- Μειώνει το κόστος και το χρήμα που θα χρειαζόταν να διαθέσει για την εκ νέου πιστοποίηση ενός ISO 27001 καθώς διαθέτει ήδη ISO 9001:2015 που είναι συμβατό με το πρώτο και χρειάζονται μόνο λίγες τροποποιήσεις (Vodafone, 2020).

Με αυτό τον τρόπο στο χαρτοφυλάκιο της που εμπεριέχει ήδη υπάρχουσες πιστοποιήσεις περί ασφάλειας η Vodafone εισάγει και αυτή την νέα εκδοχή του. Από την μία πλευρά τονώνει ακόμα πιο πολύ την σχέση της με τους πελάτες και τους συνεργάτες της, από την άλλη αποκτά ανταγωνιστικό πλεονέκτημα έναντι των αντιπάλων της. Σε μια εποχή όπου τα προσωπικά δεδομένα λόγω της τεχνολογίας είναι περισσότερο προσβάσιμα και ευάλωτα από ποτέ η εταιρεία οχυρώνεται με τις απαραίτητες διαδικασίες και ελέγχους.

Στην **Εικόνα 8** δίνεται το πιστοποιητικό έγκρισης για το ISO 27001:2013 το οποίο εκδόθηκε στις 24 Ιανουαρίου του 2019 και ίσχυε μέχρι τις 11 Νοεμβρίου του ίδιου έτους. Στο πεδίο εφαρμογής συναντάμε όλα τα στοιχεία που βρήκαμε και στα αντίστοιχα των εκδόσεων του ISO 9001 με την προσθήκη της «διαχείρισης

πληροφοριών των πελατών στην αλυσίδα καταστημάτων της Vodafone» ενώ υπάρχει και η δήλωση εφαρμοσιμότητας του προτύπου.

Lloyd's Register

ΠΙΣΤΟΠΟΙΗΤΙΚΟ ΕΓΚΡΙΣΗΣ

Με το παρόν πιστοποιείται ότι το Σύστημα Διαχείρισης της:

VODAFONE-ΠΑΝΑΦΟΝ

ΑΝΩΝΥΜΗ ΕΛΛΗΝΙΚΗ ΕΤΑΙΡΙΑ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ Α.Ε.

Τζαβέλλα 1-3, 15231 Χαλάνδρι, Ελλάδα

έχει εγκριθεί από το Lloyd's Register Quality Assurance σύμφωνα με το ακόλουθα πρότυπα:

ISO/IEC 27001:2013

Gilles Bessiere - Area Technical Manager

Εκδόθηκε από: Hellenic Lloyd's S.A.

για λογαριασμό της: Lloyd's Register Quality Assurance Limited

Το παρόν πιστοποιητικό ισχύει μόνον σε συνδυασμό με το παράρτημα πιστοποιητικού ιδίου αριθμού στο οποίο αναγράφονται οι σχετικές με την παρούσα έγκριση τοποθεσίες.

Τρέχουσα Ημερομηνία Έκδοσης: 24 Ιανουαρίου 2018
Ημερομηνία Λήξης: 11 Νοεμβρίου 2019
Αριθμός Ταυτότητας Πιστοποιητικού: 10053507

Αρχικές Εγκρίσεις:
ISO/IEC 27001 – 24 Οκτωβρίου 2007

Αριθμοί έγκρισης: ISO/IEC 27001 – 0034138

Το πεδίο εφαρμογής της έγκρισης ισχύει για:

Σχεδιασμός, ανάπτυξη, υλοποίηση, λειτουργία, συντήρηση και επιτήρηση δικτύων κινητής και σταθερής επικοινωνίας, ασυρμάτων τεχνολογιών διασύνδεσης και δικτύων δεδομένων. Σχεδιασμός, ανάπτυξη, παροχή, πώληση, τιμολόγηση και υποστήριξη προϊόντων/υπηρεσιών, κινητής και σταθερής επικοινωνίας, υπηρεσιών διασύνδεσης, δεδομένων, πρόσβασης διαδικτύου και πληροφορικής. Εμπορία εξοπλισμού κινητής και σταθερής επικοινωνίας και διαδικτύου. Σχεδιασμός, ανάπτυξη, εγκατάσταση, υποστήριξη και συντήρηση πληροφοριακών συστημάτων και λειτουργία μηχανογραφικού κέντρου. Παροχή υπηρεσιών μετά την πώληση και υπηρεσιών τηλεφωνικής εξυπηρέτησης. Διαχείριση πληροφοριών πελατών στην αλυσίδα καταστημάτων VODAFONE (Ιδιόκτητα και Συνεργατών). Πωλήσεις και εξυπηρέτηση μετά την πώληση προϊόντων και υπηρεσιών κινητής και σταθερής επικοινωνίας και πρόσβασης διαδικτύου.

Δήλωση εφαρμοσιμότητας - (SoA – Ver 4, 5/10/2017)

UKAS MANAGEMENT SYSTEMS

001

Εικόνα 8: Πιστοποιητικό ISO 27001:2013 για την Vodafone *(Πηγή*: (Vodafone, 2020))

7.8 Συνεισφορά των δύο προτύπων στην εταιρεία

Όπως είδαμε η Vodafone έχει πιστοποιηθεί στη πορεία της εξέλιξης της στο χώρο των τηλεπικοινωνιών με τα πρότυπα ISO 9001 και ISO 27001. Το πρώτο από τα δύο πρότυπα που έλαβε πιστοποίηση ήταν το ISO 9001 για το Σύστημα Διαχείρισης της Ποιότητας. Αυτή η πιστοποίηση ήταν η πρώτη που δόθηκε σε εταιρεία λιανικής πώλησης στην Ελλάδα και την θωράκισε απέναντι στους ανταγωνιστές της. Έπειτα από το ISO 9001 ακολούθησε η πιστοποίηση με το ISO 27001 για την Διαχείριση και Ασφάλεια των πληροφορίων και των δεδομένων. Έχοντας ήδη την πιστοποίηση ISO 9001 η Vodafone γνώριζε την διαδικασία που έπρεπε να ακολουθηθεί και για την επόμενη πιστοποίηση στο τομέα της ασφάλειας. Επιπλέον, επειδή υπάρχουν πολλά κοινά σημεία μεταξύ των δύο αυτών πιστοποιήσεων δεν χρειάστηκε να ακολουθήσει όλη την διαδικασία πιστοποίησης από την αρχή αλλά να γίνουν οι κατάλληλες μετατροπές στις διαφορές των δύο προτύπων.

Έχοντας εξασφαλίσει πως σαν εταιρεία παρέχει ποιοτικά προϊόντα και υπηρεσίες στους πελάτες της με βάση το ISO 9001, κινήθηκε στο τομέα της ασφάλειας με το ISO 27001 ώστε να καλύψει όλες τους τις απαιτήσεις. Η υιοθέτηση του πρώτου χάραξε το δρόμο ώστε να υιοθετηθεί και το δεύτερο και να θωρακιστεί η εταιρεία ενάντια στους ανταγωνιστές της σε θέματα πλέον όχι μόνο ποιότητας και ασφάλειας. Επομένως, το ISO 27001 ήταν ο καλύτερος πιθανός συνδυασμός που θα μπορούσε να προκύψει για το πρώτο πρότυπο.

Οι παραπάνω πιστοποιήσεις διασφάλισαν την συμμόρφωση με τα Συστήματα Διαχείρισης με σκοπό την παροχή υψηλής ποιότητας υπηρεσιών, προϊόντων και εξυπηρέτησης για τους πελάτες αλλά και τους συνεργάτες της εταιρείας, εξασφαλίζοντας παράλληλα ένα ασφαλές εργασιακό περιβάλλον για τους εργαζομένους (BusinessNews, 2017).

Συμπεράσματα

Ο στόχος αυτής της διπλωματικής εργασίας ήταν να γίνει σύγκριση μεταξύ δύο πολύ γνωστών και σημαντικών προτύπων ISO, του ISO 9001 που ασχολείται με την διαχείριση ποιότητας και οργάνωσης στην επιχείρηση και του ISO 27001 που αφορά την ασφάλεια των πληροφοριών σε μια επιχείρηση. Από την ξεχωριστή ανάλυση για τα δύο πρότυπα και την μελέτη τόσων των σημείων τομής όσο και των διαφορών τους προέκυψαν κάποια σημαντικά συμπεράσματα.

Αρχικά μπορούμε να πούμε πως βασική πιστοποίηση πλέον για κάθε επιχείρηση αποτελεί αυτή του ISO 9001 καθώς δείχνει πως η επιχείρηση εστιάζει στην ποιότητα των προϊόντων και των υπηρεσιών που παρέχει, έχει σωστή εσωτερική οργάνωση και δεσμεύεται για συνεχή ποιοτική βελτίωση των εκροών που προσφέρει στους πελάτες της. Ένα άλλο σημαντικό γνώρισμα αυτής της πιστοποίησης είναι πως έχει την απαίτηση η στόχευση της επιχείρησης να είναι πελατοκεντρική. Η νεότερη αναθεώρηση του προτύπου, το ISO 9001:2015 προσθέτει την ανάλυση με βάση την διακινδύνευση ώστε να βοηθήσει την επιχείρηση να αντιμετωπίσει πιθανές απειλές στο σύγχρονο και δύσκολο επιχειρησιακό περιβάλλον.

Όσον αφορά το ISO 27001 έχει μια μεγάλη πορεία, στην αρχή ως πρότυπο που δημιουργήθηκε στην Βρετανία και έπειτα το 2005 ως διεθνές πρότυπο ISO. Είναι το πρότυπο εκείνο που καθορίζει ότι πραγματοποιούνται όλες οι απαραίτητες ενέργειες ώστε οι πληροφορίες που κατέχει μια επιχείρηση είναι ασφαλείς. Επίσης, παρέχει στην επιχείρηση οδηγίες και σχέδια για το πώς να αντιμετωπίσει μια κατάσταση απειλής. Στο σύγχρονο περιβάλλον όπου οι υποκλοπές προσωπικών δεδομένων και άλλων πληροφοριών από τα πληροφοριακά συστήματα γίνονται ολοένα και περισσότερες μια τέτοια πιστοποίηση ενισχύει την αξιοπιστία των επιχειρήσεων στο τομέα αυτό. Επιπλέον, η τελευταία αναθεώρηση του ISO έχει το πλεονέκτημα πως συμβαδίζει και με νόμο περί προσωπικών δεδομένων GDPR.

Ένα άλλο σημαντικό συμπέρασμα είναι πως τα δύο πρότυπα ISO έχουν αρκετά κοινά σημεία που αφορούν κυρίως τις διαδικασίες ελέγχου, διοίκησης (κυρίως στο κομμάτι του πως ασκείται η ηγεσία) αλλά και ενδιαφερόμενων μερών. Το περιεχόμενο αποτελεί σημείο διαφοροποίησης. Πολλοί είναι οι οργανισμοί που προσπαθούν λόγω των κοινών σημείων να έχουν και τα δύο πρότυπα αφού η ύπαρξη του ενός συνιστά

εύκολη υπόθεση την ενσωμάτωση του δεύτερου με κάποιες διαφοροποιήσεις. Κοινό θετικό στοιχείο αποτελεί το γεγονός της εξέλιξης και ανάπτυξης των δύο προτύπων μέσω των διαρκών αναθεωρήσεων και βελτιώσεων τους. Η μεγαλύτερη διαφορά τους είναι πως το ISO 9001 δεν εμπεριέχει κάποια οδηγία την αντιμετώπιση κινδύνου της ασφάλειας των πληροφοριών.

Τέλος, με την μελέτη περίπτωσης της Vodafone Ελλάδος είδαμε πως η συγκεκριμένη επιχείρηση λαμβάνοντας τις δύο αυτές πιστοποιήσεις θεωρήθηκε πρωτοπόρος στο τομέα της. Με το ISO 9001 εξασφάλισε πως παρέχονται οι ίδιες ποιοτικές-πελατοκεντρικές υπηρεσίες σε όλα τα καταστήματα της, ενώ με το ISO 27001 μπόρεσε να ξανακερδίσει την εμπιστοσύνη των πελατών της περί ασφάλειας προσωπικών δεδομένων ύστερα από το σκάνδαλο υποκλοπών κινητών τηλεφώνων το 2005.

Επίλογος

Οι σημερινοί-οργανισμοί θέλουν να αποκτήσουν πιστοποιήσεις είτε αυτές αφορούν την ποιότητα των προϊόντων τους είτε την ασφάλεια των πληροφορίων των συστημάτων τους ή ακόμα και τις συνθήκες εργασίας σε ένα περιβάλλον εργασίας. Σε αυτήν την εργασία αναλύθηκαν δύο από τα πιο σημαντικά πρότυπα ISO, το ISO 9001 και το ISO 27001 με το πρώτο να αφορά την ποιότητα και το δεύτερο την ασφάλεια των πληροφοριών. Όπως είδαμε η ποιότητα έχει πολλές μορφές για μια επιχείρηση και πρέπει να διατηρείται. Κομμάτι ωστόσο της αξιοπιστίας μιας επιχείρησης αποτελεί και το κατά πόσο είναι ικανή να παρέχει ασφάλεια στις πληροφορίες που τις εμπιστεύονται οι πελάτες της.

Συχνό είναι το φαινόμενο στον επιχειρησιακό κόσμο να γίνεται προσπάθεια έτσι ώστε να υπάρχουν και οι δύο αυτές πιστοποιήσεις έτσι ώστε η επιχείρηση να έχει λάβει πιστοποιήσεις τέτοιες που θα την βοηθούν να λειτουργεί καλύτερα, να προσφέρει ποιοτικότερα προϊόντα και να συμβαδίζει με τους κανόνες ώστε να παρέχει την απαραίτητη ασφάλεια στα δεδομένα που κατέχει. Άλλωστε η ενσωμάτωση ενός από τα δύο πρότυπα όταν ήδη προϋπάρχει ένα από αυτά είναι πιο εύκολη καθώς δεν επαναλαμβάνεται από την αρχή η διαδικασία της εφαρμογής.

Όλα τα παραπάνω στοιχεία δεν ανήκουν μόνο σε μελέτες της διεθνούς βιβλιογραφίες αλλά βρίσκονται γύρω μας στον επιχειρηματικό κόσμο. Το παράδειγμα της μελέτης περίπτωσης με την Vodafone στη χώρα μας δείχνει πως η υιοθέτηση τέτοιων προτύπων από την εταιρεία μόνο οφέλη έφερε στην εταιρεία.

Βιβλιογραφία

Ξένη Βιβλιογραφία

Abbas Ahmed. (2011, February). *Business Performance Improvement Resource* . Ανάκτηση από Τοποθεσία Web της Business Performance Improvement Resource : https://blog.bpir.com/latest-news/china-first-in-iso-9001-iso14001-certifications-for-2009/

Basak Manders, Vries, H. J., & K. B. (2016, February-March). ISO 9001 and product innovation: A literature review and research framework. *Technovation*, pp. 41-55. doi:https://doi.org/10.1016/j.technovation.2015.11.004

Blyth M. (2008). *Risk and security management: protecting people and sites worldwide.* Hoboken, N.J.: John Wiley & Sons.

BQC-Business Quality Certification. (n.d.). Ανάκτηση από Τοποθεσία Web της BQC : https://bqc.gr/iso-27001

BusinessNews. (2017, Μάρτιος 13). *businessnews,*. Ανάκτηση από Τοποθεσία Web της business news: https://www.businessnews.gr/el/epixeiriseis/texnologia/vodafone-pistopoiiseis-gia-diaheirisi-kai-poiotita

David A. Garvin. (1988). *Managing Quality: The Strategic and Competitive Edge.* Simon and Schuster.

Deloitte. (2020). *Financial Services Global Security Study.* London : Deloitte .

Dey.M. (2007). *Information security management-A practical approach .* AFRICON .

Dr.Moyassar I. Ahmed. (2010). A comparative study of Deming's and Juran's total works: changing the quality culture toward Total Quality Management. *Quality Management* , 24.

Excellence & Lean. (2016). *Excellence-lean*. Ανάκτηση Σεπτεμβριος 13, 2020, από Τοποθεσία Web της Excellence-lean: https://www.excellence-lean.gr/ypiresies/symvouleutikes-ypiresies/business-excellence-diaxeirisi-poiotitas-systimata-iso/

Georg Disterer. (2013, April). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*, pp. 92-100. doi:10.4236/jis.2013.42011

Harris S. (2007). *CISSP All in one Exam Guide.* New York : Mc Graw Publishing .

IHS Markit. (n.d.). *IHS Markit*. Ανάκτηση 9 13, 2020 , από Τοποθεσία Web της IHS Markit: https://ihsmarkit.com/products/iso-standards.html

insilico consulting. (n.d.). Ανάκτηση από Τοποθεσία Web της insilico consulting: http://www.insilico.gr/index.php?option=com_content&view=category&id=80&Itemid=472

International Organization for Standardization. (2015). *International Classification for Standards.* Geneva: ISO. Ανάκτηση από

https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/international_classification_for_standards.pdf

ISO - International Organisation for Standardisation. (2019). *2018 Survey Results - ISO certification to various management systems.* QPro Australia. Ανάκτηση από https://www.qproaustralia.com.au/uploads/2/9/5/6/2956092/iso_certification_statistics_-_2018.pdf

ISO 27001. (2005). Information Technology, Security Techniques, Information Security Management Systems, Requirements. *International Organization for Standardization ISO.* Geneve.

ISO. (n.d.). *ISO.org* . Ανάκτηση 9 14, 2020, από Τοποθεσία Web της ISO: https://www.iso.org/organizations-in-cooperation-with-iso.html

itgovernance. (2020, June). Ανάκτηση από Τοποθεσία Web της itgovernance: https://www.itgovernance.co.uk/iso27000-family

Juan José Tarí, José Francisco Molina-Azorín, & Iñaki Heras. (2012, May). Benefits of the ISO 9001 and ISO 14001 standards: A literature review. *Journal of Industrial Engineering and Management*, σσ. 297-332. doi:http://dx.doi.org/10.3926/jiem.488

Kwo-Shing Hong, Yen-Ping Chi, Louis R Chao, & Jih-Hsing Tang. (2013). An integrated system theory of information security management. *Information Management & Computer Security*, 243-248.

Leal Rhand. (2018, March 26). *Advisera*. Ανάκτηση από Τοποθεσία Web της Advisera.com: https://advisera.com/27001academy/blog/2018/03/26/how-to-perform-background-checks-according-to-iso-27001/

Lloyd's Register. (2020). *Lloyd's Register.org*. Ανάκτηση από Τοποθεσία Web της lr.org: https://www.lr.org/el-gr/iso-27001/

Mukherjee, A. (2003, April 1). Franchise management: a model of service-quality interactions. *International Journal of Quality & Reliability Management*, σσ. 325-344. doi:https://doi.org/10.1108/02656710310461323

nqa. (n.d.). *MANAGE YOUR INTEGRATION: ISO 9001 TO ISO 27001 GAP GUIDE.* nqa. Ανάκτηση από https://www.nqa.com/getattachment/Toolink-Links/ISO-9001-to-ISO-27001-Gap-Guide/NQA-ISO-9001-to-ISO-27001-Gap-Guide.pdf?lang=en-us

Philip Bruney. (2020, August 31). *risk3sixty*. Ανάκτηση από Τοποθεσία Web της risk3sixty: https://risk3sixty.com/2020/08/31/combining-iso-9001-and-iso-27001-efforts/

Roger Atkinson. (1999). Project management: cost, time and quality two best guesses and a phenomenon, its time to accept other success criteria . *nternational Journal of Project Management*, pp. 337-342.

Roxanne Oclarino. (2020, March 10). *iso.org*. Ανάκτηση από Τοποθεσία Web της iso.org: https://www.iso.org/news/ref2488.html

Saleh Ali Husseini, Al-shami, S. S., S.-F. F., & S. A. (2018, August). Impact of ISO 9001: 2008 Certification on Consumer Satisfaction . *Journal of Advance Research in Dynamical & Control Systems*, pp. 322-331.

Sennewald, C. A. (2011). *Effective security management,.* Burlington: Butterworth-Heinemann.

Sirdeshmukh D., Singh J., & B., S. (2002, January). Consumer trust, value and loyalty in relational exchanges . *Journal of marketing* , pp. 16-37 .

SnežanaTopalović. (2014). The Implementation of Total Quality Management in Order to Improve Production Performance and Enhancing the Level of Customer Satisfaction. *8th International Conference Interdisciplinary in Engineerig* (σσ. 1016-1022). Tirgu-Mures,Romania: Procedia Technology.

Staines A. (2000). Benefits of an ISO 9001 certification – the case of a Swiss regional hospital. *International Journal of Health Care Quality Assurance*, pp. 27-33.

Stojanovic Strahinja. (2016, September 27). *Advisera*. Ανάκτηση από Τοποθεσία Web της Advisera: https://advisera.com/9001academy/blog/2016/09/27/how-to-integrate-iso-9001-and-iso-27001/

Stojanovic Strahinja. (n.d.). *advisera*. Ανάκτηση 9 13, 2020, από Τοποθεσία Web της advisera: https://advisera.com/9001academy/knowledgebase/infographic-iso-90012015-vs-2008-revision-what-has-changed/

Terje Aven. (2015). *Risk Analysis.* Stavanger: John Willey & Sons,.

Thandapani, D., K. G., S.R. Devadasan, C.G. Sreenivasa, & R. Murugesh. (2011, February). ISO 9001:2000 based quality management system via ABET-based accreditation. *International Journal of Productivity and Quality Management*, pp. 125-147. doi:10.1504/IJPQM.2011.038681

The free dictionary. (n.d.). *el.thefreedictionary*. Ανάκτηση από Τοποθεσία Web της el.thefreedictionary: https://el.thefreedictionary.com/%CE%B1%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1

TÜV HELLAS (TÜV NORD). (2016). *Ερμηνεία των Απαιτήσεων του Προτύπου ISO 9001:2015:Οδηγός για το Πρότυπο ISO 9001:2015.* TÜV HELLAS (TÜV NORD). Ανάκτηση από http://news.tuv-nord.gr/April_2016/assets/tuv-iso-9001-2015.pdf

Vodafone. (2020). *Vodafone.gr* . Ανάκτηση από Τοποθεσία Web της Vodafone.gr .

Vodafone annual. (2007). *Απολογισμός εταιρικής υπευθυνότητας Vodafone 2006-2007.* Vodafone.

Vodafone annual report. (2019). *Έκθεση Βιώσιμης Ανάπτυξης 2018-2019.* Αθήνα : Vodafone .

Vodafone- Διοικητικό Συμβούλιο. (2019). *Ετήσια Χρηματοοικονομική Έκθεση 2019- Οικονομική χρήση από 1 Απριλίου 2018 έως 31 Μαρτίου 2019.* Αθήνα: Vodafone. Ανάκτηση από file:///C:/Users/USER/Downloads/vodafone-panafon-aeet-etisies-oikonomikes-katastaseis-chrisis-1-4-2018-eos-31-3-2019.pdf

Vodafone.gr. (2020). Ανάκτηση από Τοποθεσία Web της Vodafone gr: https://www.vodafone.gr/vodafone-ellados/

Vodafone-Panafon. (2001, Οκτώβριος 1). *Vodafon.gr* . Ανάκτηση από Τοποθεσία Web της Vodafone,gr : https://www.vodafone.gr/vodafone-ellados/digital-press-room/deltia-typou/20011001-dipli-pistopoiisi-dipli-epitychia-gia-tin-panafon-services/

Vodafone-Ανασκόπηση. (2020). *Vodafone.gr* . Ανάκτηση από Τοποθεσία Web της Vodafone.gr : https://www.vodafone.gr/vodafone-ellados/arthra/anaskopisi-taxidi-sthn-poiotita/

Walker Rhet H, .., & W. Johnson Lester. (2009, January). Signaling intrinsic service quality and value via accreditation and certification. *Journal of Service Theory and Practice*, pp. 85-105.

Zoé Hoy, & Andrea Foley. (2014 , January 14). A structured approach to integrating audits to create organisational efficiencies: ISO 9001 and ISO 27001 audits. *Total quality management & business excellence* , pp. 690-702.

Ελληνική Βιβλιογραφία

Ανθής Δημήτρης. (n.d.). *Epaggelmaties*. Ανάκτηση 9 2, 2020, από Τοποθεσία Web της Epaggelmaties.com: http://www.epaggelmaties.com/anthis/iso.html

Γ. Μπαμπινιώτης. (2004). *Λεξικό για το σχολείο και το γραφείο.* Αθήνα: Κεντρο Λεξικολογίας Ε.Π.Ε.

Γουσγούνης Ι. Νικόλαος. (2017, March 8). *Successkeys.GR*. Ανάκτηση από Τοποθεσία Web της Successkeys.GR: https://www.successkeysgr.com/post/2017/03/08/4-%CF%84%CE%B1-%CE%BF%CF%86%CE%AD%CE%BB%CE%B7-%CE%B1%CF%80%CF%8C-%CF%84%CE%BF-isoiec-270012013

ΕΛΟΤ ΕΝ ISO 8402:1994. (1994). *Διαχείριση της ποιότητας και διασφάλιση της ποιότητας-Λεξιλόγιο.* ΕΛΟΤ.

Καθημερινή (ηλεκτρονική έκδοση). (2019, Νοέμβριος 13). Ανάκτηση Σεπτέμβριος 13, 2020, από Τοποθεσία Web της Kathimerini.gr: https://www.kathimerini.gr/economy/business/1051459/ayxisi-leitoyrgikon-kerdon-kai-esodon-6-i-vodafone-to-a-examino/

Κουτσογιάννη Λογιστικό Γραφείο. (2016). *Το ISO με απλά λόγια.* Μυτιλήνη: Ευ ΕΠΙΧΕΙΡΕΙΝ. Ανάκτηση από https://www.efep.gr/wp-content/uploads/2016/04/ISO-simplified-.pdf

Κυριακίδου Ντίνα. (2006, Μάρτιος 2). "Greek Watergate" Scandal Sends Political Shockwaves. *Reuters*. Ανάκτηση Σεπτέμβριος 13, 2020

Παναγιώτης Καραλίβανος. (2017, Νοέμβριος). *ΝΗΡΗΙΣ Α.Ε.* Ανάκτηση από Τοποθεσία Web της ΝΗΡΗΙΣ Α.Ε>: https://www.niriis.gr/gdpr/iso-27001-pos-voithaei/

Παπαθεωδόρου Χρήστος. (n.d.). *Πληροφοριακά συστήματα.* Τμήμα Αρχειονομίας-Βιβλιοθηκονομίας. Ιόνιο Πανεπιστήμιο.

Σπύρος Γκούμας, & Κατερίνα Τέφα. (2018). *Διαχείριση ποιότητας στη μικρή επιχείρηση.* ΙΜΕ ΓΣΕΒΕΕ.

ΤΕΧΝΙΚΟ ΕΠΙΜΕΛΗΤΗΡΙΟ ΕΛΛΑΔΟΣ. (n.d.). *Συστήματα διαχείρισης ποιότητας-Γενικές αρχές.* Τμήμα Κεντρικής Μακεδονίας.