Ελληνική Δημοκρατία
Υπουργείο Διοικητικής Ανασυγκρότησης

εκδδα
ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ & ΑΥΤΟΔΙΟΙΚΗΣΗΣ

ΕΘΝΙΚΗ ΣΧΟΛΗ ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ
ΚΑΙ ΑΥΤΟΔΙΟΙΚΗΣΗΣ

ΚΕ΄ ΕΚΠΑΙΔΕΥΤΙΚΗ ΣΕΙΡΑ

ΤΕΛΙΚΗ ΕΡΓΑΣΙΑ

ΤΙΤΛΟΣ

«Η εφαρμογή των οδηγιών του ISO 2700Χ στο Δημόσιο Τομέα»

ΤΜ. ΕΞΕΙΔΙΚΕΥΣΗΣ: Ψηφιακής Πολιτικής

Επιβλέπων:

Δρ. Αντώνιος Στασής

Σπουδαστής/στρια:

Παναγιώτης Τζανετόπουλος

ΑΘΗΝΑ – 2018

Στη Μαρία,

από την οποία μαθαίνω συνεχώς

ότι και τα αδύνατα γίνονται δυνατά.

Η ΕΦΑΡΜΟΓΗ ΤΩΝ ΟΔΗΓΙΩΝ ΤΟΥ ISO 27000Χ ΣΤΟ ΔΗΜΟΣΙΟ ΤΟΜΕΑ

«Η τεχνολογία πληροφοριών και η επιχειρηματικότητα είναι πλέον αναπόσπαστα συνυφασμένες. Δεν πιστεύω ότι κάποιος θα μπορέσει να αναφερθεί επί της ουσίας στο ένα χωρίς να αναφερθεί στο άλλο».

Billy Gates

ΕΣΔΔΑ
Τζανετόπουλος Παναγιώτης

Δήλωση

Δηλώνω ρητά ότι, η παρούσα εργασία αποτελεί αποκλειστικά προϊόν προσωπικής εργασίας, δεν παραβιάζει καθ' οιονδήποτε τρόπο πνευματικά δικαιώματα τρίτων και δεν είναι προϊόν μερικής ή ολικής αντιγραφής.

Αθήνα, 12 / 12 / 2018

Παναγιώτης Τζανετόπουλος

Ευχαριστίες

Ευχαριστώ θερμά:

- *Τον επιβλέποντά μου, **δρ. Αντώνιο Στασή**, για όλες τις πολύτιμες συμβουλές και την καθοδήγησή του σε ακαδημαϊκό και τεχνικό επίπεδο καθ' όλη τη διάρκεια εκπόνησης της παρούσας εργασίας, καθώς επίσης και για την άψογη συνεργασία μας.*
- *Τα στελέχη και τους υπαλλήλους της Γενικής Γραμματείας Πληροφοριακών Συστημάτων του Υπουργείου Οικονομικών, συγκεκριμένα τους κ.κ. **Γεώργιο Κωτσάκη**, προϊστάμενο του Αυτοτελούς Τμήματος Ασφαλείας, **Στράτο Μακριδάκη,** στέλεχος του ιδίου Τμήματος και **Δημήτριο Καπόπουλο,** στέλεχος του Αυτοτελούς Τμήματος Στρατηγικής & Προγραμματισμού, για την άμεση ανταπόκρισή τους και την παροχή σημαντικής πληροφόρησης και υποστηρικτικού υλικού σχετικά με τη λειτουργία των πληροφοριακών συστημάτων της υπηρεσίας τους, την υφιστάμενη κατάσταση και τη μελλοντική υλοποίηση βελτιωτικών δράσεων.*
- *Την κα **Αναστασία Παπαστυλιανού**, στέλεχος του ΙΝΕΠ του ΕΚΔΔΑ, καθώς και τον κο **Βασίλειο Κουρμπάνη**, προϊστάμενο του Τμήματος Στρατηγικής και Συντονισμού της ΕΓΔΙΧ και απόφοιτο της ΕΣΔΔΑ, οι οποίοι ως γνώστες του εν επικεφαλίδι θέματος, παρείχαν πολύτιμες συμβουλές.*
- *Το διδακτικό, ερευνητικό και διοικητικό προσωπικό της ΕΣΔΔΑ, για την πολύτιμη αρωγή τους και την άοκνη προσφορά τους στο έργο της Σχολής.*

- *Τέλος, ευχαριστώ από καρδιάς τους δικούς μου ανθρώπους, για την υπομονή τους και τη στήριξή τους σε όλα τα στάδια της πορείας μου στην ΕΣΔΔΑ.*

Περίληψη

Στην συγκεκριμένη εργασία θα γίνει μία ανάλυση των προτύπων ISO και ιδιαίτερα των προτύπων της οικογένειας ISO 2700 σε σχέση με την χρησιμότητα του στον δημόσιο τομέα. Η οικογένεια ISO 27000αφορά την ασφάλεια των πληροφοριών και αποτελεί ένα τομέα που δείχνει συνεχή μεταβλητότητα και προσαρμογή κάθε φορά στα νέα δεδομένα.

Στο πρώτο κεφάλαιο της εργασίας θα γίνει μία ανάλυση των προτύπων ποιότητας αλλά και θα γίνει προσπάθεια να δοθεί ένας ορισμός για την ποιότητα αυτήν καθ' αυτήν. Στην συνέχεια θα παρουσιαστούν τα πρότυπα ISO μέσα από μία σύντομη ιστορική αναδρομή των προτύπων αλλά και του οργανισμού. Ιδιαίτερη αναφορά θα γίνει στα οφέλη και τα πλεονεκτήματα που αποκτά ένας οργανισμός από την πιστοποίηση του με ένα τέτοιο πρότυπο αλλά και τα οφέλη, πιο συγκεκριμένα, του δημόσιου τομέα από μια τέτοια πιστοποίηση.

Στο δεύτερο κεφάλαιο θα μελετηθούν τα πρότυπα της οικογένειας 27000. Οι τομείς στους οποίους αυτά έχουν εφαρμογή αλλά και τα πλεονεκτήματα που απορρέουν από την πιστοποίηση. Στο συγκεκριμένο κεφάλαιο θα γίνει εκτενή αναφορά στα πρότυπα ISO/ IEC 27001:2005 & 27001:2013, το οποίο και αποτελεί το πιο διαδεδομένο πρότυπο αυτής της οικογένειας αλλά και στην διαδικασία πιστοποίησης κατά το συγκεκριμένο πρότυπο.

Στο τρίτο κεφάλαιο θα δούμε την διαδικασία πιστοποίησης με τα πρότυπα ISO/ IEC 27001:2005 & 27001:2013, από τη Γενική Γραμματεία Πληροφοριακών

Συστημάτων (ΓΓΠΣ) του Υπουργείου Οικονομικών. Αυτή η διαδικασία περιλαμβάνει τα τεχνικά χαρακτηριστικά, τις προϋποθέσεις που θα πρέπει να πληρεί ο φορέας υλοποίησης αλλά και τον αντικειμενικό σκοπό του όλου εγχειρήματος.

Λέξεις-κλειδιά:

Ασφάλεια πληροφοριών, πληροφοριακό σύστημα, πρότυπο, πιστοποίηση, ISO, 27000, 27001, 27002.

Abstract

In this work, an analysis of the ISO standards and in particular of the ISO 2700 family standards will be carried out in relation to its usefulness in the public sector. The ISO 27000 family is about information security and is a sector that shows continued volatility and adaptation to new data every time.

The first chapter of the work will analyze the quality standards, but an attempt will be made to give a definition of this quality in itself. Next, ISO standards will be presented through a brief historical review of the standards and the organization. Particular reference will be made to the benefits and advantages that an organization gains from its certification with such a model but also the benefits, in particular, of the public sector from such certification.

The second chapter will study the 27000 family standards. The areas in which they apply, as well as the benefits of certification. In this chapter, reference will be made to the ISO / IEC 27001: 2005 & 27001:2013 standard, which is the most widely used model of this family, but also to the certification process for that particular standard.

In Chapter Three we will look at the ISO / IEC 27001:2005 & 27001:2013 certification process by the General Secretariat of Information Systems (GGPS – GSIS) of the Greek Ministry of Finance. This process includes the technical characteristics, the conditions that the implementing body should fulfill, and the objective of the whole project.

Key words:

Information security, informative system, standard, certification, ISO, 27000, 27001, 27002.

Περιεχόμενα

Εισαγωγή

Στην σημερινή εποχή οι εταιρείες που παράγουν ένα προϊόν ή προσφέρουν μια υπηρεσία, έχουν πολύ μεγάλο ανταγωνισμό μεταξύ τους. Ο σκοπός αυτών των εταιρειών είναι να επικρατήσουν, μέσα στο σημερινό οικονομικό σύστημα, έτσι ώστε να είναι κερδοφόρες και να μπορούν να αναπτυχθούν περαιτέρω. Οποιαδήποτε εταιρεία όμως για να το καταφέρει αυτό θα πρέπει να είναι να βασισμένη σε ένα σοβαρό πλάνο και σε μια σωστή διοίκηση. Το σημαντικότερο όμως κομμάτι της είναι το ίδιο το προϊόν ή υπηρεσία που διαθέτει η εταιρεία στην αγορά. Αν δεν πληροί τις ανάγκες των καταναλωτών τότε είναι προφανές ότι δεν πρόκειται να καταφέρει να κερδίσει την αγορά. Για να το επιτύχει αυτό όμως θα πρέπει το προϊόν ή η υπηρεσία να έχουν την κατάλληλη ποιότητα, έτσι ώστε να ανταπεξέρχονται στις ανάγκες των καταναλωτών. Για αυτόν τον λόγο έχουν δημιουργηθεί πρότυπα διαχείρισης ποιότητας που μπορούν να καθοδηγήσουν την εκάστοτε εταιρεία σε έναν σωστό δρόμο όσον αφορά όχι μόνο την ποιότητα ενός προϊόντος ή υπηρεσίας αλλά και ολόκληρης της λειτουργίας της.

Όμως και σε επίπεδο δημόσιας διοίκησης η ανταγωνιστικότητα της κάθε ευρωπαϊκής χώρας επηρεάζεται σε μεγάλο βαθμό από την ποιότητα των παρεχόμενων υπηρεσιών του δημοσίου. Η ποιότητα αυτών των υπηρεσιών εξαρτάται σε μεγάλο βαθμό από την ποιότητα των πολυ-δημοσίων πολιτικών . Στον ορίζοντα της οικονομικής ύφεσης και στο πλαίσιο των στόχων της μείωσης των δημοσίων δαπανών, είναι σημαντικό το γεγονός ότι η απόδοση ανάκτησης συνοδεύεται από ισοδύναμη ώθηση στην βελτίωση της ποιότητας. Τα εργαλεία της διαχείρισης της ποιότητας στις δημόσιες υπηρεσίες INCO-ISO έχουν αρχίσει να εξαπλώνονται σε όλες τις χώρες της Ευρώπης από το 1990 (Ρωσίδης, Μπιτσάνη, 2011).

Βέβαια, ένα πρότυπο ποτέ δεν μπορεί να ακολουθηθεί κατά γράμμα διότι η κάθε εταιρεία ή κάθε δημόσια υπηρεσία είναι ένας ζωντανός οργανισμός με τα δικά της προβλήματα, θέλω, δυνατότητες και πρακτικές, οπότε θα πρέπει η ίδια να θεσπίσει την δικιά της πολιτική ποιότητας η οποία θα στηρίζεται σε κάποιο πρότυπο διαχείρισης ποιότητας αλλά και στην φιλοσοφία των διευθυντικών στελεχών της. Θα πρέπει όμως, να ακολουθούνται κάποια συγκεκριμένα ποιοτικά χαρακτηριστικά που θα έχουν να κάνουν με τα γενικά στοιχεία που θα πρέπει να έχει κάθε πρότυπο ποιότητας. Κάθε πρότυπο ποιότητας θα πρέπει να ασχολείται με κάποια συγκεκριμένα στοιχεία τα οποία είναι:

1. Η ποιότητα που θα πρέπει να διαθέτει ένα προϊόν ή μια υπηρεσία αλλά και πως ορίζεται η ποιότητα στο συγκεκριμένο προϊόν.

2. Τα χαρακτηριστικά που θα πρέπει να διαθέτει ένα προϊόν ή μια υπηρεσία έτσι ώστε να μπορεί να ικανοποιεί στο μέγιστο βαθμό ή και να ξεπερνά αυτό που προσδοκά ο πελάτης της εταιρείας.

3. Ο πελάτης αν και είναι ο κύριος γνώμονας για την ποιότητα ενός προϊόντος δεν θα πρέπει να ξεχνάμε και ότι κάθε προϊόν ή υπηρεσία θα πρέπει να έχει κάποιες συγκεκριμένες προδιαγραφές που θα πρέπει να ικανοποιούνται.

4. Ένα προϊόν έχει κάποια στοιχεία κατασκευής, παραγωγής, μάρκετινγκ και συντήρησης τα οποία θα πρέπει να μπορούν να συγκλίνουν όσο το δυνατόν περισσότερο με τις απαιτήσεις των πελατών (Γκίκα, 2011)

Συνοψίζοντας αυτό που μπορεί να ειπωθεί είναι ότι η διαχείριση ποιότητας ή πρότυπο ποιότητας είναι το σύνολο των προγραμματισμένων ή συστηματικών ενεργειών ή διαδικασιών που είναι απαραίτητες για να εξασφαλίσουν ότι ένα προϊόν ή υπηρεσία θα πληρεί ορισμένες προδιαγραφές.

Στην ουσία η διαχείριση ποιότητας ασχολείται με την οργάνωση της επιχείρησης και την λειτουργία της. Για παράδειγμα αν μια επιχείρηση έχει πιστοποίηση HACCP, αυτό σημαίνει ότι το σύνολο της λειτουργίας της είναι συμμορφωμένο με τους κανόνες του προτύπου διαχείρισης ποιότητας και όχι ότι η ποιότητα ενός προϊόντος είναι επαρκής. Δηλαδή αν μια εταιρεία αλλαντικών που δεν είναι πιστοποιημένη με HACCP, η οποιοδήποτε παραπλήσιο πρότυπο, ακόμα και αν παράγει κάποιο σαλάμι υψηλής ποιότητας δεν μπορεί να θεωρηθεί επαρκής για να προωθεί τα προϊόντα της σε καταστήματα τα οποία ζητάνε πιστοποίηση.

Έτσι λοιπόν σαν σύστημα διαχείρισης ποιότητας ορίζεται η οργάνωση το προσωπικό και τα μέσα που θα χρειαστούν για να διαχειριστεί η ποιότητα και κάθε τέτοιο σύστημα έχει σαν στόχο να τηρούνται και να βελτιώνονται τα χαρακτηριστικά (προδιαγραφές) των προϊόντων ή των υπηρεσιών της εταιρείας για να μπορούν τα προϊόντα της ίδια της εταιρείας να ακολουθούν τον ανταγωνισμό αλλά και τις απαιτήσεις που έχουν οι πελάτες, πράγματα τα οποία αυξάνονται με την πάροδο του χρόνου. Όλα αυτά μας οδηγούν στο συμπέρασμα ότι όλες οι λειτουργίες μιας επιχείρησης μπορούν να επηρεάσουν την τελική ποιότητα ενός προϊόντος ή μιας υπηρεσίας. Από την άλλη πλευρά όμως για μια εταιρεία ή δημόσια υπηρεσία μπορούν να υπάρξουν σημαντικά οφέλη που έχουν να κάνουν με δύο γνώμονες.

- Εσωτερικά οφέλη που πάει να πει ότι η εταιρεία βελτιώνει την εσωτερική επικοινωνία των διαφόρων τμημάτων καθότι όλα πλέον λειτουργούν με κάποιο πρότυπο, οπότε όλα τα τμήματα έχουν σχέδιο λειτουργίας χωρίς να παίρνονται αυθαίρετες αποφάσεις.
- Εξωτερικά οφέλη τα οποία έχουν να κάνουν με κυρίως με το κύρος της εταιρείας απέναντι σε προμηθευτές, πελάτες, κλπ. και αυτό είναι εύκολο να κατανοηθεί. Παραμένοντας στο παράδειγμα της εταιρείας αλλαντικών, αν δύο εταιρείες παράγουν αλλαντικά και η μία είναι πιστοποιημένη με HACCP ενώ η άλλη δεν είναι τότε είναι φυσικό τα super market να αποφασίσουν να

βάλουν στα ράφια τους την πιστοποιημένη εταιρεία αποκλείοντας την άλλη. Κάτι τέτοιο αυξάνει το γόητρο της εταιρείας την ανταγωνιστικότητά της αλλά και επιφέρει έσοδα τα οποία μπορούν να χρησιμοποιηθούν για την περαιτέρω ανάπτυξη της εταιρείας.

Κεφάλαιο 1: Συστήματα διαχείρισης ποιότητας

Η σπουδαιότητα των συστημάτων διαχείρισης ποιότητας, την σημερινή εποχή είναι αδιαμφησβήτητη. Ολόκληρη η διαδικασία από τον προγραμματισμό στην εφαρμογή και τελικά στον έλεγχο των διαδικασιών πιστοποιείται από συγκεκριμένες εταιρείες με συγκεκριμένους κανόνες. Αυτό δείχνει και την σημαντικότητα του όλου συστήματος.

Δεν θα μπορούσε όμως μια εταιρεία που παράγει ένα οποιοδήποτε προϊόν να έχει το ίδιο πρότυπο με μια εταιρεία που παρέχει υπηρεσίες. Ακόμα και δύο εταιρείες που παράγουν προϊόντα δεν θα μπορούσαν να έχουν τα ίδια πρότυπα ποιότητα. Για παράδειγμα μια εταιρεία που παράγει γαλακτοκομικά δεν ήταν δυνατόν να έχει το ίδιο πρότυπο ποιότητας με μια εταιρεία που παράγει αυτοκίνητα. Για αυτό τον λόγο λοιπόν ο κάθε τομέας που δραστηριοποιείται μια επιχείρηση έχει και τα δικά του πρότυπα ποιότητας. Ακόμη και τμήματα κάθε επιχείρησης ή δημόσιας υπηρεσίας μπορούν να πιστοποιηθούν με συγκεκριμένα πρότυπα, κάτι που δείχνει την πολυπλοκότητα των διαδικασιών και της πιστοποίησης ποιότητας.

Έτσι, έχουν αναπτυχθεί μία σειρά από πρότυπα ή συστήματα διαχείρισης τα οποία και εφαρμόζονται από τους ενδιαφερόμενους. Τα σημαντικότερα από αυτά είναι:

- ISO 14001. Το συγκεκριμένο πρότυπο είναι αρκετά γνωστό ανά τον κόσμο και είναι ένα πρότυπο γενικής φύσης. Δεν στοχεύει σε μια γκάμα υπηρεσιών ή προϊόντων αλλά γενικά στην οργάνωση μια επιχείρησης. Γενικά στόχος του είναι να βοηθήσει την επιχείρηση να λειτουργήσει πιο οργανωμένα και να κάνει σωστούς συστηματικούς ελέγχους.
- ISO 22000 & HACCP. Το συγκεκριμένο πρότυπο είναι και αυτό αρκετά γνωστό στον τομέα των επιχειρήσεων. Είναι ένα πρότυπο ποιότητας που ασχολείται με την διαχείριση της ασφάλειας τροφίμων και πλέον είναι αναγκαστικό να το χρησιμοποιούν όσοι ασχολούνται με τον κύκλο της τροφικής αλυσίδας.
- ISO 14001. Το συγκεκριμένο πρότυπο διαχείρισης ποιότητας έχει να κάνει με την συμπεριφορά της εταιρείας ως προς το περιβάλλον. Σκοπός του είναι να συμμορφώσει την συμπεριφορά των δραστηριοτήτων της εταιρείας έτσι ώστε αυτές να μην υποβαθμίζουν το περιβάλλον.
- EUROPGAP ή Agor 2 -1 και 2 - 2 που σκοπεύει στη σωστή διαχείριση της αγροτικής παραγωγής
- ISO 27001. Αυτό το πρότυπο έχει να κάνει με τις πληροφορίες, την διαχείρισή τους και την ασφάλειά τους. Στον τομέα της βιομηχανίας η οποιαδήποτε πληροφορία μπορεί να είναι αρκετή για να φέρει μια επιχείρηση σε πλεονεκτική θέση έναντι των ανταγωνιστών της και έτσι θα πρέπει να υπάρχει μια σωστή διαχείριση αυτών.
- ΕΛΟΤ 1435. Το πρότυπο αυτό είναι το πρότυπο που μπορεί να πάρει μια διαφημιστική εταιρεία που θέλει να προσφέρει υπηρεσίες επικοινωνίας.
- ΕΛΟΤ ΕΝ ISO 9001. Το συγκεκριμένο πρότυπο είναι παγκόσμια διαδεδομένο και αφορά την εφαρμογή και την ανάπτυξη ενός συστήματος διαχείρισης ποιότητας. η δυνατότητά του να αξιολογεί ένα ήδη υπάρχον πρότυπο ποιότητας (ΕΛΟΤ, 2011).

1.1 Η ποιότητα και οι προοπτικές της

Πριν γίνει ανάλυση των συστημάτων ποιότητας θα πρέπει να αναλυθεί η έννοια της ποιότητας. Εξάλλου την ποιότητα καλούνται να πιστοποιήσουν τα συστήματα. Ένας ορισμός για την ποιότητα είναι «ο βαθμός κατά τον οποίο ένα σετ χαρακτηριστικών πληρεί προϋποθέσεις», όπως αναφέρει ο οργανισμός ISO. Το πρότυπο ISO ορίζει την ποιότητα μάλλον ευρέως, διότι περιλαμβάνει κάτι περισσότερο από ένα προϊόν, και επίσης περιλαμβάνει διαδικασίες, οργάνωση, ευθύνες, οδηγίες εργασίας και πόρους. (Hoyle, 2007).

Η ποιότητα δεν σχετίζεται μόνο με τα φυσικά προϊόντα, αλλά έχει επίσης να κάνει με οτιδήποτε από την οδήγηση μια Porsche, ένα κούρεμα ή μια υποθήκη. Ο Joseph Juran καθόρισε την ποιότητα σε ένα κατανοητό τρόπο ως "καταλληλότητα για χρήση", γιατί η ποιότητα εξαρτάται πάντα από τον χρήστη ή τον πελάτη όπου και αν εφαρμόζεται. Αυτός ο ορισμός τονίζει τη σημασία του πελάτη που θα χρησιμοποιήσει το προϊόν (Zink, 1998). Επίσης ο W. Edwards Deming όρισε την καλή ποιότητα ως έναν προβλέψιμο βαθμό ομοιομορφίας και αξιοπιστίας σύμφωνα με τα κατάλληλα ποιοτικά πρότυπα του πελάτη, ενώ η Αμερικάνικη Εταιρεία Ποιότητας ορίζει ότι η ποιότητα υποδηλώνει την αριστεία στα αγαθά και τις υπηρεσίες, ιδίως στον βαθμό που καλύπτουν τις απαιτήσεις και ικανοποιούν τους πελάτες (Campridge, 2012)

Όπως αναμένεται, η ποιότητα μπορεί να οριστεί με πολλούς άλλους τρόπους πέραν των παραπάνω ορισμών. Αυτές οι διαφορετικές προοπτικές, περιλαμβάνουν την ποιότητα της κατασκευής, την ποιότητα του προϊόντος, την ποιότητα του πελάτη, την ποιότητα του περιβάλλοντος και την ποιότητα της διαδικασίας. (Hoyle, 2007). Η ποιότητα της κατασκευής επικεντρώνεται στην παραγωγική διαδικασία και εξασφαλίζει ότι τα προϊόντα κατασκευάζονται όπως προβλέπεται, σύμφωνα με τα πρότυπα παραγωγής. Ο στόχος της ανάπτυξης της ποιότητας των διαδικασιών παραγωγής είναι η πρόβλεψη της ζήτησης και η ελαχιστοποίηση της παραγωγής μη συμμορφούμενων προϊόντων (Lecklin, 2006). Μια άλλη προοπτική είναι η ποιότητα του προϊόντος που επικεντρώνεται στο σχεδιασμό του προϊόντος, δηλαδή πώς πρέπει να μοιάζει το προϊόν, πόσο πρέπει να ζυγίζει, τι χαρακτηριστικά θα πρέπει να έχει και

ούτω καθεξής. Βασικά η ποιότητα του προϊόντος είναι εξαιρετικά σημαντική όταν ξεκινάει να σχεδιάζεται το προϊόν (Lecklin, 2006).

Οι διαστάσεις της ποιότητας βοηθούν στο να κατανοήσουμε την έννοια της. Αποτελούν στοιχεία που δείχνουν στο τι εστιάζει ο πελάτης. Αυτές είναι:

- Η απόδοση. Όλα τα προϊόντα σχεδιάζονται και παράγονται αποσκοπώντας στην κάλυψη συγκεκριμένων αναγκών. Η απόδοση αφορά τον βαθμό που τα προϊόντα ή οι υπηρεσίες ανταποκρίνονται σε αυτόν τον σκοπό.
- Εξοπλισμός- πρόσθετα χαρακτηριστικά. Αφορά τον επιπλέον εξοπλισμό που παρέχουν οι εταιρείες παραγωγής των προιόντων ή των υπηρεσιών ώστε να διευκολύνουν ή να διευρύνουν την χρήση του.
- Η διάρκεια ζωής. Αναφέρεται στην ανθεκτικότητα του προϊόντος δεδομένου ότι πληρούνται συνεχώς οι προδιαγραμμένες συνθήκες χρήσης.
- Η ικανότητα εξυπηρέτησης. Αναφέρεται στις δραστηριότητες της επιχείρησης που αποσκοπούν στην επικοινωνία και την εξυπηρέτηση του πελάτη μετά την αγορά του προϊόντος.
- Η αξιοπιστία. Αναφέρεται στην ικανότητα επιτυχούς και αδιάλειπτης λειτουργίας ενός προϊόντος για ένα συγκεκριμένο χρονικό διάστημα (Στειάκακης, Κωφίδης, 2017)

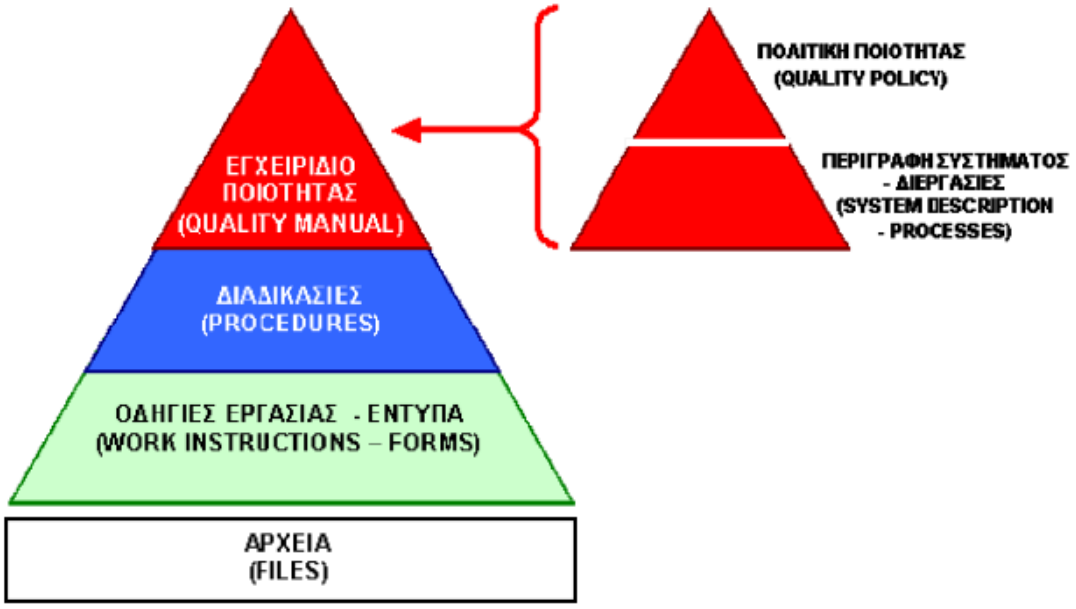
Η ποιότητα του περιβάλλοντος επικεντρώνεται στο πόσο το προϊόν είναι βλαβερό για την κοινωνία και το περιβάλλον. Όταν οι εταιρείες λαμβάνουν υπόψη την κοινωνία και το περιβάλλον, θα πρέπει επίσης να επικεντρωθούν στον κύκλο ζωής του προϊόντος και στα συστατικά του προϊόντος. Μια προοπτική που αφορά την ποιότητα είναι επίσης η ποιότητα της διαδικασίας, η οποία μπορεί να σχετίζεται με τα πάντα στην επιχείρηση. Η ποιότητα μιας διαδικασίας καθορίζεται με τη θέσπιση μετρήσεων για αυτήν. Ορίζοντας και μετρώντας την επεξεργασία, μειώνουμε τις επιπλοκές και τις βλάβες και μειώνουμε το κόστος (Lecklin, 2006). Υπάρχουν ακόμα πολλές διαφορετικές προοπτικές της ποιότητας, αλλά αυτές που παρουσιάζονται εδώ βοηθούν στο να σχηματιστεί μια ιδέα των διαστάσεών της, δηλαδή με ποια κατηγορία μπορεί να συνδεθεί. Η ποιότητα είναι ένα αληθινά τεράστιο θέμα και το επόμενο βήμα είναι να κατανοήσουμε τη διαχείριση της ποιότητας.

1.2 Διαχείριση και Αρχές Ποιότητας

Το πρότυπο ISO 9000 ορίζει τη διαχείριση ποιότητας ως "συντονισμένες δραστηριότητες για την διαχείριση και τον έλεγχο ενός οργανισμού όσον αφορά την ποιότητα " (SFS-EN ISO 9000, 2005). Η διαχείριση της ποιότητας βασίζεται στη συμμετοχή όλων των ενδιαφερομένων και στοχεύει σε μακροπρόθεσμη επιτυχία. (Zink, 1998.) Το πρότυπο ISO έχει ορίσει οκτώ αρχές τις οποίες πρέπει να λάβει υπόψιν η ενίοτε επιχείρηση όταν επιδιώκει καλύτερες επιδόσεις. Αυτές οι αρχές είναι η εστίαση στον πελάτη, η ηγεσία, η ανθρώπινη συμμετοχή, η προσέγγιση της διαδικασίας, η προσέγγιση του συστήματος στη διαχείριση, η συνεχής βελτίωση, η πραγματική προσέγγιση στη λήψη αποφάσεων και η πολύ καλή σχέση με τους προμηθευτές (Διεθνής Οργανισμός Τυποποίησης, 2013).

Η διαχείριση ποιότητας σε μία επιχείρηση ή έναν οργανισμό εφαρμόζεται μέσω ενός συστήματος διαχείρισης ποιότητας. Αυτό το σύστημα αποτελεί σημαντικό εργαλείο για την λειτουργία της επιχείρησης ή του οργανισμού. Θα πρέπει, το σύστημα, να οργανωθεί και να χρησιμοποιηθεί σωστά, να συνδράμουν οι κατάλληλοι χρήστες με τον κατάλληλο τρόπο, ώστε να είναι αποτελεσματικό και να αποδώσει τα αναμενόμενα αποτελέσματα. Σύμφωνα με τον ΕΛΟΤ ένα σύστημα διαχείρισης ποιότητας είναι στην πραγματικότητα ένα ”σύνολο αλληλοσχετιζόμενων ή αλληλοεπιδρώντων στοιχείων για την καθιέρωση Πολιτικής και Αντικειμενικών σκοπών, καθώς και για την επίτευξη των σκοπών αυτών” (Μαθιουδάκης, 2008).

Στο παρακάτω γράφημα φαίνονται όλα τα στάδια ενός προτύπου διαχείρισης ποιότητας:



Όπως φαίνεται στο σύστημα διαχείρισης ποιότητας περιλαμβάνονται όλα τα αρχεία του συστήματος, οι οδηγίες εργασίες και τα έντυπα, οι διαδικασίες και το εγχειρίδιο ποιότητας που περιλαμβάνει την περιγραφή του συστήματος, τις διεργασίες και την πολιτική ποιότητας.

Το εγχειρίδιο ποιότητας είναι το ανώτατο έγγραφο του συστήματος και είναι αυτό που δίνει την πλήρη περιγραφή του. Κάθε εταιρεία έχει το δικό της εγχειρίδιο το οποίο κάθε φορά δημιουργείται ανάλογα με τις ανάγκες της. Αυτό σημαίνει ότι σε κάθε εταιρεία το εγχειρίδιο έχει διαφορετική έκταση, οργάνωση, δραστηριότητες αλλά και διαφορετική πολιτική ποιότητας.

Η πολιτική ποιότητας, καθορίζεται από την διοίκηση, είναι η γενική συνολική κατεύθυνση και οι προθέσεις της εταιρείας σχετικά με την ποιότητα, όπως έχουν επίσημα εκφρασθεί από την ανώτατη διοίκηση. Όπως φαίνεται και στο διάγραμμα η πολιτική ποιότητας της κάθε εταιρείας είναι το ανώτατο τμήμα του συστήματος διαχείρισης ποιότητας, έτσι είναι προφανές ότι είναι και το σημαντικότερο. Μάλιστα, από την πολιτική ποιότητας απορρέει όλο το σύστημα διοίκησης ποιότητας της εταιρείας.

Το κείμενο που δημιουργείται, για την πολιτική ποιότητα της εταιρείας, θα πρέπει να είναι αναρτημένο σε εμφανή σημεία της εταιρεία έτσι ώστε όλοι οι

υπάλληλοι να μπορούν να το διαβάσουν. Αυτό γιατί είναι ιδιαίτερα σημαντικό για την εταιρεία να κατανοηθεί από τους υπαλλήλους η σημαντικότητα της πολιτικής ποιότητας και το ότι αυτήν εκφράζει όλη την λειτουργία του συστήματος διαχείρισης ποιότητας. Στον σύγχρονο κόσμο, βέβαια, οι εταιρείες που διαθέτουν ιστοσελίδα αναρτούν το κείμενο της πολιτικής ποιότητας σε αυτήν (Γκίκα, 2011).

1.3 Η ποιότητα σαν έννοια στον δημόσιο τομέα

Η συνολική διαχείριση της ποιότητας (Total Quality Management - TQM) χρησιμοποιήθηκε αρχικά στον ιδιωτικό τομέα, προκειμένου να επιτευχθεί ολοκληρωμένη παρακολούθηση και εκτίμηση όλων των σχετικών δραστηριοτήτων ενός οργανισμού, προκειμένου να υπάρξουν άριστα αποτελέσματα στις επιχειρήσεις (Matei, Andreescu, 2005).

Η Διαχείριση Ποιότητας έχει μια σειρά χαρακτηριστικών:

- ο στόχος είναι η ικανοποίηση των πολιτών,
- η ποιότητα ορίζεται από τον πολίτη,
- επηρεάζει όλες τις δραστηριότητες του οργανισμού που σχετίζονται με το προϊόν ή την υπηρεσία (είτε άμεσα είτε όχι),
- οι πολίτες-χρήστες της υπηρεσίας είναι εξωτερικοί,
- κλείνει τις δραστηριότητες ελέγχου, αλλά κυρίως αφορά τη διαχείριση του συνόλου του οργανισμού,
- όλοι εμπλέκονται στην εφαρμογή,
- η μεθοδολογία αποσκοπεί ιδιαίτερα στην πρόληψη, στοχεύει να κάνει τα σωστά πράγματα "από την αρχή", ευθύνη και συμμετοχή όλων από τον οργανισμό.

Η "ποιότητα" σαν έννοια δεν είναι νέα στη δημόσια διοίκηση. Αντίθετα, η ποιότητα ήταν, έστω και χωρίς να φαίνεται, έννοια της δημόσιας διοίκησης από τη δημιουργία του σύγχρονου διοικητικού κράτους, όταν συσχετίστηκε με την τήρηση

των κανονισμών και διαδικασιών, με επίσημη ορθότητα, τη βιωσιμότητα και την απουσία αυθαίρετων αποφάσεων (Engel, 2003).

Μια επισκόπηση για την εμφάνιση της ποιότητας στη δημόσια διοίκηση μπορεί να είναι αυτή που εξέτασε ο Engel (2003), ο οποίος υπογραμμίζει την ιδέα σύμφωνα με την οποία "η ώθηση για την ποιότητα " υπήρχε στο δημόσιο τομέα το τελευταίο μισό της δεκαετίας του '80 και σε ευρύτερη κλίμακα στη δεκαετία του '90, επιτρέποντας την ποιότητα στην δημόσια διοίκηση να γίνει "σύγχρονος όρος".

Η έννοια της ποιότητας στην δημόσια διοίκηση εκφράζεται με σειρά ορισμών, οι οποίοι στην πραγματικότητα ο ένας συμπληρώνει τον άλλον. Μεταξύ αυτών των ορισμών είναι:

- Βελτίωση του "τρόπου διακυβέρνησης" - την αρχιτεκτονική του συντάγματος και τη δομή της κυβέρνησης και της κοινωνίας και την αποτελεσματικότητα της δημόσιας δράσης (Bovaird, Löffler, 2002).

- Η ποιότητα μπορεί να καθοριστεί από την ευκαιρία του κατάλληλου χαρακτήρα (ΟΟΣΑ, 2001).

- Το σύνολο των προτύπων και των χαρακτηριστικών ενός προϊόντος σε σχέση με την ικανότητά του να ικανοποιεί τις γνωστές ή υποτιθέμενες ανάγκες που (Norma ISO 9004-2).

- Η ποιότητα είναι το επίπεδο στο οποίο ένα σύνολο εγγενών χαρακτηριστικών ικανοποιεί κάποιες απαιτήσεις - μπορεί να είναι σε διαφορετικά επίπεδα, αντίστοιχα: μη ικανοποιητική ή φτωχή; ικανοποιητική ή καλή και εξαιρετική (πρότυπο ISO 9000: 2000. Συστήματα διαχείρισης ποιότητας. Βασικές αρχές και λεξιλόγιο).

Οι Beale και Pollitt (1994) ανακάλυψαν ότι, όσον αφορά τα πρότυπα, οι γνώσεις των πελατών είναι πολύ χαμηλές, ακόμη και σε μια χώρα που τοποθετεί τις πληροφορίες σε κεντρική θέση στην πολιτική ατζέντα (Μεγάλη Βρετανία). Η Ευρωπαϊκή Επιτροπή διενήργησε το 1996 μια μελέτη που υπογραμμίζει την συνειδητοποίηση της σημασίας / ρόλου της ποιότητας στον κόσμο. Η ποιότητα της υπηρεσίας αντιπροσωπεύει μια σημαντική πτυχή της απόδοσης σε οποιονδήποτε

οργανισμό (ΟΟΣΑ, 2001) και στη δημόσια διοίκηση των κρατών επιχειρεί να επιτύχει απόδοση μέσω της στρατηγικής διαχείρισης της ποιότητας.

1.4 Μοντέλα ποιότητας στον δημόσιο τομέα

Το Ευρωπαϊκό Ίδρυμα για τη Διαχείριση της Ποιότητας (European Foundation for Quality Management, EFQM), το οποίο ιδρύθηκε το 1988 από τις ευρωπαϊκές εταιρείες υψηλών επιδόσεων με στόχο την προώθηση και διάδοση της ιδέας της επιχειρηματικής αριστείας στην Ευρώπη, ανέπτυξε και κατέχει το Μοντέλο αριστείας EFQM. Αυτό το μοντέλο βασίζεται σε οχτώ βασικές έννοιες σχετικά με την αριστεία, οι οποίες μετατρέπονται σε ένα διάγραμμα εννέα κριτηρίων που δημιουργούν ένα πλαίσιο για την αξιολόγηση της ποιότητας σε έναν οργανισμό. Η χρησιμοποιούμενη μεθοδολογία είναι αυτή της αυτοαξιολόγησης, πράγμα που σημαίνει ότι οι οργανώσεις πρέπει να αξιολογούν τις δικές τους επιδόσεις με δομημένο τρόπο, βάσει πραγματικών γεγονότων, και τον εντοπισμό των ισχυρών σημείων και των τομέων στους οποίους απαιτείται βελτίωση.

Το μοντέλο EFQM χρησιμοποιείται σημαντικά στο δημόσιο τομέα πολλών χωρών της ΕΕ (Engel, 2003), και τα τελευταία χρόνια έχει εξαπλωθεί στο επίπεδο χωρών εκτός ΕΕ.

Ένα άλλο μοντέλο μέτρησης της ποιότητας στον δημόσιο τομέα είναι το Κοινό Πλαίσιο Αξιολόγησης (Common Assessment Framework, CAF). Το ΚΠΑ είναι μέσο αυτοαξιολόγησης σχετικά με τον τρόπο λειτουργίας των δημόσιων ιδρυμάτων. Αναπτύχθηκε το 1999/2000 από τα κράτη μέλη της Ε.Ε. ως κοινό πλαίσιο του δημόσιου τομέα για την την αξιολόγηση και τη βελτίωση της δημόσιας διοίκησης και βασίζεται σε βασικές έννοιες, στο διάγραμμα και τα κριτήρια αξιολόγησης που διαχειρίζεται το μοντέλο EFQM και, όπως και το προηγούμενο, λειτουργεί με την αυτοαξιολόγηση (Engel, 2003). Παρόλα αυτά, το ΚΠΑ διαφοροποιείται από το Μοντέλο EFQM σε διάφορες διαστάσεις (επιμέρους κριτήρια ή τομείς που πρέπει να επιλυθούν , δείκτες -παραδείγματα, σύστημα καταγραφής αποτελεσμάτων) και λαμβάνει ρητά υπόψη τις ιδιαιτερότητες των δημόσιων οργανισμών.

Ο τελικός χαρακτήρας του ΚΠΑ είναι να προσφέρει ένα απλό, εύκολο και χωρίς κόστος πλαίσιο για την αυτοαξιολόγηση των δημόσιων οργανισμών στην Ευρώπη και να επιτρέψει τη χρήση καλών πρακτικών και μεθόδων αξιολόγησης (EIPA). Η σειρά ISO 9000 που αναπτύχθηκε από το 1987 είναι ένα διεθνές πρότυπο, αποδεκτό για την διασφάλιση ποιότητας στον τομέα της παραγωγής και της παροχής υπηρεσιών, προσφέροντας δείκτες και θέσεις σχετικά με τον τρόπο με τον οποίο επεξεργάζεται ένα σύστημα ποιότητας εντός ενός έτους έναν οργανισμό. Η σειρά αποτελείται από οδηγίες για τη χρήση του προτύπου (ISO 9000) και απαιτήσεις για τις οργανωτικές διαδικασίες που καθορίζονται διαφορετικού τύπου δραστηριότητες (Engel, 2003).

Η σειρά ISO 9000 συνεργάζεται με εξωτερικά των οργανισμών όργανα πιστοποίησης (που εκτελούνται από δομές πιστοποίησης) και επιτρέπει στους οργανισμούς να λαμβάνουν επίσημα πιστοποιητικά για τις δραστηριότητές τους. Τα πιστοποιητικά εκδίδονται για ένα περιορισμένο χρονικό διάστημα αλλά μπορεί επίσης να ανακληθούν.

Όσον αφορά την εφαρμογή των διεθνών κανόνων ποιότητας στην δημόσια διοίκηση, ο πρώτος κανονισμός για την ποιότητα ήταν ο ISO 9000 . Εφαρμόζονται επίσης κανονισμοί σχετικά με το περιβάλλον ISO 14000, ISO 17020 και ISO 17025 και τεχνικοί κανονισμοί στον τομέα της δημόσιας διοίκησης. Εκτιμάται ότι η εφαρμογή των προτύπων ISO 9000 είναι χρήσιμη, ειδικά για τους οργανισμούς που δεν έχουν τη διαφάνεια των γραπτών κανόνων, των διαρθρώσεων και διαδικασιών (Löffler, 2001).

1.5 Η ποιότητα στον ελληνικό δημόσιο τομέα

Κάθε μία από τις χώρες της Ε.Ε., έχοντας ως κεντρικό στόχο την ευθυγράμμισή της σύμφωνα με τα ευρωπαϊκά πρότυπα ποιότητας, επεξεργάστηκε "στρατηγικές ποιότητας" που υπογραμμίζουν την πολιτική και τους στόχους της κεντρικής διοίκησης όσον αφορά την ποιότητα της δημόσια διοίκησης ή βρίσκεται ακόμη στη διαδικασία επεξεργασίας τέτοιων στρατηγικών εγγράφων. Το θέμα της ποιότητας προσεγγίζεται επίσης σε διαφορετικά έγγραφα όπως τα εθνικά μεταρρυθμιστικά σχέδια και προγράμματα.

Παρακάτω παρουσιάζονται τα μεταρρυθμιστικά έγγραφα, οι στρατηγικές και η ποιότητα της πολιτικής διαχείρισης που έχουν εκπονηθεί στην Ελλάδα:

1. Επιχειρησιακό Πρόγραμμα "Μεταρρύθμιση της Δημόσιας Διοίκησης" 2007 - 2013, 2007,
2. Εθνικό Στρατηγικό Πλαίσιο Αναφοράς 2007 - 2013, 2006,
3. Εθνική μεταρρύθμιση του προγράμματος οικονομικής ανάπτυξης και την απασχόλησης, 2005-2008, 2005,
4. "Σχέδιο Καποδίστρια", 1997
5. Μεταρρυθμιστικό Πρόγραμμα για την Τοπική Δημόσια Διοίκηση, 1997,
6. Κώδικας συμπεριφοράς των δημοσίων υπαλλήλων, 1999,
7. Εθνικό Σχέδιο Δράσης για το ΚΠΑ 2007 - 2009 και 2010 - 2011,
8. Νόμος για την πρόσβαση σε πληροφορίες δημόσιου συμφέροντος, 1999.

Τα εργαλεία που χρησιμοποιήθηκαν για να πραγματοποιηθούν αυτές οι ενέργειες ήταν το Κοινό Πλαίσιο Αξιολόγησης (ΚΠΑ) και το πρότυπο ISO:9001.

Η παρουσία ή η απουσία στοιχείων διαχείρισης ποιότητας από τα έγγραφα μεταρρύθμισης και στρατηγικής της εθνικής δημόσιας διοίκησης της Ελλάδας απεικονίζει όχι μόνο τις εξελίξεις σε συγκεκριμένους τομείς, αλλά και υπογραμμίζει τα λιγότερο ανεπτυγμένα πεδία.

Η προσπάθεια του Ελληνικού Κράτους να εισαγάγει την έννοια της ποιότητας στην Δημόσια διοίκηση ξεκίνησε με το σχέδιο «Ιωάννης Καποδίστριας» το 1997, που καθιερώνει διαρθρωτικές τροποποιήσεις στη δημόσια διοίκηση, με την ανάθεση κεντρικών αρμοδιοτήτων σε ορισμένες τοπικές υπηρεσίες. Η κυβέρνηση θεωρεί αυτό το σχέδιο απαραίτητο βήμα προς τον εκσυγχρονισμό της διοίκησης, από το τοπικό επίπεδο. Μερικοί από τους σημαντικότερους στόχους του σχεδίου ήταν ο εκσυγχρονισμός του διοικητικού συστήματος με την παροχή υπηρεσιών υψηλής ποιότητας στους πολίτες στις αστικές και αγροτικές περιοχές και την προώθηση της διαφάνειας στην Ε.Ε., η διαχείριση των οικονομικών πόρων και την εγγύηση της νομιμότητας μέσω της υπεύθυνης εφαρμογής των πολιτικών των τοπικών αρχών με σεβασμό προς τους πολίτες (Matei, Lazar, 2011)

Στα τέλη της δεκαετίας του '90, στο πλαίσιο της Γενικής Γραμματείας της Δημόσιας Διοίκησης του Υπουργείου Εσωτερικών, δημιουργήθηκε ειδική μονάδα σχετικά με την αποτελεσματικότητα και την ποιότητα. Αυτό συνεχίστηκε με την υιοθέτηση νόμου από το Ελληνικό Κοινοβούλιο το 2004, του νόμου αριθ. 3230/2004 σχετικά με τη δημιουργία μιας Διεύθυνσης Ποιότητας και Αποδοτικότητας στο πλαίσιο της Γενικής Γραμματείας Διαχείρισης Δημόσιας Διοίκησης. Ο νόμος αυτός προέβλεπε τη δημιουργία ενός παρόμοιου δικτύου με κατευθύνσεις σε όλα τα υπουργεία και την καθιέρωση μιας ολοκληρωμένης απόδοσης στο σύστημα διαχείρισης, την εισαγωγή των μοντέλων (κυρίως ΚΠΑ) και πολιτικών ποιότητας και ένα βραβείο ποιότητας για τον δημόσιο οργανισμό με τις καλύτερες επιδόσεις.

Η μονάδα που είναι υπεύθυνη για την προώθηση του ΚΠΑ είναι η Διεύθυνση Ποιότητας και Αποτελεσματικότητας στο πλαίσιο της Γενικής Γραμματείας Δημόσιας Διοίκησης. Αυτή είναι υπεύθυνη για την προώθηση πολιτικών αποτελεσματικότητας και ποιότητας στη δημόσια διοίκηση. Η Διεύθυνση Ποιότητας και Αποτελεσματικότητας εγκαινίασε δύο σημαντικές πρωτοβουλίες που αποσκοπούσαν στη μετατροπή του τρόπου με τον οποίο πρέπει να λειτουργούν οι Ελληνικοί δημόσιοι οργανισμοί: την καθιέρωση ενός συστήματος ολοκληρωμένης διαχείρισης της απόδοσης και την εισαγωγή οργάνων ποιότητας και πολιτικής και, ειδικότερα, τη χρήση του ΚΠΑ από τη δημόσια διοίκηση.

Οι κύριοι στόχοι όσον αφορά τον εκσυγχρονισμό της δημόσιας διοίκησης στα στρατηγικά έγγραφα είναι:

- Η βελτίωση της παραγωγικότητας και της ποιότητας των δημόσιων υπηρεσιών.
- Η θέσπιση συστήματος αξιολόγησης σχετικά με τον αντίκτυπο της νέας νομοθεσίας για την ανταγωνιστικότητα
- Η διοικητική διαφάνεια - καταπολέμηση της διαφθοράς ·
- Η ανάπτυξη της ηλεκτρονικής διακυβέρνησης.
- Η δημιουργία πλαισίου για τη δια βίου μάθηση και την κατάρτιση των πολιτών - υπαλλήλων

- Η βελτίωση της διαπεριφερειακής συνεργασίας.

Οι κύριοι στόχοι όσον αφορά τη διαχείριση της ποιότητας στο Δημόσια Διοίκηση είναι:

- Η βελτίωση της αποτελεσματικότητας και της ποιότητας των δημοσίων οργανισμών, υιοθετώντας μια προσέγγιση προσανατολισμένη προς τον πολίτη-πελάτη τους

- Η απλούστευση και διευκόλυνση της πρόσβασης των πολιτών και των επιχειρήσεων στη δημόσια διοίκηση

- Η δημιουργία μιας διοικητικής κουλτούρας προσανατολισμένη προς τα ορθά αποτελέσματα

- Η μείωση της γραφειοκρατίας.

Η προσέγγιση διαχείρισης της ποιότητας σε επίπεδο κάθε κράτους μπορεί να είναι

- Συγκεντρωτική, αποκεντρωμένη ή συνδυασμός των δύο και / ή

- Φθίνουσα, ανερχόμενη ή συνδυασμός των δύο.

Κάθε χώρα μπορεί να χρησιμοποιήσει μόνο μία προσέγγιση ή μπορεί ταυτόχρονα να χρησιμοποιήσει και τις δύο προσεγγίσεις. Μετά την ανάλυση που διενεργήθηκε στα έγγραφα μεταρρύθμισης , παρατηρούμε το γεγονός ότι η Ελλάδα χρησιμοποιεί ταυτόχρονα τις δύο προσεγγίσεις, δηλαδή τη συνδυασμένη μορφή τους - η δομή της δημόσιας διοίκησης εξακολουθεί να είναι έντονα συγκεντρωμένη στην πρωτεύουσα, με σχετικά μικρή τοπική αυτονομία και με υψηλό βαθμό οικονομικής εξάρτησης από την κεντρική εκτελεστική εξουσία (Matei, Lazar, 2011)

Οι κεντρικές και φθίνουσες προσεγγίσεις χρησιμοποιούνται στις δραστηριότητες που εκτελούνται ειδικά από τα αρμόδια υπουργεία για την εφαρμογή των μέσων διαχείρισης της ποιότητας στις στρατηγικές μεταρρύθμισης κάθε χώρας, προκειμένου να μεταφράσει το ΚΠΑ, να διοργανώσει συνέδρια σχετικά με την ποιότητα, για τη σύνταξη της μεθοδολογίας και των οδηγών σχετικά με το εφαρμογή

προτύπων ποιότητας, την παρακολούθηση των προτύπων ποιότητας εφαρμογής, σε συμφωνία με διάφορους δείκτες, την εφαρμογή της ηλεκτρονικής διακυβέρνησης.

Η αποκεντρωμένη προσέγγιση χρησιμοποιείται στην τοπική διοίκηση. Κάθε τοπική διοίκηση διοργανώνει συνέδρια σχετικά με τη δική της ποιότητα.

Η αύξουσα προσέγγιση συνδέεται με την εφαρμογή προγραμμάτων ποιότητας και την ποιότητα συστήματος διαχείρισης εντός των δημόσιων οργανισμών. Τα πιο χρησιμοποιούμενα προγράμματα από αυτούς τους οργανισμούς είναι καταγγελίες και προτάσεις των πολιτών, οδηγίες και αυτοαξιολόγηση με τα μοντέλα EFQM και ΚΠΑ.

1.6 Η εφαρμογή των μοντέλων ποιότητας στον ελληνικό δημόσιο τομέα

Στην Ελλάδα έχουν οριστεί ορισμένα θεσμικά δημόσια όργανα, υπεύθυνα για την προώθηση της διαχείρισης της ποιότητας. Το όργανα που έχει οριστεί για να χειριστεί την υλοποίηση και το συντονισμό των εργαλείων διαχείρισης της ποιότητας στην εθνική διοίκηση είναι ένας κεντρικός δημόσιος οργανισμός, δηλαδή υπουργείο που είναι επιφορτισμένο με τη μεταρρύθμιση της δημόσιας διοίκησης, -το Υπουργείο Εσωτερικών.

Τα πιο συνηθισμένα, ακόμα και τώρα, εργαλεία διαχείρισης της ποιότητας είναι η σειρά από τα πρότυπα ISO 9000 (Engel, 2003) και, γενικά, η εθνική πολιτική ποιότητας των κρατών της Ε.Ε. επικεντρώθηκε περισσότερο στην ποιότητα των υπηρεσιών και των προϊόντων από ότι στο TQM.

Στην Ελλάδα, το Υπουργείο Εσωτερικών, την Αποκέντρωσης και της ηλεκτρονικής διακυβέρνησης μέσω της οδηγίας για την ποιότητα και την αποδοτικότητα από την Γενική Γραμματεία Δημόσιας Διοίκησης και Ηλεκτρονικής Διακυβέρνησης είναι υπεύθυνο για την προώθηση του ΚΠΑ και τη δημιουργία της υποστήριξης για τη χρήση του. Αυτή η οδηγία έχει ξεκινήσει δύο σημαντικές πρωτοβουλίες για τη μετατροπή του ελληνικού τρόπου που λειτουργούν οι δημόσιοι

οργανισμοί: καθιέρωση ενός ολοκληρωμένου συστήματος διαχείρισης για τις επιδόσεις και την εισαγωγή εργαλείων πολιτικών ποιότητας και θεσμών και κυρίως, χρησιμοποιώντας ΚΠΑ σε δημόσιους οργανισμούς.

Όσον αφορά την προώθηση της διαχείρισης της ποιότητας, ο θεσμός αυτός δημοσίευσε, στα Ελληνικά, "ΚΠΑ 2006", "Οδηγός για την εφαρμογή του ΚΠΑ" "Απαντήσεις στις πιο συχνές ερωτήσεις σχετικά με το ΚΠΑ "," Ένας οδηγός για τα δημόσια βήματα που τα θεσμικά όργανα πρέπει να λαμβάνουν κατά την εφαρμογή του ΚΠΑ ", με όλα αυτά να έχουν ως κύριο κοινό τους δημόσιους οργανισμούς σε κεντρικό, περιφερειακό και τοπικό επίπεδο. Το υπουργείο μετέφρασε επίσης στα ελληνικά και δημοσίευσε το «ΚΠΑ στην Εκπαίδευση», για την προώθηση της χρήσης μοντέλων ποιότητας στην εκπαίδευση. Επιπλέον, η οδηγία για την ποιότητα και την αποδοτικότητα υποστηρίζει τη χρήση του Balanced Scorecard (BSC) στους δημόσιους οργανισμούς, ως εργαλείο για την εγκαθίδρυση των στόχων και την αξιολόγηση των επιδόσεων (Υπουργείο εσωτερικών, 2018)

Το Υπουργείο Εσωτερικών υποστηρίζει τους δημόσιους οργανισμούς εφαρμόζοντας ΚΠΑ (καθοδήγηση). Για το σκοπό αυτό έχει οργανώσει εκπαιδευτικά συνέδρια και σεμινάρια για το ΚΠΑ (συνολική διαχείριση της ποιότητας, διαχείριση απόδοσης και μέτρηση της αποτελεσματικότητας της δημόσιας διοίκησης) για τους δημόσιους υπαλλήλους, ενώ το Υπουργείο Παιδείας διοργανώνει εκπαιδευτικά σεμινάρια και σεμινάρια ΚΠΑ για τους εκπαιδευτικούς.

Η Ελλάδα δεν διαθέτει Χάρτη Ποιότητας για τους Πολίτες, αλλά μέσω της πρόσβασης των πολιτών σε πληροφορίες δημοσίου συμφέροντος, αυτοί επωφελούνται από απαντήσεις από τη δημόσια διοίκηση.

Όσον αφορά τα βραβεία που δόθηκαν για την ποιότητα της δημόσιας διοίκησης, στην Αθήνα το 2007 διοργανώθηκε το πρώτο συνέδριο και το 2009 το δεύτερο συνέδριο «Το Εθνικό Βραβείο Ποιότητας για τη Δημόσια Διοίκηση», και απονεμήθηκε το Εθνικό Ελληνικό Βραβείο Ποιότητας. Οι υποψήφιοι για το βραβείο ήταν δημόσιοι οργανισμοί από κεντρικό, περιφερειακό και τοπικό επίπεδο από όλη την Ελλάδα. Το 2009 το βραβείο απονεμήθηκε στην Κεντρική Περιφέρεια της Μακεδονίας, το δεύτερο βραβείο στο Δήμο Ηρακλείου (Κρήτη), και το τρίτο βραβείο πήγε σε τρεις συμμετέχοντες: Το Κέντρο Εξυπηρέτησης Πολιτών του Δήμου

Περάματος, σε τρία τμήματα στον νομό Λάρισας και άλλα τρία τμήματα του Δήμου Αμαρουσίου. Το 2007, το πρώτο βραβείο απονέμεται στον Εθνικό Οργανισμό Ιατρικής, το δεύτερο βραβείο πήγε στο Χριστιανικό και Βυζαντινό Μουσείο και το τρίτο βραβείο πήγε στον υπεύθυνο για την οργάνωση και λειτουργία των πολιτών του Υπουργείου Εσωτερικών (Υπουργείο εσωτερικών, 2018).

Όσον αφορά την εφαρμογή των μοντέλων απόδοσης στους δημόσιους οργανισμούς, τα θεσμικά όργανα και τα πρότυπα ISO, διαπιστώνουμε για μια ακόμη φορά επίπεδα σύγκλισης. Το ΚΠΑ περιλαμβάνεται στις στρατηγικές και τα εθνικά έγγραφα της Ελληνικής κυβέρνησης (για παράδειγμα: τα εθνικά σχέδια μεταρρύθμισης) ως τρόπος αύξησης των επιδόσεων και της αποτελεσματικότητας στα δημόσια ιδρύματα και ως βάση για εκσυγχρονισμό των στρατηγικών που θα αναπτυχθούν σε θεσμικό επίπεδο συμβάλλοντας στην καλή λειτουργία των οργανώσεων του δημόσιου τομέα και της ποιότητα παροχής υπηρεσιών στους πολίτες. Επίσης, στην Ελλάδα η χρήση μοντέλων αριστείας και προτύπων ποιότητας συνιστώνται και χρησιμοποιούνται μόνο σε εθελοντική βάση. Αυτά τα μοντέλα και τα όργανα λαμβάνουν τη βοήθεια της Ε.Ε. στη διαδικασία εφαρμογής τους, στο υλικό ενίσχυσης, στην οικονομική ενίσχυση εμπειρογνωμοσύνη, κατάρτιση κ.λπ.

Οι διαδικασίες μεταρρύθμισης έδωσαν προσοχή στη δημόσια διοίκηση, στις στρατηγικές μεταρρύθμισης της Ελλάδας, που έχουν σημαντικό αντίκτυπο. Βελτιώνονται η ποιότητα και η αποτελεσματικότητα των δημόσιων υπηρεσιών σχετικά με τα κίνητρα των δημοσίων υπαλλήλων και τη διεύρυνση των δεξιοτήτων και ικανοτήτων τους (OCDE, 2001). Μετά την εξέταση της νομοθεσίας για τη δημόσια διοίκηση (καθεστώτα των δημοσίων υπαλλήλων, νόμος για τη δημόσια διοίκηση κ.λπ.) η ποιότητα έγινε μέσω της καθιέρωσης προτύπων της ΕΕ για την ποιότητα του δημόσιου τομέα και τη σύγκλιση προς τις αρχές του European Administrative Space:

a) Επαγγελματισμός
b) Υπομονή
c) Αποτελεσματικότητα
d) Λογικότητα
e) Αμεσότητα

f) Αντικειμενικότητα

g) δικαιοσύνη.

1.7 Ιστορική αναδρομή των συστημάτων ποιότητας

Το συνέδριο των εθνικών οργανισμών τυποποίησης που καθιέρωσε το ISO πραγματοποιήθηκε στο Λονδίνο από τις 14 έως τις 26 Οκτωβρίου 1946. Το ISO γεννήθηκε από την ένωση δύο οργανισμών, Την Διεθνής Ομοσπονδία των Εθνικών Ενώσεων Τυποποίησης (ISA), που ιδρύθηκε στη Νέα Υόρκη το 1926 και εδρεύει στην Ελβετία και την Επιτροπή Συντονισμού των Ηνωμένων Εθνών (UNSCC), η οποία ιδρύθηκε μόλις το 1944 και εδρεύει στο Λονδίνο. Πολλά από τα καταστατικά και τον εσωτερικό κανονισμό της I S O υιοθετούνται από την ISA και από τις 67 τεχνικές επιτροπές που ίδρυσε το ISO το 1947, η πλειοψηφία τους ήταν προηγουμένως επιτροπές της ISA

Το 1951 δημοσιεύεται το πρώτο πρότυπο ISO (που ονομάζεται «Συστάσεις» αρχικά), ISO / R 1: 1951 Τυπική θερμοκρασία αναφοράς για βιομηχανικές μετρήσεις μήκους. Έκτοτε, το πρότυπο έχει ενημερωθεί πολλές φορές και είναι πλέον το ISO 1: 2002 προδιαγραφές γεωμετρικών προϊόντων (GPS) - Τυπική θερμοκρασία αναφοράς για τις γεωμετρικές προδιαγραφές του προϊόντος.

Το 1955, τα μέλη ISO συγκεντρώνονται στη Στοκχόλμη για την 3η Γενική Συνέλευση. Στις αρχές του 1955, το ISO έχει 35 μέλη και 68 πρότυπα (που ονομάζονται «συστάσεις»).

Το 1960, το ISO δημοσιεύει το πρότυπο ISO 31 για τις ποσότητες και τις μονάδες (το οποίο από τότε έχει αντικατασταθεί από ISO 80 000).

Το ISO 31 βασίζεται στο SI (Système international d'unités). Το SI ορίζει μία μονάδα για κάθε ποσότητα, για παράδειγμα, το μέτρο για την απόσταση και το δευτερόλεπτο για το χρόνο. Ο στόχος του συστήματος SI είναι να επιτευχθεί

ομοιομορφία σε μονάδες μέτρησης παγκοσμίως. Το ISO 80 000 ορίζει τις μονάδες αυτές και τον τρόπο χρήσης τους.

Κατά τη διάρκεια της δεκαετίας του 1960, το ISO εργάζεται για να συμπεριλάβει περισσότερες αναπτυσσόμενες χώρες στις εργασίες του για τη Διεθνή Τυποποίηση. Το 1961 ιδρύει το DEVCO, μια επιτροπή για θέματα αναπτυσσόμενων χωρών, και το 1968 εισάγει την ιδιότητα μέλους του Ανταποκριτή. Αυτό επιτρέπει στις αναπτυσσόμενες χώρες να ενημερώνονται για τις εργασίες διεθνούς τυποποίησης χωρίς το πλήρες κόστος της ένταξης στο ISO. Η ιδιότητα του ανταποκριτή εξακολουθεί να είναι δημοφιλής επιλογή για πολλές χώρες σήμερα. Στις αρχές του 2012, το ISO είχε 49 ανταποκριτές μέλη.

Το 1968, το ISO δημοσιεύει το πρώτο του πρότυπο για τα εμπορευματοκιβώτια μεταφοράς εμπορευμάτων. Το φορτίο και η συσκευασία είναι ένας από τους τομείς στους οποίους το ISO είναι ιδιαίτερα δραστήριος, αλλάζοντας τον τρόπο με τον οποίο ταξιδεύουν τα εμπορεύματα σε όλο τον κόσμο.

Το 1971, το ISO δημιουργεί τις δύο πρώτες τεχνικές επιτροπές του στον τομέα του περιβάλλοντος: την ποιότητα του αέρα και την ποιότητα του νερού. Σήμερα στις επιτροπές αυτές συμμετέχουν και άλλες ομάδες περιβαλλοντικών εμπειρογνωμόνων που επικεντρώνονται σε πολλά θέματα, όπως η ποιότητα του εδάφους, η περιβαλλοντική διαχείριση και η ανανεώσιμη ενέργεια.

Το 1987, η ISO δημοσιεύει το πρώτο της πρότυπο διαχείρισης ποιότητας. Τα πρότυπα της «οικογένειας» ISO 9000 έχουν καταστεί μερικά από τα πιο γνωστά και καλύτερα πρότυπα πώλησης.

Το 1996, το ISO εκδίδει το πρότυπο του συστήματος περιβαλλοντικής διαχείρισης ISO 14001. Το πρότυπο παρέχει εργαλεία για επιχειρήσεις και οργανισμούς για να τους βοηθήσει να εντοπίσουν και να ελέγξουν τις περιβαλλοντικές τους επιπτώσεις.

Το 2003, ο Alan Bryden διορίζεται Γενικός Γραμματέας. Σύμφωνα με την πενταετή θητεία του, το ISO διευρύνει το έργο του για την κάλυψη νέων τεχνολογιών όπως η νανοτεχνολογία και τα βιοκαύσιμα. Ο Bryden υποστηρίζει επίσης ενεργά το

έργο της ISO για την κοινωνική ευθύνη, το οποίο οδηγεί στην καθιέρωση του ISO 26000 το 2010.

Το 2005, η κοινή τεχνική επιτροπή ISO και IEC της JTC1 εγκαινιάζει το ISO / IEC 27001, ένα πρότυπο συστήματος διαχείρισης για την ασφάλεια των πληροφοριών. Καθώς οι επιχειρήσεις εξαρτώνται όλο και περισσότερο από την τεχνολογία των πληροφοριών, η διασφάλιση του συστήματος και η ελαχιστοποίηση των κινδύνων είναι όλο και πιο σημαντική. Το ISO 27001: 2005 έχει γίνει ένα από τα πιο δημοφιλή πρότυπα ISO.

Το 2010 ένα βραβείο Emmy απονέμεται για κοινές εργασίες που παράγουν προηγμένο πρότυπο κωδικοποίησης βίντεο. Το πρότυπο επιτρέπει την υψηλή συμπίεση των ηχητικών και κινούμενων εικόνων, επιτρέποντας τη ροή στο διαδίκτυο με ελάχιστη απώλεια ποιότητας.

Το 2010, εγκαινιάζει το ISO 26000, το πρώτο διεθνές πρότυπο που παρέχει κατευθυντήριες γραμμές για την κοινωνική ευθύνη. Καθώς η κοινωνική ευθύνη έχει γίνει ένα καθημερινό μέρος των επιχειρήσεων, το ISO 26000 έχει καθιερωθεί ως παγκόσμιο σημείο αναφοράς για οργανισμούς που ενδιαφέρονται για τις επιπτώσεις τους στην ευρύτερη κοινωνία.

Το 2011 με την ενέργεια μια από τις πιο κρίσιμες προκλήσεις που αντιμετωπίζει η διεθνής κοινότητα, το ISO 50001 παρέχει σε οργανισμούς του δημόσιου και ιδιωτικού τομέα στρατηγικές διαχείρισης για την αύξηση της ενεργειακής απόδοσης, τη μείωση του κόστους και τη βελτίωση της ενεργειακής απόδοσης.

Το πρότυπο ISO 37001 είναι το πρώτο διεθνές πρότυπο συστήματος διαχείρισης κατά της δωροδοκίας που έχει σχεδιαστεί για να βοηθήσει τους οργανισμούς να καταπολεμήσουν τον κίνδυνο δωροδοκίας στις δικές τους πράξεις και στις παγκόσμιες αλυσίδες αξίας τους. Έχει τη δυνατότητα να μειώσει τον εταιρικό κίνδυνο και το κόστος της δωροδοκίας παρέχοντας ένα εύχρηστο επιχειρησιακό πλαίσιο για την πρόληψη, τον εντοπισμό και την αντιμετώπιση της δωροδοκίας. Δημοσιεύεται το 2016

Το 2017 το ISO γιορτάζει 70 χρόνια. Έχει προχωρήσει πολύ από το 1947 και το 2017 έχει 163 μέλη και συνολικά πάνω από 21.000 πρότυπα. Πάνω από 70 χρόνια η οικογένεια των προτύπων ISO έχει αυξηθεί σημαντικά και σήμερα καλύπτει σχεδόν όλες τις πτυχές της τεχνολογίας και των επιχειρήσεων.

Το ISO δημοσιεύει το διεθνές πρότυπο για την υγεία και την ασφάλεια στην εργασία:

ISO 45001: 2018, Συστήματα διαχείρισης της υγείας και της ασφάλειας στην εργασία - Απαιτήσεις με καθοδήγηση για χρήση, είναι ένα νέο διεθνές πρότυπο που σχεδιάστηκε για να βοηθήσει οργανισμούς κάθε μεγέθους να μειώσουν τους τραυματισμούς και τις ασθένειες στο χώρο εργασίας σε όλο τον κόσμο (ISO, 2018).

1.8 Πλεονεκτήματα και οφέλη από την εφαρμογή ενός συστήματος διαχείρισης

Η εφαρμογή ενός συστήματος διαχείρισης ποιότητας δεν είναι υποχρεωτική από τον νόμο. Υπάρχουν όμως σημαντικά πλεονεκτήματα που απορρέουν από την εφαρμογή του που κάνουν ελκυστικό ένα ISO σε κάθε επιχείρηση ή οργανισμό. Σύμφωνα με τον Μαθιουδάκη (2008) αυτά μπορούν να διακριθούν σε βραχυπρόθεσμα, σε μεσοπρόθεσμα και σε μακροπρόθεσμα πλεονεκτήματα.

Βραχυπρόθεσμα

- Η επικαιροποίηση και η ενημέρωση από πλευράς της επιχείρησης για τις αλλαγές τις νομοθεσίας. Η εφαρμογή ενός συστήματος διαχείρισης επιβάλει την μελέτη των τελευταίων νομοθετημάτων την συμμόρφωση με αυτά την συλλογή και τον έλεγχο διαταγμάτων, οδηγιών τόσο των εγχωρίων όσο και αυτών της Ευρωπαϊκής Ένωσης.
- Η ενημέρωση και η εκπαίδευση του εργατικού δυναμικού του οργανισμού για την στρατηγική, την πολιτική και τους στόχους που έχει θέσει η διοίκηση.

Αυτό θα διευκολύνει τόσο το έργο της διοίκησης στο να κάνει κατανοητό στους εργαζομένους το πλάνο και τους στόχους αλλά επιπλέον θα γίνουν κατανοητά στους εργαζομένους και τα καθήκοντα που αυτοί θα έχουν.

- Σε συνέχεια αυτού του πλεονεκτήματος, η αποσαφήνιση των καθηκόντων, των αρμοδιοτήτων και των ρόλων των εργαζομένων, των διευθύνσεων και γενικά του εργατικού δυναμικού της επιχείρησης σε κάθε επίπεδο ιεραρχίας
- Η ανάπτυξη ενός συστήματος καταγραφής των γεγονότων, των ατελειών, των αποκλίσεων και γενικά του τι πήγε στραβά τόσο σε επίπεδο εργαζομένων όσο και σε επίπεδο στόχων από την πλευρά της διοίκησης.

Μεσοπρόθεσμα

- Η βελτίωση της λειτουργίας και της οργάνωσης της επιχείρησης ή του οργανισμού. Αυτό μπορεί να επιτευχθεί σταδιακά μέσω της τυποποίησης, λόγω του συστήματος διαχείρισης, συγκεκριμένων λειτουργιών, τμημάτων και δραστηριοτήτων.
- Η καλύτερη συνέργια και επικοινωνία μεταξύ διαφορετικών τμημάτων ή επιπέδων του οργανισμού. Η τυποποίηση των διαδικασιών οδηγεί σταδιακά στην καλύτερη λειτουργία ανάμεσα στα τμήματα ή επίπεδα γιατί υπάρχουν ξεκάθαρα καθήκοντα που εκτελούνται από κάθε τμήμα.
- Η ανάπτυξη καινούργιων διαδικασιών ή η βελτίωση των ήδη υφιστάμενων προς ένα νέο πιο αποτελεσματικό μοντέλο λειτουργίας με βάση τα πρότυπα διαχείρισης.
- Η καλύτερη συμμόρφωση της επιχείρησης ή του οργανισμού στις απαιτήσεις της ισχύουσας νομοθεσίας και η μείωση των πιθανοτήτων να μην περάσει κάποιο έλεγχο ή να μην είναι σύννομη με αυτήν.
- Η καλύτερη αξιολόγηση των αποτελεσμάτων. Ιδιαίτερα σε ότι έχει να κάνει με τις αποκλίσεις ή τις ατέλειες ως προς το πρόγραμμα. Η επιχείρηση έχει την δυνατότητα για επεξεργασία των δεδομένων και εξαγωγή σωστότερων αποτελεσμάτων τα οποία και θα αποτελέσουν εφαλτήριο για βελτίωση τόσο της διοίκησης όσο και ολόκληρου του συστήματος γενικότερα.
- Πιο εκπαιδευμένο προσωπικό το οποίο θα είναι και καλύτερα καταρτισμένο και ευαισθητοποιημένο στα επί μέρους τμήματα εφαρμογής του συστήματος διαχείρισης.

- Η πολύ σημαντική βελτίωση των συνθηκών εργασίας, κάτι που θα προκαλέσει και την αύξηση της παραγωγικότητας της εργασίας.
- Η δημιουργία συνθηκών που να μειώνουν τον κίνδυνο έκθεσης των εργαζομένων σε επισφαλείς καταστάσεις, κάτι που συνεπάγεται την μείωση των εργατικών ατυχημάτων.
- Η ανάπτυξη ενός συστήματος ή μίας σειράς από δείκτες που θα μετρούν αντικειμενικά τα αποτελέσματα των διεργασιών, των προιόντων και τις ποιότητας τους ή των παρεχόμενων υπηρεσιών του οργανισμού.
- Η δημιουργία ενός κλίματος ασφάλειας όσον αφορά τους εργαζομένους. Η ανάλυση των επιμέρους καθηκόντων τους έχει αποδειχθεί ότι προσφέρει σιγουριά στους εργαζομένους για το επίπεδο εργασίας τους και αυξάνει την παραγωγικότητα τους αντίστοιχα βελτιώνει την σχέση εργαζομένων-διοίκησης αφού γίνεται ξεκάθαρο το τι θα πρέπει να περιμένει ο ένας από τον άλλο.
- Η βελτίωση των διαδικασιών ελέγχου στην επιχείρηση και η εξασφάλιση της μετρησιμότητας των αποτελεσμάτων.
- Η βελτίωση των διαδικασιών αντιμετώπισης κρίσεων.

Μακροπρόθεσμα

- Η συνεχής βελτίωση της οργάνωσης της επιχείρησης, της παραγωγικότητας της εργασίας και εν τέλει της βιωσιμότητας της ίδιας της επιχείρησης. Παράλληλα η βελτίωση αυτή βοηθά στην μείωση του κόστους και στην αύξηση των κερδών.
- Η ανάπτυξη της ικανότητας να αναγνωρίζονται και να εκτιμώνται σχετικά άμεσα οι όποιες επισφαλείς ή επικίνδυνες καταστάσεις για την επιχείρηση.
- Η ανάπτυξη ενός συστήματος μέτρησης μέσω ειδικών δεικτών που να ανταποκρίνεται στις ανάγκες της επιχείρησης. Η στατιστική επεξεργασία των δεδομένων θα βοηθήσει στην δημιουργία καταλληλότερων και αποτελεσματικότερων μεθόδων μέτρησης.
- Η πλήρη συμμόρφωση της επιχείρησης ή του οργανισμού με την ισχύουσα νομοθεσία κάτι που θα παρέχει και νομοθετική κάλυψη στους υπευθύνους και τους διαχειριστές του οργανισμού.

- Η ανάπτυξη ενός αποτελεσματικού συστήματος ελέγχου των τμημάτων, των λειτουργιών, των διεργασιών, των δραστηριοτήτων σε όλες τις δομές εντός του οργανισμού.
- Η βελτίωση της αξιολόγησης των αποτελεσμάτων ελέγχου, των διορθωτικών ενεργειών και των προληπτικών ενεργειών που έχουν ληφθεί.
- Η βελτίωση της παραγωγικής διαδικασίας, η αύξηση της παραγωγής των αγαθών ή των παρεχόμενων υπηρεσιών.
- Η ανάπτυξη μιας υγιούς σχέσης εμπιστοσύνης ανάμεσα στους εργαζόμενους και την διοίκηση του οργανισμού.

1.9 Τα πιο γνωστά πρότυπα ISO

Τα τελευταία χρόνια τα πρότυπα ποιότητας είναι συνυφασμένα με τον Διεθνή Οργανισμό τυποποίησης (International Organization for Standardization, ISO). Αυτός ο διεθνής οργανισμός είναι στην πραγματικότητα μία ανεξάρτητη μη κυβερνητική οργάνωση που δημιουργήθηκε από 162 χώρες με σκοπό την δημιουργία πρότυπων-εγγράφων που παρέχουν τις απαιτήσεις, προδιαγραφές, οδηγίες ή τα χαρακτηριστικά που μπορούν να χρησιμοποιηθούν με συνέπεια για να διασφαλιστεί ότι τα υλικά, τα προϊόντα, οι διαδικασίες και οι υπηρεσίες είναι κατάλληλα για το σκοπό τους (ISO, 2018). Έτσι ο οργανισμός έχει δημιουργήσει μία σειρά από πρότυπα που αφορούν συγκεκριμένους τομείς, με σκοπό την όσο καλύτερη διαχείριση της ποιότητας.

ISO 9000

Η "οικογένεια" ISO 9000 ασχολείται με διάφορες πτυχές της διαχείρισης της ποιότητας και περιέχει μερικά από τα καλύτερα γνωστά πρότυπα ISO. Τα πρότυπα παρέχουν καθοδήγηση και εργαλεία για εταιρείες και οργανισμούς που θέλουν να διασφαλίσουν ότι τα προϊόντα και οι υπηρεσίες τους ανταποκρίνονται με συνέπεια στις απαιτήσεις του πελάτη και ότι η ποιότητα βελτιώνεται συνεχώς.

Το πρότυπο ISO 9001: 2015 καθορίζει τα κριτήρια για ένα σύστημα διαχείρισης ποιότητας και αποτελεί το μοναδικό πρότυπο στην οικογένεια για το οποίο μπορεί να πιστοποιηθεί (αν και αυτό δεν αποτελεί απαίτηση). Μπορεί να χρησιμοποιηθεί από οποιονδήποτε οργανισμό, είτε μεγάλο είτε μικρό, ανεξάρτητα από τον τομέα δραστηριότητάς του. Στην πραγματικότητα, υπάρχουν πάνω από ένα εκατομμύριο εταιρείες και οργανισμοί σε περισσότερες από 170 χώρες πιστοποιημένες σύμφωνα με το πρότυπο ISO 9001.

Το πρότυπο αυτό βασίζεται σε μια σειρά αρχών διαχείρισης της ποιότητας, όπως η ισχυρή εστίαση στους πελάτες, το κίνητρο και οι επιπτώσεις της ανώτατης διοίκησης, η προσέγγιση της διαδικασίας και η συνεχής βελτίωση. Αυτές οι αρχές εξηγούνται λεπτομερέστερα στις Αρχές Διαχείρισης Ποιότητας. Η χρήση του προτύπου ISO 9001: 2015 συμβάλλει στη διασφάλιση συνεκτικών και ποιοτικών προϊόντων και υπηρεσιών, τα οποία με τη σειρά τους αποφέρουν πολλά επιχειρηματικά οφέλη. Το ISO έχει μια σειρά προτύπων για συστήματα διαχείρισης ποιότητας που βασίζονται στο πρότυπο ISO 9001 και είναι προσαρμοσμένα σε συγκεκριμένους τομείς και βιομηχανίες. Αυτά περιλαμβάνουν:

- ISO 13485 - Ιατρικές συσκευές
- ISO 17582 - Εκλογικές οργανώσεις σε όλα τα επίπεδα διακυβέρνησης
- ISO 18091 - Τοπική αυτοδιοίκηση
- ISO / TS 22163 - Απαιτήσεις συστήματος διαχείρισης επιχειρήσεων για τους σιδηροδρομικούς οργανισμούς
- ISO / TS 29001 - Βιομηχανίες πετρελαίου, πετροχημικών και φυσικού αερίου
- ISO / IEC 90003 - Μηχανική λογισμικού (Kumar, Balakrishnan, 2011).

ISO 22000

Η οικογένεια διεθνών προτύπων ISO 22000 εξετάζει τη διαχείριση της ασφάλειας των τροφίμων. Οι συνέπειες των μη ασφαλών τροφίμων μπορεί να είναι σοβαρές και τα πρότυπα διαχείρισης της ασφάλειας των τροφίμων της ISO βοηθούν τους οργανισμούς να εντοπίζουν και να ελέγχουν τους κινδύνους για την ασφάλεια των τροφίμων. Δεδομένου ότι πολλά από τα σημερινά προϊόντα διατροφής διαπερνούν επανειλημμένα εθνικά σύνορα, απαιτούνται διεθνή πρότυπα για να εξασφαλιστεί η ασφάλεια της παγκόσμιας αλυσίδας εφοδιασμού τροφίμων.

Ο σκοπός του ISO 22000 Το ISO 22000: 2018 ορίζει τις απαιτήσεις για ένα σύστημα διαχείρισης της ασφάλειας των τροφίμων και μπορεί να πιστοποιηθεί σε. Καθορίζει τι πρέπει να κάνει ένας οργανισμός για να αποδείξει την ικανότητά του να ελέγχει τους κινδύνους για την ασφάλεια των τροφίμων, προκειμένου να διασφαλίσει ότι τα τρόφιμα είναι ασφαλή. Μπορεί να χρησιμοποιηθεί από οποιονδήποτε οργανισμό ανεξάρτητα από το μέγεθος ή τη θέση του στην τροφική αλυσίδα.

Το ISO 22001 επικεντρώνεται ειδικά στα τρόφιμα και τα ποτά, ενώ το ISO 22002 επικεντρώνεται στην παραγωγή τροφίμων. Οι υπηρεσίες μεταφοράς τροφίμων, τα εστιατόρια, οι επιχειρήσεις εστίασης και οι επιχειρήσεις παραγωγής τροφίμων θα θέλουν σίγουρα να λάβουν πιστοποίηση σύμφωνα με τα πρότυπα ISO 22000. Μέχρι σήμερα έχουν εκδοθεί περισσότερες από είκοσι έξι χιλιάδες πιστοποιήσει

ISO 14000

Η οικογένεια προτύπων ISO 14000 παρέχει πρακτικά εργαλεία για επιχειρήσεις και οργανισμούς κάθε είδους που επιθυμούν να διαχειριστούν τις περιβαλλοντικές ευθύνες τους. Το ISO 14001: 2015 και τα υποστηρικτικά πρότυπα όπως το ISO 14006: 2011 επικεντρώνονται στα περιβαλλοντικά συστήματα για να το επιτύχουν. Τα άλλα πρότυπα στην οικογένεια επικεντρώνονται σε συγκεκριμένες προσεγγίσεις όπως οι έλεγχοι, οι επικοινωνίες, η επισήμανση και η ανάλυση κύκλου ζωής, καθώς και οι περιβαλλοντικές προκλήσεις όπως η κλιματική αλλαγή.

Το πρότυπο ISO 14001: 2015 καθορίζει τα κριτήρια για ένα σύστημα περιβαλλοντικής διαχείρισης και μπορεί να πιστοποιηθεί. Σχεδιάζει ένα πλαίσιο που μια εταιρεία ή ένας οργανισμός μπορεί να ακολουθήσει για να δημιουργήσει ένα

αποτελεσματικό σύστημα περιβαλλοντικής διαχείρισης. Μπορεί να χρησιμοποιηθεί από οποιονδήποτε οργανισμό ανεξάρτητα από τη δραστηριότητα ή τον τομέα του.

Η χρήση του ISO 14001: 2015 μπορεί να παρέχει τη διαβεβαίωση στη διοίκηση και τους υπαλλήλους, καθώς και στους εξωτερικούς ενδιαφερόμενους, ότι ο περιβαλλοντικός αντίκτυπος μετράται και βελτιώνεται.

ISO 26000

Οι επιχειρήσεις και οι οργανώσεις δεν λειτουργούν σε κενό. Η σχέση τους με την κοινωνία και το περιβάλλον στο οποίο λειτουργούν είναι ένας κρίσιμος παράγοντας στην ικανότητά τους να συνεχίσουν να λειτουργούν αποτελεσματικά. Χρησιμοποιείται επίσης όλο και περισσότερο ως μέτρο της συνολικής απόδοσής τους.

Το ISO 26000 παρέχει καθοδήγηση σχετικά με τον τρόπο λειτουργίας των επιχειρήσεων και των οργανισμών με κοινωνικά υπεύθυνο τρόπο. Αυτό σημαίνει ότι ενεργεί με δεοντολογικό και διαφανή τρόπο που συμβάλλει στην υγεία και την ευημερία της κοινωνίας.

Το πρότυπο ISO 26000: 2010 παρέχει καθοδήγηση και όχι απαιτήσεις, οπότε δεν μπορεί να πιστοποιηθεί αντίθετα με ορισμένα άλλα γνωστά πρότυπα ISO. Αντ 'αυτού, βοηθάει στην αποσαφήνιση της κοινωνικής ευθύνης, βοηθά τις επιχειρήσεις και τις οργανώσεις να μεταφέρουν τις αρχές σε αποτελεσματικές ενέργειες και μοιράζεται τις βέλτιστες πρακτικές που σχετίζονται με την κοινωνική ευθύνη σε παγκόσμιο επίπεδο. Απευθύνεται σε όλους τους τύπους οργανισμών ανεξάρτητα από τη δραστηριότητα, το μέγεθος ή την τοποθεσία τους.

Το πρότυπο ξεκίνησε το 2010 μετά από πέντε χρόνια διαπραγματεύσεων μεταξύ πολλών διαφορετικών ενδιαφερομένων σε όλο τον κόσμο. Εκπρόσωποι της κυβέρνησης, των ΜΚΟ, της βιομηχανίας, των ομάδων καταναλωτών και των οργανώσεων εργασίας σε όλο τον κόσμο συμμετείχαν στην ανάπτυξή της, πράγμα που σημαίνει ότι αντιπροσωπεύει διεθνή συναίνεση.

Υποστήριξη για την εφαρμογή του ISO 26000 Το ISO 26000 αναπτύχθηκε από μια ομάδα εργασίας περίπου 500 εμπειρογνωμόνων. Κατά τη δημοσίευση αυτού του προτύπου η ομάδα εργασίας διαλύθηκε. Έγγραφα για την υποστήριξη της εφαρμογής του προτύπου ISO 26000: Πρωτόκολλο επικοινωνίας - Περιγράφει τις κατάλληλες διατυπώσεις που μπορούν να χρησιμοποιήσουν οι οργανισμοί για να επικοινωνήσουν σχετικά με τη χρήση του ISO 26000 Βασικά εκπαιδευτικά υλικά ISO 26000 με τη μορφή καθοδήγησης του PowerPoint και του πρωτοκόλλου εκπαίδευσης [PDF] Αυτά που συνδέουν το πρότυπο ISO 26000 με τις κατευθυντήριες γραμμές του ΟΟΣΑ για τις πολυεθνικές επιχειρήσεις και την ατζέντα 2030 (στόχοι αειφόρου ανάπτυξης) του ΟΗΕ.

ISO 31000

Οι κίνδυνοι που επηρεάζουν τους οργανισμούς μπορούν να έχουν συνέπειες από την άποψη της οικονομικής απόδοσης και της επαγγελματικής φήμης, καθώς και των περιβαλλοντικών, ασφαλιστικών και κοινωνικών αποτελεσμάτων. Ως εκ τούτου, η διαχείριση του κινδύνου βοηθά αποτελεσματικά τους οργανισμούς σε ένα περιβάλλον γεμάτο αβεβαιότητα.

ISO 31000: 2018, Διαχείριση κινδύνων - Κατευθυντήριες γραμμές, παρέχει αρχές, πλαίσιο και διαδικασία διαχείρισης κινδύνων. Μπορεί να χρησιμοποιηθεί από οποιονδήποτε οργανισμό ανεξάρτητα από το μέγεθος, τη δραστηριότητα ή τον τομέα του. Η χρήση του ISO 31000 μπορεί να βοηθήσει τους οργανισμούς να αυξήσουν την πιθανότητα επίτευξης στόχων, να βελτιώσουν τον εντοπισμό ευκαιριών και απειλών και να κατανείμουν αποτελεσματικά και να χρησιμοποιήσουν πόρους για την αντιμετώπιση κινδύνων. Ωστόσο, το ISO 31000 δεν μπορεί να χρησιμοποιηθεί για σκοπούς πιστοποίησης, αλλά παρέχει οδηγίες για προγράμματα εσωτερικού ή εξωτερικού ελέγχου. Οι οργανισμοί που τη χρησιμοποιούν μπορούν να συγκρίνουν τις πρακτικές διαχείρισης κινδύνων με ένα διεθνώς αναγνωρισμένο σημείο αναφοράς, παρέχοντας ορθές αρχές για αποτελεσματική διαχείριση και εταιρική διακυβέρνηση.

Υπάρχουν ορισμένα άλλα πρότυπα που σχετίζονται επίσης με τη διαχείριση κινδύνου.

- Οδηγός ISO 73: 2009, Διαχείριση κινδύνων - Λεξιλόγιο συμπληρώνει το ISO 31000 παρέχοντας μια συλλογή όρων και ορισμών σχετικά με τη διαχείριση του κινδύνου.
- IEC 31010: 2009, Διαχείριση κινδύνων - Οι τεχνικές εκτίμησης επικινδυνότητας επικεντρώνονται στην εκτίμηση κινδύνου. Η αξιολόγηση των κινδύνων βοηθά τους υπεύθυνους λήψης αποφάσεων να κατανοήσουν τους κινδύνους που θα μπορούσαν να επηρεάσουν την επίτευξη των στόχων καθώς και την επάρκεια των ήδη υφιστάμενων ελέγχων.
- Το IEC 31010: 2009 επικεντρώνεται στις έννοιες, διαδικασίες και την επιλογή των τεχνικών εκτίμησης επικινδυνότητας.

ISO 50001

Η αποτελεσματική χρήση της ενέργειας βοηθά τους οργανισμούς να εξοικονομήσουν χρήματα καθώς και να συμβάλλουν στη διατήρηση των πόρων και στην αντιμετώπιση της κλιματικής αλλαγής. Το πρότυπο ISO 50001 υποστηρίζει τους οργανισμούς σε όλους τους τομείς να χρησιμοποιούν πιο αποτελεσματικά την ενέργεια, μέσω της ανάπτυξης ενός συστήματος διαχείρισης ενέργειας (EnMS).

Το ISO 50001 βασίζεται στο μοντέλο συνεχούς βελτίωσης του συστήματος διαχείρισης που χρησιμοποιείται και για άλλα γνωστά πρότυπα όπως το ISO 9001 ή το ISO 14001. Αυτό διευκολύνει τους οργανισμούς να ενσωματώσουν τη διαχείριση ενέργειας στις συνολικές προσπάθειές τους για βελτίωση της ποιότητας και της περιβαλλοντικής διαχείρισης.

Το ISO 50001: 2018 παρέχει ένα πλαίσιο απαιτήσεων για τους οργανισμούς ώστε να:

- Αναπτύξουν την πολιτική τους για αποτελεσματικότερη χρήση της ενέργειας.
- Καθορίσουν τους στόχους για την εκπλήρωση της πολιτικής.
- Χρησιμοποιήσουν τα δεδομένα για καλύτερη κατανόηση και λήψη αποφάσεων σχετικά με τη χρήση ενέργειας.
- Μετρήσουν τα αποτελέσματα των ενεργειών τους.

- Ελέγξουν πόσο καλά λειτουργεί η πολιτική και τέλος.
- Να βελτιώνουν συνεχώς τη διαχείριση ενέργειας.

Όπως και άλλα πρότυπα συστήματος διαχείρισης ISO, η πιστοποίηση σύμφωνα με το ISO 50001 είναι δυνατή αλλά όχι υποχρεωτική. Ορισμένες οργανώσεις αποφασίζουν να εφαρμόσουν το πρότυπο μόνο για τα οφέλη που προσφέρει. Άλλοι αποφασίζουν να λάβουν πιστοποίηση γι' αυτό, για να επιδείξουν εξωτερικά κόμματα που έχουν εφαρμόσει ένα σύστημα διαχείρισης ενέργειας. Το ISO δεν εκτελεί πιστοποίηση.

1.10 Το BRITISH STANDARD BS 7799-2:1999

Πρόδρομος του ISO 27000 που θα αναλυθεί παρακάτω αποτελεί το British Standard, το οποίο και δημιουργήθηκε το 2002 με σκοπό την προστασία της πληροφορίας. Στην προσπάθεια αυτή συνεργάστηκαν μία σειρά από επιτροπές και οργανισμοί στο Ηνωμένο Βασίλειο.

Το British Standard δημιουργήθηκε και εξελίχθηκε για τους διευθυντές επιχειρήσεων και για το προσωπικό τους ώστε να έχουν ένα μοντέλο για το πώς να στηθεί και να διαχειριστεί ένα αποτελεσματικό ISMS (Information Security Management system). Η εφαρμογή ενός ISMS θα πρέπει να είναι στρατηγική απόφαση για έναν οργανισμό και ο σχεδιασμός και η εφαρμογή του να λαμβάνει υπόψιν τις ανάγκες της επιχείρησης και τους στόχους της, της απαιτήσεις που αφορούν την ασφάλεια, τις διαδικασίες που χρησιμοποιούνται καθώς και το μέγεθος και την δομή του οργανισμού. Είναι επίσης αναμενόμενο ότι απλές καταστάσεις απαιτούν και αντίστοιχα απλούς ISMS (DISC Board, 2002)

Το British Standard προάγει την εφαρμογή μιας προσέγγισης για την δημιουργία, εφαρμογή, λειτουργία, επίβλεψη, συντήρηση και βελτίωση της αποτελεσματικότητας ενός ISMS σε έναν οργανισμό. Οι οργανισμοί πρέπει να αναγνωρίζουν και να διαχειρίζονται αρκετές δραστηριότητες ώστε να λειτουργούν

επαρκώς. Κάθε δράση που χρησιμοποιεί πόρους και διαχειρίζεται την παραγωγή, θεωρείται μια επεξεργασία. Συχνά, το αποτέλεσμα μιας επεξεργασίας είναι η πρώτη ύλη για μια επόμενη. Μια προσέγγιση επεξεργασιών ενθαρρύνει τους χρήστες της να δώσουν έμφαση στην σημαντικότητα των παρακάτω:

1. Την κατανόηση των απαιτήσεων των πληροφοριών ασφαλείας της εταιρίας και την ανάγκη εφαρμογής κανόνων και στόχων για την ασφάλεια αυτών των πληροφοριών.
2. Την εφαρμογή και τον χειρισμό των διαδικασιών που αφορούν το συνολικό επιχειρηματικό ρίσκο του οργανισμού.
3. Την παρακολούθηση και μελέτη της απόδοσης και αποτελεσματικότητας του ISMS
4. Την συνεχή βελτίωση βάση προγραμματισμού και μετρήσεων.

Το μοντέλο, γνωστό και ως «Σχεδιασμός-Εφαρμογή-Έλεγχος-Δράση», μπορεί να εφαρμοστεί σε όλες τις ISMS Διαδικασίες, όπως αυτό υιοθετείται σε αυτό το Standard.

Το ISMS σχεδιάστηκε για να εξασφαλίζει επαρκείς και ανάλογους χειρισμούς ασφαλείας, οι οποίοι προστατεύουν επαρκώς τις πληροφορίες, και να προσφέρει ασφάλεια και αυτοπεποίθηση σε πελάτες και λοιπούς ενδιαφερόμενους. Αυτό σημαίνει την διατήρηση και την βελτίωση σε σχέση με τον ανταγωνισμό, την χρηματική διαχείριση, το κέρδος, την νομική συμμόρφωση και την επαγγελματική εικόνα ως προς τον καταναλωτή.

Οι απαιτήσεις που αναπτύσσονται σε αυτήν την Βρετανική Standard είναι γενικές και έχουν σκοπό να είναι εφαρμόσιμες σε όλους τους οργανισμούς, ανεξάρτητα με τον τύπο , το μέγεθος και την φύση της επιχείρησης. Οποιαδήποτε απαίτηση δεν μπορεί να εφαρμοστεί λόγω της φύσεως ενός οργανισμού/επιχείρησης, τότε αυτή μπορεί να εξαιρεθεί.

Όπου γίνονται τέτοιες εξαιρέσεις, δεν γίνονται δεκτές αιτήσεις συμμόρφωσης εκτός και αν οι εξαιρέσεις αυτές δεν επηρεάζουν την ικανότητα ή/και την ευθύνη του οργανισμού στο να παρέχουν πληροφορίες ασφαλείας που πληρούν τις απαιτήσεις ασφαλείας και είναι σύμφωνες με τους κανονισμούς. Οποιαδήποτε εξαίρεση

χειρισμών που είναι απαραίτητη για τα κριτήρια ρίσκου, πρέπει να δικαιολογηθεί με πειστήρια από τα νομικά πρόσωπα του οργανισμού.

Κεφάλαιο 2^{ο}: Τα πρότυπα 2700X

Η σειρά προτύπων 27000 τα τελευταία χρόνια έχει συνεχώς αυξανόμενη ζήτηση και αποτελεί ένα συνεχώς μεταβαλλόμενο πεδίο δράσης. Αυτό οφείλεται στο γεγονός ότι υπάρχει πολύ μεγάλη πίεση στην πάντα ανταγωνιστική και εξελισσόμενη αγορά αλλά και ενδεχομένως λόγω της αύξησης της ευαισθητοποίησης όσον αφορά την ασφάλεια των πληροφοριών και τις απειλές που συνδέονται με αυτές.

Ενώ τα πρότυπα παρέχουν γενικές κατευθυντήριες γραμμές για τη δημιουργία του συστήματος, καθώς και τις απαιτήσεις που είναι απαραίτητες για την εκπλήρωση των κριτηρίων πιστοποίησης, παρέχουν ελάχιστες πληροφορίες όσον αφορά την πραγματική διαδικασία εφαρμογής. Αυτό είναι το σημαντικότερο λόγος που έχουν δημιουργηθεί εταιρείες που ειδικεύονται στη διαβούλευση με επιχειρήσεις (Kovac, 2014).

2.1 Τι είναι το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών

Οι άνθρωποι, οι κυβερνήσεις και οι οργανώσεις ανησυχούν όλοι για θέματα ασφάλειας πληροφοριών που έχουν οικονομικά, κοινωνικά, πολιτικά και τεχνικά χαρακτηριστικά. Ένα Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών ή ISMS (Information Security Management System), όπως είναι πιο γνωστό στην διεθνή βιβλιογραφία είναι ένα σύστημα που διαχειρίζεται τα ευαίσθητα δεδομένα ενός οργανισμού, δημιουργώντας, λειτουργώντας, αναθεωρώντας και βελτιώνοντας την ασφάλεια των πληροφοριών, η οποία καλύπτει τη συμπεριφορά των εργαζομένων, καθώς και τα δεδομένα και την τεχνολογία.

Το ΣΔΑΠ βοηθά τους οργανισμούς να δημιουργήσουν αντίμετρα για την ασφάλεια των πληροφοριών ευπάθειες, που παρέχει μια ασφαλή βάση για να

αναπτυχθεί και να ανταποκριθεί σε πολλά νομικά τις προσδοκίες και τις απαιτήσεις ασφάλειας των πληροφοριών για τους οργανισμούς.

Ένα ΣΔΑΠ αποτελείται από διαφορετικές διαδικασίες, οι οποίες αρχίζουν με τον προσδιορισμό των απαιτήσεων ασφάλειας και συνεχίζουν με το να πληρούν αυτές τις απαιτήσεις με τις απαραίτητες στρατηγικές και μετρήσεις αποτελεσμάτων.

Οι περισσότερες απαιτήσεις ασφάλειας προέρχονται από την επιχείρηση η οποία απαιτεί την δημιουργία και εφαρμογή του συστήματος. Υπάρχουν, όμως και άλλες πηγές απαιτήσεων ασφάλειας όπως νομικές, κανονιστικές και συμβατικές απαιτήσεις. Οι απαιτήσεις ασφάλειας του οργανισμού, οι στόχοι, η διαδικασία καθώς και το μέγεθος είναι χαρακτηριστικά που καθορίζουν ένα ΣΔΑΠ. Για την προστασία των περιουσιακών στοιχείων ενός οργανισμού, το ΣΔΑΠ παρέχει ένα σύνολο διαδικασιών και οδηγιών για τη διαχείριση πόρων και δραστηριοτήτων. Επιπλέον, για να διασφαλιστεί η συνεπής εφαρμογή των αρχών ασφάλειας και της δήλωσης πολιτικής, το ΣΔΑΠ αποτελείται από όλα τα μέσα και τις μεθόδους που η ηγεσία πρέπει να χρησιμοποιήσει για να ικανοποιήσει την ασφάλεια των πληροφοριών σε όλα τα καθήκοντα και τις δραστηριότητες (Boehmer, 2009).

Ο βασικός στόχος ενός ΣΔΑΠ είναι να διαχειριστεί τον κίνδυνο. Προκειμένου να προσδιοριστεί και να μετρηθεί ο οργανωτικός κίνδυνος και να διασφαλιστεί η συνέχεια της επιχείρησης, εφαρμόζονται πολιτικές ασφάλειας και έλεγχοι για τον μετριασμό των κινδύνων. Για την υποστήριξη της υλοποίησης της πολιτικής ασφάλειας, απαιτείται εκτενής τεκμηρίωση όλων των διαδικασιών ασφαλείας. Η διαχείριση της ασφάλειας των πληροφοριών ως αποτέλεσμα της εφαρμογής ενός ΣΔΑΠ απαιτεί μια διαδικασία για τη δημιουργία, την επικοινωνία και τη διατήρηση πολιτικών και διαδικασιών εντός ενός οργανισμού. Η τυποποίηση των διαδικασιών διαχείρισης της ασφάλειας πληροφοριών παρέχει αρκετά πλεονεκτήματα, όπως μείωση του κόστους ή βελτιωμένη συμβατότητα του συστήματος.

Ένα πρότυπο ΣΔΑΠ παρέχει απαιτήσεις για ένα σύστημα, το οποίο θα μπορούσε να μετριάσει τα συμβάντα ασφάλειας ΙΤ, τις συμβατικές κυρώσεις ή την απώλεια φήμης, όπως αποκάλυψη εμπιστευτικών πληροφοριών για τους πελάτες.

Ένα διεθνές πρότυπο για τη ρύθμιση της ασφάλειας των πληροφοριών θα μπορούσε να βελτιώσει τις μεθόδους ασφάλειας πληροφοριών σε ένα ανταγωνιστικό περιβάλλον, το οποίο παρέχει κοινά σημεία αναφοράς μεταξύ οργανισμών και χωρών. Σε διεθνές επίπεδο, ένα κοινό πρότυπο ΣΔΑΠ θα μπορούσε να παράσχει συνεπή τρόπο αντιμετώπισης των ζητημάτων ασφάλειας των πληροφοριών μεταξύ των χωρών. Η συμμόρφωση με τις νομοθεσίες για την ασφάλεια των πληροφοριών σε διεθνές επίπεδο είναι μία από τις ανησυχίες των οργανισμών στις διεθνείς επικοινωνίες, οι οποίες θα μπορούσαν να αντιμετωπιστούν με ένα πρότυπο ΣΔΑΠ όπως το ISO 27001:2013 (Shojaie, 2018).

2.2 Η οικογένεια προτύπων 2700X

Για αρκετά χρόνια οι επιχειρήσεις αλλά και οι οργανισμοί αναζητούν έναν πρότυπο – στόχο αναφοράς για τη μέτρηση της ασφάλειας των πιθανών συνεργατών τους αλλά για την δική τους ασφάλεια. Αν και δεν είναι τέλειο, το ISO 17799 προέκυψε ως πρότυπο επιλογής, επειδή ξεπέρασε πολλές από τις κρίσιμες ελλείψεις του προγενέστερου SAS 70. Ειδικότερα, παρείχε ένα πλήρες σύνολο θεμάτων σχετικά με την ασφάλεια και ένα αντικειμενικό μέσο για τη μέτρηση της συμμόρφωσης. Ακολουθώντας την ίδια προσέγγιση που χρησιμοποιήθηκε με τα Πρότυπα διασφάλισης ISO 900X, ο Διεθνής Οργανισμός Τυποποίησης (ISO) έχει διαθέσει την περιοχή αριθμοδότησης 27000 για μια σειρά από Πρότυπα ασφαλείας πληροφοριών (Gossels, Mackey, 2007).

Το πολύ μεγάλο, όμως, πεδίο εφαρμογής ώθησε τον Παγκόσμιο Οργανισμό Τυποποίησης να δημιουργήσει μία ολόκληρη σειρά από πρότυπα που εντάσσονται στην οικογένεια 27000. Αυτά είναι:

- ISO/ IEC 27000, σύστημα διαχείρισης ασφάλειας πληροφοριών. Αυτό αποτελεί μία επισκόπηση – εισαγωγή στα πρότυπα ISO 27k και περιέχει και

το λεξιλόγιο όρων. Αυτό το πρότυπο παρέχει στον χρήστη συνολικά το σημείο εκκίνησης με το οποίο μπορεί να εισαχθεί στην οικογένεια 27000

- ISO/ IEC 27001, σύστημα διαχείρισης ασφάλειας πληροφοριών, οι προϋποθέσεις. Αποτελεί το πρότυπο για ένα σύστημα διαχείρισης ασφάλειας πληροφοριών βάση του οποίου έχουν πιστοποιηθεί χιλιάδες επιχειρήσεις και οργανισμοί στον κόσμο.
- ISO/ IEC 27002, είναι ο κώδικας πρακτικής για τους ελέγχους ασφάλειας των πληροφοριών. Αποτελεί μια εύλογα ολοκληρωμένη δέσμη στόχων ελέγχου ασφάλειας πληροφοριών και γενικά αποδεκτών ελέγχων ασφάλειας ορθής πρακτικής (ISO, 2018).
- ISO/ IEC 27003, αποτελεί τις οδηγίες εφαρμογής ενός συστήματος διαχείρισης ασφάλειας πληροφοριών. Στην πραγματικότητα παρέχει τις ορθές συμβουλές ή οδηγίες σχετικά με την εφαρμογή του ISO27k, επεκτείνοντας τμήμα τμήμα σε όλο το σώμα του ISO / IEC 27001.
- ISO/ IEC 27004, περιέχει τα μέτρα μέτρησης στην διαχείριση της ασφάλειας πληροφοριών.
- ISO/ IEC 27005, το πρότυπο για την διαχείριση κινδύνων ασφάλειας πληροφοριών. Αναφέρει γενικά τις αρχές διαχείρισης κινδύνου πληροφοριών χωρίς να καθορίζει συγκεκριμένες μεθόδους, αποτελεί ένα πρότυπο που χρειάζεται αναθεώρηση για να καλύψει τις σημερινές ανάγκες (ISO, 2018).
- ISO/ IEC 27006, αναφέρει τις απαιτήσεις για φορείς που παρέχουν έλεγχο και πιστοποίηση συστημάτων διαχείρισης της ασφάλειας των πληροφοριών. Είναι το πρότυπο που προσφέρει καθοδήγηση για τους οργανισμούς πιστοποίησης.
- ISO/ IEC 27007, οι κατευθυντήριες γραμμές για τον έλεγχο των συστημάτων διαχείρισης της ασφάλειας των πληροφοριών. Ελέγχει τα στοιχεία συστήματος διαχείρισης του ISMS.
- ISO/ IEC 27008, οι κατευθυντήριες γραμμές για τους ελεγκτές σχετικά με τους ελέγχους ασφάλειας πληροφοριών. Ελέγχει τα στοιχεία ασφάλειας των πληροφοριών του ISMS.
- ISO/ IEC 27009, αποτελεί ειδική τομεακή εφαρμογή των απαιτήσεων ISO / IEC 27001.
- ISO/ IEC 27010, πρότυπο για την διαχείριση της ασφάλειας πληροφοριών για διατομεακές και δια-οργανωτικές επικοινωνίες. Έχει εφαρμογή στην

ανταλλαγή πληροφοριών σχετικά με την ασφάλεια των πληροφοριών μεταξύ βιομηχανικών τομέων ή / και εθνών, ιδίως εκείνων που επηρεάζουν την κρίσιμη υποδομή των κρατών ή των οργανισμών.

- ISO/ IEC 27011, Οδηγίες διαχείρισης της ασφάλειας των πληροφοριών για οργανισμούς τηλεπικοινωνιών βάσει του ISO / IEC 27002. Έλεγχοι ασφάλειας πληροφοριών για τη βιομηχανία τηλεπικοινωνιών, γνωστοί επίσης και ως "ITU-T Recommendation x.1051"
- ISO/ IEC 27013, αναφέρει οδηγίες για την ολοκληρωμένη εφαρμογή των προτύπων ISO / IEC 27001 και ISO / IEC 20000-1. Στην πραγματικότητα αυτό το πρότυπο συνδυάζει το ISO27k / ISMS με τη διαχείριση υπηρεσιών IT / ITIL.
- ISO/ IEC 27014, διακυβέρνηση της ασφάλειας των πληροφοριών. Διακυβέρνηση στο πλαίσιο της ασφάλειας των πληροφοριών · αναφέρεται επίσης "ITU-T Recommendation X.1054".
- ISO/ IEC 27015, το πρότυπο με τις οδηγίες διαχείρισης της ασφάλειας των πληροφοριών για τις χρηματοπιστωτικές υπηρεσίες. Αποτελεί την εφαρμογή του ISO27k στη βιομηχανία χρηματοδότησης.
- ISO/ IEC 27016, πρότυπο διαχείρισης της ασφάλειας πληροφοριών – στη Οργανωτική οικονομία. Στο πρότυπο αυτό η οικονομική θεωρία εφαρμόζεται στην ασφάλεια των πληροφοριών.
- ISO/ IEC 27017, ο κώδικας πρακτικής για ελέγχους ασφάλειας πληροφοριών για υπηρεσίες cloud computing βάσει του ISO / IEC 27002. Παρέχει τους Ελέγχους ασφάλειας πληροφοριών για cloud computing.
- ISO/ IEC 27018, Κώδικας πρακτικής για ελέγχους για την προστασία προσωπικών δεδομένων που υποβάλλονται σε επεξεργασία στις δημόσιες υπηρεσίες.
- ISO/ IEC 27019, οι κατευθυντήριες γραμμές διαχείρισης ασφάλειας πληροφοριών βασισμένες στο ISO / IEC 27002 για συστήματα ελέγχου διαδικασιών ειδικά για την ενεργειακή βιομηχανία. Πρότυπο για την ασφάλεια πληροφοριών για ICS / SCADA / ενσωματωμένα συστήματα (όχι μόνο αυτά που χρησιμοποιούνται στην ενεργειακή βιομηχανία), στο πρότυπο αυτό εξαιρείται η πυρηνική βιομηχανία.

- ISO/ IEC 27021, οι απαιτήσεις ικανότητας για επαγγελματίες στην διαχείριση της ασφάλειας πληροφοριών. Το πρότυπο αυτό προσφέρει καθοδήγηση σχετικά με τις δεξιότητες και τις γνώσεις που απαιτούνται για να εργαστεί κανείς σε αυτόν τον τομέα.
- ISO/ IEC 27023, αποτελεί μία χαρτογράφηση των αναθεωρημένων εκδόσεων ISO / IEC 27001 και ISO / IEC 27002. Αποτελεί το πρότυπο με τις τελευταίες συμβουλές για τους χρήστες που ενημερώνουν τα ISMS τους από τις εκδόσεις 2005 έως 2013.
- ISO/ IEC 27030, Κατευθυντήριες γραμμές για την ασφάλεια και την ιδιωτική ζωή στο Internet of things (IoT). Ένα πρότυπο σχετικά με τις πτυχές του κινδύνου πληροφοριών, της ασφάλειας και της ιδιωτικής ζωής του IoT.
- ISO/ IEC 27031, οι κατευθυντήριες γραμμές για την ετοιμότητα της τεχνολογίας πληροφοριών και επικοινωνιών για τη συνέχεια της επιχείρησης. Συνέχεια (δηλαδή ανθεκτικότητα, διαχείριση συμβάντων και ανάκτηση καταστροφών) για τις ICT, υποστηρίζοντας τη γενική επιχειρηματική συνέχεια.
- ISO/ IEC 27032, οι κατευθυντήριες γραμμές για την ασφάλεια στον κυβερνοχώρο. Στην πραγματικότητα αυτό το πρότυπο αφορά στην ασφάλεια του Διαδικτύου.
- ISO/ IEC 27033, το πρότυπο αυτό έχει μία σειρά από εφαρμογές:
    I. -1, επισκόπηση και ιδέες για την ασφάλεια των δικτύων.
    II. -2, κατευθυντήριες γραμμές για το σχεδιασμό και την υλοποίηση της ασφάλειας του δικτύου.
    III. -3, σενάρια δικτύωσης αναφοράς - απειλές, τεχνικές σχεδιασμού και θέματα ελέγχου.
    IV. -4, διασφάλιση επικοινωνιών μεταξύ δικτύων που χρησιμοποιούν πύλες ασφαλείας.
    V. -5, διασφάλιση επικοινωνιών μεταξύ δικτύων με τη χρήση εικονικών ιδιωτικών δικτύων (VPN).
    VI. -6, ασφάλιση της πρόσβασης σε ασύρματο δικτύου IP.
- ISO/ IEC 27034, πρότυπο ασφαλείας πολλαπλών εφαρμογών, προωθεί την ιδέα μιας επαναχρησιμοποιήσιμης βιβλιοθήκης λειτουργιών ελέγχου

ασφάλειας πληροφοριών, προδιαγραφόμενων, σχεδιασμένων και δοκιμασμένων. Αυτό το πρότυπο περιλαμβάνει:

I. -1, ασφάλεια εφαρμογών - Επισκόπηση και έννοιες.
II. -2, οργανικό κανονιστικό πλαίσιο.
III. -3, διαδικασία διαχείρισης ασφάλειας εφαρμογών.
IV. -4, επικύρωση ασφάλειας εφαρμογών.
V. -5, πρωτόκολλα και δομή δεδομένων ελέγχου ασφάλειας εφαρμογών.

- ISO/ IEC 27035, Στην πραγματικότητα αφορά τα περιστατικά που αφορούν τα συστήματα και τα δίκτυα IT.
- ISO/ IEC 27036, οι πτυχές της ασφάλειας των πληροφοριών όσον αφορά το outsourcing.
- ISO/ IEC 27037, οι κατευθυντήριες γραμμές για τον προσδιορισμό, τη συλλογή, την απόκτηση και τη διατήρηση ψηφιακών αποδεικτικών στοιχείων.
- ISO/ IEC 27038, αφορά τις προδιαγραφές για ψηφιακή επεξεργασία και την επεξεργασία ψηφιακών εγγράφων.
- ISO/ IEC 27039, το πρότυπο για την επιλογή, εγκατάσταση και λειτουργία συστημάτων ανίχνευσης και πρόληψης εισβολής (IDPS).

2.1 Πλεονεκτήματα της πιστοποίησής ISO/IEC 27001

Όπως για κάθε πιστοποίηση με ISO έτσι και για το πρότυπο 27000 η εφαρμογή του από μία επιχείρηση ή έναν οργανισμό συνεπάγεται και κάποια πλεονεκτήματα που κάνουν αυτό το πρότυπο θελκτικό σε αυτές. Έτσι, παρόλο που το ISO 27000 δεν είναι υποχρεωτικό για κάποια εταιρεία ή οργανισμό με βάση κάποιον νόμο, υπάρχουν μία σειρά από πρακτικούς λόγους και πλεονεκτήματα που οδηγούν στην εφαρμογή του.

Σύμφωνα με τους Calder και Watkins (2006), μία πιστοποίηση με ISO 27000 δημιουργεί πολύ καλύτερο περιβάλλον συνεργασίας τόσο για τους εφιστάμενους

πελάτες μιας επιχείρησης όσο και για τους δυνητικούς της πελάτες. Αυτό το περιβάλλον λέει ότι η επιχείρηση έχει επενδύσει έτσι ώστε να έχει ακριβείς και αποτελεσματικές διαδικασίες προστασίας των πληροφοριών του, αυτό αποτελεί πολύ σημαντικό βήμα στην ανάπτυξη μιας σχέσης εμπιστοσύνης.

Ένας δεύτερος λόγος είναι η ενημέρωση του συστήματος ασφαλείας. Τόσο η πιστοποίηση όσο και ο τακτικός εξωτερικός έλεγχος μέσω της αξιολόγησης, εξασφαλίζουν στην επιχείρηση ή τον οργανισμό την ικανότητα βελτίωσης του συστήματος του. Αυτήν η παράμετρος είναι πολύ σημαντική στον τομέα των ψηφιακών πληροφοριών, έναν τομέα που μεταβάλλεται συνεχώς με εκπληκτική ταχύτητα και οι απειλές εμφανίζονται σχεδόν καθημερινά.

Επιπλέον, κάθε πιστοποίηση παρέχει μία ανεξάρτητη εξωτερική επικύρωση ότι η επιχείρηση εφαρμόζει αποτελεσματικά όλες τις απαιτήσεις του προτύπου ποιότητας και επιδεικνύει την απαραίτητη επιμέλεια, τόσο της διοίκησης του όσο και των στελεχών και του εργατικού προσωπικού, στον εντοπισμό των αναγκών ασφαλείας που αυτήν έχει (Arnason, Willett, 2007).

Μέσω της πιστοποίησης με ISO 27000, στην πραγματικότητα μία επιχείρηση μειώνει το κόστος ελέγχου και αυξάνει την πιθανότητα να διατηρήσει απόρρητες τις πληροφορίες που επιθυμεί.

Ο Bohmer (2009), θεωρεί ότι για να μπορέσει μία επιχείρηση να αντιληφθεί το πραγματικό οικονομικό όφελος από την εφαρμογή ενός προτύπου ISO 27000 ή ενός συστήματος ISMS θα πρέπει η επένδυση σε αυτό να είναι συγκρίσιμη ως προς το όφελος που φέρνει αυτό στην επιχείρηση ή τον οργανισμό. Επειδή αυτό δεν είναι αρκετά εύκολο να εφαρμοστεί από κάθε επιχείρηση προτείνει, για την σύγκριση μεταξύ κόστους επένδυσης και όφελος που προκύπτει από την επένδυση, την χρήση Βασικών Δεικτών απόδοσης (Key Performance Indicators). Αυτοί οι δείκτες θα μπορούν να μετρούν τόσο την οικονομική αποδοτικότητα όσο και την αποτελεσματικότητα του προτύπου. Αν οι δείκτες δεν είναι ικανοί να προσφέρουν σωστά αποτελέσματα, λόγω της δυσκολίας μέτρησης τότε, ο Bohmer, προτείνει την Συνδυαστική βελτιστοποίηση. Μία τεχνική κατά την οποία η επιχείρηση σταθμίζει τα οφέλη του μιας πολιτικής που ακολουθεί από την πλευρά του κινδύνου για κάθε

έλεγχο με το κόστος του κάθε ελέγχου ως προς την αποφυγή ή την μεταφορά του κινδύνου.

Αν τώρα θα έπρεπε να αναφέρουμε σε όρους επιχειρηματικότητας τα σημαντικότερα πλεονεκτήματα από την εφαρμογή ενός προτύπου ISO 27000 αυτά θα ήταν:

- **Η αύξηση της ανταγωνιστικότητας:** τόσο οι υφιστάμενοι όσο και οι δυνητικοί πελάτες μιας επιχείρησης θα επιθυμούσαν την συνεργασία με μια επιχείρηση που θα μπορούσε να προστατεύει επαρκώς τα δεδομένα τους.

- **Η προβολή της εμπορικής εικόνας της επιχείρησης:** η εφαρμογή μιας πιστοποίησης ISO είναι στην πραγματικότητα μία δημόσια δήλωση συμμόρφωσης της επιχείρησης με κάποιες πιστοποιημένες διαδικασίες.

- **Η σημαντική μείωση του κινδύνου:** η εφαρμογή ενός ISO και οι έλεγχοι που αυτήν συνεπάγονται διασφαλίζουν την μείωση της πιθανότητας κλοπής των πληροφοριών και μειώνει την επίπτωση των περιστατικών/ παραβιάσεων.

- **Η συμμόρφωση της επιχείρησης σε κανονιστικές απαιτήσεις:** κάθε πιστοποίηση προϋποθέτει συστηματικό εντοπισμό των σχετικών απαιτήσεων και εφαρμογή τους.

- **Η αύξηση του κύρους της επιχείρησης και της εμπιστοσύνης:** αυτό αφορά την εμπιστοσύνη των πελατών, των εργαζομένων, των συνεργατών, των φορέων και γενικά όλων των ενδιαφερομένων μερών που βρίσκονται στο εσωτερικό και εξωτερικό περιβάλλον της επιχείρησης ή του οργανισμού.

- **Η συνεχής επαγρύπνηση:** τόσο μέσω της εφαρμογής εσωτερικά όσο και μέσω των εξωτερικών ελέγχων (Δερβιτσιώτης, 2001).

2.3 Το πρότυπο ISO/IEC 27001

Η οικογένεια των ISO/IEC 27000, όπως είδαμε παραπάνω, αποτελείται από πάρα πολλά πρότυπα. Η ανάλυση όλων αυτών των προτύπων ξεφεύγει από τα όρια αυτής της εργασίας. Σε αυτήν την παράγραφο θα γίνει μία όσο το δυνατόν πληρέστερη ανάλυση για το ISO/IEC 27001 το οποίο και αποτελεί το πρότυπο με την μεγαλύτερη ζήτηση αλλά και την μήτρα όλων των υπόλοιπων προτύπων της οικογένειας 27000.

Το ISO/ IEC 27001 έχει επίσημη ονομασία: Διαχείριση της Ασφάλειας Πληροφοριών – Προδιαγραφές και Οδηγίες Χρήσης. Σκοπός του είναι να υπηρετήσει ως βάση για τον έλεγχο τρίτων. Δεν αποτελεί έκπληξη το γεγονός ότι είναι προσανατολισμένο στη διαδικασία. Το πρότυπο περιέχει μια εισαγωγή και επτά κεφάλαια όπως φαίνεται παρακάτω:

- Πεδίο εφαρμογής.
- Παραπομπές.
- Οροί και ορισμοί.
- Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών.
- Ευθύνη Διοίκησης.
- Διαχειριστική ανασκόπηση του ISMS.
- Βελτίωση ISMS.

Το πρότυπο περιγράφει επίσης μια διαδικασία πιστοποίησης σε έξι στάδια από τα ακόλουθα βήματα:

- Ορισμός μιας πολιτικής ασφάλειας πληροφοριών.
- Καθορισμός του πεδίου εφαρμογής του συστήματος διαχείρισης της ασφάλειας των πληροφοριών.
- Εκτέλεση μιας αξιολόγησης κινδύνου ασφαλείας.
- Διαχείριση του εντοπισμένου κίνδυνου.
- Επιλογή ελέγχου που θα εφαρμοστεί.

- Προετοιμασία μιας δήλωσης εφαρμογής.

Περιγράφει επίσης μια προσέγγιση αναδρομικής διαχείρισης του κύκλου ζωής του PDCA που αποτελείται από: Σχέδιο (δημιουργία της διαχείρισης της ασφάλειας των πληροφοριών συστήματος), Δράση (χειριστείτε το ISMS), Έλεγχος (Παρακολούθηση και έλεγχος το ISMS) και πράξη (διατήρηση και βελτίωση του ISMS).

Για να επιτευχθεί πιστοποίηση, το ISMS ενός οργανισμού πρέπει να αξιολογηθεί από έναν ελεγκτή που εργάζεται για έναν οργανισμό πιστοποίησης, ο οποίος πρέπει να είναι διαπιστευμένος από το εθνικό όργανο διαπίστευσης για το σχετική περιοχή.

Η διαδικασία πιστοποίησης απαιτεί σαφή διαχωρισμό των καθηκόντων σε αυτόν τον οργανισμό που εκτελείται η πιστοποίηση, και δεν πρέπει να συμμετέχει στην παροχή είτε συμβουλευτικής είτε εκπαίδευσης (Gossels, Mackey, 2007).

Το διεθνές πρότυπο ISO / IEC 27001 έχει δημιουργηθεί για να παράσχει τις απαιτήσεις για τη θέσπιση, εφαρμογή, διατήρηση και συνεχή βελτίωση της ασφάλειας των πληροφοριών στο σύστημα διαχείρισης. Η υιοθέτηση μιας ασφάλειας πληροφοριών για το σύστημα διαχείρισης είναι μια στρατηγική απόφαση για έναν οργανισμό. Η δημιουργία και η εφαρμογή του συστήματος διαχείρισης της ασφάλειας των πληροφοριών του οργανισμού επηρεάζεται από τις ανάγκες και τους στόχους του οργανισμού, τις απαιτήσεις ασφάλειας, τις χρησιμοποιούμενες οργανωτικές διαδικασίες και το μέγεθος και τη δομή και οργάνωσή του. Όλοι αυτοί οι παράγοντες επηρεάζουν την αλλαγή με την πάροδο του χρόνου

Η διαχείριση της ασφάλειας των πληροφοριών διατηρεί την εμπιστευτικότητα, τη διαθεσιμότητα και την ακεραιότητα των πληροφοριών εφαρμόζοντας μια διαδικασία διαχείρισης κινδύνων και δίνει εμπιστοσύνη στα ενδιαφερόμενα μέρη ότι υπάρχουν κίνδυνοι και διαχειρίζονται επαρκώς. Η ασφάλεια των πληροφοριών εξετάζεται στο σχεδιασμό διαδικασιών, συστημάτων ελέγχου και πληροφορικής (Kovac, 2014).

2.4 Η διαδικασία πιστοποίησης με ISO /IEC 27001:2013

Η διαδικασία πιστοποίησης με ISO /IEC 27001:2013 απαιτεί μία σειρά από βήματα τα οποία πρέπει να γίνουν με χρονολογική σειρά ώστε να υλοποιηθεί. Τα βήματα αυτά είναι:

- Η απόφαση για την εφαρμογή του ISO /IEC 27001:2013.
- Ο καθορισμός της πολιτικής ασφαλείας των πληροφοριών. Θα πρέπει να γίνει προσδιορισμός των επιχειρηματικών στόχων και αν θα πρέπει να γίνει βελτίωση των ήδη υπάρχοντών συστημάτων ασφαλείας.
- Ο καθορισμός του πεδίου εφαρμογής του ISMS. Θα πρέπει να γίνει μία σύγκριση με το υπάρχον σύστημα ασφαλείας με τις απαιτήσεις του ISO /IEC 27001:2013 και να επιλεγούν οι επιχειρηματικές μονάδες, τα τμήματα ή τα συστήματα που θα εφαρμοστεί το ISMS
- Η αξιολόγηση του κινδύνου. Θα πρέπει να καθοριστεί μία μέθοδος εκτίμησης του κινδύνου, να γίνει απογραφή των στοιχείων του ενεργητικού για προστασία και στην συνέχει να γίνει ταξινόμηση των στοιχείων αυτών με βάση την αξιολόγηση του κινδύνου.
- Η διαχείριση του προσδιορισμένου κινδύνου. Θα πρέπει να δημιουργηθεί ένα σχέδιο αντιμετώπισης των κινδύνων και να προσδιοριστούν οι κατάλληλες ενέργειες για την διαχείριση των πόρων, των ευθυνών και των προτεραιοτήτων για την διαχείριση των κινδύνων που απορρέουν από την ασφάλεια των πληροφοριών.
- Η επιλογή των ελέγχων που θα εφαρμοστούν.
- Η εφαρμογή των ελέγχων. Θα πρέπει να αναπτυχθούν τα προγράμματα για την εφαρμογή των εντοπισμένων στοιχείων ελέγχου.
- Η προετοιμασία για την πιστοποίηση. Θα πρέπει να γίνει έλεγχος της λειτουργίας του ISMS και διεξαγωγή πλήρους κύκλου εσωτερικών ελέγχων, ανασκοπήσεων και δραστηριοτήτων της διοίκησης.
- Η υποβολή της αίτησης για πιστοποίηση (InfoCloud, 2018).

2.5 Ελληνικοί οργανισμοί που έχουν πιστοποιηθεί με ISO/ IEC 27001:2013

Στην Ελλάδα μία σειρά από οργανισμοί και υπηρεσίες έχουν πιστοποιηθεί με ISO/ IEC 27001:2013. Ιδιαίτερα μετά την ανακοίνωση της Ευρωπαϊκής Ένωσης για την αλλαγή του κανονισμού σχετικά με την προστασία των προσωπικών δεδομένων πάρα πολλοί οργανισμοί έσπευσαν να συμμορφωθούν με αυτόν.

Από τους φορείς της κεντρικής διοίκησης πολλά υπουργεία έχουν πιστοποιηθεί ή είναι σε διαδικασία πιστοποίησης με το συγκεκριμένο πρότυπο:

- Το υπουργείο οικονομικών
- Η ανεξάρτητη αρχή δημοσιών εσόδων
- Το υπουργείο οικονομίας και ανάπτυξης
- Το υπουργείο εσωτερικών
- Το υπουργείο παιδείας
- Το υπουργείο τουρισμού
- Το υπουργείο υγείας

Εκτός όμως από φορείς της κεντρικής διοίκησης υπάρχουν και μία σειρά από άλλους οργανισμούς που έχουν πιστοποιηθεί με ISO/ IEC 27001:2013. Ενδεικτικά αναφέρουμε:

- Το Πανεπιστήμιο Πειραιώς
- Το Πανεπιστήμιο Θεσσαλίας
- Το Πανεπιστήμιο Πατρών
- Το Πανεπιστήμιο Αιγαίου
- Το Ελληνικό Ανοιχτό Πανεπιστήμιο
- Το Γενικό Νοσοκομείο ευαγγελισμός
- Ο Ο.Π.Ε.Κ.Ε.Π.Ε.
- Η υπηρεσία πολιτικής αεροπορίας
- Πάρα πολλοί δήμοι στην χώρα

- Η Ελληνική Ολυμπιακή Επιτροπή
- Η Εθνική τράπεζα της Ελλάδος
- Ο Τειρεσίας
- Το χρηματιστήριο Αθηνών
- Το εθνικό ταμείο Επιχειρηματικότητας & Ανάπτυξης (ΕΤΕΑΝ)
- Η Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων (ΕΕΤΤ)
- Τα ΕΛΤΑ
- Το Κέντρο Πληροφορικής Υποστήριξης Ελληνικού Στρατού (ΚΕ.ΠΥ.Ε.Σ.)
- Η Προεδρία Ελληνικής Δημοκρατίας

Κεφάλαιο 3^{ο}: Η διαδικασία πιστοποίησης της ΓΓΠΣ

Το 2016 η Γενική Γραμματεία Πληροφοριακών Συστημάτων του Υπουργείου Οικονομικών (ΓΓΠΣ), λόγω της αλλαγής του Ευρωπαϊκού Κανονισμού για την Προστασία Προσωπικών Δεδομένων (ΕΚ/2016/679/GDPR) προχώρησε στην επιτάχυνση των διαδικασιών εφαρμογής του πρότυπου ISO/ IEC 27001:2013. Στόχοι ήταν:

A. Η συνεχής βελτίωση του επιπέδου ασφαλείας των προσωπικών δεδομένων των χρηστών και των εγγεγραμμένων του οργανισμού όπως αυτά διαχειρίζονται από τα πληροφορικά συστήματα.
B. Το συγκεκριμένο σύστημα να αποτελέσει μία αποτελεσματική και ολοκληρωμένη πρόταση οργάνωσης των προσωπικών δεδομένων και να εξασφαλίζει στον οργανισμό την νόμιμη διαχείριση τους σύμφωνα με τις προδιαγραφές του νέου Ευρωπαϊκού κανονισμού.

Το ISO/ IEC 27001 είναι ένα σύστημα διαχείρισης της ασφάλειας των πληροφοριών. Ένα σύνολο από μέτρα, υποδομές και διαδικασίες ενός οργανισμού ή μίας επιχείρησης που έχει βασικό στόχο την προστασία των πληροφοριών και των δεδομένων που έχει στην κατοχή του ο οργανισμός και συλλέγονται μέσα στα πλαίσια των υπηρεσιών που αυτός παρέχει. Το σύστημα θα πρέπει να ελαχιστοποιήσει τις πιθανότητες αυτά τα δεδομένα να:

- απωλεσθούν,
- διαρρεύσουν σε τρίτους,
- αλλοιωθούν.

3.1 Τεχνική περιγραφή του συστήματος για τον Οργανισμό

Η διαδικασία πιστοποίησης μιας επιχείρησης ή ενός οργανισμού με το πρότυπο ISO/ IEC 27000 αποτελείται από μία σειρά από βήματα. Αυτά έχουν να

κάνουν τόσο με την καταγραφή της υφιστάμενης κατάστασης στην επιχείρηση ή τον οργανισμό όσο και με την ολοκλήρωση αυτών που προβλέπει το πρότυπο. Αρχικά θα πρέπει να αναφέρουμε ότι στο ISO/ IEC 27000 περιέχει δέκα θεματικές ενότητες, αυτές αφορούν τις βασικές περιοχές διαχείρισης των ψηφιακών πληροφοριών. Αυτές οι θεματικές ενότητες είναι:

- Η πολιτική ασφαλείας των πληροφοριών. Αφορά την κατανόηση τόσο των επιχειρησιακών όσο και των επιμέρους στόχων της επιχείρησης και έπειτα την δημιουργία της κατάλληλης πολιτικής ασφαλείας των πληροφοριών.
- Η υποδομή ασφαλείας των ψηφιακών πληροφοριών. Αφορά την διαμόρφωση ενός πλαισίου εφαρμογής και ελέγχου της ασφάλειας των πληροφοριών μέσα στον οργανισμό.
- Η κατάταξη και ο έλεγχος πόρων. Αφορά την λεπτομερή καταγραφή των ανθρώπινων και κεφαλαιακών πόρων του οργανισμού ή της επιχείρησης και τον προσδιορισμό του επιπέδου ασφαλείας που απαιτείται από τον οργανισμό με βάση αυτούς τους πόρους.
- Η ασφάλεια του προσωπικού. Αφορά την μείωση των πιθανοτήτων να προκύψει ανθρώπινο σφάλμα ή απάτη ή κακή χρήση των πληροφοριών του οργανισμού. Σε αυτήν την θεματική ενότητα εντάσσεται και η διασφάλιση ότι το εργατικό προσωπικό του οργανισμού.
- Η ασφάλεια του περιβάλλοντος. Αφορά την όποια αποτροπή της αναρμόδιας πρόσβασης, της όποιας ζημιάς ή παρέμβασης στις κτιριακές και επιχειρησιακές εγκαταστάσεις και πληροφορίες του οργανισμού.
- Η διαχείριση των υπολογιστών και των δικτύων. Αυτήν η ενότητα αφορά την εξασφάλιση της εύρυθμης και ασφαλούς λειτουργίας των υπολογιστικών συστημάτων του οργανισμού, την επεξεργασία των πληροφοριών και την ελαχιστοποίηση του κινδύνου να τεθούν αυτά τα συστήματα εκτός λειτουργίας. Επίσης, αφορά την προστασία των λογισμικών και των πληροφοριών στα δίκτυα.
- Ο έλεγχος πρόσβασης. Αφορά τον έλεγχο του ποιος έχει πρόσβαση στις πληροφορίες του οργανισμού, στην εξασφάλιση της προστασίας των δικτύων και την αποτροπή μη εγκεκριμένης πρόσβασης σε υπολογιστές αλλά και την ανίχνευση των όποιων παραβάσεων.

- Η ανάπτυξη και η συντήρηση του συστήματος. Αφορά την εξασφάλιση ότι υπάρχει η απαραίτητη ασφάλεια στα λειτουργικά και πληροφοριακά συστήματα ώστε να αποτραπεί η απώλεια, η τροποποίηση ή η κακή χρήση των πληροφοριών των χρηστών. Η θεματική αυτή εξασφαλίζει ότι τα προγράμματα και οι απαραίτητες δραστηριότητες υποστήριξης διευθύνονται με ασφαλή τρόπο.
- Ο σχεδιασμός της εταιρικής συνέχειας. Αφορά την διαμόρφωση του τρόπου αντιμετώπισης των διακοπών των επιχειρησιακών.
- Η συμμόρφωση. Αφορά την αποφυγή παραβιάσεων ή απόπειρας παραβίασης εγκληματικού ή αστικού δικαίου.

3.2 Προϋποθέσεις φορέα υλοποίησης

Στον διαγωνισμό που προκηρύχθηκε από τον ΟΠΕΚΕΠΕ, για επιλογή συμβούλου, ο φορέας που θα επιλέγονταν να υλοποιήσει το έργο θα έπρεπε να καλύπτει κάποιες σημαντικές προϋποθέσεις. Κάποιες από αυτές τις προϋποθέσεις ήταν τυπικές όπως πχ να δραστηριοποιείται στην ελληνική επικράτεια ή να διαθέτει επιχειρηματική δομή, κάποιες άλλες όμως είχαν πιο ουσιαστικό χαρακτήρα ως προς την σωστή και πιστοποιημένη υλοποίηση του έργου. Αυτές ήταν:

- Ο φορέας υλοποίησης θα πρέπει να διαθέτει πιστοποίηση ISO 9000:2008, στο πεδίο εφαρμογής της παροχής συμβουλευτικών υπηρεσιών αλλά και στις υπηρεσίες εκπαίδευσης.
- Ο φορέας υλοποίησης θα πρέπει να είναι πιστοποιημένος με ISO 27001:2013 στον τομέα της παροχής συμβουλευτικών υπηρεσιών και υπηρεσιών εκπαίδευσης.
- Ο φορέας υλοποίησης θα πρέπει να διαθέτει εμπειρία στην υλοποίηση προτύπων 27000. Η εμπειρία θα αποδεικνύονταν από το γεγονός ότι θα είχε ήδη υλοποιήσει τουλάχιστον 8 έργα ανάπτυξης συστημάτων Διαχείρισης Ασφαλείας Πληροφοριών ISO 27000. Τα συγκεκριμένα έργα θα έπρεπε να

έχουν πιστοποιηθεί από επίσημο φορέα και επιπλέον θα έπρεπε να υποβάλλεται και βεβαίωση καλής εκτέλεσης του έργου από τον πιστοποιημένο οργανισμό ή επιχείρηση.

- Ο φορέας υλοποίησης θα πρέπει να διαθέτει τόσο ανθρώπινους όσο και κεφαλαιακούς ή υλικούς πόρους ικανούς για να φέρουν σε πέρας τις απαιτήσεις για την υλοποίηση του έργου. Συγκεκριμένα θα έπρεπε να διαθέτει άτομα με πανεπιστημιακή εκπαίδευση αλλά επίσης να διαθέτουν και μία από τις επαγγελματικές πιστοποιήσεις στον τομέα της ασφάλειας πληροφοριών CISA, CISM, CISSP, ISO 27001 Lead Auditor, Offensive Security Certified Professional (OSCP).

3.3 Σκοπός της υλοποίησης του έργου

Σκοπός του έργου είναι η διαχείριση της ασφάλειας των πληροφοριών του οργανισμού. Το ISO/ IEC 27001:2013 είναι ένα πρότυπο που έχει εφαρμογή σε πάρα πολλούς τομείς της οικονομίας όπως η βιομηχανία, το εμπόριο και η παροχή υπηρεσιών τόσο του ιδιωτικού όσο και του δημόσιου τομέα. Επιπλέον η εφαρμογή του δεν περιορίζεται στις πληροφορίες που αποθηκεύονται σε υπολογιστές αλλά αφορά την ασφάλεια όλων των πληροφοριών με όποιον τρόπο και αν αυτές αποθηκεύονται, φυσικά σε χαρτί, αποθηκευμένες σε βάσεις δεδομένων, ή έχουν αποσταλεί ηλεκτρονικά μέσω ηλεκτρονικού ταχυδρομείου.

Η ΓΓΠΣ, έχοντας αναγνωρίσει ότι υπάρχει σημαντική ανάγκη για την διασφάλιση όλων των πληροφοριών που έχει ο οργανισμός (Υπ. Οικονομικών) στην κατοχή του αλλά και ότι πρέπει να συμμορφωθεί με το νέο νομικό και κανονιστικό πλαίσιο που διαμορφώνεται από τους νέους κανονισμούς της Ευρωπαϊκής Ένωσης προχώρησε σε αυτόν τον διαγωνισμό για να αναβαθμίσει το σύστημα Ασφαλείας Πληροφοριών που εφάρμοζε από το 2005.

3.4 Το πλήρες αντικείμενο του έργου

Η όλη διαδικασία του έργου αφορά την υλοποίηση ενός συστήματος ασφαλείας των πληροφοριών του οργανισμού με το πρότυπο ISO/IEC 27001:2013. Στην πραγματικότητα το αντικείμενο του έργου αποτελείται από πιο εξειδικευμένα αντικείμενα που οδηγούν στην πλήρη υλοποίηση του έργου. Έτσι ο φορέας υλοποίησης του συγκεκριμένου έργου θα πρέπει:

- Να παρέχει εξειδικευμένες υπηρεσίες συμβουλευτικής που να αφορούν τον σχεδιασμό, την εγκατάσταση και την λειτουργία του Συστήματος Διαχείρισης της Ασφάλειας των Πληροφοριών κατά ISO/IEC 27001:2013. Το πεδίο εφαρμογής θα είναι όλες οι δραστηριότητες και οι διευθύνσεις και οι πληροφορίες της ΓΓΠΣ.
- Να παρέχει μία μελέτη ανάλυσης αλλά και αποτίμησης και διαχείρισης της επικινδυνότητας ώστε να εντοπιστούν οι όποιες αδυναμίες και τα όποια ευάλωτα σημεία στις υποδομές, τις διευθύνσεις και τις διαδικασίες του οργανισμού. Η μελέτη αυτή θα πρέπει να είναι βασισμένη σε μία πρότυπη αναγνωρισμένη μέθοδο και να συνοδεύεται από κάποιο αυτοματοποιημένο εργαλείο που να κάνει πιο εύκολη την εφαρμογή της. Τέλος θα πρέπει να μπορεί να επιλέγει αντίμετρα από μία αρκετά μεγάλη βιβλιοθήκη αντίμετρων.
- Να αναπροσαρμόσει το Σχέδιο Επιχειρησιακής Συνέχειας του οργανισμού, πάντα βάση της παραπάνω μελέτης ανάλυσης αποτίμησης και διαχείρισης της επικινδυνότητας.
- Να παρέχει τεχνική και διοικητική εκπαίδευση στο εργατικό δυναμικό του οργανισμού. Τουλάχιστον στο αρμόδιο στελεχιακό δυναμικό που σχετίζεται με την ασφάλεια των πληροφοριών. Η εκπαίδευση θα πρέπει να περιλαμβάνει και την κατάρτιση στις νέες διαδικασίες και πρακτικές προκειμένου να διαχειριστούν το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών και μετά τη λήξη του έργου.

Συμπεράσματα

Η πιστοποίηση της ποιότητας είτε αφορά την διαδικασία παραγωγής είτε αφορά το προϊόν, την παροχή υπηρεσίας ή την λειτουργία ενός συγκεκριμένου τμήματος μιας επιχείρησης ή ενός οργανισμού αποτελεί μία πρακτική που προσφέρει σημαντικά οφέλη στον οργανισμό. Τα οφέλη έχουν να κάνουν με την αναβάθμιση του προϊόντος και κατά συνέπεια της ίδιας της επιχείρησης ή του οργανισμού. Αυτά τα οφέλη μπορεί να είναι είτε βραχυπρόθεσμα είτε μεσοπρόθεσμα είτε μακροπρόθεσμα.

Αντίστοιχα και ο δημόσιος τομέας μέσω των πιστοποιήσεων των παροχών υπηρεσιών που προσφέρει αποκτά σημαντικά οφέλη. Οφέλη που έχουν να κάνουν με την αξιοπιστία, την αντικειμενικά καλύτερη ποιότητα των υπηρεσιών, την μείωση του κόστους αλλά και την απλοποίηση των διαδικασιών λειτουργίας ενός οργανισμού ή μίας υπηρεσίας. Αυτό έχει οδηγήσει πολλούς φορείς της δημόσιας διοίκησης να προβούν σε διαδικασίες πιστοποίησης με διάφορα πρότυπα του Διεθνούς Οργανισμού Πιστοποίησης (ISO).

Η ασφάλεια των πληροφοριών που διακινούνται στην σημερινή κοινωνία αποτελεί ένα σημαντικό πρόβλημα για κάθε οργανισμό. Ολόκληρη η οικογένεια προτύπων ISO 2700X έχει πεδίο δράσης την ασφάλεια των πληροφοριών. Η ανάπτυξη ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ), επίσης προσφέρει σημαντικά οφέλη σε έναν οργανισμό και η πιστοποίηση αυτού από ένα διεθνή φορέα αποτελεί σημαντική παρακαταθήκη για την εύρυθμή λειτουργία των διευθύνσεων του οργανισμού και την ομαλή συνέχεια του.

Η αλλαγή του Ευρωπαϊκού κανονισμού για την προστασία των προσωπικών δεδομένων αποτέλεσε αφορμή για πολλούς δημόσιους φορείς, όπως και για τη ΓΓΠΣ, να εκσυγχρονίσει τα συστήματα ασφαλείας των πληροφοριών του και να τα εναρμονίσει με τις νέες κοινοτικές οδηγίες.

Βιβλιογραφία

Ελληνική βιβλιογραφία

Γκίκα Γ, Συστήματα διαχείρισης ποιότητας –γενικές αρχές, σημειώσεις σεμιναρίου, ΤΕΕ, 2011 αναρτημένο στο: https://www.arcmeletitiki.gr/images/uploads/pdf/arc_sdp7.pdf

Δερβιτσιώτης Κ, Ανταγωνιστικότητα με Διοίκηση Ολικής Ποιότητας, εκδόσεις INTERBOOKS, Αθήνα, 2001

ΕΛΟΤ, Γενικός κανονισμός αξιολόγησης και πιστοποίησης συστημάτων διαχείρισης ποιότητας, Αθήνα, 2011 αναρτημένο στο: http://www.elot.gr/gracqs.pdf

Μαθιουδάκης Γ, «Πρότυπα Συστημάτων Διαχείρισης : Οφέλη από την εφαρμογή τους, Τεχνικό Επιμελητήριο Ελλάδος, 2008

Ρωσίδης Ι, Μπιτσάνη Ε, Η Διοίκηση Ολικής Ποιότητας στο Δημόσιο Τομέα. Η περίπτωση της Ελλάδος, **Conference Paper,** Conference: 2ο Πανελλήνιο Συνέδριο Εφαρμοσμένων Οικονομικών, Βόλος 2011

Στειακάκης Ε, Κωφίδης Ν, Διοίκηση και έλεγχος ποιότητας, εκδόσεις Τζιόλα, Θεσσαλονίκη, 2017.

Ξένη βιβλιογραφία

Arnason S, Willett K, How to achieve 27001 certification: an example of applied compliance management, auerbach publications, New York, 2007

Beale, V., Pollitt. C. „Charters at the grass-roots: A first report", Local Government Studies, 20 (2), 1994

Boehmer W, Cost-benefit trade off analysis of an ISMS based on ISO 27001. Availability, reliability and security, ARES apos 09, 2009

Bovaird, T., Löffler, E., Parrado-Díez, S. (eds.): Developing Local Governance Networks in Europe, Baden-Baden: Nomos, 2002

Calder A, Watkins S, International IT governance: an executive guide to ISO 17799/ISO 27001, Kogan Publishers, London, 2006

Cambridge University Press - Quality and Reliability in Engineering, Tirupathi R. Chandrupatla, 2012

DISC Board, Standard Policy and Strategy committee, British Standard information security management systems, London, 2002

Engel, C., „Common Assessment Framework – the State of Affairs", *EIPASCOPE*, nr. Maastricht, 2003

Gossels J, Mackey R, ISO 2700X: A cornerstone of true security, article at ISSA Journal, April 2007

Hoyle, D. Quality Management Essentials. UK, Oxford: Butterworth – Heinemann, 2007

InfoCloud, An Overview of ISO/IEC 27000 family of Information Security Management System Standards, Published by the Office of the Government Chief Information Officer, Hong Kong, 2017

Kovac S, Introducing a system for information security management by ISO/IEC 27001, Masaryk university, Brno, 2014

Kumar D, V. Balakrishnan, A Study on ISO 9001 Quality Management System Certifications – Reasons behind the Failure of ISO Certified Organizations, Global Journal of Management and Business Research Volume 11 Issue 9 Version 1.0 September 2011

Lecklin, O. Quality as a Success Factor of a Company (in Finnish), Kauppakaari, Helsinki, 2006

Löffler, E., „Quality Awards as a Public Sector Benchmarking Concept for OCDE Member Countries. Some Guidelines for Quality Award Organizers", Public Administration Development, 2001

Matei A., Andreescu, S., „Managementul calităţii totale în sectorul public. Experienţe europene", Proceedings, Editor Matei, L., International Conference Public administration at the beginning of the third millennium. Disseminating the best Japanese practices in Romania, Bucharest, Romania, 2005

Matei L, Lazar C, Quality Management and the Reform of Public Administration in Several States in South-Eastern Europe. Comparative Analysis, article at Theoretical and Applied Economics Volume XVIII, (2011)

Shojaie B, Dissertation with the aim of achieving a doctoral degree at the Faculty of Mathematics, Informatics and Natural Sciences Department of Informatics of Universitat Hamburg, Hamburg, 2018

Zink, K.J. (1998) Total Quality Management as a Holistic Management Concept. Springer

Ηλεκτρονική βιβλιογραφία

http://www.plan.gr/diaxeirisi-poiotitas-iso-haccp

https://www.iso.org/home.html

https://www.iso.org/standards.html

https://www.iso.org/about-us.html

http://www.greece.lrqa.com/standards-and-schemes/iso-iec27001/

http://www.opekepe.gr/one.asp?id=1448286421&year=2015&cat=P

www.gspa.gr

www.mnec.gr/en/economics/National_Strategic_Reference_Framework_for_07-13/

www.mnec.gr/en/economics/growth_programme_2005-8/

www.mnec.gr/en/economics/reform_programme_2005-2008/

www.mnec.gr/export/sites/mnec/en/economics/National_Strategic_Reference_Framework_for_2007-13/ESPA_eng.pdf

www.ypes.gr/en

Διαδικτυακός Τόπος της ΓΓΠΣ: http://www.gsis.gr/

Παραρτήματα

Εθνική Σχολή Δημόσιας Διοίκησης και Αυτοδιοίκησης (ΕΣΔΔΑ)
Πειραιώς 211, ΤΚ 177 78, Ταύρος
τηλ: 2131306349 , fax: 2131306479
www.ekdd.gr