ΙΩΑΝΝΗΣ ΚΥΡΙΑΖΟΓΛΟΥ

ΕΓΧΕΙΡΙΔΙΟ ΕΛΕΓΧΟΥ ΠΛΗΡΟΦΟΡΙΚΗΣ

(IT AUDITING HANDBOOK)

Μεθοδολογίες και Εργαλεία Ελέγχου Πληροφορικής
για να βελτιώσετε τη διαχείριση των συστημάτων
και υποδομών πληροφορικής σας

FYLATOS PUBLISHING

Συγγραφέας: ΙΩΑΝΝΗΣ ΚΥΡΙΑΖΟΓΛΟΥ

Γραφιστική επιμέλεια και σχεδιασμός εξωφύλλου: Χρύσα Γκανούδη
© Fylatos Publishing

e-mail. contact@fylatos.com
web: www.fylatos.com

ISBN: 978-960-658-172-4

ΙΩΑΝΝΗΣ ΚΥΡΙΑΖΟΓΛΟΥ

ΕΓΧΕΙΡΙΔΙΟ ΕΛΕΓΧΟΥ ΠΛΗΡΟΦΟΡΙΚΗΣ

(IT AUDITING HANDBOOK)

Μεθοδολογίες και Εργαλεία Ελέγχου Πληροφορικής
για να βελτιώσετε τη διαχείριση των συστημάτων
και υποδομών πληροφορικής σας

Εκδόσεις Φυλάτος
Fylatos Publishing
MMXXIII

Αφιερωμένο στη σύντροφο της ζωής μου Sandy,
στον γιο μου Χρήστο, την κόρη μου Μιράντα
και τον σύζυγό της Δημήτρη,
και στη μονάκριβη και υπέροχη δική μας Μελίνα
με τα γαλαζοπράσινα μάτια, που συνεχώς και διακαώς φωτίζει και
συμπληρώνει το σύμπαν της ύπαρξής μας.

ΠΕΡΙΕΧΟΜΕΝΑ

ΣΥΝΟΨΗ ΠΕΡΙΕΧΟΜΕΝΩΝ ΤΟΥ ΒΙΒΛΙΟΥ

Αυτό το βιβλίο εισάγει την έννοια του Ελέγχου Πληροφορικής, περιγράφει τα βασικά στοιχεία που τον αποτελούν (π.χ. **Πλαίσιο Ελέγχου Πληροφορικής, Σχέδιο Ελέγχου Πληροφορικής, Μεθοδολογία Ελέγχου Πληροφορικής (4 φάσεων και 22 βημάτων), Πρότυπο Έκθεσης Ελέγχου Πληροφορικής,** κ.λπ.) και παρουσιάζει διάφορες συμπληρωματικές πτυχές που υποστηρίζουν την εκτέλεση αποτελεσματικών ελέγχων πληροφορικής, όπως:

1. **Ένα σύνολο από 9 Προγράμματα Ελέγχου Πληροφορικής** για Οργάνωση, Στρατηγική και Διαχείριση Προσωπικού, Ανάπτυξη, Απόκτηση και Υλοποίηση Συστήματος, και Λειτουργία Κεντρικών Εφαρμογών και Εφαρμογών Γραφείου, Προμήθειες και Ανάθεση Υπηρεσιών Outsourcing και Cloud, Λειτουργία Κέντρου Δεδομένων και Λογισμικό Συστήματος, Δικτύων και Βάσης Δεδομένων.
2. **Έξι Ερωτηματολόγια Ελέγχου Πληροφορικής** για θέματα, όπως: Φυσική & Περιβαλλοντική Ασφάλεια, Ασφάλεια Εφαρμογών, Αξιολόγηση Ιδιωτικότητας, Αξιολόγηση Περιβάλλοντος Εφαρμογών, Διαβεβαίωσης της Ενσωμάτωσης Μέτρων Ελέγχου σε Σύστημα Πληροφορικής και Αξιολόγηση Ιστοχώρου.
3. **Ένα Παράρτημα με δέκα ενότητες** με ένα Γλωσσάριο Όρων και Εννοιών, Πρότυπα Διαχείρισης Τεχνολογίας, Περιοχές Ελέγχου Πληροφορικής και Θέματα, Κίνδυνοι Ασφάλειας Πληροφοριών και Ιδιωτικότητας Δεδομένων, κ.λπ.

ΑΝΤΙ ΠΡΟΛΟΓΟΥ

Το βιβλίο του κ. Κυριαζόγλου **πραγματεύεται το θεωρητικό πλαίσιο και θεμελιώνει πρακτικά θέματα του εσωτερικού ελέγχου Πληροφορικής σε επιχειρήσεις και οργανισμούς,** απευθυνόμενο έτσι σε ευρύ κοινό-στόχο που περιλαμβάνει τόσο επαγγελματίες εσωτερικούς ελεγκτές και διοικητικά στελέχη καθώς και στελέχη του τμήματος πληροφορικής των επιχειρήσεων και οργανισμών, όσο και προπτυχιακούς και μεταπτυχιακούς φοιτητές και ερευνητές.

Στο πλαίσιο του βιβλίου εξετάζεται το πεδίο εφαρμογής του ελέγχου πληροφορικής υπό το πρίσμα τόσο των γενικών μέτρων πληροφορικής (IT General Controls), όσο και των μέτρων λειτουργίας πληροφοριακών εφαρμογών (IT Application Controls). Προτείνεται Μοντέλο Λειτουργίας του Ελέγχου Πληροφορικής οργανωμένο σε 5 πυλώνες το οποίο συνιστά ένα πολύτιμο «Εγχειρίδιο Ελέγχου Πληροφορικής», εργαλείο θεμελιώδους αξίας της σύγχρονης εταιρικής διακυβέρνησης και ειδικότερα της Διακυβέρνησης Πληροφορικής (IT Governance).

Οι 5 πυλώνες του «Εγχειριδίου Ελέγχου Πληροφορικής», αναλύονται διεξοδικά μέσω της παράθεσης των διαδικασιών, μεθοδολογιών, πολιτικών και προτύπων που θα συμβάλλουν στην ολοκληρωμένη υποστήριξη και επίβλεψη του ελεγκτικού έργου πληροφορικής ενώ πλαισιώνονται από έξι (6) ερωτηματολόγια ελέγχου πληροφορικής με 200+ ερωτήσεις για θέματα, όπως: Ασφάλεια περιβάλλοντος και εφαρμογών, Αξιολόγηση Ιδιωτικότητας, κλπ.

Εν κατακλείδι, το βιβλίο του κ. Κυριαζόγλου «Εγχειρίδιο Ελέγχου Πληροφορικής (IT Auditing Handbook)» αξίζει μια θέση στη βιβλιοθήκη τόσο των επαγγελματιών εσωτερικών ελεγκτών, των διοικητικών στελεχών και των στελεχών του τμήματος πληροφορικής επιχειρήσεων και οργανισμών γιατί αποτελεί χρήσιμο εργαλείο για την ενσωμάτωση του ελέγχου πληροφορικής στις ελεγκτικές διαδικασίες μιας επιχείρησης/οργανισμού, καθώς και τη βελτίωση και αύξηση της αποτελεσματικότητας του, όσο και στη βιβλιοθήκη προπτυχιακών και μεταπτυχιακών φοιτητών και

ερευνητών για την απόκτηση γνώσης και κατανόησης των βασικών εννοιών του ελέγχου πληροφορικής όσο και την εξειδίκευση και περαιτέρω μελέτη του.

Δέσποινα Πολίτου – Κοινωνία της Πληροφορίας Μ.Α.Ε.
Υπεύθυνη Τμήματος Προγραμματισμού,
Συντονισμού & Παρακολούθησης Έργων
Διεύθυνση Διαχείρισης Έργων / Γενική Διεύθυνση Έργων

Λεωφ. Συγγρού 194,
Καλλιθέα, Τ.Κ. 17671
T +30 213 1300 700
M info@ktpae.gr
www.ktpae.gr
#transformingGReece

Ο Ιωάννης Κυριαζόγλου ξεκινάει με μια εύστοχη παρατήρηση, ότι τα πληροφοριακά συστήματα λειτουργούν ως φάρμακα στο περιβάλλον μίας σύγχρονης επιχείρησης. Όμως αν δε χρησιμοποιηθούν με πειθαρχία μπορεί να προκαλέσουν ανεπιθύμητες παρενέργειες ακόμα και με καταστροφικά αποτελέσματα. Είναι λοιπόν αναγκαίο, συνεχίζει ο συγγραφέας, να χρειάζονται κανόνες, πολιτικές και διαδικασίες.

Πρέπει να προλαβαίνουμε την αποτυχία, παρατηρεί και όλοι όσοι εργαζόμαστε στην πληροφορική γνωρίζουμε πολύ καλά, κάποιες φορές και από την προσωπική μας εμπειρία, πόσο μεγάλη σημασία έχει η πρόληψη. Στην καθημερινότητα των ανθρώπων εμφανίζονται συχνά πυκνά έννοιες όπως ο ψηφιακός μετασχηματισμός και η ψηφιοποίηση και ολοένα περισσότεροι χρησιμοποιούν ψηφιοποιημένες υπηρεσίες του δημοσίου και του ιδιωτικού τομέα. Για εμάς, τους επαγγελματίες της πληροφορικής, αυτό σημαίνει νέες απαιτήσεις στις οποίες καλούμαστε να ανταπεξέλθουμε.

Τα δεδομένα που καλούμαστε να διαχειριστούμε είναι σαφώς πιο πολλά σε σύγκριση με ό,τι συνέβαινε πριν από 20 ή 30 χρόνια και οι κίνδυνοι είναι σαφώς περισσότεροι σήμερα από το παρελθόν. Ο αριθμός των χρηστών έχει επίσης αυξηθεί και ταυτόχρονα έχουν αυξηθεί και οι κίνδυνοι. Την ίδια στιγμή και όπως σωστά παρατηρεί και ο συγγραφέας, η διαχωριστική γραμμή μεταξύ ενός IT auditor και ενός ελεγκτή μη πληροφορικής, μειώνεται γρήγορα, καθώς επιχειρήσεις και δημόσιοι οργανισμοί αυτοματοποιούν ολοένα και περισσότερες διαδικασίες. Εδώ, είναι σημαντικό οι ελεγκτές να κατανοούν το περιβάλλον ελέγχου, ώστε στο τέλος να κατανοούνται οι πιθανοί επιχειρηματικοί κίνδυνοι και να αξιολογούνται τα εφαρμοζόμενα μέτρα. Γνωρίζουμε όλοι όσοι εργαζόμαστε στην πληροφορική πως κατά το παρελθόν μία από τις πιο δύσκολες «αποστολές» μας ήταν να πείσουμε τα ανώτερα διοικητικά κλιμάκια για την ανάγκη προστασίας των συστημάτων πληροφορικής και διασφάλισης της ακεραιότητας των δεδομένων που χειριζόμαστε. Σήμερα βρισκόμαστε σε μια εντελώς διαφορετική κατάσταση.

Τα περιστατικά κυβερνοεπιθέσεων λειτουργούν ως υπενθύμιση για την τεράστια σημασία των συστημάτων προστασίας και, ταυτόχρονα, αναδεικνύουν τον κρίσιμο ρόλο που έχουν οι ελεγκτές πληροφορικής. Επίσης έχουν αμβλύνει σε κάποιο βαθμό τον δισταγμό που

χαρακτήριζε πολλές φορές τις εισηγήσεις για επενδύσεις σε υποδομές προστασίας και ασφαλείας. Πολύ σωστά ο συγγραφέας επισημαίνει πως η ανώτατη διοίκηση και οι αρμόδιες επιτροπές ελέγχου πρέπει να επανεξετάζουν περιοδικά το προφίλ κινδύνου και να προσδιορίζουν εάν το τρέχον μοντέλο εσωτερικού ελέγχου που έχουν εφαρμόσει, είναι το βέλτιστο για τον οργανισμό τους και τα συνδεδεμένα μέρη.

Όσο οι ψηφιακές διαδικασίες θα γίνονται μέρος του DNA των σύγχρονων επιχειρήσεων και, βεβαίως, των δημοσίων οργανισμών, βιβλία όπως αυτό που κρατάτε στα χέρια σας αποτελούν πολύτιμη πηγή πληροφόρησης και καθοδήγησης τόσο για τους συναδέλφους μας στην Πληροφορική όσο και για εκείνους που έχουν την ευθύνη λήψης των τελικών αποφάσεων σε έναν οργανισμό.

Νίκη Τσούμα
Πρόεδρος ΔΣ & Διευθύνουσα Σύμβουλος, ΗΔΙΚΑ Α.Ε,

«Το βιβλίο αποτελεί ένα απαραίτητο εγχειρίδιο για τις σημερινές επιχειρήσεις που βασίζουν τις λειτουργίες τους καθώς και τα λογιστικά συστήματα τους στον τομέα της πληροφορικής. Ο έλεγχος των πληροφοριακών συστημάτων εξηγείται λεπτομερώς ως προς τη χρησιμότητα και την εφαρμογή του. Η παρουσίαση διαφορετικών μεθοδολογιών και το εύρος των παραδειγμάτων ανάγουν το βιβλίο σε έναν πλήρη οδηγό για τον εσωτερικό έλεγχο των πληροφοριακών συστημάτων. Η ύπαρξη των ερωτηματολογίων καθοδηγεί το χρήστη στη διαδικασία του εσωτερικού ελέγχου με ακριβή και αποτελεσματικό τρόπο. Ένα απαραίτητο εργαλείο για στελέχη στο χώρο της πληροφοριακής υποστήριξης εταιρειών διεθνών προδιαγραφών.»

Dr Androniki Triantafylli
BSc,MSc (LSE), PhD(AUEB), SFHEA(Snr Fellow)
Reader (Associate Professor) in Accounting
Director of Student Engagement and Advising
School of Business and Management - Queen Mary University of London 4th Floor, Francis Bancroft Building,
Mile End Road, London E1 4NS, U.K.
Email:a.triantafylli@qmul.ac.uk

ΠΡΟΛΟΓΟΣ: ΕΙΣΑΓΩΓΗ ΣΤΟΝ ΕΛΕΓΧΟ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΠΕΡΙΛΗΨΗ

Ο πρόλογος περιγράφει τον βασικό ρόλο των πληροφοριών στη λειτουργία των επιχειρήσεων καθώς και τις αιτίες, κινδύνους, στόχους και οφέλη της εφαρμογής διαδικασιών του ελέγχου πληροφορικής.

1. ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΕΠΙΧΕΙΡΗΣΕΙΣ

Η υπολογιστική τεχνολογία και οι συγγενείς υποδομές (Information and Communications Technology (ITC)), τα αυτοματοποιημένα πληροφοριακά συστήματα, η εθνική, διεθνής ή και επιχειρησιακή υποδομή δικτύωσης (το λεγόμενο 'network backbone') και οι συμπληρωματικές τεχνολογίες αποθήκευσης μαζικών πληροφοριών, παρέχουν σε όλους τις πληροφορίες τα λεπτομερειακά στοιχεία για τη λειτουργία της συγκεκριμένης εταιρίας, άμεσα, έγκυρα και με σχετική συνήθως ασφάλεια.

Η τεχνολογία αυτή και τα Συστήματα Πληροφορικής που είναι τα επακόλουθά της (γρήγορη και πιο αποτελεσματική πληροφόρηση), διέπουν τη μοντέρνα επιχείρηση σε όλες τις δραστηριότητές της (ανταγωνιστικότερη, καλύτερη και οικονομικότερη παραγωγή) και έχουν ως αποτέλεσμα την καλύτερη εξυπηρέτηση των πελατών της και του ευρύτερου κοινωνικού συνόλου.

Όλα αυτά τα τεχνολογικά στοιχεία, που γενικά απαρτίζουν την τεχνολογία πληροφορικής (IT: Information Technology), και τα συναφή πληροφοριακά συστήματα (IS: Information Systems) που λειτουργούν με βάση και εντός αυτού του τεχνολογικού πλαισίου, παρέχουν τα εξής οφέλη στις σύγχρονες επιχειρήσεις και οργανισμούς (ενδεικτικά):

1. Πιο γρήγορη και πιο αποτελεσματική πληροφόρηση για τη λήψη αποφάσεων σε όλα τα επίπεδα της οργάνωσης,

2. Αυξημένη ανταγωνιστικότητα σε όλες τις υπηρεσίες που προσφέρονται από τη συγκεκριμένη οργανωτική μονάδα,
3. Βελτιωμένες παραγωγικές επεξεργασίες και διαχειριστικές διαδικασίες, και
4. Καλύτερη ποιότητα σε προϊόντα και υπηρεσίες στους πελάτες (για ιδιωτικές επιχειρήσεις), πολίτες (για δημόσιους οργανισμούς), και γενικότερα για την κοινωνία και οικονομία.

Με δεδομένο τον γρήγορο ρυθμό ανάπτυξης της πληροφοριακής και υπολογιστικής τεχνολογίας, έναν ρυθμό χωρίς προηγούμενο στην ιστορία της ανθρωπότητας, είναι τώρα ακόμη πιο εύκολο για τις επιχειρήσεις και τους οργανισμούς να μεταβιβάσουν σχεδόν όλες τις επιχειρηματικές τους συναλλαγές και λειτουργίες να εκτελούνται από ολοκληρωμένα πληροφοριακά συστήματα.

Αυτά τα συστήματα είναι σαν φάρμακα. Ενδυναμώνουν τον συγκεκριμένο οργανισμό (ή επιχείρηση) και τον διευκολύνουν να θεραπεύσει ή να επιλύσει ένα συγκεκριμένο πρόβλημα ή λειτουργική αστοχία.

Με βάση το παραπάνω παράδειγμα (δηλαδή αυτό των φαρμάκων), εάν αυτά τα συστήματα δε χρησιμοποιηθούν με πειθαρχία, μπορεί να δημιουργήσουν χαώδεις καταστάσεις και πολλές φορές όχι τα αναμενόμενα αποτελέσματα. Ακόμη και τη μερική ή ολική καταστροφή.

Αυτά τα ολοκληρωμένα πληροφοριακά συστήματα πρέπει λοιπόν, να λειτουργήσουν εντός ενός επιχειρησιακού περιβάλλοντος που το διέπουν κανόνες, πολιτικές και διαδικασίες και ένα σύστημα διαχείρισης κινδύνων. Αυτά συνολικά απαρτίζουν το πλαίσιο εταιρικής διακυβέρνησης το οποίο, στην περίπτωση των πληροφοριακών συστημάτων, συμπληρώνεται και από ένα πλαίσιο τεχνολογικής διακυβέρνησης.

Επίσης, οι πληροφορίες είναι και θεωρούνται ως το σύγχρονο και στρατηγικό όπλο κάθε οργανισμού, και είναι πια στρατηγική περιουσία του οργανισμού.

Η δαπάνη για τη συλλογή, επεξεργασία και διάχυση των πληροφοριών, μέσω συστημάτων πληροφορικής, απαιτούν υπέρογκα ποσά, πόρους και προσπάθεια.

2. ΒΑΣΙΚΕΣ ΛΕΙΤΟΥΡΓΙΕΣ ΔΙΟΙΚΗΣΗΣ

Σύμφωνα με τη σύγχρονη θεωρία διοίκησης και από την εμπειρία από μεγάλο αριθμό έργων παροχής υπηρεσιών σε διεθνές επίπεδο, σε όλες τις δραστηριότητες κάθε οργανισμού, ανεξαρτήτως μεγέθους, οι πέντε (5) βασικές λειτουργίες του μάνατζμεντ (management) που εξασκούνται για τη διοίκηση του συγκεκριμένου οργανισμού είναι:

1. Σχεδίαση (planning): Μελέτη των μελλοντικών θεμάτων και σχεδίαση των στόχων και πώς θα επιλυθούν
2. Οργάνωση (organizing): Σχεδίαση της δομής για τη χρήση ανθρώπινων και άλλων πόρων για την επίτευξη των στόχων
3. Συντονισμός (coordinating): Συντονισμός όλων των δραστηριοτήτων και επιβεβαίωση ότι όλα τα μέσα και οι πόροι θα είναι διαθέσιμα για να επιτευχθούν οι στόχοι
4. Διοίκηση (directing): Εκτέλεση όλων των ενεργειών (εσωκλειόμενων της ηγετικής ικανότητας, καθοδήγησης και παρακίνησης του προσωπικού) για να λειτουργεί ο οργανισμός σωστά
5. Έλεγχος (controlling): Επιβεβαίωση ότι όλες οι ενέργειες και δραστηριότητες εκτελούνται σύμφωνα με τα εγκεκριμένα σχέδια και στόχους

Η τελευταία λειτουργία, δηλαδή ο έλεγχος, δεν επιτυγχάνεται πλήρως ή και καθόλου, και είναι μία από τις βασικότερες αιτίες της ‘αποτυχίας ένταξης συστημάτων πληροφορικής’

Για να προλαμβάνονται λοιπόν δυσάρεστες επιπτώσεις πρέπει να προλαβαίνουμε την αποτυχία. Απαιτείται λοιπόν, για την άριστη προφύλαξη, αξιοπιστία και χρήση/αξιοποίηση των κρίσιμων αυτών οντοτήτων, η πλήρης λειτουργία ενός συστήματος ελέγχου και επιστημονικές τεχνικές/μέθοδοι για την πιστοποίηση πιθανών λανθασμένων κινήσεων και προτάσεων βελτίωσης λειτουργίας όλου του πληροφοριακού πλαισίου για τη σύγχρονη επιχείρηση και οργανισμό.

3. ΑΙΤΙΕΣ ΕΛΕΓΧΟΥ ΕΠΙΧΕΙΡΗΣΕΩΝ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗΣ

Σύμφωνα με την επιτροπή COSO (ΗΠΑ) της Treadway Commission (on Fraudulent Reporting: **https://www.coso.org/Pages/guidance.aspx**) η κύρια αιτία ελέγχου και συστήματος εσωτερικών ελέγχων στις επιχειρήσεις είναι για να επιτευχθούν οι επιχειρησιακοί στόχοι.

Για την επίτευξη των στόχων της επιχείρησης οι συνηθισμένοι επιχειρησιακοί κίνδυνοι πρέπει να ελεγχθούν και να ελαχιστοποιηθούν.

3.1. Επιχειρησιακοί κίνδυνοι

Οι κίνδυνοι αυτοί είναι:

1. Λανθασμένη συντήρηση αρχείων (erroneous record-keeping)
2. Μη αποδεκτό σύστημα λογιστικής (έλλειψη αρχών, προτύπων κ.λπ.)
3. Επιχειρησιακή διακοπή (business interruption)
4. Λανθασμένες αποφάσεις της διοίκησης (από λάθος πληροφορίες, ενέργειες, αποφάσεις, κ.λπ.)
5. Οικονομική και διαχειριστική απάτη
6. Επιβολή προστίμων από κυβερνητικούς φορείς
7. Υπερβολικό κόστος λειτουργίας
8. Καταστροφή ή και φθορά πόρων (σκόπιμη ή άσκοπη)
9. Ανταγωνιστικό μειονέκτημα (μη επαρκής αντίδραση της επιχείρησης στις εξελίξεις της αγοράς)

Η διοίκηση της εταιρίας ή του οργανισμού, με βάση τους κανόνες εταιρικής διακυβέρνησης και των διεθνών πρακτικών, πρέπει να λάβει όλα τα απαραίτητα μέτρα για να επιβιώσει η επιχείρηση, αντιμετωπίζοντας και ελαχιστοποιώντας τους συνηθισμένους αυτούς κινδύνους και να λειτουργεί εντός των νόμιμων πλαισίων και ορίων που θέτει η τοπική και διεθνής κοινωνία και οικονομία.

3.2. Κίνδυνοι πληροφορικής

Για την επίτευξη των στόχων της πληροφορικής οι συνηθισμένοι κίνδυνοι που πρέπει να ελεγχθούν και να ελαχιστοποιηθούν είναι:

1. Απάτη (fraud)
2. Κλοπή ηλεκτρονικών πληροφοριών και δεδομένων
3. Κλοπή 'φυσικών' πληροφοριών, μέσων, εξοπλισμού, λογισμικού, κ.λπ.
4. Μη συμμόρφωση με τις διατάξεις του νόμου-πλαισίου για την προστασία προσωπικών δεδομένων (invasion of privacy)
5. Φθορά ή και ζημιά εξοπλισμού, περιφερειακών, λογισμικού δεδομένων, τεχνικών αρχείων (audit trail, logging), ηλεκτρονικής μεταφοράς δεδομένων (EDI), κ.λπ.
6. Παρεμβολή στις τηλεπικοινωνίες και μη εγκεκριμένες προσβάσεις (interception of communications, user illegal access, legal user but illegal transaction)
7. Παράνομη καταγραφή ηλεκτρομαγνητικών σημάτων
8. (Μη) σκόπιμη λανθασμένη καταχώρηση στοιχείων
9. Μειωμένη ακεραιότητα πληροφοριών από μη νόμιμη αλλαγή στοιχείων, λογισμικού και βάσεων δεδομένων
10. Σαμποτάζ ή άλλες παράνομες πράξεις από το προσωπικό ή και συνεργάτες
11. Παράνομη εισβολή (illegal intrusion) σε χώρους υπολογιστών, συστήματα, εξοπλισμό, και δίκτυα (hacking), και
12. Διακοπή λειτουργίας συστημάτων, εξοπλισμού, λογισμικού, περιβάλλοντος, διαδικασιών, εγκαταστάσεων, μηχανισμών αρχειοθέτησης και φύλαξης αντιγράφων, διαδικασιών ασφάλειας, οργανωτικών δομών, κ.λπ.

4. ΟΡΙΣΜΟΣ ΕΛΕΓΧΟΥ ΠΛΗΡΟΦΟΡΙΚΗΣ

Ο Έλεγχος Πληροφορικής είναι η διαδικασία απόκτησης βέλτιστης διασφάλισης για το εάν ο σχεδιασμός, η ανάπτυξη, η υλοποίηση, η λειτουργία και η συντήρηση συστημάτων πληροφορικής πληρούν τους επιχειρηματικούς στόχους, προστατεύουν τα περιουσιακά στοιχεία πληροφοριών και διατηρεί την ακεραιότητα των δεδομένων, μεταξύ άλλων. *Για τον ορισμό και άλλων εννοιών ελέγχου, βλ., Παράρτημα 1 'Γλωσσάριο όρων και Εννοιών Ελέγχου'.*

Με άλλα λόγια, ο έλεγχος πληροφορικής είναι μια ανασκόπηση και εξέταση της εφαρμογής συστημάτων πληροφορικής και ελέγχων πληροφορικής για να διασφαλιστεί ότι τα συστήματα πληρούν τις επιχειρηματικές απαιτήσεις, ανάγκες και στόχους του οργανισμού, χωρίς να διακυβεύεται η ασφάλεια, το απόρρητο, το κόστος και άλλα κρίσιμα επιχειρηματικά ζητήματα και παράγοντες.

5. ΣΤΟΧΟΙ ΣΥΣΤΗΜΑΤΟΣ ΕΛΕΓΧΟΥ ΠΛΗΡΟΦΟΡΙΚΗΣ

Οι στόχοι ενός Συστήματος Ελέγχου Πληροφορικής είναι:

1. Η αξιολόγηση των συστημάτων και διαδικασιών που ισχύουν επί του παρόντος και λειτουργούν για την ασφάλεια των εταιρικών δεδομένων που διατηρούνται μέσω πληροφοριακών υποδομών.
2. Ο προσδιορισμός ύπαρξης πιθανών κινδύνων στα πληροφοριακά αγαθά της εταιρίας και εξεύρεση τρόπων ελαχιστοποίησης αυτών των κινδύνων.
3. Η επαλήθευση της αξιοπιστίας και της ακεραιότητας των πληροφοριών.
4. Η προστασία όλων των περιουσιακών στοιχείων της εταιρίας.
5. Ο έλεγχος ότι οι διαδικασίες διαχείρισης πληροφοριών συμμορφώνονται με τους νόμους, τις πολιτικές και τα πρότυπα που ισχύουν για την Πληροφορική.

6. Η εξέταση και διαπίστωση της αναποτελεσματικότητας των συστημάτων πληροφορικής και των συναφών πρακτικών διαχείρισης.
7. Η βελτίωση της ποιότητα των πληροφοριών, δηλ., της αποτελεσματικότητας, αποδοτικότητας, εμπιστευτικότητας, διαθεσιμότητας, συμμόρφωσης, εγκυρότητας και αντοχής, σύμφωνα με το Διεθνές Ινστιτούτο Ελεγκτών Πληροφορικής (ISACA).

6. ΕΥΡΟΣ ΕΛΕΓΧΟΥ ΠΛΗΡΟΦΟΡΙΚΗΣ

Για τους ανωτέρω αναφερόμενους σκοπούς έχει θεσμοθετηθεί στις προηγμένες τεχνολογικά χώρες, ο ρόλος και η ίδρυση ενός πλαισίου και συστήματος εσωτερικού ελέγχου μέσα στο οποίο λειτουργεί και το τμήμα Ελέγχου Συστημάτων Πληροφορικής (IT Auditing).

Η λειτουργία εσωτερικού ελέγχου της εταιρίας ή μιας εξωτερικής οντότητας μπορεί να διενεργεί ελέγχους πληροφορικής σε συνδυασμό με έλεγχο οικονομικών καταστάσεων, επισκόπηση εσωτερικών ελέγχων ή άλλων ελέγχων (π.χ. έλεγχος συμμόρφωσης με τον GDPR).

Ανεξάρτητα από τον τύπο του ελέγχου, ο ελεγκτής πληροφορικής θα πρέπει να αξιολογήσει τις πολιτικές και τις διαδικασίες που καθοδηγούν το συνολικό περιβάλλον Πληροφορικής της ελεγχόμενης οντότητας, διασφαλίζοντας ότι υπάρχουν οι αντίστοιχοι έλεγχοι και μηχανισμοί επιβολής.

Το πεδίο εφαρμογής του ελέγχου πληροφορικής θα περιλαμβάνει τη λήψη απόφασης για την έκταση του ελέγχου, την κάλυψη των συστημάτων πληροφορικής και των λειτουργικοτήτων τους, τις διαδικασίες πληροφορικής (π.χ. Ασφάλεια, Ανάπτυξη Συστημάτων, Ανάκαμψη από Καταστροφές, κ.λπ.) που θα ελεγχθούν, τις τοποθεσίες των συστημάτων πληροφορικής που θα καλυφθούν και τη χρονική περίοδο που θα καλυφθεί, κ.λπ.

7. ΜΕΤΡΑ ΔΙΑΚΥΒΕΡΝΗΣΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

Μέτρα Διακυβέρνησης είναι ο συνδυασμός μηχανισμών, μεθόδων, κανόνων, πολιτικών και διαδικασιών που διασφαλίζουν την προστασία των περιουσιακών στοιχείων της εταιρίας, την ακρίβεια και την αξιοπιστία των αρχείων της και τη λειτουργική τήρηση των προτύπων διαχείρισης.

Εντός αυτού του επιχειρησιακού πλαισίου ελέγχου τα μέτρα διακυβέρνησης πληροφορικής (IT Governance Controls) καθορίζονται ως συγκεκριμένες ενέργειες, συνήθως αποτυπωμένες σε πολιτικές, διαδικασίες, πρακτικές εφαρμογής, κ.λπ., που εκτελούνται από ανθρώπους, εξοπλισμό ηλεκτρονικών υπολογιστών και επικοινωνιών, ή και λογισμικό (software) με μόνο στόχο τη διαβεβαίωση επίτευξης των συγκεκριμένων επιχειρησιακών στόχων της πληροφορικής.

Η γενική κατεύθυνση και αναγκαιότητα των μέτρων ελέγχου πληροφορικής σχετίζονται με την ασφαλή επεξεργασία, εμπιστευτικότητα και διαθεσιμότητα των δεδομένων και τη γενικότερη διοίκηση της διεύθυνσης πληροφορικής της επιχείρησης ή οργανισμού.

Τα μέτρα ελέγχου πληροφορικής διαχωρίζονται σε γενικά μέτρα πληροφορικής (IT General Controls) και σε μέτρα λειτουργίας πληροφοριακών εφαρμογών (IT Application Controls), σύμφωνα με διάφορες πηγές.

Γενικά μέτρα πληροφορικής είναι τα μέτρα που εφαρμόζονται σε όλες τις δραστηριότητες της πληροφορικής (συστήματα, υπηρεσίες, θέματα, επεξεργασίες, συναλλαγές, κ.λπ.) και στα δεδομένα της επιχείρησης ή οργανισμού σε ένα συγκεκριμένο περιβάλλον πληροφορικής. Αφορούν περιοχές όπως: Στρατηγική, ανάπτυξη και συντήρηση συστημάτων, λειτουργία κέντρου δεδομένων, τράπεζες δεδομένων, λειτουργικό σύστημα, κ.λπ.

Τα μέτρα λειτουργίας πληροφοριακών εφαρμογών είναι τα μέτρα που αρμόζουν στην επεξεργασία συναλλαγών από συγκεκριμένα πληροφοριακά συστήματα, όπως: Γενική λογιστική, διαχείριση προσωπικού, πωλήσεις, έλεγχος αποθηκών, μισθοδοσία, κ.λπ.

Σχετίζονται δε, με την επεξεργασία και αποθήκευση δεδομένων σε ψηφιακά αρχεία και βάσεις δεδομένων, βασισμένα και οργανωμένα από συστήματα ηλεκτρονικών υπολογιστών και συγκεκριμένων εφαρμογών και προγραμμάτων εφαρμογών, και που έχουν στόχο τη διαβεβαίωση ότι όλες οι επιχειρησιακές συναλλαγές είναι

εγκεκριμένες, και επεξεργάζονται και αποθηκεύουν και αναφέρουν τα αποτελέσματά των με ακρίβεια, ασφάλεια και εγκυρότητα.

8. ΟΦΕΛΗ ΕΛΕΓΧΟΥ ΠΛΗΡΟΦΟΡΙΚΗΣ

Τα οφέλη του ελέγχου πληροφορικής, είναι συνήθως:

1. Κατανόηση των κινδύνων ανάπτυξης και λειτουργίας συστημάτων πληροφορικής
2. Βελτίωση των εργασιών σχεδιασμού, ανάπτυξης, εφαρμογής και βελτίωσης νέων και υπαρχόντων συστημάτων πληροφορικής
3. Αύξηση της ικανότητας της διοίκησης στην επίτευξη στρατηγικών στόχων
4. Διαβεβαίωση υψηλών προτύπων των συστημάτων και υποδομών πληροφορικής σε όλες τις επιχειρήσεις και οργανισμούς

9. ΣΗΜΑΣΙΑ ΤΩΝ ΜΕΤΡΩΝ ΔΙΑΚΥΒΕΡΝΗΣΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΓΙΑ ΤΟΝ ΕΛΕΓΚΤΗ ΠΛΗΡΟΦΟΡΙΚΗΣ

Σε γενικές γραμμές, οι ελεγκτές πληροφορικής καλούνται να εξετάσουν μέτρα που σχετίζονται με την τεχνολογία, ενώ οι ελεγκτές που δεν ανήκουν στον τομέα της πληροφορικής αξιολογούν οικονομικούς, ρυθμιστικούς και ελέγχους συμμόρφωσης, κ.λπ.

Καθώς όλο και περισσότερες εταιρείες και δημόσιοι οργανισμοί βασίζονται στην πληροφορική για να αυτοματοποιήσουν τις δραστηριότητές τους, η γραμμή που χωρίζει τον ρόλο ενός ελεγκτή πληροφορικής και ενός ελεγκτή μη πληροφορικής μειώνεται επίσης γρήγορα.

Τουλάχιστον, όλοι οι ελεγκτές πρέπει να κατανοούν το περιβάλλον ελέγχου της ελεγχόμενης οντότητας, ώστε να παρέχουν διασφάλιση σχετικά με τους εσωτερικούς ελέγχους που λειτουργούν σε μια εταιρία, λειτουργία, σύστημα κ.λπ.

Ο ρόλος του ελεγκτή είναι να κατανοεί τους πιθανούς επιχειρηματικούς κινδύνους και κινδύνους πληροφορικής που αντιμετωπί-

ζει η συγκεκριμένη εταιρία (ελεγχόμενη οντότητα) και με τη σειρά του να αξιολογεί εάν τα εφαρμοζόμενα μέτρα είναι επαρκεί για την επίτευξη του στόχου ελέγχου.

Στην περίπτωση των ελέγχων πληροφορικής, είναι σημαντικό για τον ελεγκτή να κατανοήσει την έκταση των γενικών ελέγχων σε λειτουργία, να αξιολογήσει την επίβλεψη της διοίκησης και την ευαισθητοποίηση του προσωπικού στη λειτουργία της εταιρίας και να ανακαλύψει πόσο αποτελεσματικά είναι τα μέτρα διακυβέρνησης πληροφορικής στη συγκεκριμένη εταιρία κ.λπ.

10. ΜΟΝΤΕΛΟ ΛΕΙΤΟΥΡΓΙΑΣ ΕΛΕΓΧΟΥ ΠΛΗΡΟΦΟΡΙΚΗΣ

Τα τμήματα εσωτερικού ελέγχου συνεχίζουν να αντιμετωπίζουν προκλήσεις που σχετίζονται με ένα διευρυνόμενο σύμπαν ελέγχου, αλλαγές στους νόμους και κανονισμούς, μεγαλύτερους τεχνολογικούς κινδύνους και αυξημένες πιέσεις στον προϋπολογισμό.

Η ανώτατη διοίκηση και οι επιτροπές ελέγχου θα πρέπει να επανεξετάζουν περιοδικά το προφίλ κινδύνου της εταιρίας τους και να προσδιορίζουν εάν το τρέχον μοντέλο εσωτερικού ελέγχου τους είναι το βέλτιστο για την εταιρία και τα σημαντικά ενδιαφερόμενα μέρη (stakeholders).

Το μοντέλο λειτουργίας του τμήματος εσωτερικού ελέγχου θα πρέπει να βασίζεται στα καθοριστικά χαρακτηριστικά της εταιρίας, καθώς και στη συγκεκριμένη δυνατότητα εφαρμογής και πιθανά οφέλη και προκλήσεις που σχετίζονται με κάθε μοντέλο λειτουργίας.

Τα ίδια ισχύουν με το Μοντέλο Λειτουργίας Ελέγχου Πληροφορικής.

Είναι η κύρια υπευθυνότητα του τμήματος εσωτερικού ελέγχου να διαμορφώσει και να υλοποιήσει ένα αντίστοιχο και συγκεκριμένο Μοντέλο Λειτουργίας Ελέγχου Πληροφορικής.

Το μοντέλο που περιγράφεται στη συνέχεια, βασίζεται στην εμπειρία μου από μεγάλο αριθμό έργων παροχής υπηρεσιών ελέγχου πληροφορικής σε διεθνές επίπεδο και σε διάφορες εταιρείες και δημόσιους οργανισμούς.

Το προτεινόμενο **Μοντέλο Λειτουργίας Ελέγχου Πληροφορικής** περιέχει τους εξής 5 πυλώνες:

1. Οργάνωση Ελέγχου Πληροφορικής
2. Μεθοδολογίες Ελέγχου Πληροφορικής
3. Εργαλεία Εκτέλεσης Ελέγχου Πληροφορικής
4. Υποστηρικτικά Εργαλεία Ελέγχου
5. Μέτρα Διακυβέρνησης Πληροφορικής

Όλα αυτά και τα συστατικά τους στοιχεία αναπτύσσονται στα επόμενα κεφάλαια αυτού του βιβλίου, για τους τέσσερις πρώτους πυλώνες. Τα 'Μέτρα Διακυβέρνησης Πληροφορικής' που αποτελούν τον πέμπτο πυλώνα περιέχονται στο Παράρτημα 10 και το οποίο περιέχει έναν ενδεικτικό κατάλογο μέτρων διακυβέρνησης πληροφορικής.

ΜΕΡΟΣ Α:
ΟΡΓΑΝΩΣΗ ΕΛΕΓΧΟΥ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΣΤΟΧΟΣ

Ο στόχος του πρώτου μέρους (πυλώνας 'Οργάνωση Ελέγχου Πληροφορικής') του Μοντέλου Λειτουργίας Ελέγχου Πληροφορικής που αναπτύσσεται σε αυτό το βιβλίο ('*Εγχειρίδιο Ελέγχου Πληροφορικής')*, είναι η κατανόηση των αιτιών, της ανάγκης και των συστατικών στοιχείων της αποτελεσματικής οργάνωσης ενός Συστήματος Ελέγχου Πληροφορικής για τις ανάγκες της εταιρίας σας.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Τα κεφάλαια που αποτελούν το πρώτο μέρος είναι:

ΑΠΟΤΕΛΕΣΜΑ

Το αποτέλεσμα της κατανόησης και της μελέτης του υλικού του προλόγου και των ανωτέρω κεφαλαίων είναι:

1. Η καλύτερη οργάνωση των ελεγκτών πληροφορικής
2. Ο πιο αποδοτικότερος σχεδιασμός ελέγχων πληροφορικής
3. Η πιο ολοκληρωμένη υποστήριξη και επίβλεψη του ελεγκτικού έργου πληροφορικής από τη διοίκηση του τμήματος εσωτερικού ελέγχου και την ανώτατη διοίκηση της εταιρίας

ΑΞΙΟΠΟΙΗΣΗ

Το ανωτέρω υλικό μπορεί επίσης να αξιοποιηθεί και από τα στελέχη του τμήματος πληροφορικής της εταιρίας σας για την πληρέστερη προετοιμασία των και την καλύτερη συμμετοχή των σε ελέγχους πληροφορικής που σχεδιάζονται να εκτελεσθούν στην εταιρία σας.

Εξωτερικές οντότητες [π.χ. Ρυθμιστικές Αρχές (Επιτροπή Κεφαλαιαγοράς για εισηγμένες στο Χρηματιστήριο, Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, Εφορία, κ.λπ.), μέτοχοι, ευρύ κοινό, πελάτες, κ.λπ.], μπορούν να αξιοποιήσουν αυτό το υλικό για διάφορους λόγους, όπως: Ενημέρωση για επένδυση, αποφυγή απάτης, άσκηση δικαιωμάτων καταναλωτή, άσκηση δικαιωμάτων πρόσβασης προσωπικών δεδομένων, κ.λπ.

ΘΕΣΠΙΣΗ ΚΑΙ ΔΙΑΤΗΡΗΣΗ ΤΗΣ ΕΝΟΤΗΤΑΣ ΟΡΓΑΝΩΣΗΣ ΕΛΕΓΧΟΥ ΠΛΗΡΟΦΟΡΙΚΗΣ

Τα συστατικά στοιχεία της οργάνωσης ελέγχου πληροφορικής θεσπίζονται και διατηρούνται ως εξής:

1. Πλαίσιο και Οργάνωση Ελέγχου Πληροφορικής: Θεσπίζονται στην αρχή και βελτιώνονται μετά την εκτέλεση ελέγχων, όπως απαιτείται.
2. Εγχειρίδιο Λειτουργίας Εσωτερικού Ελέγχου: Δημιουργείται ανάλογα με τις επιχειρησιακές ανάγκες και βελτιώνεται μετά την εκτέλεση ελέγχων, όπως απαιτείται.
3. Σχέδιο Ελέγχου Πληροφορικής: Δημιουργείται ανάλογα με τις επιχειρησιακές ανάγκες (π.χ. κάθε τριετία), βελτιώνεται και ανακοινώνεται ετησίως με βάση το Σχέδιο Εσωτερικού Ελέγχου και την ανάλυση κινδύνων πληροφορικής (βλ. Κεφάλαιο 7, στο Δεύτερο Μέρος).

ΚΕΦΑΛΑΙΟ 1: ΠΛΑΙΣΙΟ ΕΛΕΓΧΟΥ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΠΕΡΙΛΗΨΗ

Αυτό είναι το πρώτο συστατικό στοιχείο το πρώτου μέρους ('Οργάνωση Ελέγχου Πληροφορικής') του Εγχειριδίου Ελέγχου Πληροφορικής.

Το κεφάλαιο αυτό περιγράφει το πλαίσιο εσωτερικού ελέγχου, το πλαίσιο ελέγχου πληροφορικής και τους τύπους και φάσεις ελέγχου πληροφορικής.

ΠΕΡΙΕΧΟΜΕΝΑ

1.1. ΟΡΙΣΜΟΙ ΕΣΩΤΕΡΙΚΟΥ ΚΑΙ ΕΞΩΤΕΡΙΚΟΥ ΕΛΕΓΧΟΥ

Η υπηρεσία εσωτερικού ελέγχου (Internal Audit) είναι μια ανεξάρτητη, αντικειμενική δραστηριότητα διασφάλισης και παροχής συμβουλών, σχεδιασμένη για να προσθέσει αξία και να βελτιώσει τις λειτουργίες μιας εταιρίας ή ενός οργανισμού. Βοηθά την εταιρία ή τον οργανισμό να επιτύχει τους στόχους, με μια συστηματική και πειθαρχημένη προσέγγιση για να εκτιμήσει και να βελτιώσει:

1. Την αποτελεσματικότητα των λειτουργιών της

1. Της διαχείρισης κινδύνων
2. Των μέτρων λειτουργίας (controls)
3. Της εταιρικής διακυβέρνησης

Ο εξωτερικός έλεγχος έχει ιδιαίτερη σημασία για τις επιχειρήσεις, καθώς επίσης και για το επενδυτικό κοινό. Οι εξωτερικοί ελεγκτές είναι οι μόνοι που μπορούν να διαβεβαιώσουν την αξιοπιστία των οικονομικών καταστάσεων μιας επιχείρησης, λόγω των προσόντων που έχουν και της ανεξαρτησίας τους με την ελεγχόμενη οικονομική μονάδα.

1.2. ΔΙΑΔΙΚΑΣΙΑ ΕΣΩΤΕΡΙΚΟΥ ΕΛΕΓΧΟΥ

Σε γενικές γραμμές, ένας τυπικός έλεγχος περιλαμβάνει τα ακόλουθα βήματα:

Βήμα 1. Συζήτηση με τη διοίκηση της εταιρικής υπηρεσίας που θα ελεγχθεί για τους στόχους του ελέγχου, το χρονοδιάγραμμα, τη μορφή και τη διανομή της έκθεσης ελέγχου.

Βήμα 2. Αξιολόγηση της ευρωστίας των εσωτερικών ελέγχων και των συστημάτων των επιχειρήσεων και λειτουργιών.

Βήμα 3. Δοκιμές των εσωτερικών μέτρων και ελέγχων (internal measures and controls) για να διασφαλιστεί η σωστή λειτουργία τους.

Βήμα 4. Συζήτηση με τη διοίκηση της εταιρικής υπηρεσίας που ελέγχεται όλων των προκαταρκτικών παρατηρήσεων.

Βήμα 5. Συζήτηση με τη διοίκηση της εταιρικής υπηρεσίας του σχεδίου εκθέσεως ελέγχου και των απαντήσεών τους, εάν υπάρχουν, πριν από την κυκλοφορία της τελικής έκθεσης ελέγχου.

Βήμα 6. Επανεξέταση των κρίσιμων ζητημάτων που τέθηκαν στις εκθέσεις ελέγχου για να διαπιστωθεί αν έχουν επιλυθεί με επιτυχία.

1.3. ΠΡΟΤΥΠΑ ΕΡΓΟΥ ΕΛΕΓΧΟΥ

Τα Διεθνή Ελεγκτικά Πρότυπα (International Auditing Standards) αποτελούν το ρυθμιστικό πλαίσιο που περιέχουν τις αρχές και διαδικασίες, με βάση τις οποίες εκτελείται το ελεγκτικό έργο. Η βασική τους λειτουργία είναι η υποχρεωτική καθοδήγηση για όλους τους επαγγελματίες που ασκούν εσωτερικό έλεγχο. Η κατανόηση και η εφαρμογή των Διεθνών Προτύπων βελτιώνει την εταιρική διακυβέρνηση, ενώ παράλληλα στηρίζει το έργο των Επιτροπών Ελέγχου και της Διοίκησης.

Τα Διεθνή Ελεγκτικά Πρότυπα εκδίδονται από το 'Συμβούλιο Διεθνών Προτύπων Ελέγχου και Διασφάλισης' (International Auditing and Assurance Standards Board "IASB") και έχουν ως κύριο σκοπό την επίτευξη της ομοιόμορφης εκτέλεσης, σε διεθνές επίπεδο, όλων των ελεγκτικών εργασιών.

Το Διεθνές Ινστιτούτο Εσωτερικών Ελεγκτών αποτελεί έναν ρυθμιστικό φορέα που παρέχει στους επαγγελματίες του εσωτερικού ελέγχου σε όλον τον κόσμο μια αξιόπιστη καθοδήγηση μέσα από το Πλαίσιο Διεθνών Επαγγελματικών Προτύπων [IPPF: International Standards for the Professional Practice of Internal Auditing (Standards)] για την εκτέλεση του έργου του εσωτερικού ελέγχου.

1.4. ΠΡΟΤΥΠΑ ΕΛΕΓΧΟΥ ΠΛΗΡΟΦΟΡΙΚΗΣ

Υπάρχουν διάφορα πρότυπα για τον Έλεγχο Πληροφορικής που έχουν εκδοθεί από διάφορους οργανισμούς, όπως COSO, INTOSAI, IFAC, ISACA, κ.λπ. Το πιο διαδεδομένο θεωρείται το πλαίσιο COBIT της ISACA. Για περισσότερες πληροφορίες, βλ., *'Παράρτημα 2. Πρότυπα Διαχείρισης Τεχνολογίας'.*

1.5. ΤΥΠΟΙ ΕΣΩΤΕΡΙΚΟΥ ΕΛΕΓΧΟΥ

Οι βασικότεροι τύποι εσωτερικού ελέγχου είναι οι εξής:

1.5.1. Οικονομικός έλεγχος (Financial Audit). Ο στόχος αυτού του ελέγχου είναι να διαπιστώσει τον βαθμό στον οποίο διασφαλίζεται η σωστή απεικόνιση, ακρίβεια και αξιοπιστία των χρηματοοικονομικών καταστάσεων.

1.5.2. Έλεγχος παραγωγής (Production Audit). Ο στόχος αυτού του ελέγχου είναι να διαπιστώσει εάν και κατά πόσο τηρούνται οι διαδικασίες σε όλο το εύρος της παραγωγής, οι παραγόμενες ποσότητες είναι σύμφωνες με το εγκεκριμένο από τη διοίκηση πρόγραμμα, γίνεται σωστή χρήση του μηχανολογικού εξοπλισμού, τηρούνται οι προδιαγραφές των προϊόντων και εκπαιδεύονται τα στελέχη.

1.5.3. Διοικητικός έλεγχος (Management Audit). Ο στόχος αυτού του ελέγχου είναι να διαπιστώσει τον βαθμό στον οποίο τα τμήματα διοικούνται σωστά. Εξετάζεται και αξιολογείται η αποτελεσματικότητα του σχεδιασμού και η στρατηγική της εταιρίας ως προς την επίτευξη των στόχων, τη διαχείριση του ανθρώπινου δυναμικού και γενικότερα όλων των δραστηριοτήτων του που αφορούν τα θέματα της διοίκησης.

1.5.4. Έλεγχος Πληροφορικής (IT Audit). Ο στόχος αυτού του ελέγχου είναι να διαπιστώσει τον βαθμό στον οποίο διασφαλίζεται η αξιοπιστία, εμπιστευτικότητα και ακεραιότητα των διαθέσιμων πληροφοριών, που έγκειται στην αποτελεσματικότητα των πληροφοριακών συστημάτων, τη σωστή χρήση των πόρων, την ενίσχυση της ασφάλειας υποδομών και πληροφοριών, την ορθότητα, πληρότητα και ακρίβεια των συναλλαγών και της ενημέρωσης των αρχείων των πληροφοριών και τη συντήρηση των ετήσιων και ιστορικών στοιχείων.

1.6. ΤΥΠΟΙ ΕΛΕΓΧΟΥ ΠΛΗΡΟΦΟΡΙΚΗΣ

Οι έλεγχοι πληροφορικής μπορούν να εκτελεσθούν από εσωτερικούς ελεγκτές καθώς και από εξωτερικούς ελεγκτές ή άλλους συμβούλους επιχειρήσεων ή και ειδικούς επιστήμονες.

Οι διάφοροι πιο συνηθισμένοι τύποι ελέγχου πληροφορικής είναι οι εξής:

Τύπος 1. Επισκόπηση Γενικών Μέτρων Διακυβέρνησης Πληροφορικής

Μια επισκόπηση και αξιολόγηση των γενικών ελέγχων και μέτρων (*General Controls Review*) που διέπουν τη διακυβέρνηση πληροφορικής μιας εταιρίας, όπως:

(α) Την οργάνωση της διεύθυνσης και προμηθειών πληροφορικής

(β) Την ανάπτυξη, λειτουργία και συντήρηση των συστημάτων πληροφορικής

(γ) Την ανάπτυξη και εφαρμογή μέτρων φυσικής και λογικής ασφάλειας του εξοπλισμού και των συστημάτων πληροφορικής

(δ) Την εξέταση των διαδικασιών λειτουργίας ενός κέντρου δεδομένων

(ε) Τη διαχείριση του λογισμικού του συστήματος (operating system software), κ.λπ.

Πιο αναλυτικά η επισκόπηση και αξιολόγηση μπορεί να περιλαμβάνει μία ή περισσότερες περιοχές ελέγχου πληροφορικής (IT AUDIT AREAS), όπως:

- ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: ΕΤΑΙΡΙΚΗ ΔΙΑΚΥΒΕΡΝΗΣΗ
- ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: ΔΙΑΚΥΒΕΡΝΗΣΗ ΠΛΗΡΟΦΟΡΙΚΗΣ
- ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: ΟΡΓΑΝΩΣΗ ΠΛΗΡΟΦΟΡΙΚΗΣ
- ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: ΣΤΡΑΤΗΓΙΚΗ ΠΛΗΡΟΦΟΡΙΚΗΣ
- ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: ΑΣΦΑΛΕΙΑ ΣΥΣΤΗΜΑΤΩΝ
- ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: ΣΧΕΔΙΑΣΜΟΣ ΕΚΤΑΚΤΩΝ ΑΝΑΓΚΩΝ
- ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: ΝΟΜΙΚΑ ΘΕΜΑΤΑ ΠΛΗΡΟΦΟΡΙΚΗΣ
- ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ
- ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: ΠΕΡΙΒΑΛΛΟΝ ΕΡΓΑΣΙΑΣ
- ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: ΑΝΑΠΤΥΞΗ ΚΑΙ ΣΥΝΤΗΡΗΣΗ ΣΥΣΤΗΜΑΤΩΝ
- ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: ΛΕΙΤΟΥΡΓΙΑ ΥΠΟΛΟΓΙΣΤΙΚΟΥ ΚΕΝΤΡΟΥ
- ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: ΣΥΝΤΗΡΗΣΗ ΛΕΙΤΟΥΡΓΙΚΟΥ ΣΥΣΤΗΜΑΤΟΣ
- ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: ΔΙΑΧΕΙΡΙΣΗ ΔΕΔΟΜΕΝΩΝ & ΒΑΣΗΣ ΔΕΔΟΜΕΝΩΝ

- ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: ΠΡΟΣΩΠΙΚΟΙ ΥΠΟΛΟΓΙΣΤΕΣ
- ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: ΥΠΟΣΤΗΡΙΞΗ ΧΡΗΣΤΩΝ
- ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: ΤΗΛΕΠΙΚΟΙΝΩΝΙΕΣ & ΔΙΚΤΥΑ ΔΕΔΟΜΕΝΩΝ
- ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: ΛΕΙΤΟΥΡΓΙΑ ΕΦΑΡΜΟΓΩΝ (Application Controls)

Η κάθε περιοχή διέπεται από συγκεκριμένα μέτρα (πολιτικές, διαδικασίες, κ.λπ.) για την καλύτερη οργάνωση και λειτουργία της συνολικής πληροφορικής της εταιρίας. Ενδεικτικά τέτοια μέτρα περιέχονται στο δεύτερο βιβλίο 'Διακυβέρνηση Πληροφορικής'.

Τύπος 2. Επισκόπηση Ειδικών Μέτρων Λειτουργίας Εφαρμογών Πληροφορικής

Μια ανασκόπηση και αξιολόγηση των ελέγχων και μέτρων λειτουργίας (*Application Controls Review*) για ένα συγκεκριμένο πληροφοριακό σύστημα (information system) ή εφαρμογή (application). Αυτό θα περιλαμβάνει την εξέταση των ελέγχων κατά την εισαγωγή, επεξεργασία και παραγωγή των δεδομένων του πληροφοριακού συστήματος, τα θέματα επικοινωνιών δεδομένων, τη διαδικασία της ασφάλειας των δεδομένων, τον έλεγχο των αλλαγών του συστήματος, καθώς και ζητήματα ποιότητας των δεδομένων.

Τύπος 3. Επισκόπηση της Διαδικασίας Ανάπτυξης Εφαρμογών Πληροφορικής

Μια πολύ λεπτομερειακή ανασκόπηση και αξιολόγηση (*System Development Review*) της μεθοδολογίας, των ελέγχων και των μέτρων ανάπτυξης ενός συγκεκριμένου πληροφοριακού συστήματος (information system) ή εφαρμογής (application). Αυτό περιλαμβάνει την αξιολόγηση της αναπτυξιακής διαδικασίας, καθώς και των προϊόντων που παράγονται. Επίσης έμφαση δίνεται στην αναπτυξιακή διαδικασία για να εκτιμηθεί κατά πόσον ο σχεδιασμός του συστήματος, και ανάπτυξη γίνεται με συγκροτημένο τρόπο, σε ένα ελεγχόμενο περιβάλλον, και σύμφωνα με την καθορισμένη μεθοδολογία.

Τύπος 4. Επισκόπηση της Ασφάλειας Πληροφορικής

Μια πολύ λεπτομερειακή ανασκόπηση και αξιολόγηση (*Security Audit*) της μεθοδολογίας, των ελέγχων και των μέτρων ασφάλειας και προστασίας στα συστήματα πληροφορικής για να εκτιμηθεί ο βαθμός στον οποίον τηρείται εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των δεδομένων και των συστημάτων, ανάλογα με το προφίλ κινδύνου της πληροφορικής και το εταιρικό προφίλ κινδύνου της εταιρίας ή οργανισμού.

Τύπος 5. Ειδικός Έλεγχος Επιβεβαίωσης Πληροφοριών

Μια πολύ λεπτομερειακή αξιολόγηση της στρατηγικής και των φυσικών, τεχνικών και διοικητικών μέτρων ασφάλειας (*Information Assurance*) όλων των εταιρικών πληροφοριών (προσωπικών, οικονομικών, φήμης, έρευνας, κ.λπ.) και συστημάτων πληροφορικής για τη διαβεβαίωση ότι προστατεύονται επαρκώς τα χαρακτηριστικά της ακεραιότητας (integrity), διαθεσιμότητας (availability), εχεμύθειας (confidentiality), πιστοποίησης (authentication) και μη άρνησης (non-repudiation) όλων των συστημάτων και δεδομένων που συντηρούν.

Τύπος 6. Ειδικός Έλεγχος Συμμόρφωσης Πληροφορικής

Μια πολύ λεπτομερειακή αξιολόγηση της στρατηγικής και των φυσικών, τεχνικών και διοικητικών μέτρων συμμόρφωσης πληροφορικής (*IT Compliance*) για τη διαβεβαίωση ότι η εταιρία συμμορφώνεται επαρκώς με τις ισχύουσες νομικές διατάξεις, κανόνες ρυθμιστικών αρχών, και διεθνών προτύπων σχετικά με την προστασία και διαχείριση όλων τα δεδομένων, πληροφοριών και συστημάτων πληροφορικής που λειτουργούν στη συγκεκριμένη εταιρία.

1.7. ΓΕΝΙΚΗ ΠΡΟΣΕΓΓΙΣΗ ΚΑΙ ΦΑΣΕΙΣ ΕΛΕΓΧΟΥ ΠΛΗΡΟΦΟΡΙΚΗΣ

1.7.1. Γενική Προσέγγιση Ελέγχου Πληροφορικής

Υπάρχουν 3 προσεγγίσεις για τη διεξαγωγή ελέγχων πληροφορικής:

(α) Γύρω από τον υπολογιστή (Auditing Around the Computer),

(β) Με τη βοήθεια του υπολογιστή (Auditing With the Computer) και

(γ) Διά μέσου του υπολογιστή (Auditing Through the Computer).

1.7.2. Φάσεις Ελέγχου Πληροφορικής

Φάση 1. Αρχικός έλεγχος και αξιολόγηση της περιοχής ή συστήματος που πρόκειται να ελεγχθεί.

Φάση 2. Λεπτομερής εξέταση και αξιολόγηση των μέτρων. Αυτό περιλαμβάνει την επανεξέταση των πολιτικών, διαδικασιών και συστημάτων τεκμηρίωσης: Ο ελεγκτής εξετάζει έγγραφα, όπως περιγραφές, διαγράμματα, λίστες προγραμμάτων, τεκμηρίωση συστημάτων, κ.λπ.

Στον έλεγχο στο γραφείο έλεγχο (desk checking), ο ελεγκτής επεξεργάζεται ψεύτικα ή πραγματικά δεδομένα μέσα από τη λογική του προγράμματος.

Φάση 3. Έλεγχος συμμόρφωσης: Ο ελεγκτής διενεργεί ελέγχους προκειμένου να διαπιστωθεί ότι τα μέτρα διακυβέρνησης πληροφορικής (πολιτικές, διαδικασίες, πρακτικές, κ.λπ.) που καθορίζονται από τη διοίκηση λειτουργούν όπως έχει προγραμματιστεί.

Φάση 4. Ουσιαστικές Δοκιμές: Οι ουσιαστικές δοκιμές (Substantive Testing) είναι η άμεση επαλήθευση των οικονομικών μεγεθών ή και εκτέλεση των συναλλαγών. Παραδείγματα περιλαμβάνουν την επιβεβαίωση των λογαριασμών του λογιστηρίου, μισθοδοσίας, δοκιμή ενός πληροφοριακού συστήματος, κ.λπ. Μπορούν να χρησιμοποιηθούν διάφορες τεχνικές και λογισμικό, όπως:

Test Data approach, Integrated-Test-Facility (ITF) Approach, Parallel Simulation, και Audit Software.

Φάση 5. Ανάλυση και Έκθεση Ελέγχου.

Για περισσότερες αναλυτικές λεπτομέρειες δείτε Κεφάλαιο 5 (Σχέδιο Ελέγχου Πληροφορικής) και Κεφάλαιο 6 (Μεθοδολογία Ελέγχου Πληροφορικής).

1.8. ΠΟΤΕ ΚΑΙ ΠΩΣ ΧΡΗΣΙΜΟΠΟΙΕΙΤΑΙ ΤΟ ΠΛΑΙΣΙΟ ΕΛΕΓΧΟΥ ΠΛΗΡΟΦΟΡΙΚΗΣ

Το Πλαίσιο Ελέγχου Πληροφορικής θεσπίζεται στην αρχή λειτουργίας του τμήματος εσωτερικού ελέγχου και έναρξη ελέγχων πληροφορικής και βελτιώνεται μετά την εκτέλεση ελέγχων, όπως απαιτείται.

Χρησιμοποιείται για:

1. Την καλύτερη οργάνωση των ελεγκτών πληροφορικής,
2. Τον πιο αποδοτικότερο σχεδιασμό ελέγχων πληροφορικής, και
3. Την πιο ολοκληρωμένη υποστήριξη και επίβλεψη του ελεγκτικού έργου πληροφορικής από τη διοίκηση του τμήματος εσωτερικού ελέγχου και την ανώτατη διοίκηση της εταιρίας.
4. Μπορεί επίσης να αξιοποιηθεί και από τα στελέχη του τμήματος πληροφορικής της εταιρίας σας για την πληρέστερη προετοιμασία των και την καλύτερη συμμετοχή των σε ελέγχους πληροφορικής που σχεδιάζονται να εκτελεσθούν στην εταιρία σας.

«Το βιβλίο αυτό είναι όλο ευανάγνωστο και χρήσιμο, χωρίς τίποτα περιττό. Αναλυτικότατος, εμπεριστατωμένος οδηγός, αξιοποιήσιμος όχι μόνον στην οργάνωση αποτελεσματικών ελέγχων των λειτουργιών πληροφορικών συστημάτων αλλά, νομίζω και για τον αποτελεσματικό σχεδιασμό τους. Εξαιρετικά κατατοπιστικό για τη βέλτιστη οργάνωση της ανάπτυξης και προστασίας τέτοιων συστημάτων, των λειτουργιών τους και τη διαφύλαξη των δεδομένων που συγκεντρώνουν.

Αποτελεί συστηματικό, πρακτικό βοήθημα για την προετοιμασία πιστοποιήσεων κατά ISO.»

Νίκος Β. Σταθόπουλος, CEO
Εταιρία Προηγμένων Εφαρμογών Συστημάτων Διοίκησης
ISON Psychometrica

«Το πόνημα του κ. Κυριαζόγλου έχει δομηθεί σε απλή και κατανοητή γλώσσα, χωρίς να χάνει σε επιστημονική αξία, όντας έτσι κατάλληλο, τόσο για τον ειδικευμένο επαγγελματία όσο και για εκείνον που κάνει τα πρώτα του βήματα στον χώρο του IT Auditing.»

Παναγιώτης Ψωρόιδας
Managing Partner
TRIAENA Synergies & Consulting P.C.

www.fylatos.com