ΔΙΑΤΜΗΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΣΤΑ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

Διπλωματική Εργασία

ΕΛΕΓΧΟΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ – ΣΥΓΧΡΟΝΑ ΘΕΜΑΤΑ ΚΑΙ ΤΑΣΕΙΣ ΣΤΗΝ ΕΛΛΑΔΑ

του

ΧΑΡΑΛΑΜΠΟΥ ΣΑΛΤΣΙΔΗ ΤΟΥ ΣΩΚΡΑΤΗ

Υποβλήθηκε ως απαιτούμενο για την απόκτηση του Μεταπτυχιακού
Διπλώματος Ειδίκευσης στα Πληροφοριακά Συστήματα

Θεσσαλονίκη, Ιανουάριος 2018

Περίληψη

Τα πληροφοριακά συστήματα αποτελούν ζωτικά στοιχεία κάθε επιχείρησης, καθώς μέσω αυτών συντελούνται, συντονίζονται σημαντικές λειτουργίες και υποστηρίζονται αποφάσεις. Παρ' όλα αυτά, ως συστήματα τεχνολογίας, παρουσιάζουν ευπάθειες και καθίστανται ευάλωτα σε κινδύνους, γι' αυτό είναι απαραίτητος ο έλεγχος τους. Μεγάλες πολυεθνικές εταιρείες με εμπειρία στον έλεγχο αναλαμβάνουν να επιλύσουν θέματα που αφορούν τους κινδύνους αυτού του είδους. Ο έλεγχος των πληροφοριακών συστημάτων βασίζεται σε Διεθνή Πρότυπα και σε φορείς που παρέχουν ανάλογη εκπαίδευση και πιστοποιήσεις. Τέλος, το μάθημα του ελέγχου πληροφοριακού συστημάτων οφείλει να ενσωματώνεται σε αντίστοιχα προγράμματα σπουδών, ώστε οι εν δυνάμει ελεγκτές να παίρνουν την κατάλληλη εκπαίδευση εντός των πανεπιστημιακών ιδρυμάτων και να είναι άρτια καταρτισμένοι.

Abstract

Information systems are vital elements of any business, and through them important functions are coordinated and decisions are supported. Nevertheless, as technology systems, they have vulnerabilities and become vulnerable to risks, so there is need for internal control. Large multinational companies with experience in controlling, undertake to resolve issues related to information systems risks. The control of information systems is based on international standards and on entities providing training and allied certifications. Finally, the course of information systems audit must be integrated in university programs, in order to get the potential auditors, the proper training.

Περιεχόμενα

ΕΙΣΑΓΩΓΗ

Στο σύγχρονο οικονομικό, τεχνολογικό και επιχειρησιακό περιβάλλον οι πληροφορίες αποτελούν πολύτιμα δεδομένα, με βάση τα οποία λαμβάνονται αποφάσεις, χαράσσονται στρατηγικές και αξιολογούνται καταστάσεις. Κάθε οικονομική μονάδα οφείλει να γνωρίζει και να διαχειρίζεται με τέτοιο τρόπο τις πληροφορίες που την αφορούν, ώστε να προλαμβάνει απειλές και κινδύνους και να λαμβάνει τις απαραίτητες αποφάσεις για την ευημερία και την ομαλή λειτουργία της.

Τα πληροφοριακά συστήματα είναι συστήματα τα οποία διαχειρίζονται τις πληροφορίες αυτές και εγγυώνται την ασφάλεια και την αξιοπιστία των δεδομένων, των συναλλαγών και των διαδικασιών που λαμβάνουν χώρα σε μια επιχείρηση ή οργανισμό. Παρ' όλα αυτά, ο έλεγχος των συστημάτων αυτών κρίνεται αναγκαίος, ώστε να επιτευχθούν οι διαδικασίες που προαναφέρθηκαν.

Στόχος της παρούσας διπλωματικής εργασίας είναι η ανάδειξη της σημασίας του ελέγχου των πληροφοριακών συστημάτων, των συνήθων κινδύνων, απειλών και προκλήσεων, καθώς και η υπογράμμιση της σημαντικότητας της σωστής κατάρτισης των ελεγκτών, μέσα από αναγνωρισμένες πιστοποιήσεις και ειδικά μαθήματα σε προγράμματα σπουδών πανεπιστημιακών ιδρυμάτων.

Στο πρώτο κεφάλαιο, αναλύεται ο έλεγχος των πληροφοριακών συστημάτων και τα είδη αυτού, τα στάδια ελέγχου, τα εργαλεία και τα αντικείμενα ελέγχου και τέλος, αναλύονται οι κίνδυνοι και τα διάφορα μέτρα προστασίας.

Στο δεύτερο κεφάλαιο, παρουσιάζονται οι 4 μεγάλες πολυεθνικές ελεγκτικές εταιρείες, οι παρεχόμενες υπηρεσίες τους και οι μελέτες περίπτωσης εφαρμογών ελέγχου.

Στο τρίτο κεφάλαιο, παρουσιάζονται οι φορείς ελέγχου πληροφοριακών συστημάτων και οι αντίστοιχες πιστοποιήσεις (CISA κλπ), ενώ στο τέταρτο κεφάλαιο αναλύεται η δομή ενός μαθήματος που αφορά τον έλεγχο πληροφοριακών συστημάτων.

Στο πέμπτο κεφάλαιο, η διπλωματική εργασία καταλήγει με τα συμπεράσματα, ενώ ακολουθεί η βιβλιογραφία.

ΚΕΦΑΛΑΙΟ 1 ΈΛΕΓΧΟΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ – IT AUDITING

Κάθε πληροφοριακό σύστημα, λόγω του καίριου ρόλου του στην επιχείρηση ή στον οργανισμό που το χρησιμοποιεί, οφείλει να πληροί όλες τις συνθήκες που αφορούν τη διασφάλιση των δεδομένων που διαχειρίζεται. Επίσης, τα συστήματα αυτά θα πρέπει να περνάνε από διάφορους τύπους ελέγχου, ώστε να διασφαλίζεται η ομαλή λειτουργία τους. Στο παρόν κεφάλαιο, περιγράφεται και αναλύεται η έννοια του ελέγχου των πληροφοριακών συστημάτων (IT auditing), τα υπάρχοντα είδη ελέγχου, τα εργαλεία και τα αντικείμενα ελέγχου, τα Διεθνή Πρότυπα και τέλος μέτρα προστασίας των συστημάτων.

1.1 ΟΡΙΣΜΟΣ ΕΛΕΓΧΟΥ

Ο έλεγχος πληροφοριακής τεχνολογίας (information technology audit- IT audit) ή ο έλεγχος πληροφοριακών συστημάτων (information systems audit- IT audit) είναι η εξέταση και η αξιολόγηση των ελέγχων που σχετίζονται με την πληροφοριακή τεχνολογία. Πιο συγκεκριμένα, μπορούμε να πούμε ότι είναι η διαδικασία κατά την οποία συλλέγονται και αξιολογούνται στοιχεία του συστήματος, με σκοπό να διαπιστωθεί εάν και σε ποιο βαθμό τα πληροφοριακά συστήματα των επιχειρήσεων βοηθούν στην διαφύλαξη των στοιχείων του ενεργητικού, στην διασφάλιση της ακεραιότητας των δεδομένων, στην αποτελεσματική λειτουργία προκειμένου να επιτευχθούν οι στόχοι της επιχείρησης και στην αποδοτικότερη χρήση των πόρων της επιχείρησης (Pathak, 2005).

Στην ουσία ο έλεγχος των πληροφοριακών συστημάτων μέσα σε μια επιχείρηση περιλαμβάνει την εισροή των δεδομένων, την επεξεργασία τους και την εκροή τους σε μορφή πληροφοριών. Οι έλεγχοι χρησιμοποιούνται κυρίως για τους λόγους που προαναφέρθηκαν αλλά και για να αξιολογηθεί η ικανότητα της επιχείρησης να διανείμει κατάλληλα τις πληροφορίες στους αρμόδιους τομείς της.

Έτσι, ο έλεγχος περιλαμβάνει τη διαφύλαξη των στοιχείων του ενεργητικού (δηλαδή του υλικό-hardware, λογισμικό- software, αρχεία δεδομένων-files, συμπληρωματικό εξοπλισμό) είναι η προστασία τους από βλάβες, καταστροφές, παράνομη χρήση και κλοπή. Επίσης, περιλαμβάνει τη διασφάλιση της ακεραιότητας των δεδομένων, που είναι πάρα πολύ

σημαντική για τη σωστή λειτουργία της επιχείρησης. Τα δεδομένα μίας επιχείρησης θα πρέπει να διαθέτουν κάποιες ιδιότητες όπως είναι η πληρότητα, η ακρίβεια, η σαφήνεια και η καθαρότητα. Η διατήρηση δεδομένων από μια εταιρία επιφέρει κάποιο κόστος, έτσι η ωφέλεια που προκύπτει από την διασφάλιση της ακεραιότητας των δεδομένων πρέπει να υπερβαίνει το κόστος διατήρησης τους σε συνδυασμό με το κόστος των ελέγχων που χρειάζονται γι' αυτήν. Επιπλέον, ο έλεγχος περιλαμβάνει την αποτελεσματική λειτουργία των πληροφοριακών συστημάτων. Ένα πληροφοριακό σύστημα για να είναι αποτελεσματικό θα πρέπει να μπορεί να πετυχαίνει τους στόχους του. Τις περισσότερες φορές οι έλεγχοι για την αποτελεσματικότητα του συστήματος πραγματοποιούνται σε δύο φάσεις, αρχικά κατά τη διάρκεια του σχεδιασμού και βασίζονται στις απαιτήσεις των χρηστών αλλά και σε δεύτερο φάση κατά την πρώτη περίοδο της λειτουργίας του. Τέλος, περιλαμβάνει την αποδοτική χρήση των πόρων, δηλαδή την αξιοποίηση όσων των δυνατόν λιγότερων εισροών προκειμένου να πετύχει τους στόχους του. Οι εισροές που μπορεί να έχει ένα πληροφοριακό σύστημα είναι τα περιφερειακά συστήματα, το λογισμικό, τα κανάλια μεταφοράς και η ανθρώπινη εργασία και όλα αυτά μεταφράζονται σε χρήμα (Δημητριάδης, 1998).

Τα πληροφοριακά συστήματα κατά τη λειτουργία τους πρέπει να έχουν την δυνατότητα να ελέγχουν την αποτελεσματικότητα και την αποδοτικότητα του τεχνολογικού υλικού και του λογισμικού της επιχείρησης καθώς και να βελτιστοποιούν τη χρήση τους. Επίσης, πρέπει να κάνουν σωστή χρήση της τεχνολογικής υποδομής, των διαθέσιμων πόρων, αλλά και να εξακριβώνουν την ορθότητα, την πληρότητα και την αξιοπιστία των πληροφοριών. Επιπρόσθετα, πρέπει να αξιολογούν τον βαθμό στον οποίο λαμβάνονται υπόψη και διαφυλάσσονται οι εταιρικοί πόροι πληροφοριακών συστημάτων, να εκτιμούν τον βαθμό συμμόρφωσής τους με τις πολιτικές, τα σχέδια και τις διαδικασίες του οργανισμού, να συντάσσουν και να εξετάζουν την αρτιότητα και την επάρκεια των διαφόρων επιχειρησιακών ελέγχων, να αποφεύγουν διάφορες οικονομικές και διαχειριστικές απάτες προκειμένου να προστατεύουν την επιχείρηση από διάφορους εσωτερικούς και εξωτερικούς κινδύνους. Τέλος, πρέπει να προστατεύουν τις ατομικές ελευθερίες σύμφωνα με το νομοθετικό πλαίσιο της αρχής προστασίας δεδομένων (Κυριαζόγλου, 2001).

1.2 ΕΙΔΗ ΕΛΕΓΧΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Οι πιο σημαντικές κατηγορίες των ελέγχων είναι, οι γενικοί έλεγχοι ή αλλιώς οι έλεγχοι υποδομής και οι έλεγχοι εφαρμογών (Laudon, 2007). Οι γενικοί έλεγχοι σχετίζονται με το σχεδιασμό, την ασφάλεια και τη χρήση των προγραμμάτων αλλά και γενικά με την ασφάλεια των δεδομένων και των πληροφοριών όλης της επιχείρησης. Το πεδίο εφαρμογής των γενικών ελέγχων είναι όλες οι μηχανολογικές εφαρμογές, οι οποίες αποτελούνται από υλικό και λογισμικό συστήματος και από χειροκίνητες διαδικασίες στο περιβάλλον ελέγχου. Οι γενικοί έλεγχοι περιλαμβάνουν ελέγχους στον υλικό εξοπλισμό, στο λογισμικό του συστήματος, στην ασφάλεια των δεδομένων, στη λειτουργία των ηλεκτρονικών υπολογιστών, στους διαχειριστικούς ελέγχους και στους ελέγχους υλοποίησης.

Οι έλεγχοι λογισμικού παρακολουθούν τη χρήση του λογισμικού συστήματος και δίνουν πρόσβαση στα προγράμματα που χρειάζεται ή απαγορεύουν την πρόσβαση στα προγράμματα που δεν έχουν εξουσιοδότηση. Οι έλεγχοι υλικού γίνονται προκειμένου να διασφαλίσουν την ασφάλεια του υλικού των υπολογιστών και να εντοπίσουν οποιαδήποτε πρόβλημα μπορεί να υπάρχει στον εξοπλισμό. Οι υπολογιστές και ο εξοπλισμός τους, θα πρέπει να προστατεύονται από τυχόν πυρκαγιές ή ακραίες θερμοκρασίες που μπορεί να προκύψουν μέσα στην επιχείρηση. Οι έλεγχοι ασφάλειας δεδομένων διασφαλίζουν ότι όλες οι πληροφορίες και τα δεδομένα που υπάρχουν μέσα στην επιχείρηση είτε βρίσκονται στους υπολογιστές της είτε σε δίσκους, είτε οπουδήποτε αλλού δεν υπόκεινται σε μη εξουσιοδοτημένη πρόσβαση ή σε καταστροφές όταν χρησιμοποιούνται ή όταν είναι αποθηκευμένα. Οι διαχειριστικοί έλεγχοι εξασφαλίζουν ότι οι γενικοί έλεγχοι και οι έλεγχοι εφαρμογών μέσα στην επιχείρηση πραγματοποιούνται με τον σωστό τρόπο. Και οι έλεγχοι υλοποίησης εξασφαλίζουν τον σωστό έλεγχο και τη σωστή διαχείριση κατά τη διαδικασία ανάπτυξης των συστημάτων στα διάφορα στάδια.

Οι έλεγχοι εφαρμογών είναι οι έλεγχοι που πραγματοποιούνται σε κάθε εφαρμογή του υπολογιστή. Οι έλεγχοι εφαρμογών δεν χρησιμοποιούνται με τον ίδιο τρόπο σε όλα τα πληροφοριακά συστήματα αλλά εξαρτώνται από τη φύση και τη σπουδαιότητα της κάθε εφαρμογής. Οι έλεγχοι αυτοί χωρίζονται σε ελέγχους εισόδου, σε ελέγχους επεξεργασίας και σε ελέγχους εξόδου, και έχουν σαν στόχο την εγκυρότητα και την πληρότητα των πληροφοριών. Οι έλεγχοι εισόδου ελέγχουν την ακρίβεια και την πληρότητα των

πληροφοριών όταν αυτές εισέρχονται στο σύστημα. Οι έλεγχοι επεξεργασίας ελέγχουν την ακρίβεια και στην πληρότητα των δεδομένων όταν πραγματοποιείται η ενημέρωση αυτών. Και οι έλεγχοι εξόδου εξασφαλίζουν την ακρίβεια και την πληρότητα των τελικών αποτελεσμάτων.

Εκτός από τα δύο είδη ελέγχου που έχουμε αναλύσει παραπάνω, υπάρχουν και ο έλεγχος της συνέχειας και ο έλεγχος αποκατάστασης ζημιών. Ο έλεγχος της συνέχειας εξασφαλίζει την ύπαρξη αντιγράφων- backup των δεδομένων αλλά και του υλικού της επιχείρησης. Και ο έλεγχος της αποκατάστασης ζημιών εξασφαλίζει την αποκατάσταση του πληροφοριακού συστήματος μετά από μερική ή ολική διακοπή της λειτουργίας του (Hunton et al, 2005).

Μία άλλη κατηγοριοποίηση των ελέγχων είναι οι προληπτικοί, οι διαγνωστικοί-διερευνητικοί και οι επανορθωτικοί έλεγχοι. Οι προληπτικοί έλεγχοι έχουν σκοπό την πρόληψη της εμφάνισης ενός λάθους, μιας παράλειψης ή μιας κακόβουλης ενέργειας. Οι διαγνωστικοί – διερευνητικοί έλεγχοι έχουν στόχο τον εντοπισμό και την αναφορά των προβλημάτων όταν αυτά έχουν εμφανιστεί. Και οι επανορθωτικοί έλεγχοι έχουν στόχο την ελαχιστοποίηση των επιδράσεων μιας απειλής, τη διόρθωση των προβλημάτων που έχουν προκύψει και την μεταβολή των πληροφοριακών συστημάτων έτσι ώστε να ελαχιστοποιηθεί ο κίνδυνος εμφάνισης παρόμοιων προβλημάτων στο μέλλον (Κάτσικας και συν, 2004).

1.3 ΣΤΑΔΙΑ ΕΛΕΓΧΟΥ

Ο έλεγχος ενός πληροφοριακού συστήματος περιλαμβάνει τρία στάδια, το στάδιο του σχεδιασμού, το στάδιο της διεξαγωγής και το στάδιο της υποβολής εκθέσεων ελέγχου. Όλα τα στάδια αυτά είναι απαραίτητα για να εφαρμοστεί σωστά οποιοσδήποτε έλεγχος. Ακόμα και ο πιο μικρός έλεγχος κινδυνεύει να αποτύχει αν δεν εφαρμοστούν αυτά τα τρία στάδια.

Το πρώτο στάδιο περιλαμβάνει τον σχεδιασμό του ελέγχου (Audit Planning). Ο σχεδιασμός του ελέγχου πραγματοποιείται σε συμφωνία του IT Auditor με τη διοίκηση της επιχείρησης. Ο σχεδιασμός του ελέγχου έχει σκοπό να βοηθήσει τον ελεγκτή να μειώσει τους κινδύνους και να τους φέρει σε ένα αποδεκτά χαμηλό επίπεδο (Moroney, 2012). Στο στάδιο

αυτό γίνεται ο προσδιορισμός του πεδίου εφαρμογής, η σχεδίαση ελέγχου του συστήματος σύμφωνα με τους στόχους του ελέγχου και σύμφωνα με την ισχύουσα νομοθεσία, η αναφορά των προβλεπόμενων κινδύνων, η λεπτομερής αναφορά του είδους, των στόχων, της έκτασης, του χρονοδιαγράμματος του ελέγχου και των πόρων που απαιτούνται και η συμπλήρωση του προγράμματος ελέγχου.

Προκειμένου να πραγματοποιηθούν όλα τα παραπάνω πρέπει να γίνει σαφής καθορισμός των στόχων ελέγχου με βάση τους στόχους της επιχείρησης, τους διαθέσιμους πόρους της, των αρχείων και των εγγράφων της, πρέπει να συγκεντρωθεί όλο το απαραίτητο υλικό, τα έγγραφα, τα αντίγραφα, οι εκθέσεις προηγούμενων ελέγχων και οτιδήποτε άλλο αρχείο είναι σημαντικό για την επιχείρηση. Επίσης, πρέπει να πραγματοποιηθεί μία συζήτηση με τη διοίκηση της επιχείρησης για να προκύψει μία τελική συμφωνία και να αναλυθούν τα ρίσκα που απαιτούνται για την λειτουργία και την αξιοποίηση των συγκεκριμένων συστημάτων πληροφορικής.

Το δεύτερο στάδιο του ελέγχου περιλαμβάνει την διεξαγωγή του ελέγχου. Το στάδιο αυτό περιλαμβάνει με λεπτομέρεια όλες τις δοκιμές ελέγχου που χρησιμοποιούνται κατά την εκτέλεση των εργασιών και των δοκιμών. Υπάρχουν τρεις τύποι δοκιμών ελέγχου, οι δοκιμές εφαρμογής κανόνων, οι δοκιμές αδυναμιών και οι δοκιμές επιβεβαίωσης. Οι δοκιμές εφαρμογής κανόνων διασφαλίζουν ότι η επιχείρηση εφαρμόζει σωστά όλες τις εταιρικές της πολιτικές και τις λειτουργίες της όπως προβλέπεται από τους κανονισμούς της. Οι δοκιμές αδυναμιών εφαρμόζονται όταν οι δοκιμές εφαρμογής κανόνων δεν μπορούν να αποδώσουν μέσα στην επιχείρηση. Τέλος, οι δοκιμές επιβεβαίωσης χρησιμοποιούνται για να επιβεβαιώσουν την ύπαρξη και την αξία συγκεκριμένων παγίων, εσόδων, εξόδων κλπ.

Ο IT Auditor εκτός από τις δοκιμές ελέγχουν που πρέπει να πραγματοποιήσει μέσα στην επιχείρηση πρέπει να επιλέξει και την μέθοδο ελέγχου που θα χρησιμοποιήσει σε κάθε περίπτωση.

Το τρίτο στάδιο ελέγχου περιλαμβάνει την υποβολή εκθέσεων ελέγχου. Ο ελεγκτής μετά το πέρας της διεξαγωγής του ελέγχου συντάσσει μία έκθεση ελέγχου στην οποία αναγράφει όλα τα αποδεικτικά στοιχεία που έχει συγκεντρώσει κατά τη διάρκεια του ελέγχου. Ο ελεγκτής στην έκθεσή του δίνει ιδιαίτερη σημασία στην ανάλυση των κινδύνων της επιχείρησης. Στο τέλος, ο ελεγκτής παραθέτει τα συμπεράσματά του για κάθε θετικό ή

αρνητικό σημείο της επιχείρησης που έχει εντοπίσει κατά τη διάρκεια του ελέγχου και ενημερώνει τα διοικητικά στελέχη της επιχείρησης γι' αυτά. Η έκθεση αυτή μπορεί να χρησιμοποιηθεί για μελλοντικές βελτιώσεις και για μελλοντικούς ελέγχους.

1.4 ΕΡΓΑΛΕΙΑ ΕΛΕΓΧΟΥ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Κατά την υλοποίηση των ελέγχων, οι ελεγκτές χρησιμοποιούν εργαλεία όπως οι περιγραφικές εκθέσεις, τα διαγράμματα ροής και τα ερωτηματολόγια.

Α) Περιγραφικές Εκθέσεις (Internal Control Narratives)

Οι περιγραφικές εκθέσεις χρησιμοποιούνται για έλεγχο συγκεκριμένων κινδύνων. Είναι δηλαδή εκθέσεις στις οποίες περιγράφεται κάθε σημαντικό στοιχείο του ελέγχου του συστήματος. Αποτελεί ένα εργαλείο που διασφαλίζει ότι θα καταγραφούν σωστά όλα τα σημαντικά στοιχεία του ελέγχου αλλά η αποτελεσματικότητα του σχετίζεται με την εμπειρία αλλά και την ικανότητα του εκλεκτή στην γραπτή επικοινωνίας και στην σύνταξη εκθέσεων.

Β) Διαγράμματα Ροής (Flowcharts)

Τα διαγράμματα ροής χρησιμοποιούνται για να παρουσιάσουν σχηματικά τα σημεία ελέγχου, όπως διαδικασίες, ροές δεδομένων και στάδια της διαδικασίας ελέγχου. Για να επιτευχθεί αυτή η σχηματική αναπαράσταση χρησιμοποιούνται σύμβολα και βέλη (Viator et al. 1992). Τα διαγράμματα αυτά δεν είναι απαραίτητο να δημιουργούνται από τους ελεγκτές με το χέρι μίας και υπάρχουν διαθέσιμα λογισμικά υπολογιστών που εξειδικεύονται στη δημιουργία τέτοιων διαγράμματα. Το μεγαλύτερο πλεονέκτημα των διαγραμμάτων ροής είναι ότι η σχηματική αναπαράσταση βοηθά πολύ στην εύκολη κατανόησή, γεγονός που διευκολύνει την όλη διαδικασία.

Γ) Ερωτηματολόγια Εσωτερικού Ελέγχου (Internal Control Questionnaires)

Τα ερωτηματολόγια χρησιμοποιούνται από τους ελεγκτές για την συλλογή πληροφοριών σχετικών με τους ελέγχους. Έτσι, ο ελεγκτής / σχεδιαστής του ερωτηματολογίου οφείλει να θέσει τα σωστά ερωτήματα σχετικά με ποικίλες εφαρμογές, διαδικασίες και κινδύνους. Οι πληροφορίες που συλλέγονται μέσω των ερωτηματολογίων αποτελούν δεδομένα που

μπορούν να χρησιμοποιηθούν στα δύο εργαλεία που προαναφέρθηκαν, τις περιγραφικές εκθέσεις και τα διαγράμματα ροής.

1.5 ΑΝΤΙΚΕΙΜΕΝΑ ΕΛΕΓΧΟΥ

1.5.1 ΚΙΝΔΥΝΟΙ ΚΑΙ ΔΙΑΧΕΙΡΙΣΗ

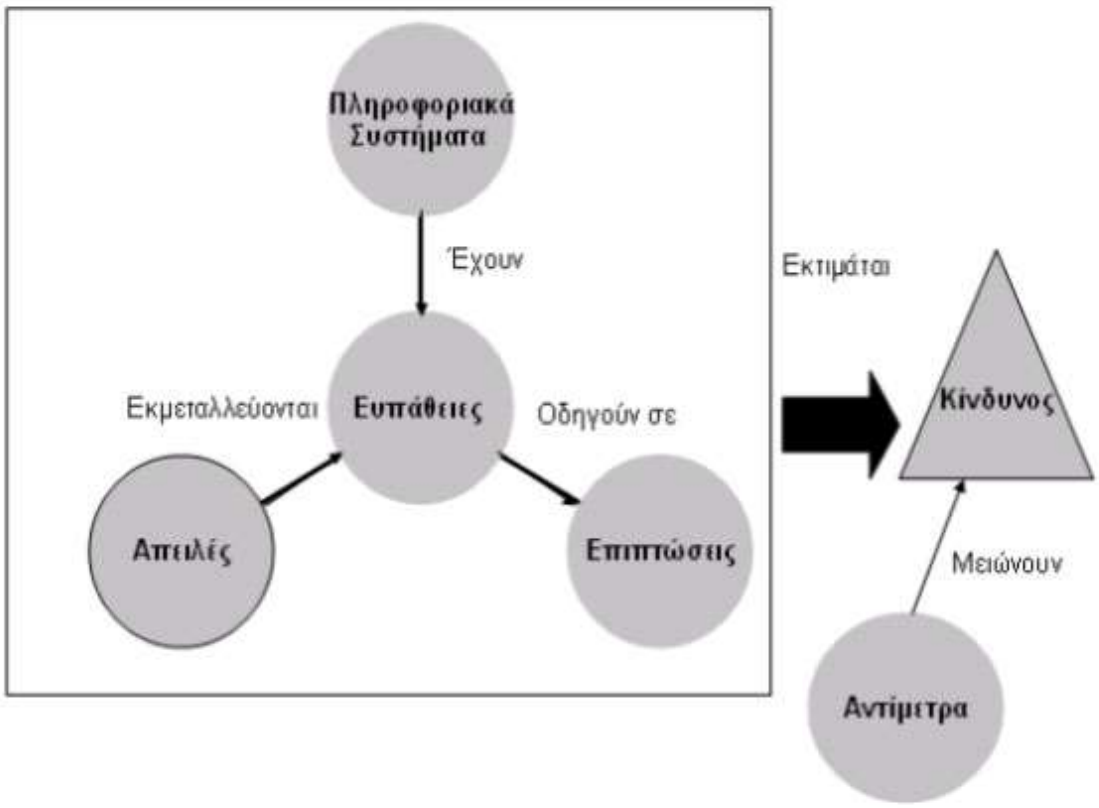
Τα πληροφοριακά συστήματα καλούνται να αντιμετωπίσουν τους κινδύνους που μπορεί να απειλήσουν τη σωστή λειτουργία της επιχείρησης ή του οργανισμού. Οι κίνδυνοι αυτοί μπορεί να σχετίζονται με το υλικό (hardware), με τα οικονομικά στοιχεία και με τους εργαζομένους της επιχείρησης. Πριν όμως εξετάσουμε τους κινδύνους αυτούς είναι καλό να δώσουμε κάποιους ορισμούς σχετικά με την έννοια του κινδύνου.

Απειλή μπορεί να θεωρηθεί οποιοδήποτε γεγονός μπορεί να κάνει το σύστημα και τις υπηρεσίες μιας επιχείρησης να είναι μη διαθέσιμα ή που μπορεί να αποκαλύψει ευαίσθητες πληροφορίες της επιχείρησης.

Ευπάθεια είναι η αδυναμία ή η σχεδιαστική ατέλεια ενός συστήματος, που πιθανόν να γίνει η αιτία για την παραβίαση της ασφάλειας και της ακεραιότητας του. Η ευπάθεια ορίζεται ως το γινόμενο της πιθανότητας να συμβεί μια απειλή επί την πιθανότητα η απειλή αυτή να είναι επιτυχής.

Ο κίνδυνος εκφράζει το ενδεχόμενο της απώλειας, της καταστροφής ή της βλάβης ενός τμήματος του συστήματος.

Το αντίμετρο είναι ένα μέτρο που μπορεί να ανιχνεύσει, να προλάβει ή να μειώσει οποιαδήποτε απώλεια σχετίζεται με την εμφάνιση μιας απειλής.



Σχήμα 2.1 Ευπάθειες και Απειλές Πληροφοριακών Συστημάτων

Μια επιχείρηση οφείλει να γνωρίζει, να καταγράφει και να αναλύει τους πιθανούς κινδύνους της, με στόχο την αποτελεσματική λειτουργία των πληροφοριακών συστημάτων της αλλά και την αποδοτικότερη λειτουργία της ίδιας της επιχείρησης. Οι κίνδυνοι αυτοί μπορεί να προέρχονται είτε από το εξωτερικό είτε από το εσωτερικό περιβάλλον μιας επιχείρησης και μπορεί να εμφανιστούν σε κάθε στάδιο και σε κάθε λειτουργία της επιχείρησης. Κάποια από τα είδη των κινδύνων που σχετίζονται με την ασφάλεια των πληροφοριακών συστημάτων και προσανατολίζονται προς τον ανθρώπινο παράγοντα είναι (Κυριαζόγλου, 2001):

1) Η ανθρώπινη συμπεριφορά

2) Η απόκλιση από τους κανόνες λειτουργίας

3) Η ελλιπής ή ανεπαρκής εξέταση του εξωτερικού περιβάλλοντος

4) Η δυσλειτουργία του συστήματος

5) Η μη αποδοτική αξιοποίηση των πόρων της επιχείρησης ή του οργανισμού

Επίσης, έχουμε τους επιχειρησιακούς κινδύνους (business risks). Οι επιχειρησιακοί κίνδυνοι χωρίζονται σε εσωτερικούς (internal) και εξωτερικούς (external). Στους εσωτερικούς περιλαμβάνονται ο ανθρώπινος παράγοντας, ο τεχνολογικός παράγοντας και κάποιοι λειτουργικοί παράγοντες, ενώ στους εξωτερικούς συγκαταλέγονται η οικονομία, οι φυσικές καταστροφές και η πολιτική (Miles, 2011).

Οι επιχειρησιακοί κίνδυνοι διακρίνονται στους στρατηγικούς, στους χρηματοοικονομικούς, στους λειτουργικούς, στους κινδύνους συμμόρφωσης και στους άλλους κινδύνους.

Στρατηγικοί Κίνδυνοι (*strategic risk*): Οι στρατηγικοί κίνδυνοι συνδέονται με τις δραστηριότητες του συγκεκριμένου οργανισμού ή της επιχείρησης και προκύπτουν από το επιχειρηματικό περιβάλλον. Με τον όρο επιχειρησιακό περιβάλλον εννοούμε τις μεταβολές της προσφοράς και της ζήτησης, τις ανταγωνιστικές δομές, την εισαγωγή των νέων τεχνολογιών, τα περιουσιακά στοιχεία, τις συγχωνεύσεις και τις εξαγορές και τις επενδυτικές σχέσεις.

Χρηματοοικονομικοί Κίνδυνοι (*financial risk*): Οι χρηματοοικονομικοί κίνδυνοι συνδέονται με την οικονομική διάρθρωση και τις συναλλαγές της επιχείρησης.

Λειτουργικοί Κίνδυνοι: Οι λειτουργικοί κίνδυνοι συνδέονται με τις επιχειρησιακές και διοικητικές διαδικασίες της επιχείρησης.

Κίνδυνος συμμόρφωσης (*Νομικός Κίνδυνος*): Οι κίνδυνοι συμμόρφωσης είναι οι κίνδυνοι που συνδέονται με την ανάγκη για συμμόρφωση με τους κανόνες και τους κανονισμούς της κυβέρνησης.

Άλλοι κίνδυνοι: Διαφορετικοί κίνδυνοι που δεν εντάσσονται στις παραπάνω κατηγορίες, όπως οι φυσικές καταστροφές (πλημμύρες).

Τα σημαντικότερα σημεία, στα οποία ελλοχεύουν οι κίνδυνοι για την επιχείρηση και τα πληροφοριακά συστήματά της, είναι η πρόσβαση στο διαδίκτυο, η ασφάλεια και η ακεραιότητα των δεδομένων, η απόκτηση και η ανάπτυξη του λογισμικού, η διαχείριση των

αρχείων (τροποποίηση / διαγραφή) και το κακόβουλο λογισμικό, καθιστώντας πλέον απαραίτητους τους ανάλογους ελέγχους (Silltow, 2003)(Beard et Wen, 2007).

Υπάρχουν αρκετά διαθέσιμα εργαλεία ώστε να καθίσταται δυνατός ο καθορισμός του επιπέδου του κινδύνου στον οποίο εκτίθεται μια επιχείρηση, όπως είναι οι δείκτες μέτρησης κινδύνου, οι οποίοι μπορούν να χρησιμοποιούνται από την επιχείρηση όποτε κρίνεται απαραίτητο. Επίσης, ο παρακάτω τύπος καθίσταται χρήσιμος ως προς τον υπολογισμό του επιπέδου του κινδύνου μέσω της αναμενόμενης ζημίας και αποτελεί άλλο ένα χρήσιμο εργαλείο στη διάθεση της επιχείρησης (Hunton et al., 2004):

Αναμενόμενη αξία κινδύνου =
Εκτιμώμενη ζημία από συγκεκριμένο κίνδυνο * % Πιθανότητα ζημίας

Expected value of risk =
Estimated Loss from Specific Risk * % Likelihood of Loss

Όταν, όμως, ένας κίνδυνος εμφανιστεί, είναι εξίσου σημαντικό να διαχειρίζεται με τον κατάλληλο τρόπο.

Ιδιαίτερη σημασία πρέπει να δίνεται στην ιεράρχηση των αναγκών της διαχείρισης και τη συνεχή βελτίωσης της με στόχο την ενίσχυση του έργου της διαχείρισης κινδύνου. Έτσι, το Institute of Internal Auditors ανέπτυξε μια μεθοδολογία βημάτων τα οποία πρέπει ακολουθούνται. (Scott, 2008). Αναλυτικότερα :

1) Καθορισμός των επιχειρηματικών στόχων, ώστε να μπορούν να οργανωθούν καλύτερα οι έλεγχοι.

2) Καθορισμός των καίριων στοιχείων που μπορούν να βοηθήσουν στην

επίτευξη των επιχειρηματικών στόχων που έχουν τεθεί.

3) Έλεγχος της λειτουργικότητας των πληροφοριακών συστημάτων.

4) Επιλογή των εφαρμογών πληροφορικής που

χρήζουν ελέγχου.

5) Καθορισμός των πιθανών κινδύνων καθώς και των στόχων του ελέγχου.

6) Σχεδιασμός ενός αποτελεσματικού πλάνου υλοποίησης του ελέγχου.

1.5.2 ΠΑΡΑΒΑΣΕΙΣ ΚΑΙ ΑΠΕΙΛΕΣ

Παραπάνω αναλύθηκαν οι κίνδυνοι που αντιμετωπίζουν τα πληροφοριακά συστήματα. Πέραν όμως από τους κινδύνους αυτούς τα πληροφοριακά συστήματα απειλούνται από πιθανές παραβιάσεις. Έτσι, π.χ. παραβίαση αποτελεί η εισβολή στο σύστημα κάποιου μη εξουσιοδοτημένος χρήστης, ο οποίος θα αποκτήσει πρόσβαση σε διαβαθμισμένα δεδομένα (με περιορισμένη πρόσβαση) ή θα τα αλλοιώσει ή θα τα καταστρέψει. Οι παραβιάσεις αυτές μπορούν να σχετίζονται το υλικό (κλοπή ή καταστροφή μιας συσκευής), το λογισμικό (ιοί ή παράνομη αντιγραφή) ή τα δεδομένα (παρακολούθηση ή υποκλοπή δεδομένων).

Κατά την πλειονότητά τους, οι παραβιάσεις προέρχονται από εξωτερικούς παράγοντες και, συνήθως, ο οργανισμός ή η επιχείρηση το αντιλαμβάνεται αφού έχει παρέλθει αρκετός χρόνος. Παρακάτω, ακολουθούν παραδείγματα των πιο κοινών παραβιάσεων που μπορεί να αντιμετωπίσει ένα πληροφοριακό συστήματα (https://www.enisa.europa.eu/):

Λάθη και Παραλείψεις

Τα πιθανά λάθη και οι παραλείψεις αποτελούν κίνδυνο για την ασφάλεια του συστήματος. Τα λάθη και οι παραλείψεις προκαλούνται συνήθως από τους χρήστες του συστήματος που επεξεργάζονται και εισάγουν τα δεδομένα καθημερινά, καθώς, ακουσίως, γίνονται, λανθασμένες ενέργειες ή παραλείψεις στην διαχείριση των δεδομένων. Ένας ακόμη παράγοντας που αποτελεί σοβαρή παράλειψη είναι η συντήρηση και η ενημέρωση του λογισμικού. Πολλά από τα σύγχρονα συστήματα παρέχουν υποστήριξη και καθοδήγηση στους χρήστες για την αποφυγή τέτοιων λαθών και παραλείψεων. Τέλος, κάποια από αυτά διαθέτουν συστήματα ελέγχου και εντοπισμού λαθών σαν μέτρο πρόληψης.

Απάτη και Κλοπή

Τα πληροφοριακά συστήματα διαθέτουν μηχανισμούς ελέγχου της πρόσβασης των χρηστών στα δεδομένα, συστήματα παρακολούθησης, συστήματα απογραφής, χρηματοπιστωτικά συστήματα κ.α. Είναι σύνηθες το φαινόμενο οι μηχανισμοί αυτοί των συστημάτων να δέχονται επίθεση με στόχο την απάτη ή την κλοπή. Η επίθεση αυτή μπορεί να γίνει είτε από χρήστες του συστήματος είτε από εξωτερικούς χρήστες που καταφέρνουν να εισβάλουν. Έχει παρατηρηθεί πως στην πλειοψηφία τους τέτοιες επιθέσεις γίνονται από παλιούς χρήστες του συστήματος που είναι εξουσιοδοτημένοι και έτσι έχουν εύκολη πρόσβαση στο σύστημα.

Φυσικές απειλές και απειλές υποδομών

Οι απειλές που σχετίζονται με τις υποδομές περιλαμβάνουν τις διακοπές ρεύματος ή αυξομείωση της τάσης, απώλεια επικοινωνίας, διαρροές νερού, προβλήματα αποχέτευσης, πυρκαγιά, πλημμύρα, πολιτικές αναταραχές, απεργίες κ.α. Η καταστροφή μέρους των υποδομών προκαλεί σε υπολειτουργία του συστήματος η μια μεγαλύτερη μεγέθους καταστροφή μπορεί να επιφέρει τη συνολική κατάρρευση του συστήματος.

Κακόβουλος Κώδικας

Ο κακόβουλος κώδικας αναφέρεται σε ιούς (virus), σκουλήκια (worms), δούρειους ίππους (Trojan horse), λογικές βόμβες (logic bombs) και οποιαδήποτε άλλη μορφή ανεπιθύμητου λογισμικού. Ο κακόβουλος κώδικας χρησιμοποιείται από εξωτερικούς χρήστες με στόχο να δημιουργήσει πρόβλημα στην λειτουργία του συστήματος ή να προκαλέσει ρωγμή στην ασφάλεια ώστε να δώσει την δυνατότητα στον εξωτερικό χρήστη να αποκτήσει πρόσβαση στο σύστημα.

1.5.3 ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ

Τα μέτρα προστασίας είναι οι διαδικασίες και οι ενέργειες που περιορίζουν τις ευπάθειες ενός πληροφοριακού συστήματος. Περιλαμβάνουν τη φυσική ασφάλεια του συστήματος, δηλαδή την προστασία ολόκληρου του εξοπλισμού του υπολογιστή, την ασφάλεια του υπολογιστικού συστήματος με την έννοια της ασφάλειας των πληροφοριών

του υπολογιστή που διαχειρίζεται άμεσα το λειτουργικό σύστημα. Ακόμη περιλαμβάνουν την ασφάλεια των βάσεων δεδομένων και των δικτύων επικοινωνιών.

Το πόσο αποτελεσματικά είναι αυτά τα μέτρα προστασίας εξαρτάται από τον τρόπο χρησιμοποίησής τους αλλά και από το μέγεθος του προβλήματος που υπάρχει. Προκειμένου λοιπόν, τα μέτρα αυτά να είναι όσο το δυνατόν αποτελεσματικότερα είναι καλό να γίνονται τακτικές αναθεωρήσεις, να εκπαιδεύεται σωστά το προσωπικό και να οργανώνονται έτσι ώστε να είναι εύκολη η χρήση τους.

Οι κατηγορίες των μέτρων προστασίας είναι (Πάγκαλος, Μαυρίδης, 2002):

1) Μέτρα προσπέλασης συστήματος, τα οποία εξασφαλίζουν ότι οι μη εξουσιοδοτημένοι χρήστες δεν εισάγονται στο σύστημα, όπως είναι το identification and authentication των χρηστών, των προγραμμάτων ή των μηχανημάτων καθώς και των εξουσιοδοτήσεων που αυτά διαθέτουν, για την προσπέλαση των προστατευμένων πόρων του συστήματος, με συνδυασμένη χρήση συνθηματικών και ψηφιακών πιστοποιητικών.

2) Μέτρα προσπέλασης δεδομένων, που ελέγχουν ποια άτομα μπορούν να έχουν πρόσβαση, σε ποια δεδομένα και με ποιο σκοπό. Οι εφαρμογές των βάσεων δεδομένων απαιτούν τυπικά έναν υψηλό βαθμό λεπτομέρειας του ελέγχου προσπέλασης. Το σύστημα θα πρέπει να φροντίζει, έτσι ώστε οι εξουσιοδοτημένοι χρήστες να μπορούν να ενεργήσουν μόνο στα πλαίσια των κανόνων που καθορίζονται από την πολιτική ασφάλειας. Όσον αφορά τους ελέγχους προσπέλασης, συναντώνται οι ακόλουθες έννοιες:

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

3) Διαχείριση συστήματος και ασφάλειας, ορίζοντας τις ευθύνες του διαχειριστή συστήματος.

4) Σχεδιασμός συστήματος, με βάση την αξιοποίηση βασικών χαρακτηριστικών και δυνατοτήτων ασφάλειας του υλικού και λογισμικού.

Οι τύποι μέτρων προστασίας για την πρόληψη της εκμετάλλευσης των ευπαθειών ενός πληροφοριακού συστήματος είναι (Πάγκαλος & Μαυρίδης, 2002):

1) Κρυπτογράφηση (encryption). Η κρυπτογράφηση αναφέρεται στο μετασχηματισμό των δεδομένων σε μια ακατανόητη μορφή έτσι ώστε να μην μπορούν να γίνουν κατανοητά από μη εγκεκριμένους χρήστες. Η κρυπτογραφία παρέχει τέσσερις βασικές λειτουργίες – αντικειμενικούς σκοπούς:

- *Εμπιστευτικότητα*: Η πληροφορία προς μετάδοση είναι προσβάσιμη μόνο στα εξουσιοδοτημένα μέλη. Η πληροφορία είναι ακατανόητη σε κάποιον τρίτο.
- *Ακεραιότητα*: Η πληροφορία μπορεί να αλλοιωθεί μόνο από τα εξουσιοδοτημένα μέλη
- *Μη απάρνηση*: Ο αποστολέας ή ο παραλήπτης της πληροφορίας δεν μπορεί να αρνηθεί την αυθεντικότητα της μετάδοσης ή της δημιουργίας της.
- *Πιστοποίηση*: Οι αποστολέας και παραλήπτης μπορούν να εξακριβώνουν τις ταυτότητές τους καθώς και την πηγή και τον προορισμό της πληροφορίας με διαβεβαίωση ότι οι ταυτότητές τους δεν είναι πλαστές.

2) Μέτρα Λογισμικού (software controls). Τα μέτρα λογισμικού αναφέρονται σε προγράμματα που πρέπει να είναι ασφαλή και αξιόπιστα για αποτροπή εξωτερικών επιθέσεων.

3) Μέτρα Υλικού (hardware controls).Τα μέτρα υλικού αποτελούν διάφορες συσκευές που έχουν σκοπό να συμβάλουν στην ασφάλεια των υπολογιστών.

4) Φυσικά Μέτρα Υλικού (physical controls).Τα φυσικά μέτρα υλικού αποτελούν τα λιγότερο δαπανηρά μέτρα για την ασφάλεια των συστημάτων

5) Πολιτικές Ασφάλειας (security policies). Οι πολιτικές ασφαλείας αποτελούν κάποια άλλα μέτρα ασφάλειας όπως για παράδειγμα ο έλεγχος προσπέλασης.

ΚΕΦΑΛΑΙΟ 2 ΟΙ 4 ΜΕΓΑΛΕΣ ΕΛΕΓΚΤΙΚΕΣ ΕΤΑΙΡΕΙΕΣ

Στον τομέα της λογιστικής και της ελεγκτικής, συχνά, χρησιμοποιείται ο όρος Big 4 ως αναφορά στις 4 μεγαλύτερες πολυεθνικές εταιρείες που παρέχουν ελεγκτικές, φορολογικές, συμβουλευτικές, νομικές υπηρεσίες και αναλογιστικές μελέτες. Αυτές οι εταιρείες είναι η Deloitte, η Ernst & Young, η PricewaterhouseCoopers (PWC) και η Klynveld Peat Marwick Goerdeler (KPMG). Στο παρόν κεφάλαιο θα αναλυθούν τα προφίλ και οι δράσεις των συγκεκριμένων εταιρειών.

2.1 DELOITTE

Η Deloitte ιδρύθηκε το 1845 στο Λονδίνο και από τότε μέχρι σήμερα έχει καταφέρει να γίνει μία λογιστική/ ελεγκτική εταιρεία, η οποία προσφέρει ολοκληρωμένες ελεγκτικές, φορολογικές, χρηματοοικονομικές και συμβουλευτικές υπηρεσίες. Η Deloitte διαθέτει ένα εκτεταμένο διεθνές δίκτυο μέσω του οποίου έχει καταφέρει να εξασφαλίσει άμεση πρόσβαση στη γνώση, πολλές συνεργασίες και την στήριξη της τοπικής κοινότητας σε πολλές χώρες του κόσμου. Η Deloitte μετρά 35 χρόνια εμπειρίας στην Ελλάδα, παρέχοντας ένα μεγάλο εύρος συμβουλευτικών και ελεγκτικών υπηρεσιών σε όλους τους τομείς της οικονομίας, συμπεριλαμβανομένων των χρηματοοικονομικών υπηρεσιών, της ναυτιλίας, της ενέργειας, των τηλεπικοινωνιών, της βιομηχανίας, του τουρισμού, των καταναλωτικών προϊόντων, της υγείας και του ευρύτερου δημόσιου τομέα (www.deloitte.com).

Η Deloitte έχει αναπτύξει τη δική της προσέγγιση ελέγχου με βάση τα Διεθνή Ελεγκτικά Πρότυπα (ISA) που έχουν εκδοθεί από την IFAC. Το εργαλείο που χρησιμοποιεί η εταιρεία είναι το The DeloitteAudit". Ο έλεγχος και η υποστήριξη στην τεχνολογία είναι τα κύρια χαρακτηριστικά που παρέχει το εργαλείο αυτό. Μέσα από μια συστηματική ανάλυση των κινδύνων προς τις βασικές επιχειρηματικές διαδικασίες, η επιχείρηση δίνει έμφαση σε συγκεκριμένους τομείς, στους οποίους οι συναλλαγές και τα γεγονότα είναι σημαντικά για την ποιότητα και την αξιοπιστία της χρηματοοικονομικής πληροφόρησης. Κεντρικό σημείο της προσέγγισης της εταιρείας είναι ο προσδιορισμός των σχετικών κινδύνων μέσω μιας προσεκτικής αξιολόγησης της βιομηχανίας και των δραστηριοτήτων του πελάτη.

Ανάθεση Ελεγκτικού Έργου

Η ανάθεση ενός ελεγκτικού ελέγχου σε κάποιον εταίρο ακολουθεί συγκεκριμένη και νόμιμη διαδικασία. Η ομάδα ελέγχου για κάθε έργο απαρτίζεται από τον (κύριο) εταίρο, από άλλους ελεγκτές διαφόρων βαθμίδων, καθώς και από ειδικούς εκπροσώπους της εταιρίας σε διάφορα εξειδικευμένα αντικείμενα. Ο (κύριος) εταίρος προσδιορίζει την ομάδα ελέγχου με βάση το μέγεθος, τη φύση και την πολυπλοκότητα των εργασιών της ελεγχόμενης οντότητας. Η ομάδα ενεργεί κάτω από τον έλεγχο και εποπτεία του (κύριου) εταίρου, στον οποίο έχει ανατεθεί η διεκπεραίωση του έργου. Ο (κύριος) εταίρος λαμβάνει υπόψιν του διάφορους παράγοντες προκειμένου να καθορίσει την ομάδα ελέγχου έτσι ώστε συλλογικά η ομάδα να διαθέτει τις κατάλληλες δεξιότητες και δυνατότητες καθώς και τον απαραίτητο χρόνο για να διεκπεραιώσει το ελεγκτικό έργο. Γι' αυτό το σκοπό ο (κύριος) εταίρος λαμβάνει υπόψιν του, διάφορους παράγοντες προκειμένου να προσδιορίσει τη σύνθεση της ελεγκτικής ομάδας, όπως:

Α) Το μέγεθος και την πολυπλοκότητα των εργασιών του πελάτη

Β) Το εφαρμοστέο πλαίσιο χρηματοοικονομικής πληροφόρησης το οποίο διέπει τις ελεγχόμενες οικονομικές καταστάσεις

Γ) Τις υποχρεώσεις ανεξαρτησίας και αποφυγής συγκρούσεως ενδιαφερόντων συμφερόντων

Δ) Τα προσόντα και την εμπειρία του διαθέσιμου προσωπικού

Ελεγκτική Προσέγγιση

Όλες οι εταιρίες-μέλη του Δικτύου της Deloitte εφαρμόζουν ανά πάσα στιγμή την ελεγκτική προσέγγιση που ακολουθεί το Δίκτυο της Deloitte παγκοσμίως για το σχεδιασμό και την εκτέλεση των ελεγκτικών έργων, όπως αυτή επικαιροποιείται σε διαρκή βάση, προσαρμοσμένη, εφόσον χρειάζεται, στις απαιτήσεις της Ελληνικής νομοθεσίας. Η προσέγγιση περιλαμβάνει πολιτικές και οδηγίες που βοηθούν στο σχεδιασμό και στην εκτέλεση αναθέσεων ελεγκτικού έργου και βασίζεται στα Διεθνή Ελεγκτικά Πρότυπα (ISA) που εκδίδονται από το Διεθνές Συμβούλιο Ελεγκτικών Προτύπων (International Auditing and Assurance Standards Board) της Διεθνούς Ομοσπονδίας Λογιστών (International Federation of Accountants – IFAC).

Η προσέγγιση αυτή, ακολουθεί την εξής διαδικασία:

1) Κατανόηση της ελεγχόμενης οντότητας και του επιχειρησιακού περιβάλλοντος

2)Δοκιμασίες της λειτουργικής αποτελεσματικότητας των μηχανισμών εσωτερικού ελέγχου

3)Ουσιαστικές ελεγκτικές διαδικασίες

4) Διαρκή βελτίωση της παραγωγικότητας / αποτελεσματικότητας του ελέγχου

2.2 ERNST & YOUNG

Η Ernst & Young είναι μία ελεγκτική εταιρία που εδρεύει στο Λονδίνο, της οποίας οι κύριες δραστηριότητες είναι η διεξαγωγή οικονομικών και διαχειριστικών ελέγχων και εργασιών πραγματογνώμονος, σύμφωνα με την κείμενη νομοθεσία. Η Ernst & Young παρέχει επίσης συμβουλές και υπηρεσίες σε φορολογικά θέματα και σε θέματα διοίκησης και μηχανοργάνωσης επιχειρήσεων, και διενεργεί κάθε πράξη που κατατείνει στην επίτευξη των πιο πάνω εταιρικών σκοπών (www.ey.com). Πιο συγκεκριμένα, οι δραστηριότητές της αφορούν:

Α) Assurance (Ασφάλιση) 41%: δημοσιονομικός έλεγχος, συμβουλευτικές υπηρεσίες χρηματοοικονομικής ελεγκτικής, έρευνα για απάτη, υπηρεσίες αειφορίας

Β) Φόροι (Tax) 26%: φόροι μεταβίβασης, έμμεση φορολογία, φόροι επί των συναλλαγών

Γ) Συμβουλευτική (Advisory) 24%: αναλογιστικές μελέτες, διασφάλιση IT κινδύνων, βελτίωση επιδόσεων

Δ) Transaction Advisory Services (TAS) (9%)

Τον Μάιο του 2015, εκδόθηκε η νέα Κεντρική Μεθοδολογία Ελέγχου της Ernst & Young (EY Global Methodology – EY GAM), η οποία επανασχεδιάστηκε έτσι ώστε να είναι πιο ευανάγνωστη και πιο εύχρηστη και να υποστηρίζει το νέο εργαλείο για την τεκμηρίωση των στοιχείων του ελέγχου, το EY Canvas.

Το εργαλείο που χρησιμοποιεί η ΕΥ είναι το GAMx. Αυτό το λογισμικό ελέγχου εξασφαλίζει ότι η μεθοδολογία ελέγχου της επιχείρησης εφαρμόζεται με συνέπεια και με αποτελεσματικότητα και ότι οι διαδικασίες ελέγχου της είναι επαρκώς τεκμηριωμένες. Το λογισμικό αυτό ελέγχου έχει πρόσβαση στα ελεγκτικά πρότυπα και στις μεθόδους και καθοδηγεί την επιχείρηση με τη βοήθεια των εργαλείων πληροφορικής. Το εργαλείο αυτό βοηθάει την επιχείρηση να εφαρμόζει αποτελεσματικούς ελέγχους. Συνεχώς αναπτύσσει καινούργιες εφαρμογές και βελτιώνει τις ήδη υπάρχουσες προκειμένου να είναι αποτελεσματική.

Μεθοδολογία Ελέγχου

Η Ernst & Young παρέχει ένα κεντρικό πλαίσιο για την παροχή ποιοτικών ελεγκτικών υπηρεσιών με την εφαρμογή διαδικασιών, κρίσεων και ελεγκτικών διαδικασιών σε όλα τα έργα ελέγχου. Ένας από τους ακρογωνιαίους λίθους της, είναι η πραγματοποίηση (η επανεξέταση και η τροποποίηση, όπου κριθεί απαραίτητο, κατά τη διάρκεια του ελέγχου) της αξιολόγησης κινδύνων και ο καθορισμός της φύσης, του χρόνου και της έκτασης των ελεγκτικών διαδικασιών, ο οποίος βασίζεται πάνω σε αυτήν την αξιολόγηση των κινδύνων. Επιπλέον, η Ernst & Young GAM δίνει έμφαση στην άσκηση κατάλληλου επαγγελματικού σκεπτικισμού κατά την εκτέλεση των ελεγκτικών διαδικασιών. Η Ernst & Young GAM βασίζεται στα Διεθνή Ελεγκτικά Πρότυπα (ISAs) και στην Ελλάδα, έχει δεχθεί τις απαραίτητες προσθήκες, προκειμένου να είναι συμβατή με τα Ελληνικά Ελεγκτικά Πρότυπα και τις ρυθμιστικές ή νομοθετικές απαιτήσεις.

Με την χρήση της τεχνολογίας, επιλέγεται η προσέγγιση του ελέγχου, εντός των πλαισίων της μεθοδολογίας που εφαρμόζεται, βάσει των απαιτήσεων του ελέγχου της οντότητας που ελέγχεται. Για παράδειγμα, υπάρχουν προσεγγίσεις στον έλεγχο για εισηγμένες εταιρείες και για οντότητες που δεν παρουσιάζουν πολυπλοκότητα στον έλεγχο (non-complex). Ο ελεγκτής έχει πλέον στην διάθεσή του μία έκδοση της Ernst & Young, η οποία είναι οργανωμένη σε αλληλοεξαρτώμενες φάσεις, σχεδιασμένη να εστιάζει τόσο στους επιχειρηματικούς κινδύνους, όσο και στους κινδύνους που συνδέονται με τις οικονομικές καταστάσεις του πελάτη και στο πως αυτοί οι κίνδυνοι επηρεάζουν τον έλεγχο των οικονομικών καταστάσεων. Τέλος, η Ernst & Young συμμορφώνεται με τα σχετικά πρότυπα επαγγελματισμού και δεοντολογίας, που περιλαμβάνουν την ανεξαρτησία από την εταιρεία που ελέγχεται.

2.3 PRICEWATERHOUSECOOPERS (PWC)

Η PricewaterhouseCoopers είναι μία λογιστική /ελεγκτική πολυεθνική εταιρία, που εδρεύει στο Λονδίνο και θεωρείται ως η πιο διάσημη από τις Big4, καθώς διαθέτει ένα δίκτυο επιχειρήσεων σε 157 χώρες.

Η PWC χρησιμοποιεί στους ελέγχους της 3 λογισμικά. Το Aura, που είναι μια παγκόσμια πλατφόρμα ελέγχου που χρησιμοποιείται από σχεδόν 100.000 ελεγκτές σε όλο τον κόσμο. Τα βασικά πλεονεκτήματα του Aura:

- Είναι το μοναδικό λογισμικό παγκοσμίως με δυνατότητα ενσωματωμένων IP
- Κάνει συστηματική ανάλυση κινδύνου επικεντρώνοντας στις σημαντικότερες παραμέτρους
- Διαθέτει τεχνολογία ροής εργασιών με αποτέλεσμα να μπορεί να ελέγχει τις διαδικασίες, τα ατομικά καθήκοντα δίνοντας την δυνατότητα για έγκαιρη αναθεώρηση των εργασιών
- Δυνατότητα συνεργασίας των κέντρων παροχής υπηρεσιών και των ελεγκτικών
  ομάδες μέσω της εφαρμογής
- Παρακολούθηση σε πραγματικό χρόνο της προόδου, με δυνατότητα χρήσης σε πολλές συσκευές

Το λογισμικό Halo αλλάζει τον τρόπο διενέργειας του ελέγχου, με την χρήση τεχνολογιών αιχμής παρέχει την εικόνα των δεδομένων σε πραγματικό χρόνο. Τα βασικά πλεονεκτήματα του Halo:

- Μπορεί να διαχειριστεί μεγάλους όγκους συναλλαγών μπορεί να ανακριθούν και να αναλυθούν.
- Αποτελεσματικότερη εκτίμηση των κινδύνων
- Διαθέτει την δυνατότητα να επεξεργάζεται πληροφορίες από πολλά συστήματα

- Έλεγχοι μπορούν να πραγματοποιηθούν εκτός του χώρου και κατά την διάρκεια όλου το χρόνου
- Το Halo έχει ενσωματωμένους αλγορίθμους και απεικονίσεις που βοηθούν τους ελεγκτές να κατανοήσουν τις επιχειρήσεις και να παρέχουν καλύτερες υπηρεσίες

Το λογισμικό Connect είναι ένα εργαλείο που βοηθά τους ελεγκτές παρέχοντας πιο γρήγορη, πιο αποτελεσματική και πιο ασφαλή ανταλλαγή πληροφοριών σε κάθε στάδιο του ελέγχου. Δίνει τη δυνατότητα στους ελεγκτές και στους ελεγχόμενους να ελέγχουν την πρόοδο οποιαδήποτε στιγμή. Τα βασικά πλεονεκτήματα Connect είναι:

- Πρόσβαση όπου κι αν βρίσκεστε. Οι πελάτες της PwC μπορούν να έχουν πρόσβαση στην πρόοδο του ελέγχου
- Είναι ένα ασφαλές web-based εργαλείο με δυνατότητα ανταλλαγής εγγράφων και παραδοτέων
- Προσφέρει αποτελεσματική διαχείρισης ροής εργασιών

Η δραστηριότητα και οι προσφερόμενες υπηρεσίες της συνοψίζονται στον παρακάτω πίνακα:

Advisory	**Audit and Assurance**	**Tax**	**Training Services**
Strategy & perations	Capital Markets Group	Corporate Income Tax	Tax trainings
Business Process Outsourcing	International nancial R reporting andards	Finance, Treasury & Securitisation	Accounting / IFRS trainings
Deals	Shipping Industry Services	Indirect Taxes	Shipping trainings
Finance Function Effectiveness		International Tax Services	Banking & Finance trainings

People & Organisation		Mergers & Acquisitions	Real Estate trainings
Risk Assurance Services		Transfer Pricing	Payroll, HR & Business English trainings
Texhnology		Tax Compliance	
		International Assignment Services	
		Real Estate Compliance	

Η δομή της εταιρικής διακυβέρνησης της PwCIL αποτελείται από:

Παγκόσμιο Συμβούλιο (Global Board), υπεύθυνο για την διακυβέρνηση της PwCIL και για την εποπτεία της Ηγετικής Ομάδας Δικτύου.

Ηγετική Ομάδα Δικτύου (Network Leadership Team), υπεύθυνη να ορίζει τη γενική στρατηγική του PwC και τα πρότυπα και τις πολιτικές τα οποία οι εταιρίες μέλη συμφωνούν να εφαρμόσουν.

Συμβούλιο Στρατηγικής (Strategy Council), που αποτελείται από ανώτατα στελέχη / μερικών από τις μεγαλύτερες εταιρίες – μέλη του δικτύου της PwC, καθορίζει τις αλλαγές στην στρατηγική κατεύθυνση του δικτύου έτσι ώστε να διευκολύνει τη συνέπεια στην εφαρμογή της από το δίκτυο.

Εκτελεστική Ομάδα Δικτύου (Network Executive Team), η οποία αναφέρεται στην ηγετική ομάδα δικτύου και συντονίζει τους τομείς υπηρεσιών.

Σύστημα διασφάλισης ποιότητας

Η εταιρία διαθέτει σύστημα διασφάλισης της ποιότητας των ελεγκτικών της υπηρεσιών έτσι ώστε να συμμορφώνεται με τα Διεθνή Πρότυπα. Το σύστημα διασφάλισης ποιότητας της PwC αναπτύσσεται σύμφωνα με όσα επιτάσσει το υπ' αριθμό 1 Διεθνές Πρότυπο Ποιοτικής Αξιολόγησης. Παρακάτω παρατίθενται τα 6 θεμελιώδη συστατικά στοιχεία:

1. Δέσμευση της ηγεσίας για τη διασφάλιση ποιότητας (Leadership responsibilities for the quality within the firm). Η ηγεσία δεσμεύεται για τη λήψη μέτρων που απαιτούνται για τη λειτουργία του συστήματος διασφάλισης της ποιότητας και έχει καθιερώσει μία εταιρική κουλτούρα που ενσωματώνει τις σημαντικές αρχές της ανεξαρτησίας και τις επαγγελματικής συμπεριφοράς.

2. Εφαρμογή κανόνων δεοντολογίας (Ethical requirements). Οι κανόνες αυτοί εστιάζουν στην ακεραιότητα, στην αντικειμενικότητα και στην ανεξαρτησία.

3. Αποδοχή και διατήρηση πελατών (Acceptance and Continuance of client relations and specific engagements). Η PwC εφαρμόζει ένα συστηματικό πλαίσιο αξιολόγησης των κινδύνων που σχετίζονται με τη διενέργεια ενός ελέγχου χρησιμοποιώντας σύστημα υποστήριξης απόφασης για την αποδοχή ή διατήρηση ενός πελάτη, το οποίο έχει αναπτυχθεί για αποκλειστική χρήση τωνμελών τους.

4. Διοίκηση ανθρωπίνων πόρων (Human Resources). Η PwC εφαρμόζει αυστηρά κριτήρια τόσο για την πρόσληψη των επαγγελματιών της όσο και για τη μετέπειτα ανέλιξη στην εταιρία, προσφέροντας συνεχή επαγγελματική ανάπτυξη, επίβλεψη και κατεύθυνση στο ανθρώπινο δυναμικό της.

5. Διενέργεια ελεγκτικών εργασιών (Engagement Performance). Όσον αφορά τη διενέργεια των ελεγκτικών εργασιών, η PwC ακολουθεί μια συνεπή παγκόσμια μεθοδολογία για τους ελέγχους, με περιεκτικές πολιτικές και διαδικασίες που απεικονίζουν τις νέες επαγγελματικές εξελίξεις, μειώνοντας τον κίνδυνο και προσφέροντας ποιοτικές υπηρεσίες.

6. Παρακολούθηση και εποπτεία (Monitoring). Η PwC ελέγχει την αποτελεσματικότητα του συστήματος διασφάλισης ποιοτικού ελέγχου των ελεγκτικών υπηρεσιών πραγματοποιώντας η ίδια, ή αναθέτοντας σε τρίτους, ανεξάρτητους ελέγχους ποιότητας. Το παραπάνω σύστημα διασφάλισης ποιότητας αξιολογείται ετησίως, με βάση το πλαίσιο που επιτάσσει το ISQC 1.

2.4 KLYNVELD PEAT MARWICK GOERDELER (KPMG)

Η KPMG είναι μία από τις μεγαλύτερες εταιρείες επαγγελματικών υπηρεσιών στον κόσμο και ένας από τους Big Four ελεγκτές, μαζί με την Deloitte, EY και PwC. Η έδρα της εταιρείας αυτής βρίσκεται στην Ολλανδία. Η εταιρεία απασχολεί περίπου 173.965 και έχει τρεις γραμμές υπηρεσιών: ελεγκτικές, φορολογικές και συμβουλευτικές. Το όνομα KPMG σημαίνει Klynveld Peat Marwick και Goerdeler. Κάθε ένα από αυτά τα ονόματα αντιπροσωπεύει μία από τις σημαντικότερες συνεργασίες που συνθέτει την ιστορία της KPMG.

Το λογισμικό που χρησιμοποιεί η KPMG ονομάζεται IDEA και παρέχει επαγγελματικό έλεγχο και χρηματοδότηση και αποτελεί μία αποδοτική και αποτελεσματική λύση για ελέγχους υψηλής απόδοσης. Το λογισμικό αυτό χρησιμοποιείται επίσης από τις φορολογικές αρχές σε όλο τον κόσμο για να ελέγχουν τις συναλλαγών των φορολογουμένων και την ορθότητα των δεδομένων του συστήματος. Το λογισμικό αυτό παρέχει ολοκληρωμένη ανάλυση των συναλλαγών, ανάλυση των δεδομένων και εύρεση των ανωμαλιών του συστήματος. Το εργαλείο IDEA είναι ένα ολοκληρωμένο, ισχυρό και εύκολο στη χρήση εργαλείο για την ανάλυση των δεδομένων που αναλύει γρήγορα το 100% των δεδομένων, ελέγχει την ακεραιότητα των δεδομένων της επιχείρησης και έτσι ανοίγει το δρόμο για έναν πιο γρήγορο και πιο αποτελεσματικό έλεγχο.

Ελεγκτικές Υπηρεσίες	**Φορολογικές Υπηρεσίες**	**Συμβουλευτικές Υπηρεσίες**
Έλεγχοι χρηματοοικονομικών καταστάσεων	Φορολογία Εταιρειών	Συμβουλευτικές υπηρεσίες για τη Διοίκηση
Επισκόπηση ιστορικής χρηματοοικονομικής πληροφόρησης Εργασίες εύλογης και περιορισμένης διασφάλισης	Ενδοομιλικές συναλλαγές	Συμβουλευτικές υπηρεσίες Διαχείρισης Κινδύνων

Άλλες αναθέσεις διασφάλισης Προσυμφωνημένες διαδικασίες	Υπηρεσίες σχετικές με έμμεσους φόρους	Deal Advisory
Καθοδήγηση στη σύνταξη χρηματοοικονομικών καταστάσεων	Υπηρεσίες Διεθνώς Μετακινούμενου Προσωπικού	Οικογενειακές επιχειρήσεις
Αποσπάσεις εξειδικευμένου προσωπικού	Υπηρεσίες λογιστηρίου	
	Υπηρεσίες μισθοδοσίας	
	Φορολογικά εργαλεία & πληροφορίες	

Σύστημα διασφάλισης ποιότητας

Η KPMG International διατηρεί πολιτικές διασφάλισης ποιότητας που εφαρμόζονται σε όλες τις εταιρείες-μέλη. Αυτές οι πολιτικές και οι συναφείς διαδικασίες έχουν σχεδιαστεί έτσι ώστε να καθοδηγούν τις εταιρείες μέλη να συμμορφώνονται με τα σχετικά επαγγελματικά πρότυπα, τις κανονιστικές και νομικές απαιτήσεις και να εκδίδουν τις κατάλληλες εκθέσεις ελέγχου. Παράλληλα, βασίζονται στο Διεθνές Πρότυπο Δικλείδων Διασφάλισης Ποιότητας 1 (Δ.Π.Δ.Δ.Π. 1) που έχει εκδοθεί από το Διεθνές Συμβούλιο Προτύπων Ελέγχου Και Διασφάλισης (IAASB) και στον Κώδικα της Δεοντολογίας των Επαγγελματιών Λογιστών που έχει εκδοθεί από το Διεθνές Συμβούλιο Προτύπων Δεοντολογίας των Λογιστών (IESBA). Και τα δύο αφορούν εταιρείες που διενεργούν τακτικούς ελέγχους και άλλα έργα διασφάλισης και συναφών υπηρεσιών.

Οι πολιτικές της KPMG International αντικατοπτρίζουν ατομικά στοιχεία διασφάλισης ποιότητας που βοηθούν τα μέλη του προσωπικού της να ενεργούν με

ακεραιότητα και αντικειμενικότητα, να διενεργούν την εργασία τους με επιμέλεια και να συμμορφώνονται με τους σχετικούς νόμους, κανονισμούς και επαγγελματικά πρότυπα. Ενώ πολλές διαδικασίες διασφάλισης ποιότητας της KPMG είναι διατμηματικές και ισχύουν εξίσου για την φορολογική και συμβουλευτική εργασία.

Το πλαίσιο διασφάλισης ποιότητας ελέγχου ακολουθεί παρακάτω:

Α) Το παράδειγμα της ηγεσίας (Tone at the top)
Β) Σχέσεις με τους σωστούς πελάτες
Γ) Σαφή πρότυπα και ισχυρά εργαλεία ελέγχου
Δ) Στελέχωση, εξέλιξη και τοποθέτηση κατάλληλα εκπαιδευμένου προσωπικού
Ε) Δέσμευση με την τεχνική αρτιότητα και την παράδοση υπηρεσιών ποιότητας
ΣΤ) Διενέργεια αποτελεσματικών και αποδοτικών ελέγχων
Η) Δέσμευση για συνεχή βελτίωση

Σχήμα 3.1 Το παράδειγμα της ηγεσίας

2.5 ΜΕΛΕΤΕΣ ΠΕΡΙΠΤΩΣΗΣ – CASE STUDIES

Σε αυτό το σημείο θα παρουσιαστούν κάποιες έρευνες που σχετίζονται με τον εσωτερικό έλεγχο και με τα πληροφοριακά συστήματα.

Ο Abu-Musa πραγματοποίησε μία έρευνα στο άρθρο του με τίτλο «Information technology and its implications for internal auditing- An empirical study of Saudi organizations», η οποία είχε στόχο να εξετάσει την επίδραση που είχε η πληροφορικής τεχνολογίας στις δραστηριότητες των εσωτερικών ελεγκτών. Επίσης, με την έρευνα που πραγματοποίησε ήθελε να δει κατά πόσο οι αξιολογήσεις της πληροφοριακής τεχνολογίας που γίνονται στις Σαουδικές επιχειρήσεις διαφέρουν μεταξύ τους καθώς και ποιοι είναι οι στόχοι της αξιολόγησης και τα χαρακτηριστικά των αξιολογήσεων αυτών. Η έρευνα αυτή πραγματοποιήθηκε με τη βοήθεια ερωτηματολογίων. Περίπου 700 ερωτηματολόγια μοιράστηκαν τυχαία σε ένα δείγμα Σαουδικών οργανισμών, που βρίσκονται σε πέντε μεγάλες Σαουδικές πόλεις. Συνολικά, βρέθηκαν 218 έγκυρα ερωτηματολόγια και αυτά μπόρεσαν να χρησιμοποιηθούν στην έρευνα. Τα ερωτηματολόγια αυτά αντιπροσωπεύουν ποσοστό ανταπόκρισης 30,7%, συλλέχθηκαν και αναλύθηκαν χρησιμοποιώντας το Στατιστικό Πακέτο Κοινωνικών Επιστημών – SPSS, έκδοση 15. Σύμφωνα λοιπόν με την έρευνα του, οι εσωτερικοί ελεγκτές πρέπει να ενισχύσουν τις δεξιότητές τους σχετικά με τα πληροφοριακά συστήματα, με τον σχεδιασμό τους, με την διοίκησή τους και με την εποπτεία τους. Επίσης, η έρευνα έδειξε ότι οι περισσότεροι εσωτερικοί ελεγκτές δίνουν μεγάλη προσοχή στους πιο συνηθισμένους κινδύνους και ελέγχους όπως είναι η ακεραιότητα των δεδομένων, η προστασία των προσωπικών δεδομένων, η ασφάλεια, η διαφύλαξη των περιουσιακών στοιχείων και τη επεξεργασία και η παραμετροποίηση των εφαρμογών. Αντίθετα, οι εσωτερικοί ελεγκτές δεν δίνουν τόσο μεγάλη σημασία στις δραστηριότητες ανάπτυξης και προμήθειας συστημάτων. Τέλος, στην έρευνα διαπιστώθηκε ότι οι αξιολογήσεις των εσωτερικών ελεγκτών συνδέονται με τους στόχους του ελέγχου, με το είδος της επιχείρησης, με τον αριθμό των ελεγκτών των πληροφοριακών συστημάτων, με το προσωπικό του εσωτερικού ελέγχου και με την ύπαρξη νέων πληροφοριακών συστημάτων στην επιχείρηση (Abu-Musa, 2008).

Οι Bierstaker, Brody and Pacini το 2006 στο άρθρο τους με τίτλο «Accountants' perceptions regarding fraud detection and prevention methods», θέλησαν να αξιολογήσουν το βαθμό στον οποίο χρησιμοποιούνται οι μέθοδοι ανίχνευσης και πρόληψης της απάτης από

τους λογιστές και από τους εσωτερικούς ελεγκτές και γι' αυτό το λόγο δημιούργησαν μία έρευνα. Επίσης, θέλησαν να εξετάσουν τις αντιλήψεις τους σχετικά με την αποτελεσματικότητα των μεθόδων αυτών. Στην έρευνα αυτή συμμετείχαν 86 λογιστές, εσωτερικοί ελεγκτές και πιστοποιημένοι εξεταστές κατά της απάτης. Ζητήθηκε από τους συμμετέχοντες η άποψή τους σχετικά με την αποτελεσματικότητα των μεθόδων ανίχνευσης και πρόληψης της απάτης. Από την έρευνα προέκυψε ότι οι πιο συνηθισμένοι τρόποι και μέτρα καταπολέμησης της απάτης είναι οι αντιπυρικές ζώνες, η προστασία από ιούς, η προστασία των κωδικών πρόσβασης και η βελτίωση των συστημάτων εσωτερικού ελέγχου. Η δειγματοληψία και το λογισμικό ψηφιακής ανάλυσης παρόλο που λαμβάνουν υψηλές βαθμολογίες αποτελεσματικότητας δεν χρησιμοποιούνται συχνά. Η έλλειψη αυτών των μεθόδων μπορούν να οδηγήσουν σε έλλειψη των διαθέσιμων πόρων στην επιχείρηση. (Bierstaker, 2006).

Οι Hermanson, Hill and Ivancevich το 2000 στο άρθρο τους με τίτλο «Information technology-related activities of internal auditors» πραγματοποίησαν μία έρευνα με σκοπό να δουν ποιες δραστηριότητες των εσωτερικών ελεγκτών έχουν σχέση με την πληροφοριακή τεχνολογία στις επιχειρήσεις των ΗΠΑ. Η έρευνα πραγματοποιήθηκε σε πάνω από 100 διευθυντές εσωτερικού ελέγχου και έδειξε ότι οι περισσότεροι ελεγκτές επικεντρώνονται κυρίως στους πιο συνηθισμένους κινδύνους και ελέγχους, όπως είναι η διαφύλαξη των περιουσιακών στοιχείων και η ακεραιότητα και η ασφάλεια των δεδομένων. Ενώ δεν δίνουν τόση μεγάλη σημασία σε άλλους κινδύνους όπως είναι οι κίνδυνοι που σχετίζονται με την ανάπτυξη και την προμήθεια των συστημάτων. Στην ουσία η έρευνα αυτή έδειξε το ίδιο αποτέλεσμα με την έρευνα του Abu-Musa που αναλύθηκε παραπάνω. Η έρευνα έδειξε επίσης, ότι η αξιολόγηση της πληροφοριακής τεχνολογίας από τους εσωτερικούς ελεγκτές επηρεάζεται από τη φύση των στόχων ελέγχου, από τα ελεγκτικά πληροφοριακά συστήματα και από τους υπολογιστές, από το προσωπικό του εσωτερικού ελέγχουν και από την ύπαρξη νέων πληροφοριακών συστημάτων (Hermanson et al, 2000).

Οι Hunton, Wright and Wright το 2004 στο άρθρο τους με τίτλο «Are financial auditors overconfident in their ability to assess risks associated with enterprise resource planning systems?» πραγματοποίησαν μία έρευνα, η οποία είχε δύο σκοπούς. Ο πρώτος στόχος της μελέτης αυτής ήταν να εξετάσει το βαθμό στον οποίο οι οικονομικοί ελεγκτές αναγνωρίζουν τους αυξημένους κίνδυνους που σχετίζονται με τον προγραμματισμό

επιχειρηματικών πόρων (ERP) συστήματα, σε σύγκριση με τα σύστημα μη-ERP (παλαιού τύπου). Ο δεύτερος στόχος ήταν να εκτιμηθεί η τάση των οικονομικών ελεγκτών να διαβουλεύονται με τους ειδικούς της τεχνολογίας των πληροφοριών (IT) λογιστικού ελέγχου εντός της εταιρείας τους, για την αξιολόγηση των κινδύνων των ERP και των συστημάτων μη-ERP στο στάδιο του σχεδιασμού του ελέγχου. Στην έρευνα συμμετείχαν 165 ελεγκτές. Πραγματοποιήθηκε ένα πείραμα στο οποίο συμμετείχαν 2 τύποι συστημάτων (ERP έναντι μη-ERP) και 2 κατηγορίες ελεγκτών (ειδικοί ελέγχου IT - οικονομικοί ελεγκτές). Και οι δύο τύποι ελεγκτών δηλώνουν ότι υπάρχουν περισσότεροι κίνδυνοι για διακοπή των επιχειρηματικών δραστηριοτήτων, μεγαλύτερη αλληλεξάρτηση και μεγαλύτερος έλεγχος των κινδύνων σε συστήματα ERP σε σχέση με τα μη ERP συστήματα. Επιπλέον, ενώ οι ειδικοί ελέγχου IT θεωρούν σημαντικά μεγαλύτερους τους κινδύνους δικτύου, των βάσεων δεδομένων και της ασφάλειας των εφαρμογών με το σύστημα ERP, δεν αναγνωρίζουν υψηλότερους κινδύνους ασφαλείας στις περιοχές αυτές. Οι κίνδυνοι που προκύπτουν με τα ERP συστήματα και με τα μη ERP συστήματα σε όλες τις κατηγορίες κινδύνου γίνονται πολύ πιο εύκολα αντιληπτοί από τους ειδικούς ελέγχου IT σε σχέση με τους οικονομικούς ελεγκτές. Επίσης, οι ελεγκτές πληροφοριακών συστημάτων όπως είναι λογικό ενδιαφέρονται περισσότερο για τους κινδύνους στα συστήματα ERP σε σχέση με τους οικονομικούς ελεγκτές. Τέλος, τα στοιχεία από τη μελέτη δείχνουν ότι συνολικά οι οικονομικοί ελεγκτές έχουν πολύ μεγάλη αυτοπεποίθηση στο να αξιολογούν τους κινδύνους των συστημάτων ERP (Hunton, 2004).

ΚΕΦΑΛΑΙΟ 3 ΦΟΡΕΙΣ IT AUDIT

Για να εκπαιδευτεί κανείς ώστε να γίνει ελεγκτής πληροφοριακών συστημάτων θα πρέπει να απευθυνθεί στους ειδικούς πιστοποιημένους φορείς που παρέχουν τις σχετικές άδειες. Στο παρόν κεφάλαιο θα παρουσιαστούν και θα αναλυθούν οι μεγαλύτεροι οργανισμοί και φορείς που σχετίζονται με την αδειοδότηση και την εκπαίδευση των IT auditors.

3.1 ΙΝΣΤΙΤΟΥΤΟ ΕΛΕΓΧΟΥ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ISACA (INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION)

Ένας από τους στόχους του Information Systems Audit and Control Association (ISACA) είναι να προωθήσει όλα τα πρότυπα που μπορούν να εφαρμοστούν έτσι ώστε να γίνει σωστή κατάρτιση και επιμόρφωση των ελεγκτών. Επίσης, το Ινστιτούτο Ελέγχου Συστημάτων Πληροφορικής έχει σαν στόχο την προαγωγή της ελεγκτικής επιστήμης, την προώθηση ελεύθερης ανταλλαγής μεθόδων και τεχνικών που αφορούν τον έλεγχο, την ασφάλεια των πληροφοριών, τον σωστό προσδιορισμό και την προώθηση των προτύπων, την επέκταση των γνώσεων του καθώς και την υποστήριξη επαγγελματικών πιστοποιήσεων. Η ανάπτυξη και η διάδοση των προτύπων ελέγχου πληροφοριακών συστημάτων είναι ο ακρογωνιαίος λίθος της επαγγελματικής συμβολής της ISACA στα ενδιαφερόμενα μέρη του ελέγχου.

Η έδρα της Information Systems Audit and Control Association - ISACA βρίσκεται στο Σικάγο και η εταιρεία απασχολεί περισσότερα από 50.000 άτομα. Η ISACA διαθέτει πάνω από 170 τοπικά παραρτήματα διάσπαρτα σε 60 χώρες. Η εταιρεία σχετίζεται με την ασφάλεια, τον έλεγχο και την έρευνα των υπολογιστών μιας επιχείρησης, μιας βιομηχανίας ή μιας κυβερνητικής οντότητας. Επίσης, πραγματοποιεί διάφορες εκπαιδευτικές διασκέψεις και εκδίδει το διμηνιαίο περιοδικό IS Audit and Control Journal. Η ISACA έχει καθιερώσει και ένα ίδρυμα (Foundation) για την έρευνα στον τομέα του IS audit, το IT Governance Institute (Ίδρυμα Διακυβέρνησης Τεχνολογίας Πληροφοριών), ως ένα ινστιτούτο μελετών για τους ρόλους και τις σχέσεις μεταξύ της τεχνολογίας πληροφοριών και της επιχειρηματικής διακυβέρνησης.

Παράλληλα, η ISACA υποστηρίζει το διεθνώς αναγνωρισμένο επάγγελμα του πιστοποιημένου ελεγκτή πληροφοριακών συστημάτων - CISA προορισμένο για τους πεπειραμένους ελεγκτές συστημάτων πληροφοριών (www.isaca.gr). Άλλες πιστοποιήσεις που παρέχονται από το ISACA είναι:

- Πιστοποίηση Υπεύθυνου Ασφάλειας Πληροφοριών (CISM - Certified Information Security Management)
- Πιστοποίηση στην Διακυβέρνηση της Πληροφοριακής Τεχνολογίας (CGEIT - Certified in the Governance of Enterprise IT)
- Πιστοποίηση στον Έλεγχο Κινδύνων και Πληροφοριακών Συστημάτων (CRISC - Certified in Risk and Information Systems Control)

3.1.1 Η πιστοποίηση CISA

Η πιστοποίηση CISA, εκτός της διεθνούς αναγνώρισης που τυγχάνει δημιουργεί τις συνθήκες και βοηθά στην επαγγελματική ανέλιξη των πιστοποιημένων επαγγελματιών. Συγκεκριμένα, περισσότεροι από 1200 άτομα από τη CISA πιστοποιημένα διεθνώς, απασχολούνται σε θέσεις CEO (Chief Executive Officer) & CFO (Chief Financial Officer), ενώ, περίπου 8900 άτομα από τη CISA πιστοποιημένα διεθνώς, απασχολούνται σε διευθυντικές θέσεις σχετικές με επιθεώρηση και κανονιστική συμμόρφωση.

Η διαδικασία που έχει θεσπιστεί από τον ISACA επιβάλλει για την απόκτηση της επαγγελματική πιστοποίηση CISA εφόσον:

1)υπάρχει πενταετής εμπειρία σε έλεγχο ή ασφάλεια πληροφορικών συστημάτων καθώς και σε κάποιο συναφές αντικείμενο

2)υπάρχει επιτυχία σε εξετάσεις που αφορούν τον έλεγχο και την ασφάλεια των πληροφοριακών συστημάτων

3)υπάρχει συμμόρφωση με την πολιτική συνεχούς επιμόρφωσης (continuing professional education policy)

Η πιστοποίηση CISA πληροί τις απαιτήσεις που έχουν τεθεί από το πρότυπο ISO/IEC 17024. Το τελευταίο καθορίζει τις προδιαγραφές που πρέπει να πληρούν οι οργανισμοί που παρέχουν πιστοποιήσεις και ο έλεγχος έγινε από το ANSI (American National Standards Institute) (www.isaca.gr).

Στην Ελλάδα, οι εξετάσεις CISA διενεργούνται 2 φορές ετησίως (Ιούνιο και Δεκέμβριο) στις εγκαταστάσεις της Ελληνοαμερικανικής Ένωσης.

Για να συμμετάσχει κάποιος στις εξετάσεις η ISACA διαθέτει στην ιστοσελίδα το υλικό που πρέπει να μελετήσει ο υποψήφιος ώστε να προετοιμαστεί για τις εξετάσεις CISA. Το υλικό αυτό διατίθεται σε διάφορες γλώσσες αλλά όχι στα Ελληνικά

Χαρακτηριστικά αναφέρονται τα:

- Study Materials: How to Write a Study Material CISA Item
- CISA Review Manual 26th Edition
- CISA Review Questions, Answers & Explanations Manual
- CISA Review Questions, Answers & Explanations Database

Επίσης, διατίθενται από την ISACA και κάποια online σεμινάρια (Virtual Instructor-Led Training). Πολύ έμπειροι εκπαιδευτές με την χρήση του διαδικτύου παραδίδουν σεμινάρια όπου παρουσιάζουν παραδείγματα και δίνουν τις απαραίτητες οδηγίες για την εξέλιξη των εκπαιδευομένων ελεγκτών.

Για την προετοιμασία των υποψηφίων ελεγκτών έχουν δομηθεί 5 μαθήματα-ενότητες που πρέπει να μελετηθούν ώστε να είναι σε θέση οι υποψήφιοι να απαντήσουν στις 150 ερωτήσεις του τεστ. Αναλυτικότερα:

- 1. Η διαδικασία του ελέγχου Πληροφοριακών Συστημάτων (The Process of Auditing Information Systems).

  Εξετάζει κατά πόσο ο υποψήφιος γνωρίζει την διαδικασία παροχής υπηρεσιών ελέγχου, σύμφωνα με τα πρότυπα ελέγχου πληροφοριακού συστήματος με στόχο την προστασία της εταιρίας/του οργανισμού κατά τον έλεγχο των πληροφοριακών συστημάτων.

  <u>Δράσεις που πρέπει να μπορεί ο υποψήφιος να κάνει:</u>

- Σχέδιο ελέγχου των κινδύνων που βασίζεται στη συμμόρφωση με τα πρότυπα λογιστικού ελέγχου ώστε να εξασφαλιστούν οι περιοχές του συστήματος που ελέγχθηκαν
- Σχέδιο ειδικού ελέγχου για να διαπιστωθεί αν τα πληροφοριακά συστήματα προστατεύονται, ελέγχονται και να προσφέρουν στην εταιρία/στον οργανισμό
- Διεξαγωγή ελέγχων σύμφωνα με το πρότυπα ελέγχου Πληροφοριακών Συστημάτων για την επίτευξη των στόχων προγραμματισμένου ελέγχου
- Ενημέρωση για τα αποτελέσματα του ελέγχου και παροχή συστάσεων μέσω συνεδριάσεων και εκθέσεων ελέγχου για την προώθηση των απαραίτητων αλλαγών, εφόσον είναι απαραίτητες
- Επικοινωνία μετά την διεξαγωγή του ελέγχου ώστε να διαπιστωθεί αν έχουν ληφθεί τα κατάλληλα μέτρα από τη διοίκηση μέσα σε εύλογο χρονικό διάστημα

Απαιτούμενες γνώσεις:

- Γνώση των προτύπων ISACA για έλεγχο και διασφάλισης, κατευθυντήριες γραμμές, εργαλεία και τεχνικές. Γνώση του Κώδικα Επαγγελματικής Δεοντολογίας
- Γνώση της έννοιας αξιολόγηση κινδύνων, των εργαλείων και των τεχνικών που απαιτούνται για το σχεδιασμό, την εξέταση, την υποβολή εκθέσεων αλλά και την παρακολούθηση
- Γνώση των βασικών επιχειρηματικών διαδικασιών (π.χ., αγορά, μισθοδοσίας, πληρωτέους λογαριασμούς, λογαριασμούς εισπρακτέους) και γνώση του ρόλου του Πληροφοριακού Συστήματος σε αυτές τις διαδικασίες
- Γνώση των αρχών ελέγχου που σχετίζονται με τους ελέγχους στα πληροφοριακά συστήματα
- Γνώση του σχεδιασμού του ελέγχου καθώς και των τεχνικών διαχείρισης του ελέγχου, διαχείριση του ρίσκου συμπεριλαμβανομένης και της παρακολούθησης

- ❖ Γνώση των ισχυόντων νόμων και κανονισμών που επηρεάζουν το πεδίο του ελέγχου, τη συλλογή και τη διατήρηση αποδεικτικών στοιχείων καθώς και τη συχνότητα των ελέγχων
- ❖ Γνώση των τεχνικών συλλογής αποδεικτικών στοιχείων (π.χ. παρατήρηση, έρευνα, έλεγχος, συνέντευξη, η ανάλυση των δεδομένων, εγκληματολογικές τεχνικές έρευνας, τεχνικές ελέγχου με τη βοήθεια υπολογιστή [CAATs]) που χρησιμοποιούνται για τη συλλογή, την προστασία και τη διατήρηση των ελεγκτικών τεκμηρίων
- ❖ Γνώση των διαφορετικών μεθοδολογιών δειγματοληψίας και άλλες αναλυτικές διαδικασίες
- ❖ Γνώση σύνταξης τεχνικών εκθέσεων και επικοινωνίας (π.χ., τη διευκόλυνση, τη διαπραγμάτευση, την επίλυση συγκρούσεων, δομή της έκθεσης ελέγχου, θέμα της έκθεσης, διαχείριση της περίληψης και τον έλεγχο των αποτελεσμάτων)
- ❖ Η γνώση των διασφάλισης ποιότητας για τη διασφάλιση της ποιότητας του ελέγχου
- ❖ Η γνώση των διαφόρων τύπων των ελέγχων (π.χ., εσωτερικές, εξωτερικές, οικονομικές) και των μεθόδων για την αξιολόγηση

- 2. Διακυβέρνησης και διαχείρισης της πληροφορικής (Governance and Management of IT).

  Επιβεβαιώνεται ότι ο εξεταζόμενος διαθέτει τις απαραίτητες ηγετικές και οργανωτικές γνώσεις.

  <u>Δράσεις που πρέπει να μπορεί ο υποψήφιος να κάνει:</u>

  - ❖ Αξιολόγηση της στρατηγικής σχετικά με την πληροφορική καθώς και τις διαδικασίες για την ανάπτυξη, την έγκριση, την υλοποίηση και τη συντήρηση τους
  - ❖ Αξιολόγηση της αποτελεσματικότητας της διαχείρισης της πληροφορικής ώστεν να καθορίσει αν οι αποφάσεις της πληροφορικής, οι κατευθύνσεις και οι επιδόσεις είναι οι αναμενόμενες σύμφωνα με τους στόχους

- Αξιολόγηση της οργανωτικής δομής και των ανθρώπινων πόρων (του προσωπικό) για να εξακριβώσει αν υποστηρίζουν τις στρατηγικές και τους στόχους
- Αξιολόγηση των πολιτικών της πληροφορικής, τα πρότυπα και των διαδικασίων για να εξακριβώσει αν υποστηρίζουν τη στρατηγική της πληροφορικής και αν συμμορφώνονται με τις ρυθμιστικές και νομικές απαιτήσεις.
- Αξιολόγηση της διαχείριση των πόρων, συμπεριλαμβανομένων των επενδύσεων, των προτεραιοτήτων, της κατανομής και της χρήσης
- Αξιολόγηση του χαρτοφυλακίου πληροφορικής, συμπεριλαμβανομένων των επενδύσεων και των προτεραιοτήτων
- Αξιολόγηση των πρακτικών διαχείρισης κινδύνου για να καθοριστεί αν αξιολογούνται, παρακολουθούνται, καταγράφονται και διαχειρίζονται σωστά οι πιθανοί κίνδυνοι
- Αξιολόγηση των ελέγχων (π.χ., συνεχής παρακολούθηση, τη διασφάλιση της ποιότητας [QA])
- Αξιολόγηση της παρακολούθησης και της υποβολής εκθέσεων για να ελεγχθεί αν υπάρχει επαρκή και έγκαιρη πληροφόρηση
- Αξιολόγηση της επιχειρησιακής συνέχειας της εταιρίας καθώς και του σχεδίου αποκατάστασης των καταστροφών για να καθοριστεί αν η εταιρία είναι ικανή να συνεχίσει τις βασικές τις δραστηριότητες κατά την περίοδο μιας καταστροφής του πληροφοριακού συστήματος

Απαιτούμενες γνώσεις:

- Γνώση του σκοπού της στρατηγικής πληροφορικής, τις πολιτικές, τα πρότυπα και των διαδικασιών
- Γνώση της διακυβέρνησης, της διαχείρισης, της ασφάλειας, των πλαισίων ελέγχου, των σχετικών προτύπων, των κατευθυντήριων γραμμών και των πρακτικών
- Γνώση της οργανωτικής δομής, των ρόλων και των ευθυνών που σχετίζονται με την πληροφορική, συμπεριλαμβανομένου του διαχωρισμού των καθηκόντων

- Η γνώση των σχετικών νόμων, κανονισμών και προτύπων που επηρεάζουν την εταιρία/τον οργανισμό
- Γνώση της κατεύθυνσης της τεχνολογίας της εταιρίας/του οργανισμού, της αρχιτεκτονικής και των επιπτώσεων τους
- Γνώση των διαδικασιών για την ανάπτυξη, την εφαρμογή και την συντήρηση της στρατηγικής πληροφορικής
- Γνώση της χρήσης των μοντέλων ικανότητας και την ωριμότητας
- Γνώση των τεχνικών βελτιστοποίησης των διαδικασιών
- Η γνώση της διαχείρισης των πόρων πληροφορικής (π.χ., διαχείριση χαρτοφυλακίου, τη διαχείριση αξίας, της διαχείρισης του προσωπικού)
- Η γνώση της επιλογής του κατάλληλου προμηθευτή πληροφορικής, τη διαχείριση των συμβάσεων, τις διαδικασίες διαχείρισης των σχέσεων και την παρακολούθηση των επιδόσεων
- Η γνώση της διαχείρισης επιχειρηματικού κινδύνου
- Η γνώση για την παρακολούθηση των πρακτικών και της υποβολής εκθέσεων σχετικά με τους ελέγχους απόδοσης (π.χ., συνεχής παρακολούθηση, τη διασφάλιση της ποιότητας)
- Η γνώση της διαχείρισης της ποιότητας και των συστημάτων διασφάλισης ποιότητας
- Η γνώση των πρακτικών για την παρακολούθηση και την υποβολή εκθέσεων σχετικά με την απόδοση της πληροφορικής (π.χ. τους βασικούς δείκτες απόδοσης)
- Η γνώση της ανάλυσης των επιπτώσεων στις επιχειρήσεις
- Η γνώση των κανόνων και των διαδικασιών για την ανάπτυξη, τη συντήρηση και τη δοκιμή του σχεδίου επιχειρησιακής συνέχειας
- Η γνώση των διαδικασιών που χρησιμοποιούνται για να επικαλεστεί και να εκτελέσει το σχέδιο επιχειρησιακής συνέχειας ώστε να επιστρέψει η εταιρία στην κανονική της λειτουργία

- 3. Απόκτηση, Ανάπτυξη και Λειτουργία Πληροφοριακού Συστήματος (Information Systems Acquisition, Development and Implementation)

  Διασφαλίζει ότι ο υποψήφιος διαθέτει τις ικανότητες για την παρακολούθηση της απόκτησης, της ανάπτυξης και τις σωστής λειτουργίας των εφαρμογών του πληροφοριακού συστήματος σύμφωνα με τους στόχους της εταιρίας/του οργανισμού.

  <u>Δράσεις που ο υποψήφιος πρέπει να μπορεί να κάνει:</u>

  - ❖ Αξιολόγηση των επενδύσεων που σκοπεύουν να κάνουν οι επιχειρήσεις σε πληροφοριακά συστήματα, την ανάπτυξη τους και τη συντήρηση τους
  - ❖ Αξιολόγηση των διαδικασιών για την επιλογή προμηθευτή για την προμήθεια πληροφοριακού συστήματος και τη διαχείριση των συμβάσεων
  - ❖ Αξιολόγηση του πλαισίου διαχείρισης του έργου και των απαραίτητων ελέγχων για να διαπιστωθεί αν ικανοποιούνται οι ανάγκες της επιχείρησης
  - ❖ Διεξαγωγή ελέγχων για να καθοριστεί αν η υλοποίηση του πληροφοριακού συστήματος προχωρά σύμφωνα με τα σχέδια του έργου, υποστηρίζεται επαρκώς από έγγραφα, και έχει έγκαιρη και ακριβή αναφορά κατάστασης.
  - ❖ Αξιολόγηση του συστήματος ελέγχου για των πληροφορίων κατά τις φάσεις των απαιτήσεων, της απόκτησης, της ανάπτυξης αλλά και των δοκιμών
  - ❖ Αξιολόγηση της ετοιμότητας των πληροφοριακών συστημάτων για την εφαρμογή και τη λειτουργία στην παραγωγή ώστε να διαπιστωθεί ότι καλύπτονται οι ανάγκες της εταιρίας
  - ❖ Διεξαγωγή ελέγχων μετά την υλοποίηση του πληροφοριακού συστήματος για να καθοριστεί αν υλοποιούνται τα παραδοτέα σύμφωνα με τις απαιτήσεις της εταιρίας/του οργανισμού

  <u>Οι γνώσεις που απαιτούνται:</u>

  - ❖ Γνώση του οφέλους που θα έχει η εταιρία (π.χ., μελέτες σκοπιμότητας, περιπτώσεις επιχειρήσεων, το συνολικό κόστος ιδιοκτησίας, η απόδοση των επενδύσεων)

- Γνώση της πρακτικής διαχείρισης των προμηθειών και των προμηθευτών σχετικών με το πληροφοριακό σύστημα (π.χ., διαδικασία αξιολόγησης και επιλογής, της διαχείρισης των συμβάσεων, τον κίνδυνο πωλητή και διαχείριση των σχέσεων, μεσεγγύησης, αδειών λογισμικού), συμπεριλαμβανομένων των εξωτερικών αναθέσεων σε τρίτους
- Γνώση των μηχανισμών υλοποίησης του έργου (π.χ., συντονιστική επιτροπή, επιτροπή εποπτείας, το γραφείο διαχείρισης του έργου)
- Γνώση του πλαισίου ελέγχου της διαχείρισης του έργου
- Γνώση των πρακτικών διαχείρισης κινδύνων που εφαρμόζονται στα έργα
- Γνώση της ανάλυσης απαιτήσεων και πρακτικών διαχείρισης (π.χ., τις απαιτήσεις ελέγχου, την ιχνηλασιμότητα, την ανάλυση των ελλείψεων, η διαχείριση ευπάθεια, απαιτήσεις ασφαλείας)
- Γνώση της δομής της επιχείρησης που σχετίζεται με δεδομένα, εφαρμογές και τεχνολογία
- Γνώση της μεθοδολογίας και των εργαλείων ανάπτυξης του συστήματος, συμπεριλαμβανομένων των πλεονεκτημάτων και των αδυναμιών του
- Γνώση των στόχων και των τεχνικών ελέγχου που εξασφαλίζουν την πληρότητα, την ακρίβεια, την εγκυρότητα των συναλλαγών και των δεδομένων
- Γνώση των μεθόδων δοκιμών και των πρακτικών που σχετίζονται με την λειτουργία του πληροφοριακού συστήματος
- Γνώση των διαδικασιών διαχείρισης που σχετίζονται με την ανάπτυξη του πληροφοριακού συστήματος
- Γνώση των μηχανισμών ανάπτυξης των υποδομών, των πρακτικών και των εργαλείων
- Γνώση των κριτηρίων επιτυχίας του έργου και του ρίσκου κατά την υλοποίηση του
- Γνώση των στόχων και της διαδικασίας ανασκόπηση του μετά την ολοκλήρωση της υλοποίησης του (π.χ. κλείσιμο του έργου, υλοποίηση του ελέγχου, μέτρηση των επιδόσεων)

- 4. Λειτουργία, συντήρηση και διαχείριση του πληροφοριακού συστήματος (Information Systems Operations, Maintenance and Service Management)
  Διασφαλίζει ότι ο υποψήφιος γνωρίζει τις διαδικασίες σχετικά με τη λειτουργία, τη συντήρηση και τη διαχείριση πληροφοριακών συστημάτων

  <u>Δράσεις που ο υποψήφιος πρέπει να μπορεί να κάνει:</u>

  - ❖ Αξιολόγηση του πλαισίου διαχείρισης υπηρεσιών πληροφορικής και πρακτικές για να διαπιστωθεί αν οι έλεγχοι και τα επίπεδα εξυπηρέτησης τηρούνται
  - ❖ Διεξαγωγή περιοδικών αξιολογήσεων των πληροφοριακών συστημάτων για να διαπιστώσει αν εξακολουθούν να πληρούν τους στόχους της εταιρίας/του οργανισμού
  - ❖ Αξιολόγηση των εργασιών πληροφορικής (π.χ., προγραμματισμός εργασιών, διαχείριση της διάρθρωσης, ικανότητα στη διαχείριση των επιδόσεων) για να διαπιστώσει αν ελέγχονται αποτελεσματικά
  - ❖ Αξιολόγηση των συντηρήσεων και των αναβαθμίσεων ώστε να διαπιστώσει αν πραγματοποιήθηκαν αποτελεσματικά
  - ❖ Αξιολόγηση των πρακτικών διαχείρισης βάσεων δεδομένων που καθορίζουν την ακεραιότητα και τη βελτιστοποίηση των βάσεων δεδομένων.
  - ❖ Αξιολόγηση της ποιότητας των δεδομένων και της διαχείρισης του κύκλου ζωής για να διαπιστώσει αν εξακολουθούν να υλοποιούνται οι στρατηγικοί στόχοι
  - ❖ Αξιολόγηση των προβλημάτων και της διαχείρισης των περιστατικών για να διαπιστωθεί αν τα προβλήματα και τα περιστατικά ανιχνεύονται, αναλύονται, καταγράφονται και επιλύονται έγκαιρα
  - ❖ Αξιολόγηση των πρακτικών διαχείρισης για να καθορίσει αν οι αλλαγές που γίνονται στο σύστημα και στις εφαρμογές ελέγχονται επαρκώς
  - ❖ Αξιολόγηση των υπολογιστών των χρηστών για να ελεγχθεί εάν οι ακολουθούνται σωστά οι διαδικασίες
  - ❖ Αξιολόγηση της συνέχειας και της ανθεκτικότητας (backup, σχέδιο αποκατάστασης των καταστροφών) για να διαπιστώσει αν διατηρούνται σύμφωνα με τους κανόνες

Οι γνώσεις που απαιτούνται:

- Γνώση του πλαισίου διαχείρισης υπηρεσιών
- Γνώση των πρακτικών διαχείρισης των υπηρεσιών και της διαχείρισης σε επίπεδο υπηρεσιών
- Γνώση των τεχνικών για την παρακολούθηση της απόδοσης των τρίτων και τη συμμόρφωση τους με τις συμφωνίες παροχής υπηρεσιών
- Γνώση της δομής της επιχείρησης
- Γνώση των βασικών εννοιών της πληροφορικής τεχνολογίας (π.χ. το υλικό και το δίκτυο, λογισμικό συστήματος, middleware, συστήματα διαχείρισης βάσεων δεδομένων)
- Γνώση των εργαλείων και τεχνικών αντοχής του συστήματος (π.χ., το υλικό ανοχή σφαλμάτων, την εξάλειψη της μοναδικό σημείο αποτυχίας, clustering)
- Γνώση της διαχείρισης IT περιουσιακών στοιχείων, αδειών λογισμικού, διαχείρισης πηγαίου κώδικα και των πρακτικών απογραφής
- Γνώση των πρακτικών προγραμματισμού εργασιών
- Γνώση των τεχνικών ελέγχου που εξασφαλίζουν την ακεραιότητα του συστήματος
- Ικανότητα σχεδιασμού και διαχείρισης των σχετικών εργαλείων παρακολούθησης και τεχνικές
- Η γνώση των διαδικασιών παρακολούθησης της απόδοσης των συστημάτων, εργαλεία και τεχνικές
- Η γνώση της δημιουργίας αντιγράφων ασφαλείας των δεδομένων, της αποθήκευσης, της συντήρησης και των πρακτικών αποκατάστασης
- Η γνώση της διαχείρισης βάσεων δεδομένων και των πρακτικών βελτιστοποίησης
- Η γνώση της ποιότητας των δεδομένων (πληρότητα, ακρίβεια, ακεραιότητα) και της διαχείρισης του κύκλου ζωής (γήρανση, κατακράτηση)
- Η γνώση των πρακτικών διαχείρισης προβλημάτων και συμβάντων
- Η γνώση της διαχείρισης της αλλαγής, διαχείριση διαμόρφωσης, διαχείριση απελευθέρωσης και των πρακτικών διαχείρισης
- Η γνώση του λειτουργικού κινδύνου και τους ελέγχους που σχετίζονται με την πληροφορική

- ❖ Η γνώση των κανονιστικών, νομικών, συμβατικών και ασφαλιστικών θεμάτων που σχετίζονται με την αποκατάσταση καταστροφών
- ❖ Γνώση των επιπτώσεων στις επιχειρήσεις που σχετίζονται με τον προγραμματισμό αποκατάστασης των καταστροφών
- ❖ Γνώση της ανάπτυξης και της συντήρησης των σχεδίων αποκατάστασης καταστροφών
- ❖ Η γνώση σχετικά με τα οφέλη και τα μειονεκτήματα των εναλλακτικών χώρων επεξεργασίας (π.χ., ζεστές ή ψυχρές τοποθεσίες)
- ❖ Η γνώση των μεθόδων δοκιμής αποκατάστασης των καταστροφών
- ❖ Η γνώση των διαδικασιών που χρησιμοποιούνται για να ενεργοποιηθούν τα σχέδια ανάκαμψης από καταστροφή

- 5. Προστασία των πληροφοριών

  Διασφαλίζει ότι ο υποψήφιος γνωρίζει τις πολιτικές, τα πρότυπα, τις διαδικασίες και τους ελέγχους του οργανισμού για την εμπιστευτικότητα, την ακεραιότητα των πληροφοριών

  <u>Δράσεις που ο υποψήφιος πρέπει να μπορεί να κάνει:</u>

  - ❖ Αξιολόγηση της ασφάλειας των πληροφοριών και της προστασίας της ιδιωτικής ζωής με βάση τις πολιτικές, τα πρότυπα και τις διαδικασίες για την πληρότητα και την ευθυγράμμιση με τις γενικά αποδεκτές πρακτικές και τη συμμόρφωση με τις ισχύουσες εξωτερικές απαιτήσεις.
  - ❖ Αξιολόγηση του σχεδιασμού, της υλοποίησης, της συντήρησης, της παρακολούθησης και της υποβολής εκθέσεων των φυσικών και περιβαλλοντικών ελέγχων για να διαπιστωθεί αν τα περιουσιακά στοιχεία και οι πληροφορίες διαφυλάσσονται κατάλληλα
  - ❖ Αξιολόγηση του σχεδιασμού, της υλοποίησης, της συντήρησης, της παρακολούθησης και της υποβολής εκθέσεων σχετικά με το σύστημα και τη λογική του ελέγχου ασφαλείας για την επαλήθευση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών.

- Αξιολόγηση του σχεδιασμού, της υλοποίησης και της παρακολούθησης των διεργασιών και των διαδικασιών ταξινόμησης των δεδομένων για της ευθυγράμμισης με τις πολιτικές του οργανισμού, τα πρότυπα, τις διαδικασίες και τις ισχύουσες εξωτερικές απαιτήσεις.
- Αξιολόγηση των διεργασιών και των διαδικασιών που χρησιμοποιούνται για την αποθήκευση, την ανάκτηση, τη μεταφορά και τη διάθεση των περιουσιακών στοιχείων για να προσδιορίσει αν τα περιουσιακά στοιχεία και οι πληροφορίες που διαφυλάσσονται κατάλληλα.
- Αξιολόγηση του προγράμματος ασφάλειας των πληροφοριών για τον προσδιορισμό της αποτελεσματικότητας και την ευθυγράμμισή της με τις στρατηγικές και τους στόχους της οργάνωσης

Οι γνώσεις που απαιτούνται:

- Η γνώση από τις γενικά αποδεκτές πρακτικές και τις εξωτερικές απαιτήσεις (π.χ. τους νόμους, τους κανονισμούς κλπ.) που σχετίζονται με την προστασία των περιουσιακών στοιχείων και των πληροφοριών
- Γνώση των αρχών της προστασίας της ιδιωτικής ζωής
- Γνώση των τεχνικών για το σχεδιασμό, την υλοποίηση, τη συντήρηση, την παρακολούθηση και την υποβολή εκθέσεων σχετικά με τους ελέγχους ασφαλείας
- Γνώση των φυσικών και περιβαλλοντικών ελέγχων και την υποστήριξη των πρακτικών που σχετίζονται με την προστασία των περιουσιακών στοιχείων των πληροφοριών
- Γνώση των φυσικών ελέγχων πρόσβασης για τον εντοπισμό, τον έλεγχο ταυτότητας και τον περιορισμό των χρηστών σε εγκεκριμένες εγκαταστάσεις και υλικό
- Γνώση των λογικών ελέγχου πρόσβασης για τον εντοπισμό, τον έλεγχο ταυτότητας και τον περιορισμό των χρηστών σε εξουσιοδοτημένους λειτουργίες και δεδομένα

- Γνώση των ελέγχων ασφαλείας που σχετίζονται με το υλικό, το λογισμικό του συστήματος (π.χ. εφαρμογές, λειτουργικά συστήματα) και τα συστήματα διαχείρισης βάσεων δεδομένων.
- Η γνώση του κινδύνου και των ελέγχων που σχετίζονται με το virtualization των συστημάτων
- Η γνώση του κινδύνου και των ελέγχων που σχετίζονται με τη χρήση των κινητών και των ασύρματων συσκευών, συμπεριλαμβανομένων προσωπικών συσκευών (BYOD)
- Η γνώση της ασφάλειας της φωνητικής επικοινωνίας (π.χ. PBX, Voice-over Internet Protocol [VoIP])
- Η γνώση του δικτύου και της ασφάλειας στο Διαδίκτυο, τα πρωτόκολλα και τις τεχνικές
- Η γνώση της διαμόρφωσης, της υλοποίησης, της λειτουργίας και της συντήρησης των ελέγχων ασφάλειας του δικτύου
- Η γνώση των τεχνικών κρυπτογράφησης που σχετίζονται και οι χρήσεις τους
- Η γνώση της υποδομής δημόσιου κλειδιού, τα κατασκευαστικά στοιχεία και τις τεχνικές της ψηφιακής υπογραφής
- Η γνώση του κινδύνου και των ελέγχων που σχετίζονται με peer-to-peer computing, instant messaging, και web-based τεχνολογία (π.χ. κοινωνική δικτύωση, πίνακες μηνυμάτων, τα blogs, το cloud computing)
- Η γνώση των κανόνων ταξινόμησης των δεδομένων που σχετίζονται με την προστασία των περιουσιακών στοιχείων και των πληροφοριών
- Η γνώση των διεργασιών και διαδικασιών που χρησιμοποιούνται για την αποθήκευση, την ανάκτηση, τη μεταφορά και τη διάθεση των εμπιστευτικών στοιχείων ενεργητικού πληροφοριών
- Η γνώση του κινδύνου και των ελέγχων που σχετίζονται με τη διαρροή δεδομένων
- Η γνώση του κινδύνου για την ασφάλεια και τους ελέγχους που σχετίζονται με τον τελικό χρήστη
- Η γνώση των μεθόδων για την εφαρμογή ενός προγράμματος ευαισθητοποίησης σε θέματα ασφάλειας
- Η γνώση των μεθόδων επίθεσης σύστημα πληροφοριών και τεχνικών

- ❖ Η γνώση των εργαλείων πρόληψης και ανίχνευσης και των τεχνικών ελέγχου
- ❖ Η γνώση των τεχνικών δοκιμών ασφαλείας (π.χ., δοκιμές διείσδυσης, ευπάθεια σάρωσης)
- ❖ Η γνώση των διαδικασιών που σχετίζονται με την παρακολούθηση και την αντιμετώπιση περιστατικών ασφάλειας (π.χ. διαδικασίες κλιμάκωσης, η ομάδα έκτακτης ανάγκης η αντιμετώπιση περιστατικών)
- ❖ Η γνώση των διεργασιών που ακολούθησαν στη διερεύνηση της εγκληματολογίας και των διαδικασιών συλλογής και διατήρησης των δεδομένων και των αποδεικτικών στοιχείων (δηλαδή, αλυσίδα φύλαξης).
- ❖ Η γνώση των παραγόντων κινδύνου απάτης που σχετίζονται με την προστασία των περιουσιακών στοιχείων των πληροφοριών

Για την διευκόλυνση των υποψηφίων έχει δημιουργηθεί από την ISACA αποκλειστικά για τους υποψηφίους μια online κοινότητα όπου μπορούν να ανταλλάσσουν ιδέες, εμπειρίες και απορίες ώστε να μπορούν να προετοιμαστούν σωστά για τις εξετάσεις.

Τέλος, η ISACA παρέχει στους υποψήφιους έναν Οδηγό πληροφοριών που περιέχει πληροφορίες σχετικά με την εγγραφή τις εξετάσεις, τις ημερομηνίες που θα διεξαχθούν, τις προθεσμίες για τις διοικήσεις των εξετάσεων, καθώς και τους κανόνες που πρέπει να τηρηθούν την ημέρα των εξετάσεων.

3.2 ΑΛΛΟΙ ΦΟΡΕΙΣ ΕΛΕΓΧΟΥ

Εκτός από το ISACA, υπάρχουν και άλλοι φορείς ελέγχου, που παρέχουν αναγνωρισμένες πιστοποιήσεις, και παρουσιάζονται παρακάτω:

- Ινστιτούτο Εσωτερικών Ελέγχων IIA (Institute of Internal Auditors- 1941). Παρέχει το πιστοποιητικό Εσωτερικού Ελεγκτή CIA (Certified Internal Auditor), που διασφαλίζει ικανοποιητικό επίπεδο γνώσεων σχετικά με θέματα που αφορούν τον έλεγχο της πληροφοριακής τεχνολογίας. Επίσης, παρέχει το πιστοποιητικό ελέγχου αυτοαξιολόγησης (CCSA- Certification in Control Self- Assessment), το

πιστοποιητικό στην ελεγκτική διακυβέρνησης (CGAP- Certified Government Auditing Professional) και στην ελεγκτική χρηματοοικονομικών υπηρεσιών (CFSA- Certified Financial Services Auditor) (ww.theiia.org).

- Η Ένωση Επικυρωμένων Εξεταστών Απάτης (ACFE - Association of Certified Fraud Examiners- 1988), που παρέχει την πιστοποίηση CFE σε επαγγελματίες που ειδικεύονται στην απάτη

- Το Αμερικανικό Ινστιτούτο Ορκωτών Λογιστών (AICPA - American Institute of Certified Public Accountants- 1957), που παρέχει την πιστοποίηση CPA για τους ορκωτούς ελεγκτές λογιστές και την CITP για θέματα πληροφοριακής τεχνολογίας

- Ο Διεθνής Οργανισμός Πιστοποίησης Ασφάλειας Πληροφοριακών Συστημάτων (ISC)2 (International Information Systems Security Certification Consortium- 1988), που παρέχει την πιστοποίηση ασφάλειας πληροφοριακών συστημάτων (CISSP - Certified Information Systems Security Professional)

ΚΕΦΑΛΑΙΟ 4 ΔΟΜΗ ΜΑΘΗΜΑΤΟΣ IT AUDIT

4.1 ΣΤΟΧΟΙ ΜΑΘΗΜΑΤΟΣ

Οι βασικοί στόχοι ενός μαθήματος που σχετίζονται με τον έλεγχο πληροφοριακών συστημάτων είναι να οι μαθητές να αποκτήσουν το κατάλληλο θεωρητικό υπόβαθρο και να αποκτήσουν τις κατάλληλες γνώσεις που απαιτούνται για να τις εφαρμόσουν στην πράξη. Ο εκπαιδευόμενος πρέπει αρχικά να κατανοήσει τους λόγους που είναι απαραίτητος ο έλεγχος. Ο έλεγχος είναι απαραίτητος προκειμένου να διαπιστωθεί εάν και σε ποιο βαθμό τα πληροφοριακά συστήματα των επιχειρήσεων βοηθούν στην διαφύλαξη των στοιχείων του ενεργητικού, στην διασφάλιση της ακεραιότητας των δεδομένων, στην αποτελεσματική λειτουργία προκειμένου να επιτευχθούν οι στόχοι της επιχείρησης και στην αποδοτικότερη χρήση των πόρων της επιχείρησης. Επίσης, πρέπει να κατανοήσει και ποιοι είναι οι κίνδυνοι που ελλοχεύουν. Οι κίνδυνοι αυτοί μπορεί να προέρχονται είτε από το εξωτερικό είτε από το εσωτερικό περιβάλλον μιας επιχείρησης και μπορεί να εμφανιστούν σε κάθε στάδιο και σε κάθε λειτουργία της επιχείρησης. Οι κίνδυνοι αυτοί μπορεί να σχετίζονται με την

ασφάλεια των πληροφοριακών συστημάτων και μπορεί να οφείλονται και σε ανθρώπινο λάθος ή παρέμβαση. Πρέπει επιπλέον, να γνωρίζει τις απειλές και τα προβλήματα που προκύπτουν και αφορούν την ασφάλεια. Οι εκπαιδευόμενοι πρέπει να αποκτήσουν τις απαραίτητες γνώσεις στα εργαλεία λογισμικού, έτσι ώστε να μπορούν να έχουν πρόσβαση στην ανάλυση και στην διεξαγωγή των δεδομένων.

Παρατίθενται οι εξής συχνότεροι και μείζονες στόχοι:

- Κατανόηση των κινδύνων, των απειλών και των ευπαθειών ενός συστήματος
- Κατανόηση του σχεδιασμού της στρατηγικής και των διαδικασιών πραγματοποίησης του εσωτερικού ελέγχου
- Εκμάθηση μοντέλων και εργαλείων λογισμικού που σχετίζονται με τον έλεγχο, την πρόληψη και την αντιμετώπιση των κινδύνων
- Κατανόηση της ηθικής της πληροφορικής και του διαδικτύου
- Προετοιμασία για τις διαθέσιμες πιστοποιήσεις του ελεγκτή πληροφοριακών συστημάτων
- Κατανόηση του προτύπου COBIT

Πανεπιστημιακό Ίδρυμα	**Κύριοι Στόχοι**
University at Buffalo	• Κατανόηση του ρόλου του ελεγκτή και της διαδικασίας ελέγχου ΠΣ • Κατανόηση ελέγχου συστημάτων και δεδομένων • Κατανόηση πολιτικών προστασίας, μοντέλων και προβλημάτων
Nova Southeastern University	• Κατανόηση θεμελιωδών εννοιών που σχετίζονται με τον έλεγχο ΠΣ

	• Κατανόηση αρχών και πρακτικών που σχετίζονται με την ασφαλή λειτουργία των ΠΣ • Ανάπτυξη αντικειμένων εσωτερικού ελέγχου και πλαισίων • Αναγνώριση κατάλληλων διαδικασιών ελέγχου
School of Accountancy Georgia State University	• Ανάπτυξη στόχων διασφάλισης από τους κινδύνους ΠΣ • Σχεδιασμός διαδικασιών ασφάλειας • Εφαρμογή διαδικασιών ασφάλειας με εργαλεία λογισμικού
Baruch College, Zicklin School of Business	• Κατανόηση της ασφάλειας ΠΣ • Αναγνώριση κινδύνων και αντικειμένων που χρήζουν ελέγχου • Σχεδιασμός κατάλληλων διαδικασιών ελέγχου • Επιλογή λογισμικού ελέγχου • Γνώση προτύπων
University of North Carolina	• Κατανόηση γενικού πλαισίου που αφορά κινδύνους και έλεγχο ΠΣ • Κατανόηση των σημείων ελέγχου και των διαδικασιών για τον έλεγχο διαχείρισης δεδομένων

	• Κατανόηση των συστημάτων ηλεκτρονικού εμπορίου που σχετίζονται με τον έλεγχο και την ασφάλεια • Κατανόηση ζητημάτων που σχετίζονται με την ηθική των υπολογιστών

4.2 ΠΡΟΑΠΑΙΤΟΥΜΕΝΑ

Η εκπαίδευση που σχετίζεται με τα πληροφοριακά συστήματα και τον έλεγχό τους, δεν συγκαταλέγεται στα βασικά μαθήματα εκπαίδευσης. Συνεπώς ο φοιτητής/εκπαιδευόμενος απαιτείται να διαθέτει, στις περισσότερες περιπτώσεις (εκτός από ορισμένες όπου θεωρούνται προαιρετικές) γνώσεις και δεξιότητες που σχετίζονται με την πληροφορική, τα πληροφοριακά συστήματα και τον έλεγχο. Πιο συγκεκριμένα, πρέπει να διαθέτει γνώσεις που σχετίζονται με τη δομή και τη λειτουργία των πληροφοριακών συστημάτων, με τα δίκτυα και θέματα που σχετίζονται με αυτά. Τέτοια θέματα είναι η ασφάλεια των δικτύων, η ανάπτυξη και η διαχείριση εφαρμογών, η διαχείριση δεδομένων, αλλά και οι γνώσεις που σχετίζονται με το ηλεκτρονικό εμπόριο.

Πανεπιστημιακό Ίδρυμα	**Προαπαιτούμενα**
University at Buffalo	• Computer Systems • Networks • Development
Nova Southeastern University	• Information Systems Management
School of Accountancy Georgia State University	• Microcomputing Skills • Database Skills • Internet Usage
Baruch College, Zicklin School of Business	• Computer Information Systems • Database Management • Financial Accounting

University of North Carolina	• Auditing Concepts

4.3 ΠΕΡΙΕΧΟΜΕΝΟ ΜΑΘΗΜΑΤΟΣ

Το περιεχόμενο του μαθήματος που σχετίζεται με τον έλεγχο πληροφοριακών συστημάτων οφείλει να είναι προσανατολισμένο στους στόχους που αναφέρθηκαν παραπάνω. Για το λόγο αυτό, θα πρέπει να διδάσκεται με τις εξής θεματικές:

Α) Διαδικασία ελέγχου

Ο φοιτητής/εκπαιδευόμενος οφείλει να κατανοήσει και να αφομοιώσει τη διαδικασία ελέγχου, η οποία ξεκινάει από το σχεδιασμό και φτάνει ως και την παρακολούθηση. Η διαδικασία αυτή αποτελεί τη βασικότερη γνώση για να μπορέσει να εμβαθύνει περαιτέρω.

Β) Εργαλεία ελέγχου και γνώση λογισμικού

Ο φοιτητής/εκπαιδευόμενος είναι απαραίτητο να κατανοήσει και να εφοδιαστεί με όλα τα απαραίτητα εργαλεία ελέγχου (περιγραφικές εκθέσεις, διαγράμματα ροής, ερωτηματολόγια εσωτερικού ελέγχου) και το συναφές λογισμικό, ώστε να μπορεί να θέσει σε εφαρμογή τον έλεγχο.

Γ) Κίνδυνοι, Παραβάσεις, Απειλές και Μέτρα Προστασίας

Ο φοιτητής/εκπαιδευόμενος είναι απαραίτητο να κατανοήσει και να είναι σε θέση να εντοπίζει τους κινδύνους, τις παραβάσεις και τις απειλές και να μπορεί να εφαρμόσει σε κάθε περίπτωση μέτρα προστασίας.

Δ) Διεθνή Πρότυπα, Φορείς IT Audit, πιστοποιήσεις

Ο φοιτητής/εκπαιδευόμενος είναι απαραίτητο να έχει γνώση όλων των διεθνών προτύπων και των φορέων ελέγχου πληροφοριακών συστημάτων, ώστε να μπορεί να εφαρμόζει καλύτερα τις διαδικασίες ελέγχου. Επίσης, η προετοιμασία για τις σχετικές πιστοποιήσεις θεωρείται προαιρετική πλην χρήσιμη, σε περίπτωση που κάποιος ενδιαφέρεται να πιστοποιηθεί και να εξειδικευτεί στον έλεγχο πληροφοριακών συστημάτων.

ΚΕΦΑΛΑΙΟ 5 ΣΥΜΠΕΡΑΣΜΑΤΑ

Ο εσωτερικός έλεγχος των επιχειρήσεων αφορά ένα ευρύ πεδίο λειτουργιών και δραστηριοτήτων των επιχειρήσεων και των οργανισμών. Στο πεδίο αυτό συμπεριλαμβάνεται και ο έλεγχος των πληροφοριακών συστημάτων ο οποίος κρίνεται απαραίτητος για τη διαφύλαξη της ακεραιότητας των δεδομένων, την επίτευξη των στόχων και των λειτουργιών της επιχείρησης και την αποδοτική κατανάλωση των πόρων.

Η διαδικασία ελέγχου των πληροφοριακών συστημάτων αφορά κυρίως, την κατανόηση των κινδύνων, τη διασφάλιση των λειτουργιών και την αναφορά των ανεπιθύμητων γεγονότων. Οι κίνδυνοι, η αναμενόμενη αξία τους και οι τρόποι αποφυγής και διαχείρισής τους αποτελούν βασικό τμήμα του ελέγχου πληροφοριακών συστημάτων. Ο έλεγχος, λοιπόν, ακολουθεί συγκεκριμένα πρότυπα, που έχουν θεσπιστεί από το Συμβούλιο Ελεγκτικών Προτύπων (SAS) και από άλλους διεθνείς φορείς (ISO κλπ).

Οι 4 μεγάλες ελεγκτικές εταιρείες, που ηγούνται του IT auditing είναι η Deloitte, η Ernst & Young, η PricewaterhouseCoopers (PWC) και η Klynveld Peat Marwick Goerdeler (KPMG) προσφέροντας ολοκληρωμένες λύσεις εσωτερικού ελέγχου.

Συνεπώς, οι διάφοροι φορείς IT audit φροντίζουν για την κατάρτιση των ελεγκτών και παρέχουν τις αντίστοιχες πιστοποιήσεις που συμφωνούν με τα Διεθνή Πρότυπα ελέγχου. Το Ινστιτούτο Ελέγχου Συστημάτων Πληροφορικής (ISACA) υποστηρίζει την πιστοποίηση CISA για ελεγκτές πληροφοριακών συστημάτων. Εκτός, όμως, από τους διεθνώς πιστοποιημένους φορείς, τα πανεπιστήμια και τα εκπαιδευτικά ιδρύματα οφείλουν να ενσωματώσουν στο πρόγραμμα σπουδών τους συναφή αντικείμενα με το μάθημα του IT auditing, ως απαραίτητο προσόν και γνώση για όσους ασχολούνται με τα πληροφοριακά συστήματα ή την ελεγκτική. Όπως φαίνεται και από ιδρύματα που έχουν ενσωματώσει το μάθημα στο πρόγραμμά τους, στοχεύουν στην κατανόηση των κινδύνων και των ευπαθειών των συστημάτων, της στρατηγικής και των διαδικασιών του εσωτερικού ελέγχου, στην εκμάθηση των μοντέλων και των κατάλληλων εργαλείων λογισμικού.

Η στελέχωση των οργανισμών και των επιχειρήσεων με ελεγκτές που κατέχουν βαθιά γνώση των πληροφοριακών συστημάτων, των κινδύνων, των απειλών και των κατάλληλων εργαλείων, κρίνεται απαραίτητη. Το εξειδικευμένο και υψηλά καταρτισμένο ανθρώπινο

δυναμικό θεωρείται προαπαιτούμενο για την αντιμετώπιση των προκλήσεων που παρουσιάζονται στο σύγχρονο τεχνολογικό και επιχειρησιακό περιβάλλον.

ΑΝΑΦΟΡΕΣ

Ελληνική Βιβλιογραφία

Παιδαγωγικό Ινστιτούτο, «Πληροφοριακά Συστήματα», Αθήνα 1993

Κυριαζόγλου, Ι. (2001). «Έλεγχος Συστημάτων Πληροφορικής – EDP/IT Auditing». Αθήνα: Εκδόσεις Anubis

Δημητριάδης, Α. (1998), «Ελεγκτική Συστημάτων Πληροφορικής (EDP Auditing)», Αθήνα: Εκδόσεις Νέων Τεχνολογιών

Κάτσικας, Σ., Γκρίτζαλης, Δ., Γκρίτζαλης, Σ. (2004), «Ασφάλεια Πληροφοριακών Συστημάτων»

Πάγκαλος Γ., Μαυρίδης Ι., (2002) «Ασφάλεια πληροφοριακών συστημάτων και δικτύων», Αθήνα: εκδόσεις Ανικούλα

Ξενόγλωσση Βιβλιογραφία

Abu-Musa, A. (2008), "Information technology and its implications for internal auditing- An empirical study of Saudi organizations", Managerial Auditing Journal, Vol. 23, No. 5, pp. 438-466

Bierstaker, J.L., Brody, R.G. and Pacini, C. (2006), "Accountants' perceptions regarding fraud detection and prevention methods", Managerial Auditing Journal, Vol. 21, No. 5, pp. 520-535

Hermanson, D.R., Hill, M.C. and Ivancevich, D.M. (2000a), "Information technology-related activities of internal auditors", Journal of Information Systems, Vol. 14, No. 1, Supplement, pp. 39-53

Hunton, James E., Wright, A. and Wright, S. (2004), "Are financial auditors overconfident in their ability to assess risks associated with enterprise resource planning systems?", Journal of Accounting Information Systems, Vol. 18, No. 2, pp. 7-28

Hunton, J., Bryant, S., Bagranoff, N. (2005), "Information Technology Auditing"

Laudon C. Kenneth & Laudon P.Jane, (2003), «Συστήματα Πληροφοριών Διοίκησης - MIS», Εκδόσεις Κλειδάριθμος

Gallegos, F., Senft, S., Manson, D., Gonzales, C. (2004) "Information Technology Control And Audit", Auerbach Publications, 2nd edition

Viator Ralph E., Deutsch Robert A., Boomer Gary L., Brock Terry, Elliott Raymond W., Hardie Hugh E., Johston Randolph P., MacBain Mary, Metzler James C., Needle Sheldon, Steed Val, Scherer Stephen J., "Computers / Technology", Journal of Accountancy, December 1992, Vol. 174, Issue 6, pg 117-119

Laudon Kenneth C., Laudon Jane P. (2007), "Management Information Systems- Managing the Digital Firm", 10th edition

Miles, D.Anthony (2011). *Risk Factors and Business Models: Understanding the Five Forces of Entrepreneurial Risk and the Causes of Business Failure*

Moroney, R., Campbell, F., Hamilton, J. (2012). "Auditing". John Wiley & Sons.

Pathak, J. (2005), "Information Technology Auditing- An Evolving Agenda". Canada: Springer

Silltow John, "Shedding light on Information Technology Risks", Internal Auditor, December 2003,Vol. 60, Issue 6

Beard Deborah, Wen Joseph H., "Reducing the Threat Levels for Accounting Information Systems", The CPA Journal, May 2007, Vol.77, No. 5

Hunton James E., Bryant Stephanie M., Bagranoff Nancy A., "Core Concepts of Information Technology Auditing", Wiley, 2004

Scott Robert W., "Taking the Risk out of IT", Accounting Technology, May 2008, Vol. 24, Issue 4

Σύνδεσμοι

http://www.itil.org.uk/

http://www.standardsdirect.org/

http://www.caspr.org/

http://www.gao.gov/

http://www.commoncriteria.org/

http://www.tickit.org/

http://www.cert.org/octave

http://csrc.nist.gov/

http://www.pcaob.org/

http://www.bvfls.aicpa.org/

http://www.theiia.org/

https://www.enisa.europa.eu/