Ινστιτούτο Εσωτερικών Ελεγκτών Ελλάδας

NEWS

Τεύχος 32 - ΔΕΚΕΜΒΡΙΟΣ 2017

Περιοδική έκδοση του ΙΝΣΤΙΤΟΥΤΟΥ ΕΣΩΤΕΡΙΚΩΝ ΕΛΕΓΚΤΩΝ ΕΛΛΑΔΑΣ

Περιεχόμενα

Συντελεστές έκδοσης:
Στάβαρης Δημήτρης
Μέλος ΔΣ – Συντονιστής Επιτροπής Δημοσίων Σχέσεων
Κληρονόμος Λάμπρος
Συντονιστής Έκδοσης Newsletter
Κόκκα Έφη
Γεώργιος Βουσινάς
Λίλη Ζαφείρη
Ιωάννης Μιχαλόπουλος
Αλεξάνδρα Μουλαβασίλη
Ελένη Νικολάντου
Μαρία Σουρή
Εύη Φωτιάδου

ΙΝΣΤΙΤΟΥΤΟ ΕΣΩΤΕΡΙΚΩΝ ΕΛΕΓΚΤΩΝ ΕΛΛΑΔΑΣ (IEEE)
Γ΄ Σεπτεμβρίου 101 Αθήνα 10434
Τηλ.: +30 210 8259504, fax: +30 210 8229405
e-mail: info@hiia.gr, website: www.hiia.gr

Αγαπητά Μέλη,

Η αθρόα συμμετοχή σας στο Συνέδριο μας "Eyes Wide Open" και η έρευνα ικανοποίησης, με τις πηγαίες και ειλικρινείς απαντήσεις σας, αποτελούν τους βασικότερους λόγους για να πούμε με ιδιαίτερη χαρά ότι το Συνέδριο μας ήταν ένα πολύ επιτυχημένο γεγονός. Αποτελεί πλέον το ετήσιο «σημείο» συνάντησης των μελών μας και όλων όσων αγαπούν και ενδιαφέρονται για το επάγγελμα μας.

Ένα μεγάλο ευχαριστώ στους Ομιλητές, τους Χορηγούς, τους Διευθυντές των Μονάδων Εσωτερικού Ελέγχου, που στηρίζουν το Ινστιτούτο σε όλες τις δράσεις του, τους υποστηρικτές, και τους εθελοντές. Όμως, το πιο μεγάλο ευχαριστώ είναι για όλους εσάς που με την αξιοπρεπή παρουσία σας, τον επαγγελματισμό σας, την αφοσίωσή και την αγάπη σας, στηρίξατε το μεγάλο αυτό γεγονός και όλοι –συμπεριλαμβανομένων και των Ευρωπαίων επιφανών ομιλητών μας- μπορούν να μιλούν για το Ινστιτούτο και τα μέλη μας με τόση εκτίμηση και σεβασμό. Η εξαιρετική διοργάνωση του Συνεδρίου οφείλεται στη Διευθύντριά μας και την Υπεύθυνη του Γραφείου μας. Ο Πρόεδρος του ECIIA είπε πρόσφατα, σε συνάντησή μας στις Βρυξέλλες, ότι «έφυγα ενθουσιασμένος από το Συνέδριο στην Ελλάδα, τη χώρα στην οποία όλοι οφείλουμε την ύπαρξή μας». Ο ελληνικός Τύπος, λόγω των δημοσιεύσεων των Ελλήνων επιφανών ομιλητών μας, αναφέρθηκε εκτενώς στο Συνέδριο μας και στον Εσωτερικό Έλεγχο. Προσωπικά κρατώ τα καλά σας λόγια και τις προτάσεις σας και υπόσχομαι ένα ακόμη καλύτερο Συνέδριο το 2018, όπως αξίζει στα σπουδαία μέλη και τους αγαπητούς φίλους του Ινστιτούτου μας.

Στο παρόν τεύχος θα βρείτε πληροφόρηση για το ετήσιο Εκπαιδευτικό Πρόγραμμα του Ινστιτούτου που έχει έναν και μοναδικό σκοπό: την ανάπτυξη των μελών και φίλων μας. Πολλά από τα Σεμινάριά μας μπορούν να τα παρακολουθήσουν επαγγελματίες εκτός Εσωτερικού Ελέγχου, ενώ κάποια άλλα είναι απολύτως εξειδικευμένα σε ιδιαίτερα θέματα. Σας παρακαλώ πολύ να στηρίξετε το Εκπαιδευτικό Πρόγραμμα, συμμετέχοντας και διαδίδοντας τα Σεμινάριά μας και ακόμη περισσότερο τις διεθνείς Πιστοποιήσεις μας.

Εκ μέρους του Διοικητικού Συμβουλίου και του Γραφείου μας, σας εύχομαι Καλή Χρονιά με αγάπη και υγεία σε εσάς και τις οικογένειές σας και πολλές επιτυχίες στις εταιρίες σας! Προχωράμε με αισιοδοξία, αλλάζουμε και με eyes wide open γινόμαστε διαρκώς καλύτεροι.

Επόμενη σημαντική συγκέντρωσή μας θα είναι στην κοπή της πίτας μας, το πρώτο δίμηνο του 2018.

Βέρρα Μαρμαλίδου
Πρόεδρος | ΙΙΑ Ελλάδας

Ετήσιο Συνέδριο

Την Παρασκευή 20 Οκτωβρίου 2017 στο Μέγαρο Μουσικής Αθηνών, πραγματοποιήθηκε το Ετήσιο Συνέδριο του Ινστιτούτου Εσωτερικών Ελεγκτών Ελλάδας με θέμα: Eyes Wide Open.

Το Συνέδριο παρακολούθησαν πάνω από 650 άτομα από τον Ιδιωτικό και Δημόσιο τομέα.

Angela Witzany, CIA, QIAL, CRMA IIA 2016-17 Global Chairman of the Board

Farid Aractingi, Vice President, Audit, Risk and Organisation, Renault / Chairman, Renault-Nissan Consulting / Vice-President, ECIIA (European Confederation of Institutes of Internal Auditing) / Independent Director and Chairman of the Audit Committee, RCI Banque (regulated financial affiliate of Renault) and Fattal Group (importer of consumer goods in MENA region).

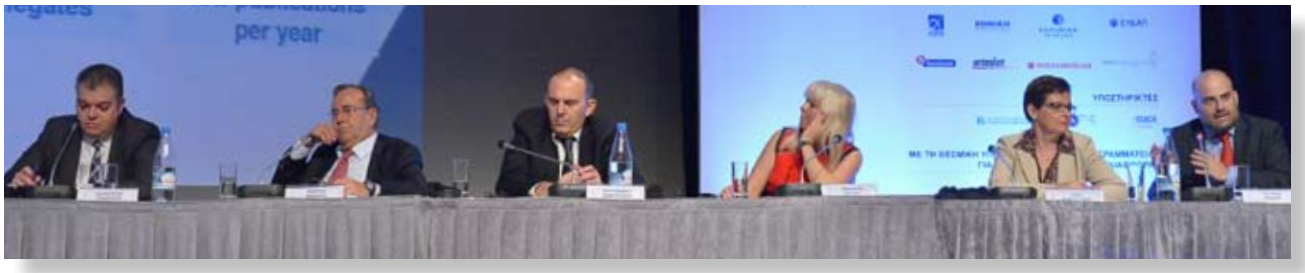
Βράβευση του IEEE από τον Πρόεδρο του ECIIA (European Confederation of Institutes of Internal Auditors) Farid Aractingi για την 20ετή παρουσία του ΙΙΑ Ελλάδας στο ECIIA

Βράβευση Σίμου Μπουρσαλιάν για τη διάκριση στις εξετάσεις CIA από τον αντιπρόεδρο του IEEE, Π. Βαλαντάση

“Οι 3 πυλώνες της Εσωτερικής μας Διακυβέρνησης» Δ. Τσούχλος

«The new legal framework for Audit Committees” Γ. Λαγός

Panel 1. «Γεωπολιτικοί κίνδυνοι, προκλήσεις και ευκαιρίες», Γ. Ραουνάς, Α. Σιάμισης, Σ. Λυγερός, Α. Συρίγος



Panel 2. "Οι 4 πυλώνες της διακυβέρνησης σε έναν κόσμο που αλλάζει. Νέα νομοθεσία, τάσεις & εμπειρίες»
Π. Τσουκάτος, Γ. Βενιέρης, Α. Δημητριάδης, Μ. Okland, Λ. Κοντογιάννη, Α. Μπίνης

Χ. Σταϊκούρας, «Ελληνική Οικονομία και Εσωτερική Διακυβέρνηση. Προκλήσεις & Ευκαιρίες»

Κ. Χρήστου, Γεν. Γραμματέας για την καταπολέμηση της διαφθοράς

Γ. Πατούλης, «Η ενίσχυση της διαφάνειας προϋπόθεση για την Αναπτυξιακή Αναγέννηση της χώρας. Η συμβολή της Αυτοδιοίκησης»

Γ. Πελεκανάκης, Π. Βαλαντάσης, Λ. Ράπτη, Δ. Στάβαρης, Γ. Σελίμης, Β. Μαρμαλίδου, Β. Πολίτου, Ε. Κόκκα, Ζ. Σόμπολος, Γ. Μπαγλατζής, Γ. Καραγεώργου.

Συνέντευξη*

Μαρία Σουρή

Παναγιώτης Δρούκας

Προέδρος ISACA Athens Chapter
Ελεγκτής Πληροφοριακών Συστημάτων στην Τράπεζα της Ελλάδος

- Πρόεδρος του Ινστιτούτου Ελεγκτών Συστημάτων Πληροφορικής (ISACA Athens Chapter).

- Απόφοιτος του Τμήματος Πληροφορικής του Πανεπιστημίου Πειραιώς, κάτοχος Master στην Πληροφορική και στα Εφαρμοσμένα Οικονομικά.

- Πιστοποιημένος στον Έλεγχο, τη Διαχείριση Κινδύνων και στη Διακυβέρνηση Πληροφοριακών Συστημάτων (CISA, CRISC, CGEIT).

- Εργάζεται στον χώρο της πληροφορικής από το 1998 και του ελέγχου πληροφοριακών συστημάτων από το 2002.

- Σήμερα Εργάζεται ως επιθεωρητής Συστημάτων Πληροφορικής στην Τράπεζα της Ελλάδος (ΤτΕ).

Ως Πρόεδρος του ISACA Athens Chapter, πείτε μας παρακαλώ λίγα λόγια για το Ινστιτούτο, καθώς και για το ποιος είναι ο βασικός του ρόλος και οι ενέργειες που επιτελεί για την ανάπτυξη της ασφάλειας των πληροφοριών.

Το Ινστιτούτο Ελέγχου Συστημάτων Πληροφορικής (ISACA Athens Chapter), το οποίο είναι παράρτημα του διεθνούς οργανισμού «Information Systems Audit and Control Association - ISACA», έχει διαγράψει μια εξαιρετική πορεία τα τελευταία χρόνια, διανύοντας μια από τις καλύτερες περιόδους της εικοσιτριάχρονης παρουσίας του στην Ελλάδα. Το Ινστιτούτο έχει καταφέρει να δώσει το παρόν σε όλα τα μεγάλα συνέδρια και εκδηλώσεις στην Ελλάδα και το εξωτερικό, διαμορφώνοντας τις εξελίξεις στις περιοχές της ασφάλειας πληροφοριών, διακυβέρνησης πληροφορικής, διαχείρισης κίνδυνου και ελέγχου πληροφοριακών συστημάτων.

Το Ινστιτούτο σήμερα διαθέτει πάνω από 450 μέλη, εκ των οποίων η συντριπτική πλειοψηφία διαθέτει κάποια από τις διεθνείς πιστοποιήσεις CISA, CISM, CGEIT και CRISC, ενώ αξίζει να σημειωθεί ότι παρά την συνεχιζόμενη οικονομική κρίση και την εκροή ανθρώπινου κεφαλαίου στο εξωτερικό έχουμε καταφέρει να κρατήσουμε σχεδόν σταθερό τον αριθμό μελών μας, κυρίως λόγω των ευκαιριών εκπαίδευσης που παρέχουμε καθώς και των επαγγελματικών ευκαιριών που εξακολουθούν να υφίστανται στην Ελλάδα παρά την κρίση.

Η καλή πορεία των τελευταίων ετών δημιουργούν όμως νέες προσδοκίες και αναπροσαρμογή των στόχων μας προς τα πάνω. Πριν από λίγα χρόνια πήραμε την πρωτοβουλία να υποστηρίξουμε με έλληνες πιστοποιημένους εκπαιδευτές τα «COBIT5 Foundation Courses», επιδοτώντας παράλληλα τη συμμετοχή των μελών μας σε αυτά. Ήταν μία πρωτοποριακή κίνηση για τα δεδομένα της εποχής, μοναδική σε πανευρωπαϊκό επίπεδο που στόχο είχε την παροχή εκπαίδευσης υψηλών προδιαγραφών σε όλους. Στη συνέχεια, κάναμε το ίδιο για το «CSX Fundamentals» και σκοπεύουμε να ακολουθήσουμε την ίδια στρατηγική για όσες θεματικές περιοχές δηλώσετε ενδιαφέρον μέσω της έρευνας μελών που πραγματοποιείται σε τακτική βάση.

Θα θέλατε παρακαλώ να μας δώσετε ένα περίγραμμα των κυριοτέρων δράσεων του Ινστιτούτου για τη χρονιά που εκπνέει, καθώς και τους βασικούς στόχους και προοπτικές για τη νέα χρονιά που πλησιάζει;

Το 2017 που πλησιάζει στο τέλος του πρόκειται να κλείσει με το ετήσιο συνέδριο του ινστιτούτου έχει προγραμματιστεί από 18-20 Δεκεμβρίου με κεντρικό θέμα την προετοιμασία και υλοποίηση προγραμμάτων δράσης για την προστασία προσωπικών δεδομένων (data privacy protection programs) εν όψη της εφαρμογής του Γενικού Κανονισμού για την Προστασία Δεδομένων (Κανονισμός ΕΕ 2016/679 ή GDPR)

καθώς και την ασφαλή μετάβαση στον ψηφιακό μετασχηματισμό.

Στο πλαίσιο αυτό έχουν προσκληθεί σημαντικοί έλληνες και ξένοι και ομιλητές με σημαντική εμπειρία όπως οι κ.κ. Χρήστος Δημητριάδης, Yves Le Roux, Μίνα Ζούλοβιτς, Andrea Simandi, Bruno Horta Soares και Ξενοφών Λιαπάκης. Με τη βοήθειά τους θα αναλυθούν από τεχνικής και νομικής πλευράς οι απαιτήσεις του GDPR καθώς και οι νέες προκλήσεις ασφάλειας που προκύπτουν εξαιτίας του ψηφιακού μετασχηματισμού (digital transformation).

> “Η εμπειρία δείχνει δυστυχώς ότι η μεγαλύτερη απειλή για την ασφάλεια των συστημάτων πληροφορικής ενός οργανισμού είναι η αμέλεια ή ολιγωρία εφαρμογής βασικών κανόνων ψηφιακής υγιεινής. Καθώς η πληροφορία αποτελεί πολύτιμο περιουσιακό στοιχείο για μια εταιρεία, δεν υφίσταται πλέον καμία δικαιολογία για την επίδειξη άγνοιας ή αδιαφορίας από την πλευρά μας.”

Με τη μακρόχρονη εμπειρία που έχετε αποκομίσει ως ελεγκτής πληροφοριακών συστημάτων, ποια θεωρείτε ότι είναι διαχρονικά η μεγαλύτερη απειλή που αντιμετωπίζει ένας οργανισμός αναφορικά με τα θέματα της πληροφορικής;

Η εμπειρία δείχνει δυστυχώς ότι η μεγαλύτερη απειλή για την ασφάλεια των συστημάτων πληροφορικής ενός οργανισμού είναι η αμέλεια ή ολιγωρία εφαρμογής βασικών κανόνων ψηφιακής υγιεινής, οι οποίοι είναι γνωστοί εδώ και καιρό, όπως:

- Λήψη αντιγράφων ασφαλείας σε εταιρικά δεδομένα (αρχεία, e-mail, κ.α.) σε οποιαδήποτε συσκευή ή μέσο αποθήκευσης και αν τηρούνται αυτά.
- Περιορισμός προσβάσεων στην πληροφορία με γνώμονα την αρχή των ελάχιστων προνομίων (least privilege principle).
- Διαρκής παρακολούθηση και έλεγχος λογαριασμών προνομιακής πρόσβασης (privileged user accounts).
- Πραγματοποίηση αναβαθμίσεων και αλλαγών σε συστήματα και εφαρμογές με ελεγχόμενο τρόπο έτσι ώστε να μην προκύπτουν διακοπές λειτουργίας ή απώλειες δεδομένων.
- Κατάλληλη οργάνωση και προετοιμασία για την έγκαιρη και αποτελεσματική αντιμετώπιση κυβερνοεπιθέσεων.

Καθώς η πληροφορία αποτελεί πολύτιμο περιουσιακό στοιχείο για μια εταιρεία, δεν υφίσταται πλέον καμία δικαιολογία για την επίδειξη άγνοιας ή αδιαφορίας από την πλευρά μας. Πόσο μάλλον όταν οι διαθέσιμες τεχνολογικές λύσεις και υπηρεσίες σήμερα μας φέρνουν όλα τα παραπάνω στο πιάτο (π.χ. cloud computing, backup as a service, security as a service, κ.α.)

Καινοτομία, τεχνολογία και εσωτερικός έλεγχος. Σε ποιο πλαίσιο κατά τη γνώμη σας δύναται ένας οργανισμός να κατακτήσει τη «μαγική», αν μου επιτραπεί ο όρος, ισορροπία, που και θα τον καταστήσει τεχνολογικά καινοτόμο και δεν θα του προκαλέσει ρήγμα αναφορικά με τη μη καταπάτηση των θεμελιωδών αρχών και κανόνων που επιτάσσει μία χρηστή εταιρική διακυβέρνηση;

Ο Εσωτερικός Έλεγχος δεν μπορεί να παραμείνει απλός θεατής σε μια εταιρεία που έχει ήδη ψηφιοποιήσει ένα μεγάλο μέρος των διαδικασιών της και να συνεχίσει να «τρέχει» παραδοσιακούς επιτόπιους ελέγχους με τον ίδιο τρόπο που τους έκανε πάντα.

Για παράδειγμα, σκεφτείτε μια εταιρεία που χορηγεί εκπτωτικά κουπόνια στους πελάτες της μέσω mobile application σύμφωνα με την ανάλυση ιστορικού αγορών πελάτη (customer profiling μέσω data analytics). Εάν κληθείτε να ελέγξετε τη διαδικασία χορήγησης εκπτωτικών κουπονιών θα το κάνετε με παραδοσιακά ερωτηματολόγια, συνεντεύξεις και συλλογή δείγματος; Πόσο αποτελεσματικός θα είναι ο έλεγχός σας όταν παραβλέπει το γεγονός πως το μεγαλύτερο μέρος των αποφάσεων λαμβάνεται από υπολογιστές μετά την επεξεργασία τεράστιων όγκων δεδομένων;

> “Ο Εσωτερικός Έλεγχος δεν μπορεί να παραμείνει απλός θεατής σε μια εταιρεία που έχει ήδη ψηφιοποιήσει ένα μεγάλο μέρος των διαδικασιών της και να συνεχίσει να «τρέχει» παραδοσιακούς επιτόπιους ελέγχους με τον ίδιο τρόπο που τους έκανε πάντα.”

Η ιδανική ισορροπία κατά τη γνώμη μου θα επέλθει όταν ο Εσωτερικός Έλεγχος αποκτήσει την απαραίτητη τεχνογνωσία αλλά και τα κατάλληλα εργαλεία που θα του επιτρέψουν να είναι αποτελεσματικότερος στη δουλειά του και να δίνει προστιθέμενη αξία στον οργανισμό. Συνεχίζοντας το παραπάνω παράδειγμα, μόνο με τη γνώση του σχετικού θεσμικού πλαισίου (Κανονισμός ΕΕ 2016/679 ή GDPR) αλλά και της χρήσης εργαλείων data analytics, ο Εσωτερικός Έλεγχος θα μπορέσει να ελέγξει τελικά εάν η ανάλυση ιστορικού

αγορών είναι σύννομη (δηλαδή συνοδεύεται από εξουσιοδότηση του πελάτη) και εάν τα αποτελέσματά της είναι σύμφωνα με την πολιτική επιβράβευσης πελατών της εταιρείας.

Κυβερνοασφάλεια: προκλήσεις και ευκαιρίες που καλούνται να αντιμετωπίσουν εν γένει οι εσωτερικοί ελεγκτές και δη οι εσωτερικοί ελεγκτές πληροφοριακών συστημάτων. Πείτε μας την άποψή σας παρακαλώ.

Η συχνότητα αλλά και η σφοδρότητα των κυβερνοεπιθεσεων που έχουν σημειωθεί πρόσφατα δεν αφήνουν κανένα περιθώριο εφησυχασμού. Μόνο τον Ιούνιο που μας πέρασε, ο ιός Petya δημιούργησε προβλήματα σε μεγάλους πολυεθνικούς ομίλους, όπως οι Mondelez, Reckitt Benckiser και Maersk. Ειδικά για τον τελευταίο που είναι ένας από τους μεγαλύτερους παίκτες παγκοσμίως στην αγορά μεταφοράς και διαχείρισης εμπορευματοκιβωτίων με μερίδιο γύρω στο 15%, οι ζημιές ανήλθαν μεταξύ US$ 200 και 300 εκ.

Όλα ξεκίνησαν από μια φαινομενικά αθώα εφαρμογή υποβολής αιτημάτων επιστροφής φόρου στην Ουκρανία που μολύνθηκε με τον ιό Petya και κατάφερε να μολύνει με τη σειρά της μέσα σε ελάχιστο χρόνο χιλιάδες servers της εταιρίας. Σαν συνέπεια της μόλυνσης, η θυγατρική Maersk Lines που ήταν υπεύθυνη για τη μεταφορά εμπορευματοκιβωτίων αναγκάστηκε να ακινητοποιήσει όλα τα πλοία της και να αναστείλει τη λειτουργία των 76 εμπορευματικών σταθμών που λειτουργεί παγκοσμίως μέχρι να αποκατασταθεί η βλάβη. Χρειάστηκε περίπου ένας μήνας προκειμένου να αποκατασταθούν σταδιακά οι λειτουργίες της εταιρείας με αποτέλεσμα να επηρεαστεί το 15% του παγκόσμιου εμπορίου με εμπορευματοκιβώτια και να εγγραφούν οι ζημιές που αναφέρθηκαν πιο πάνω σε μια περίοδο μάλιστα που η αγορά μεταφοράς εμπορευματοκιβωτίων παρουσίαζε αυξητικές τάσεις.

Σίγουρα τα μεγέθη που περιγράψαμε είναι τεράστια για μια ελληνική εταιρεία, ωστόσο καμία εταιρεία όσο μεγάλη ή μικρή και εάν είναι δεν θα μπορέσει να ανταπεξέλθει σε μια αναγκαστική αναστολή λειτουργιών τόσο μεγάλης χρονικής διάρκειας. Εάν λοιπόν δεν θέλετε να έχετε την ίδια τύχη, καλό θα είναι να αρχίσετε να χτίζετε γραμμές άμυνας καθώς και δυνατότητες εντοπισμού και ανάκαμψης από κυβερνοεπιθέσεις με την υλοποίηση κατάλληλων οργανωτικών, διαδικαστικών και τεχνικών μέτρων στην εταιρεία σας. Κάτι τέτοιο φυσικά δεν είναι καθόλου εύκολο καθώς απαιτεί προετοιμασία, οργάνωση και έλεγχο προκειμένου να επιβεβαιωθεί ότι όλα λειτουργούν με συνέπεια και αποτελεσματικότητα.

Με απλά λόγια, τι εννοούμε όταν ακούμε σχετικά με το πλαίσιο διακυβέρνησης του κυβερνοχώρου (governance of cyber risk);

Είναι μάλλον αφελές να πιστεύει κανείς ότι υπάρχουν «μαγικές λύσεις» για την αποτελεσματική αντιμετώπιση κυβερνοεπιθέσεων με τη μορφή τεχνικών λύσεων ή υπηρεσιών τρίτων που απλά μπορούμε να αγοράσουμε και στη συνέχεια να ξενοιάσουμε.

Θα πρέπει να αντιληφθούμε ότι στην εποχή που ζούμε είναι μάλλον αναχρονιστικό να ασχολείται κανείς μόνο με την προστασία των σταθερών και φορητών υπολογιστών (π.χ. με την εγκατάσταση λογισμικού endpoint protection) από κυβερνοεπιθέσεις. Και αυτό επειδή έχουμε πάψει πλέον να κάνουμε τη δουλειά μας μόνο με υπολογιστές. Είναι λοιπόν πιθανό να ανοίξουμε email από το κινητό ή την ταμπλέτα μας και να επεξεργαστούμε το πελατολόγιο ή τη μισθοδοσία της εταιρείας μας από τις ίδιες συσκευές. Συνεπώς, το άκρο που θα πρέπει να προστατευθεί δεν είναι ο υπολογιστής αλλά ο άνθρωπος, ο οποίος με τόσες δυνατότητες και συσκευές που έχει στα χέρια του είναι δυνατόν να διαρρεύσει ακούσια πληροφορίες, να πέσει θύμα μόλυνσης από ιούς σε κάποια εταιρική ή προσωπική συσκευή ή ακόμα και να πέσει θύμα υποκλοπής των συνθηματικών του.

> “Η αποτελεσματική αντιμετώπιση κυβερνοεπιθέσεων δεν μπορεί λοιπόν παρά να έχει τη μορφή πλαισίου governance of cyber risk το οποίο να περιλαμβάνει την ευαισθητοποίηση και εκπαίδευση των υπαλλήλων ενός οργανισμού, τη διαμόρφωση της κατάλληλης κουλτούρας αλλά και των κατάλληλων οργανωτικών και διαδικαστικών μέτρων για την άμεση αντίδραση σε κυβερνοεπιθέσεις.”

Η αποτελεσματική αντιμετώπιση κυβερνοεπιθέσεων δεν μπορεί λοιπόν παρά να έχει τη μορφή πλαισίου governance of cyber risk το οποίο να περιλαμβάνει την ευαισθητοποίηση και εκπαίδευση των υπαλλήλων ενός οργανισμού, τη διαμόρφωση της κατάλληλης κουλτούρας αλλά και των κατάλληλων οργανωτικών και διαδικαστικών μέτρων για την άμεση αντίδραση σε κυβερνοεπιθέσεις.

Στο ετήσιο συνέδριο εσωτερικού ελέγχου του ECIIA που διοργανώθηκε στην Ελβετία τον περασμένο Σεπτέμβριο, έγκριτοι επαγγελματίες, εσωτερικοί ελεγκτές από μεγάλες πολυεθνικές εταιρείες, έκαναν λόγο για την επιβεβλημένη ανάγκη εγκαθίδρυσης και λειτουργίας σε κάθε οργανισμό, μίας ομάδας αντιμετώπισης-διαχείρισης του κινδύνου στον κυβερνοχώρο (Cyber Risk Governance Group) και την αναγκαία στενή συνεργασία που θα πρέπει η ίδια να έχει με τη Διεύθυνση Εσωτερικού Ελέγχου του ιδίου. Ουτοπία ή πραγματικότητα για τις εταιρίες που δραστηριοποιούνται στη χώρα μας και σε τι βαθμό;

Δεν θα κουραστώ να υποστηρίζω ότι οποιοσδήποτε οργανισμός οσοδήποτε μεγάλος ή μικρός θα πρέπει να είναι σε θέση να επαναφέρει γρήγορα και σωστά τις λειτουργίες του μετά από μια κυβερνοεπίθεση.

Κάτι τέτοιο σίγουρα δεν σημαίνει ότι είναι απαραίτητο να προσλάβετε τεχνικούς σε forensic analysis, και cyber incident response & recovery που απαιτούνται για τον εντοπισμό, περιορισμό και ανάκαμψη από μια ενδεχόμενη κυβερνοεπίθεση και να τους έχετε να κάθονται. Ωστόσο, θα πρέπει να έχετε ήδη φροντίσει, μέσω συμβάσεων με παρόχους τέτοιων υπηρεσιών, να έχετε στη διάθεσή σας τους κατάλληλους ειδικούς σε ενδεχόμενη κυβερνοεπίθεση.

Επιπλέον, θα πρέπει να καταλάβετε ότι όσες υπηρεσίες ή εξοπλισμό και να αγοράσετε, η ευθύνη ανάκαμψης θα ανήκει πάντα στην εταιρεία, η οποία και θα πρέπει τελικά να έχει τον έλεγχο και τον συντονισμό των ενεργειών ανάκαμψης. Η απόφαση του πόσο μικρή ή μεγάλη θα είναι η ομάδα αντιμετώπισης κυβερνοεπιθέσεων ανήκει στη διακριτική σας ευχέρεια. Ωστόσο, επισημαίνεται πως ομάδα αυτή θα πρέπει να απαρτίζεται και από διευθυντικά στελέχη τα οποία θα κληθούν να συντονίσουν τις επικοινωνίες με πελάτες και συνεργάτες, καθώς και τη σταδιακή επαναφορά των επιχειρησιακών λειτουργιών

Νέος Ευρωπαϊκός Κανονισμός για την προστασία των προσωπικών δεδομένων GDPR τίθεται σε ισχύ από το Μάϊο 2018 και περιλαμβάνει απορρέουσες υποχρεώσεις για πληθώρα οργανισμών και επιχειρήσεων. Με δεδομένο ότι ένα από τα κυριότερα ζητήματα που τίθενται, είναι εάν τα δεδομένα βρίσκονται σε κίνδυνο, καθώς και ποιες πρακτικές και τεχνολογίες θα μειώσουν αποτελεσματικά τους κινδύνους αυτούς, ποια είναι η δική σας τοποθέτηση επί αυτών;

Η άποψή μου είναι ότι ο Γενικός Κανονισμός για την Προστασία Δεδομένων (Κανονισμός ΕΕ 2016/679 ή GDPR) δεν είναι μια απειλή η οποία πρόκειται να δημιουργήσει κύματα καταγγελιών από τους πελάτες ή να φορτώσει την εταιρεία με υπέρογκα διοικητικά πρόστιμα.

Αν τον αντιμετωπίσετε σαν απειλή χάνετε πραγματικά μια πρώτης τάξεως ευκαιρία να βάλετε σε μια τάξη τα προσωπικά σας δεδομένα και να πάρετε επιπλέον αξία από αυτά. Πριν ασχοληθούμε λοιπόν με το ερώτημα εάν τα δεδομένα μας βρίσκονται σε κίνδυνο ή όχι καλό θα ήταν να χαρτογραφήσουμε τις επιχειρηματικές διαδικασίες που συλλέγουν προσωπικά δεδομένα και να εξετάσουμε σοβαρά που αποθηκεύονται τα δεδομένα αυτά, για ποιο λόγο τα κρατάμε και τι τα κάνουμε.

Προκειμένου να μην ανακαλύψετε από την αρχή τον τροχό, υπάρχουν οδηγοί και κατευθυντήριες γραμμές από τον ISACA οι οποίοι θα σας βοηθήσουν να χαράξετε τον δικό σας οδικό χάρτη και να φτιάξετε το δικό σας πρόγραμμα δράσης για την προστασία προσωπικών δεδομένων (data privacy protection program).

> “...ο Γενικός Κανονισμός για την Προστασία Δεδομένων (Κανονισμός ΕΕ 2016/679 ή GDPR) δεν είναι μια απειλή η οποία πρόκειται να δημιουργήσει κύματα καταγγελιών από τους πελάτες ή να φορτώσει την εταιρεία με υπέρογκα διοικητικά πρόστιμα. Αν τον αντιμετωπίσετε σαν απειλή χάνετε πραγματικά μια πρώτης τάξεως ευκαιρία να βάλετε σε μια τάξη τα προσωπικά σας δεδομένα και να πάρετε επιπλέον αξία από αυτά.”

Αναφορικά με την τάση των τελευταίων ετών στο τομέα της τεχνολογίας, το Internet of Things (IoT) και με γνώμονα ότι μία από τις βασικές παραμέτρους που συνοδεύουν το IoT, σημαντικό ρόλο διαδραματίζει και η ασφάλεια. Μπορείτε παρακαλώ να μας κάνετε μία συνοπτική τοποθέτηση επί του θέματος;

Για τους λιγότερο εξοικειωμένους με την ορολογία, το IoT περιλαμβάνει το σύνολο των «έξυπνων» εταιρικών ή οικιακών συσκευών, φορητών ή μη, που είναι ταυτόχρονα συνδεδεμένες στο Internet.

Θα προσπαθήσω να απαριθμήσω μερικές προκειμένου να διαμορφώσετε μια πληρέστερη άποψη: έξυπνα ψυγεία, κλιματιστικά, εκτυπωτές, media players, κάμερες, εγκαταστάσεις συναγερμού κ.α. Φυσικά ο κατάλογος αυξάνεται συνεχώς μέρα με τη μέρα, μέχρι κάθε ηλεκτρική συσκευή να συνδεθεί τελικά στο Internet.

Γιατί όμως ασχολούμαστε με όλες αυτές τις συσκευές; Επειδή κατά κανόνα συνδέονται στο Internet μέσω του εταιρικού ή οικιακού δικτύου προκειμένου να μπορέσουμε π.χ. να εκτυπώσουμε στον εκτυπωτή του σπιτιού μας ενώ βρισκόμαστε εκτός ή να ανάψουμε το κλιματιστικό ενώ οδηγούμε προκειμένου να μας περιμένει ένα δροσερό σπίτι ή γραφείο.

Τελικά, όπως άλλωστε συμβαίνει σε κάθε περίπτωση, το επίπεδο ασφάλειας του οικιακού ή του εταιρικού μας δικτύου εξαρτάται από το επίπεδο ασφάλειας του πιο αδύναμου κρίκου, δηλαδή των συσκευών IoT. Επισημαίνεται ότι οι εν λόγω συσκευές είναι σχετικά καινούργιες και η πρόσφατη εμπειρία έχει δείξει ότι το επίπεδο ασφάλειάς τους είναι υποτυπώδες. Για περισσότερες ανατριχιαστικές λεπτομέρειες μπορείτε να ανατρέξετε στο σχετικό άρθρο των Financial Times *«The internet of things: Home is where the hackers are»*

**Η συνέντευξη εκφράζει προσωπικές και μόνο απόψεις του γράφοντος.*

Γιώργος Βουσινάς

Ο αυξανόμενος ρόλος του Εσωτερικού Ελέγχου στην ασφάλεια του κυβερνοχώρου (**cyber security**)

Με τον όρο ασφάλεια στον κυβερνοχώρο ή **κυβερνοασφάλεια** (cyber security) νοείται η διασφάλιση της απρόσκοπτης λειτουργίας των υποδομών πληροφορικής & επικοινωνιών και η προστασία της εν λόγω λειτουργίας από αστοχία της τεχνολογίας ή κακόβουλη χρήση της. Η κυβερνοασφάλεια αποτελεί το 95% της ευρύτερης έννοιας της ασφάλειας των πληροφοριών. Στη σύγχρονη εποχή, τα δεδομένα ολοένα και περισσότερο ψηφιοποιούνται και το διαδίκτυο χρησιμοποιείται για την αποθήκευση, την πρόσβαση και την ανάκτηση ζωτικής σημασίας πληροφοριών. Η προστασία αυτών των πληροφοριών δεν αποτελεί πλέον απλώς μια προτεραιότητα, αλλά έχει καταστεί αναγκαία για τις περισσότερες εταιρείες και κυβερνητικές υπηρεσίες σε όλο τον κόσμο.

Όσον αφορά την επιλογή ενός πλαισίου ελέγχου της κυβερνοοασφάλειας δεν κρίνεται απαραίτητο να επαναπροσδιοριστούν οι κατευθυντήριες γραμμές και τα υφιστάμενα πλαίσια. Οι οργανισμοί πρέπει να επιλέξουν εκείνο που είναι κατάλληλο για αυτούς (π.χ. ITIL ή COBIT), να το εντάξουν στις διαδικασίες τους και να αναλάβουν την ευθύνη ορθής λειτουργίας του. Τα δημοφιλέστερα εξ αυτών είναι τα κάτωθι:

- ISACA COBIT 5 and the Emerging Cyber Nexus
- NIST Framework for Improving Critical Infrastructure Cybersecurity
- SANS Institute and the Top 20 Critical Security Controls
- PCI DSS Control Catalog
- ISO/IEC 27001.

Η αποτελεσματική διαχείριση κινδύνων είναι απόρροια πολλαπλών επιπέδων προστασίας έναντι του κινδύνου. Ο Εσωτερικός Έλεγχος θα πρέπει να υποστηρίζει το Διοικητικό Συμβούλιο στην κατανόηση της αποτελεσματικότητας των ελέγχων κυβερνοαφάλειας. Οι τρεις γραμμές άμυνας ενάντια στους εμπλεκόμενους κινδύνους στον τομέα της κυβερνοασφάλειας δύναται να χρησιμοποιηθούν ως το κύριο μέσο για τη σωστή δόμηση των ρόλων, την απόδοση ευθυνών, την ύπαρξη λογοδοσίας κατά τη διαδικασία λήψεως αποφάσεων, καθώς και την εγκαθίδρυση κατάλληλων ελεγκτικών μηχανισμών για την επίτευξη αποτελεσματικής διακυβέρνησης της διαχείρισης κινδύνων.

Αποτελώντας την τρίτη γραμμή άμυνας, **τα μέτρα που πρέπει να λάβει ο Εσωτερικός Έλεγχος συνοψίζονται στα κάτωθι:**

1. Συνεργασία με τη Διοίκηση για την ανάπτυξη στρατηγικής και πολιτικής για την ασφάλεια στον κυβερνοχώρο,
2. Κατάλληλες ενέργειες για τη βελτίωση της ικανότητας ενός οργανισμού να εντοπίζει, να αξιολογεί και να μετριάζει τους κινδύνους που σχετίζονται με την κυβερνοασφάλεια σε αποδεκτά επίπεδα,
3. Εξαιτίας του γεγονότος ότι οι σχετιζόμενοι κίνδυνοι με ζητήματα κυβερνοασφάλειας δεν είναι μόνο εξωτερικοί, απαιτείται η αξιολόγηση και ο μετριασμός των πιθανών απειλών που θα μπορούσαν να προκύψουν από τις ενέργειες ενός εργαζομένου ή ενός επιχειρηματικού εταίρου,
4. Ανάπτυξη σχέσεων με την Επιτροπή Ελέγχου και το Διοικητικό Συμβούλιο της εταιρείας προκειμένου να αυξηθεί η ευαισθητοποίηση και οι γνώσεις σχετικά με τις απειλές στον κυβερνοχώρο, καθώς και με τη μεταβαλλόμενη φύση των κινδύνων κυβερνοασφάλειας,
5. Διασφάλιση ότι οι ενεχόμενοι κίνδυνοι στην ασφάλεια του κυβερνοχώρου ενσωματώνονται επίσημα στο Ελεγκτικό Πλάνο των μονάδων Εσωτερικού Ελέγχου,
6. Κατανόηση του τρόπου με τον οποίο οι αναδυόμενες τεχνολογίες και οι επικρατούσες τάσεις επηρεάζουν την εταιρεία και το προφίλ κινδύνου της αναφορικά με την κυβερνοασφάλεια,
7. Επισήμανση ότι η παρακολούθηση της κυβερνοασφάλειας και η ανταπόκριση σε περιστατικά εισβολής / μη εξουσιοδοτημένης πρόσβασης στον κυβερνοχώρο πρέπει να αποτελούν ύψιστη προτεραιότητα της Διοικήσεως,
8. Αντιμετώπιση φαινομένων υποστελέχωσης των τμημάτων Εσωτερικού Ελέγχου και περιορισμένων πόρων, καθώς και έλλειψης υποστηρικτικής τεχνολογίας / υποδομών, τα οποία δύναται να θέσουν εμπόδια στις προσπάθειες για την ορθή διαχείριση των κινδύνων κυβερνοασφάλειας.

Risk Management: The Know How

Ως **εταιρικό κίνδυνο** ορίζουμε μία πιθανή αρνητική διακύμανση για την εταιρεία, η οποία μπορεί να προκληθεί από οποιοδήποτε εξωτερικό ή εσωτερικό γεγονός. Η **διαχείριση των εταιρικών κινδύνων** είναι υπεύθυνη στο να αναγνωρίζει, να διατυπώνει, να αναθέτει την αντιμετώπιση των κινδύνων στις αρμόδιες επιχειρησιακές μονάδες, και στη συνέχεια να παρακολουθεί την εξέλιξή τους.

Μία πολύ σημαντική προϋπόθεση για να έχουμε αποτελεσματικό risk management είναι η ικανότητα αντίληψης πιθανών εταιρικών κινδύνων, οι οποίοι μπορεί να προκύψουν από γεγονότα στον χώρο της πολιτικής, της οικονομίας, των διεθνών εξελίξεων και της νομοθεσίας, και με τη σειρά τους να έχουν αρνητική επίπτωση στα έσοδα ή τις καθημερινές εργασίες της εταιρείας. Κατ' επέκταση, γίνεται αντιληπτό ότι είναι πάρα πολύ σημαντική η αντίληψη του εξωτερικού περιβάλλοντος, των τάσεων και της επικαιρότητας. Από την ανάλυση των εξελίξεων, «μεταφρασμένες» στο τι επιπτώσεις μπορεί να έχουν για την εταιρεία (θετικές ή αρνητικές), μπορούμε να δημιουργήσουμε έναν **χάρτη εταιρικών κινδύνων.**

Εξίσου σημαντική συνιστώσα όμως για να θεωρηθεί το risk management μίας εταιρείας ολοκληρωμένο είναι η συνεχής παρακολούθηση και των εσωτερικών κινδύνων, προκειμένου να διασφαλίζεται η ορθή τήρηση των διαδικασιών και η εύρυθμη λειτουργία των δραστηριοτήτων της εταιρείας. Το έργο της Κανονιστικής Συμμόρφωσης, οι εσωτερικοί έλεγχοι, οι αιφνίδιοι έλεγχοι ποιότητας και οι εκπαιδεύσεις των εργαζομένων είναι μόνο μερικά από τα μέσα που χρησιμοποιούνται προς τη διασφάλιση αυτών.

Στο risk management είναι ιδιαίτερα αποδοτικό να πραγματοποιείται μία **κατηγοριοποίηση των κινδύνων,** προκειμένου να διαχειρίζονται πιο αποτελεσματικά και να λαμβάνονται τα δέοντα μέτρα αντιμετώπισης για τον κάθε έναν. Οι βασικές κατηγορίες εταιρικών κινδύνων είναι:

- Στρατηγικοί, οι οποίοι εμποδίζουν την επίτευξη των στρατηγικών στόχων.
- Χρηματοοικονομικοί, οι οποίοι βάζουν σε κίνδυνο το ενεργητικό της εταιρείας και την αξιοπιστία των οικονομικών αναφορών της.
- Λειτουργικοί, οι οποίοι σχετίζονται με τις καθημερινές διαδικασίες της εταιρείας.
- Κανονιστικοί (Νομικοί/ Ρυθμιστικοί), οι οποίοι σχετίζονται με τη συμμόρφωση της εταιρείας σε νόμους και ρυθμιστικά πλαίσια.

Στη συνέχεια, ακολουθεί η **αξιολόγηση των εταιρικών κινδύνων (**risk assessment), όπου η εκάστοτε εμπλεκόμενη επιχειρησιακή μονάδα προσπαθεί να υπολογίσει κατά προσέγγιση την πιθανότητα να συμβεί η αρνητική επίπτωση που περιγράφει ο κάθε κίνδυνος και το αποτέλεσμα (οικονομική απώλεια) που θα μπορούσε να έχει στην εταιρεία. Επίσης, προσδιορίζονται και εφαρμόζονται τα μέτρα αντιμετώπισης που αρμόζουν σε κάθε περίπτωση, λαμβάνοντας πάντοτε υπόψη το risk profile της εταιρείας, βάσει του οποίου ορίζεται η ανοχή που έχει η εταιρεία όσον αφορά τον κίνδυνο σε βασικούς τομείς-κλειδιά.

Μία καλή πρακτική είναι τα αποτελέσματα του risk assessment να διατυπώνονται με σαφήνεια στα **risk reports** της εταιρείας, και να υποβάλλονται στη Διοίκηση ανά τακτά χρονικά διαστήματα, ενώ, όποτε κριθεί απαραίτητο, να πραγματοποιείται εκτάκτως ad hoc risk report.

Ελένη Νικολάντου

Επιτροπή Ελέγχου: Από το Ν.3016/2002 στον Ν.4449/2017 - Αλλαγές και απαιτήσεις της νέας νομοθεσίας για συμμόρφωση με την Οδηγία 2014/56/ΕΚ και του Κανονισμού 573/2014 του Ευρωπαϊκού Κοινοβουλίου

Στις 24 Ιανουαρίου 2017 δημοσιεύτηκε και τέθηκε σε άμεση ισχύ ο **Ν.4449/2017** (ΦΕΚ Α 7/24.1.2017), ο οποίος μεταξύ άλλων δίνει πλέον φυσική υπόσταση και ενεργό ρόλο στην Ελεγκτική Επιτροπή (εφεξής ΕΕ) των εισηγμένων εταιρειών. Η ΕΕ εξελίσσεται δυναμικά από επόπτης των Εσωτερικών Ελεγκτών με το Ν.3016/2002, σε αναπόσπαστο συνδετικό κρίκο μεταξύ των Εσωτερικών και των Εξωτερικών ελεγκτών, του Διοικητικού Συμβουλίου και των μετόχων της εταιρείας.

Με το άρθρο 44 του Ν.4449/2017, ενισχύεται σημαντικά ο ρόλος της ΕΕ με αυξημένες αρμοδιότητες, υποχρεώσεις και ευθύνες έναντι των μετόχων και των Εποπτικών αρχών. Συγκεκριμένα με την παρ.1 του άρθρου 44, η **δομή** της πρέπει να είναι τουλάχιστον **3μελής** και τα μέλη της υποχρεωτικά **μη εκτελεστικά**, ενώ απαιτείται και **πλειοψηφία των ανεξάρτητων μελών.** Ο Πρόεδρος είναι υποχρεωτικά ανεξάρτητο μη εκτελεστικό μέλος, ενώ όλα τα μέλη πρέπει να διαθέτουν επαρκή γνώση στον τομέα που δραστηριοποιείται η ελεγχόμενη οντότητα, και τουλάχιστον ένα μέλος της ΕΕ να διαθέτει επαρκή γνώση στην ελεγκτική και λογιστική.

Οι αρμοδιότητες της ΕΕ περιλαμβάνουν την **παρακολούθηση:**

- **της διαδικασίας του υποχρεωτικού ελέγχου** των χρηματοοικονομικών καταστάσεων της εταιρείας και ενημέρωση του Δ.Σ. σχετικά με τη συμβολή του στην ακρίβεια, ορθότητα και πληρότητα της χρηματοοικονομικής πληροφόρησης. Η ΕΕ λαμβάνει υπόψη της τη **συμπληρωματική έκθεση** που υποβάλει ο Ορκωτός Ελεγκτής και η οποία περιλαμβάνει τα αποτελέσματα του εξωτερικού ελέγχου και ό,τι άλλο είναι άξιο αναφοράς προς το Δ.Σ. (άρθρο 44 παρ. 3α του Ν.4449/2017).
- **της διαδικασία σύνταξης της χρηματοοικονομικής πληροφόρησης** από τις οργανωτικές μονάδες της εταιρείας καθώς και την ορθή δημοσιοποίηση των πληροφοριών αυτών στο επενδυτικό κοινό (ανακοινώσεις σε ΧΑ, δελτία τύπου) (άρθρο 44 παρ. 3β και 3δ του Ν.4449/2017).
- **της επάρκειας και αποτελεσματικότητας** του συνόλου των **πολιτικών, διαδικασιών και δικλείδων ασφαλείας** της εταιρείας, της **ορθής λειτουργίας, της ανεξαρτησίας και του χωρίς περιορισμό έργου της Μονάδας Εσωτερικού Ελέγχου** (άρθρο 44 παρ. 3γ του Ν.4449/2017).
- **της ανεξαρτησίας των Ορκωτών Ελεγκτών** (χρονικό διάστημα συνεργασίας, τυχόν ασυμβίβαστες μη ελεγκτικές υπηρεσίες, επίπεδο αμοιβής). Ο Ορκωτός Ελεγκτής υποβάλλει ετησίως τη **δήλωση ανεξαρτησίας** του και συζητά με τα μέλη της ΕΕ οποιαδήποτε απειλή για την ανεξαρτησία του και τις τυχόν διασφαλίσεις (άρθρο 44 παρ. 3ε του Ν.4449/2017).
- **της διαδικασίας επιλογής των Ορκωτών Ελεγκτών** η οποία πρέπει να βασίζεται σε σχετική έρευνα αγοράς με τουλάχιστον δύο εναλλακτικές προτάσεις και με απόλυτα δικαιολογημένο τρόπο της τελικής επιλογής του νόμιμου ελεγκτή (άρθρο 44 παρ. 3στ του Ν.4449/2017).

Η Επιτροπή Κεφαλαιαγοράς εποπτεύει την τήρηση της παρ. 1 καθώς και των περ. α, β και γ της παρ. 3 και σε περίπτωση μη συμμόρφωσης δύναται να επιβάλει στην εταιρεία, στα μέλη του Δ.Σ. ή/και στα μέλη της ΕΕ **πρόστιμα που κυμαίνονται από 3.000€-600.000€.** Ομοίως, η **Τράπεζα της Ελλάδος** διενεργεί ελέγχους στα εποπτευόμενα από αυτήν πρόσωπα (πιστωτικά ιδρύματα και ασφαλιστικές εταιρείες) και σε περίπτωση παράβασης δύναται να επιβάλει διοικητικές κυρώσεις και υψηλά χρηματικά πρόστιμα.

Προς συμμόρφωση των ανωτέρω απαιτήσεων, οι ΕΕ των εισηγμένων εταιρειών θα πρέπει μεταξύ άλλων να πραγματοποιούν συχνές συνεδριάσεις με την **τήρηση πρακτικών,** να υποβάλλουν **αναφορές προς το Δ.Σ.** για ουσιώδη θέματα χρηματοοικονομικής πληροφόρησης και να **ενημερώνουν τους μετόχους στις Γ.Σ. για τα πεπραγμένα.**

Is Your Internal Audit Team As Productive As It Could Be?

...το άρθρο του Dr. Hernan Murdock (CIA, CRMA, VP - Audit Division at MIS Training Institute) πάνω στους παράγοντες-κλειδιά για την παραγωγικότητα της Μονάδας Εσωτερικού Ελέγχου

Η επιτυχία ή αποτυχία ενός τμήματος Εσωτερικού Ελέγχου έγκειται σε πολλές περιπτώσεις στην ικανότητα της ομάδας να λειτουργεί ως συνεκτική μονάδα προς την επίτευξη των στόχων της. Λόγω της φύσεως των υπηρεσιών που παρέχει, ο Εσωτερικός Ελεγκτής θα πρέπει να συνδυάζει τις τεχνικές του δεξιότητες ταυτόχρονα με αποτελεσματική επικοινωνία, διαπροσωπικές σχέσεις, team building, ικανότητα επίλυσης διαφορών και διαχείρισης αλλαγών.

Οι υψηλά παραγωγικές Μονάδες Εσωτερικού Ελέγχου μοιράζονται την ευθύνη για την ποσότητα και την ποιότητα της συλλογικής τους εργασίας, αξιοποιούν στο μέγιστο τις ικανότητες της ομάδας και εργάζονται με το αίσθημα του επείγοντος.

Οι παρακάτω δραστηριότητες αποτελούν απαραίτητη βάση για την εξασφάλιση της επιτυχίας:

1. Hire: Η διαδικασία πρόσληψης των Εσωτερικών Ελεγκτών θα πρέπει να ευθυγραμμίζεται με το όραμα, τις ανάγκες και τις επιθυμίες του τμήματος και να επικεντρώνεται στην εξεύρεση ατόμων που ταιριάζουν σε τεχνικό επίπεδο και μοιράζονται κοινές αξίες.
2. Visualize: Μεταξύ της ομάδας θα πρέπει να αναπτυχθεί και να καλλιεργηθεί ένα φιλόδοξο όραμα με σαφείς και μετρήσιμους στόχους.
3. Communicate: Τα καθήκοντα θα πρέπει να ανακοινώνονται με τέτοιο τρόπο ώστε να είναι πλήρως κατανοητά, πιθανά ζητήματα θα πρέπει να διευθετούνται και να προσφέρονται ευκαιρίες εξέλιξης και βελτίωσης.
4. Manage: Κινητοποιείστε τα μέλη της ομάδας μέσω αποτελεσματικού σχεδιασμού, συναντήσεων, ανάθεση καθηκόντων, αναφορών προόδου και δημιουργικής επίλυσης προβλημάτων. Έτσι, θα ελαχιστοποιηθούν περιπτώσεις εμφάνισης δυσλειτουργικής συμπεριφοράς, όπως ο εφησυχασμός, η απάθεια και η κοινωνική οκνηρία.
5. Lead: Η αποτελεσματική ηγεσία γεννά την εμπιστοσύνη, το πάθος, τη συνέπεια και την καινοτομία. Καλλιεργήστε τις ηγετικές ικανότητες των ανερχόμενων ταλέντων και το όραμα του τμήματος θα γίνει πραγματικότητα. Οι Μονάδες Εσωτερικού Ελέγχου χρειάζονται άτομα που να μπορούν να οργανώσουν, να ελέγξουν και να επιλύσουν προβλήματα αλλά χρειάζονται επίσης και άτομα που να κατέχουν υψηλά επίπεδα συναισθηματικής νοημοσύνης και μπορούν να παρακινήσουν, να εμπνεύσουν, να διδάξουν, και να αντιμετωπίσουν την αλλαγή και την αβεβαιότητα.
6. Delegate: Όταν η ανάθεση αρμοδιοτήτων γίνεται αποτελεσματικά, τότε ο Επικεφαλής της Μονάδας Εσωτερικού Ελέγχου πολλαπλασιάζει τη συνεισφορά της Μονάδας στην εταιρεία αξιοποιώντας τις προσπάθειες των μελών της ομάδας. Σε διαφορετική περίπτωση, βρίσκεται αντιμέτωπος με ένα πλήθος ημιτελών ή ανεπαρκώς εκτελεσμένων εργασιών.
7. Develop: Η δια βίου μάθηση, τα αποτελεσματικά προγράμματα εκπαίδευσης και κατάρτισης και η ανάπτυξη των soft skills προσδίδουν ανταγωνιστικό πλεονέκτημα στην ομάδα, ώστε να αναγνωριστεί ως βασικός παράγοντας αλλαγής μέσα στην επιχείρηση, διατηρώντας ταυτόχρονα αποτελεσματικές σχέσεις με τα υπόλοιπα τμήματα του οργανισμού.
8. Motivate: Οι ομάδες που καταφέρνουν να ξεχωρίζουν είναι εκείνες οι οποίες έχουν έναν κοινό σκοπό, είναι δημιουργικές και επιδέξιες. Τα άτομα διέπονται από διαφορετικά κίνητρα, οπότε οι επικεφαλής των ομάδων θα πρέπει να είναι καλοί ακροατές και να κατανοούν επαρκώς το προσωπικό τους, ώστε να εντοπίζουν ποιο είναι το κίνητρο του κάθε μέλους της ομάδας και να ανακαλύπτουν τον καλύτερο τρόπο επιβράβευσης των υψηλών επιδόσεων. Τέλος, η ανάπτυξη δεξιοτήτων επίλυσης συγκρούσεων επιφέρει το σεβασμό των συναδέλφων και ενισχύει το επίπεδο εμπιστοσύνης μεταξύ τους.
9. Evaluate: Ότι έχει σημασία θα πρέπει να μετρείται και να αξιολογείται, αλλά και ότι μετριέται θα πρέπει να έχει σημασία. Δώστε βάση στα ποιοτικά χαρακτηριστικά κατά την αξιολόγηση της απόδοσης, ώστε το κάθε μέλος της ομάδας να κατανοεί τις αδυναμίες του κ να εξελίσσει τις δυνατότητές του.
10. Recognize: Ενώ οι χρηματικές απολαβές ως ανταμοιβή της αποδοτικότητας είναι πάντα ευπρόσδεκτες, η παρακίνηση των εργαζομένων μπορεί να ενισχυθεί περαιτέρω μέσω ποικίλων εσωτερικών και εξωτερικών βραβεύσεων, πχ. ευέλικτο ωράριο εργασίας, υπάλληλος του μήνα κτλ.

Πηγή

What's new?

Ιωάννης Μιχαλόπουλος

1. New Guidance and links

The following guidance was recently released by The IIA:

Implementation Guides

Title	Date
NEW! Engagement Planning: Assessing Fraud Risks	October 2017

2. IIA Selected News

• 04-October-2017
CIA Spotlight: Certification plus Promotion Equals Opportunity
• 16-October-2017
Blog: Seven Signs You Might Be a Jurassic Auditor
• 30-October-2017
Blog: 5 Things That Should Spook Internal Auditors about the Future
• 15-November-2017
Anti-Fraud Collaboration Releases Report on Misconduct

3. The IIA Risk Resource Exchange

Internal Audit's Role in Assuring Accurate Board Information
For boards of directors to ensure their organizations achieve objectives, they must have good, reliable information on which to base critical decisions involving strategy, finances, and risks, among other things. While internal audit's role traditionally has been after the fact, it must contribute at the front end of the board process as well, by assessing the risk of the board failing to understand business issues or making inadequate decisions based on the quality of the information available.
Download the new issue and share it with your audit committee.

Special Edition: Artificial Intelligence — Considerations for the Profession of Internal Auditing
This special edition of Global Perspectives and Insights explores the internal audit's role in Artificial Intelligence by discussing associated risks and opportunities. The paper also introduces an AI Auditing Framework comprised of six components, all set within the context of an organization's AI strategy.
Access now

4. Leadership Development

On the Rise: 2017
Internal Auditor speaks with 15 "Emerging Leaders" who have made a difference in their organizations and stand out among their peers. These high-performing, innovative practitioners are raising the bar for today's young audit professionals and emerging as the thought leaders of tomorrow. **Read more**

5. Certifications & Qualifications - CPE Requirements

NEW! In 2018, two of your CPE/CPD credits must be earned in Ethics. While this is not a requirement for 2017, we recommend you begin planning now. **Learn more.**

6. Certifications and Qualifications - Social Media

Social Open Badging — Now Available.
Holders of IIA credentials can also tell their professional story on popular social and professional networking sites, personal websites, or in emails with web-enabled credentials. The IIA is using the Acclaim system to represent your credentials as badges, so you can more effectively manage your IIA credential portfolio online. Backed by Pearson, the world's largest education company, this new standard for communicating learning achievements provides:
• a web-enabled version of your credential(s)
• a place to manage your badge(s)
• an overview of the skills required for the credential(s)
• a secure means of storing and publishing your credential(s)
• a way for employers to verify your credential(s)
For more information on Acclaim's Open Badging, please review the Frequently Asked Questions (FAQ). You may also download «A Badge Earner's Guide to Acclaim.»

Click here to download the Badge Earner's Guide

7. ΣΕΒ

Μηνιαίο Δελτίο για το ρυθμιστικό περιβάλλον
• 26 Οκτωβρίου 2017 *Το βίωμα της εργασίας (employee experience) και οι εργασιακές ρυθμίσεις*
• 26 Σεπτεμβρίου 2017 *Ρυθμιστικό Περιβάλλον & Επιχειρήσεις - 26 Σεπτεμβρίου - Μηνιαίο Ενημερωτικό*

News from IIA

1. Release of the Revised CIA Exam Syllabi

https://global.theiia.org/certification/CIA-Certification/Pages/cia-exam-why-and-how-its-changing.aspx

2. NEW! Practice Guide: Engagement Planning: Establishing Objectives and Scope. Recommended Guidance

New! Practice Guide Thoroughly Examines IIA *Standards* 2200–2220

Engagement Planning: Establishing Objectives and Scope covers key elements of engagement planning including establishing the objectives and scope while taking the organization's objectives into consideration.

Members download for free

3. New COSO ERM Framework

New! COSO Enterprise Risk Management Framework

COSO Enterprise Risk Management – Integrating with Strategy and Performance focuses on the challenges and expectations of ERM in today's landscape and highlights the importance of including ERM in strategic planning as well as embedding it throughout the organization.

Learn more about the new ERM.

QIAL Case Study Window Opens Soon

Up-and-coming and established internal audit leaders can pursue the QIAL credential that validates leadership qualities imperative to earning a seat at the table. Position yourself for success by visiting the QIAL webpages or the QIAL Planning Schedule today.

Take steps now to register for the Case Study window open in October.

4. Global perspectives and Insights

Global Perspectives and Insights

Developed in response to a high demand for timely thought leadership that is powerful, timely, relevant, topical and responsive to global geopolitical and economic influences, The IIA created Global Perspectives and Insights. This new thought-leadership series, offers insight and direction on key issues, with perspectives that resonate globally.

5. Courage Is Easy When There's Nothing on the Line, by Richard Chambers

"To be clear, I do not take lightly that acting in the face of adversity may pose great professional and personal vulnerabilities. But internal audit's ability to provide assurance, help organizations overcome risks, and become trusted advisors to our stakeholders depends greatly on our willingness to speak out."

https://iaonline.theiia.org/blogs/chambers/2017/Pages/Courage-Is-Easy-When-Theres-Nothing-on-the-Line.aspx

News from ECIIA

http://www.eciia.eu/

1. Ο κ. Farid Aractingi εξελέγη νέος Πρόεδρος του ECIIA, τον Σεπτέμβριο του 2017.

The ECIIA elected Farid Aractingi as President of its management board at the body's annual conference in Switzerland. Aractingi (centre in image) was previously Vice President of ECIIA. He is Chief Audit, Risk and Organisation Officer of Renault and a former Chairman of the Board of the IFACI, the French Institute of Internal Auditors, where he is now an honorary member."I'm looking forward to building on the great progress ECIIA has made in being the voice of the internal audit profession across Europe," Aractingi said. "Henrik has done a fantastic job of raising the profession's profile and authority among our many stakeholders over the past three years. I intend to build upon that firm foundation." Henrik Stein stepped down as President. Thierry Thouvenot (left in image) was elected Vice President. Thouvenot has been IIA Luxembourg Chairman since 2012. Gabrielle Rudolf von Rohr (right in image) was appointed ECIIA Treasurer.

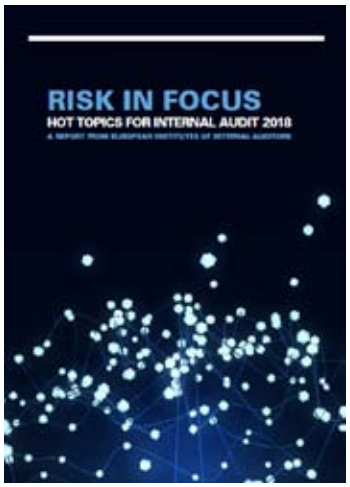
2. Μετά από νέες εκλογές το Σεπτέμβριο του 2017, το νέο Δ.Σ. του ECIIA, στην πρώτη του συνεδρίαση με Πρόεδρο τον κ. Farid Aranktingi.

3. Στο πολύ επιτυχημένο συνέδριο του ECIIA στη Βασιλεία μίλησε ο κ. Γιώργος Καλορίτης, Γενικός Διευθυντής και CAE του Ομίλου της Εθνικής Τράπεζας , πρώην πρόεδρος ΙΙΑ Ελλάδας, με θέμα New Generation Auditing. Το ΙΙΑ Ελλάδας πάντα μπροστά με εξωστρέφεια!

4. Νέος οδηγός για την εταιρική διακυβέρνηση και την κυβερνο-ασφάλεια.

5. Η Banking Committee του ECIIA με επικεφαλής τον κ. Henrik Stein επισκέφθηκε την Ευρωπαϊκή Κεντρική Τράπεζα και συζήτησε με το Διευθυντή Εσωτερικού Ελέγχου της Τράπεζας καθώς και με άλλους Διευθυντές Εσωτερικού Ελέγχου άλλων Κεντρικών Τραπεζών της Ευρώπης όπως της Bank of England, Bank of France, Italy κλπ. Αποφασίστηκε η μεταξύ τους συνεργασία. Σε επόμενο τεύχος μας θα έχετε την ευκαιρία να διαβάσετε μία σημαντική συνέντευξη του κ. Klaus Gressenbauer (Head of IA ECB and Chairman of the CBAE Group) προς την κ. Μαρία Σουρή, senior Auditor στο Χρηματιστήριο Αθηνών, μέλος του Ινστιτούτου μας.

6. Hot topics for Internal Audit 2018 από τα Μεγάλα Ευρωπαϊκά IIA.



7. Η Ευρωπαϊκή Επιτροπή εξέδωσε μέτρα ενίσχυσης της κυβερνοασφάλειας στην Ευρώπη

The European Commission has launched measures to strengthen cyber security across Europe.

It proposes to extend the powers of ENISA, Europe's current cyber agency. In particular, the proposals aim to ensure ENISA is better placed to support member states in implementing the NIS Directive. And the agency will become a centre of expertise on cybersecurity certification, if the proposals are approved.

"ECIIA welcomes the strengthening of cross-border efforts to tackle the growing threat of cybercrime," Henrik Stein, ECIIA President, says. "A more standardised certification system for ICT products across Europe could help improve assurance and transparency in the market."

Implementing the NIS Directive is seen by the Commission as vital plank in its cyber strategy.

"The NIS Directive is a first essential step with a view to promoting a culture of risk management, by introducing security requirements as legal obligations for the key economic actors," says the paper.

Internal auditors will play an important role in ensuring organisations comply with the new security requirements and have systems in place to better combat cybercrime.

The cyber security package was issued by the Directorate-General for Communications Networks, Content and Technology.

It builds on the Commissions objectives to:

- increase capabilities and preparedness of member states and businesses
- improve cooperation and coordination across Member States and EU institutions, agencies and bodies
- increase EU level capabilities to complement the action of Member States, in particular in the case of cross-border cyber crises
- Boost awareness of citizens and businesses on cybersecurity issues
- Increase the overall transparency of cybersecurity assurance of ICT products and services to strengthen trust in the digital single market and in digital innovation, and
- Avoid fragmentation of certification schemes in the EU and related security requirements and evaluation criteria across Member States and sectors.

8. European Forum for Internal Audit Banking Regulation and Supervision

Το ECIIA banking Committee διοργάνωσε στη Φρανκφούρτη μία σημαντική ημερίδα τον Οκτώβριο, παρουσία 100 περίπου Chief Audit Executives των συστημικών Τραπεζών στην Ευρώπη και εκπροσώπων της ECB και της EBA. Από την Αθήνα συμμετείχαν εκπρόσωποι των Μονάδων Εσωτερικού Ελέγχου των 4 συστημικών Τραπεζών. Μπορείτε να δείτε τη agenda πιο κάτω. Στα break out sessions συζητήθηκε η θεματολογία 5 position papers, τα οποία θα εκδοθούν στη συνέχεια από την ECIIA banking committee.

Το Ινστιτούτο μας θα διοργανώσει ειδική ενημέρωση για τα εν λόγω papers.

Λοιπές Δράσεις

For One IIA

1. Στο **ετήσιο Συνέδριο του IIA Τουρκίας**. Το Ινστιτούτο μας, σε συνεργασία με το IIA Τουρκίας, το Πανεπιστήμιο Μακεδονίας και του Μαρμαρά, συμφώνησαν στην συνδιοργάνωση μια κοινής ημερίδα/διημερίδας, στη Θεσσαλονίκη, μετά από 2 χρόνια.

Ήταν το δεύτερο βήμα προς το σχεδιασμό αυτού του γεγονότος. Το πρώτο έγινε στην ημερίδα μας στη Θεσσαλονίκη, το Μάιο 2017. Η παρούσα φωτογραφία δημοσιεύτηκε από τους Τούρκους συναδέλφους μας στο LinkedIn και απέσπασε τα θετικά σχόλια του κ. Richard Champers από το IIA Global.

2. Ο Εσωτερικός Έλεγχος ενώνει τους Ελεγκτές. Με την **Πρόεδρο του IIA Fyrom,** στο leadership forum που διοργάνωσε το ΙΙΑ.

3. Συμμετοχή στο ετήσιο συνέδριο της ΚΕΔΕ

Το Ινστιτούτο μας συμμετείχε για πρώτη φορά σε συζήτηση panel για τον Εσωτερικό Έλεγχο, στο πολύ σημαντικό συνέδριο της ΚΕΔΕ, μετά από την τιμητική πρόσκληση του Προέδρου κ. Πατούλη. Τον ευχαριστούμε θερμά για την τιμή και την ευκαιρία που μας έδωσε να αναδείξουμε ενώπιον τόσων σημαντικών εκπροσώπων της Τοπικής Αυτοδιοίκησης τα πλεονεκτήματα ενός ανεξάρτητου και αντικειμενικού Εσωτερικού Ελέγχου.

4. Συμμετείχαμε στο Συνέδριο «**Επιχειρήσεις και Κοινωνία των Πολιτών: Καταπολεμώντας τη διαφθορά για την προώθηση της Βιώσιμης Οικονομικής Ανάπτυξης»,** σε συζήτηση panel με θέμα «Οι προκλήσεις διαφθοράς που αντιμετωπίζει ο ελληνικός ιδιωτικός τομέας», που διοργανώθηκε από το ΟΟΣΑ, στην Αθήνα.

ΠΙΣΤΟΠΟΙΗΣΕΙΣ CIA Η πιστοποίηση "Certified Internal Auditor – CIA" είναι η μόνη παγκοσμίως αποδεκτή πιστοποίηση για τους Εσωτερικούς Ελεγκτές και παραμένει το πρότυπο βάσει του οποίου αποδεικνύεται η ικανότητα και ο επαγγελματισμός στο πεδίο του Εσωτερικού Ελέγχου. Από την εισαγωγή του προγράμματος το 1973, έδωσε την δυνατότητα και την ευκαιρία στους Εσωτερικούς Ελεγκτές σε παγκόσμιο επίπεδο να επικοινωνήσουν την ικανότητά τους να συνεισφέρουν ως "παίκτες – κλειδιά" στην επιτυχία των οργανισμών που προσφέρουν τις υπηρεσίες τους.

Από το 2000, το Ε.Ι.Ε.Ε. είναι ο μοναδικός επίσημα διαπιστευμένος φορέας στην Ελλάδα για τη διενέργεια και στη χώρα μας των εξετάσεων για τίτλους πιστοποίησης "Certified Internal Auditor – CIA". Οι προϋποθέσεις για τη συμμετοχή στις εξετάσεις είναι:

- Ο υποψήφιος να είναι μέλος του Ελληνικού Ινστιτούτου Εσωτερικών Ελεγκτών (Ε.Ι.Ε.Ε.).
- Οι υποψήφιοι απαιτείται να υποβάλλουν για την συμμετοχή τους στις εξετάσεις, την αίτηση συμμετοχής, character reference form, αντίγραφο πτυχίου και το experience verification form με την ολοκλήρωση των εξετάσεων για την απόκτηση του πιστοποιητικού.
- Για να αποκτήσετε την πιστοποίηση θα πρέπει να έχετε προϋπηρεσία 2 χρόνια στον Εσωτερικό Έλεγχο ή στον εξωτερικό Έλεγχο, internal control, compliance, quality assurance.

Για περισσότερες πληροφορίες σχετικά με τις εξετάσεις (περιεχόμενο, τρόπος διεξαγωγής, εγγραφής για συμμετοχή κλπ) μπορείτε να επικοινωνείτε με την Γραμματεία του Ε.Ι.Ε.Ε. (210-82.59.504).

CPE Ethics Reporting Requirement for 2018.

Για όλους τους κατόχους πιστοποιήσεων ΙΙΑ, από την έναρξη του 2018 θα πρέπει να συγκεντρώνουν 2 ώρες εκπαίδευσης σε θέματα επιχειρησιακής ηθικής/δεοντολογίας μέσα στα πλαίσια του continuing professional education (CPE) που απαιτείται για να διατηρούν ενεργή την πιστοποίησή τους.

Η νέα απαίτηση συμβαδίζει με τον Κώδικα Δεοντολογίας του ΙΙΑ και ενθαρρύνει όλους τους πιστοποιημένους εσωτερικούς ελεγκτές να έχουν τις απαραίτητες γνώσεις στα θέματα επιχειρησιακής ηθικής και αποδεικνύει τη δέσμευση στα υψηλότερα επαγγελματικά πρότυπα.

Για το λόγο αυτό μέσα στο εκπαιδευτικό πρόγραμμα του 2018 έχουν συμπεριληφθεί δύο σεμινάρια με σχετική θεματολογία.

CPE reporting

Θυμίζουμε σε όλους τους κατόχους πιστοποιήσεων από το ΙΙΑ (CIA, CCSA, CFSA, CRMA, CGAP, QIAL) ότι θα πρέπει **μέχρι 31.12.2017** να έχουν συμπληρώσει το CPE reporting form στο CCMS.

Περισσότερες πληροφορίες για τις πιστοποιήσεις ΙΑΑ στα παρακάτω links:

CIA | CCSA | CFSA | CGAP | CRMA | QIAL

CIA Learning Kit (3 parts)

Προετοιμαστείτε για τις εξετάσεις του CIA (Certified Internal Auditor) στο χρόνο που εσείς μπορείτε.

Μέσω του CIA Learning Kit οι χρήστες θα μπορέσουν να αποκτήσουν μια πλήρη αντίληψη των βασικών εννοιών και γνώσεις αναφορικά με την σύγχρονη εφαρμογή εσωτερικού ελέγχου. Ταυτόχρονα θα προετοιμαστούν και θα λάβουν τις κατευθύνσεις για τις εξετάσεις CIA, με μία μεθοδολογία που απαιτεί τον ελάχιστο χρόνο και προσπάθεια, και για τα τρία parts.

The Institute of Internal Auditors | Global

Εκπαίδευση 2018

Δημήτρης Στάβαρης

		ΤΙΤΛΟΣ ΣΕΜΙΝΑΡΙΟΥ	ΕΙΣΗΓΗΤΕΣ
1	ΜΑΚΡΟΧΡΟΝΙΟ ΣΕΜΙΝΑΡΙΟ	Ολοκληρωμένο Πρόγραμμα Βασικής Εκπαίδευσης στον Εσωτ. Ελεγχο 2018	Ιωάννης Βαρβατσουλάκης
		Ολοκληρωμένο Πρόγραμμα Βασικής Εκπαίδευσης στον Εσωτ. Ελεγχο 2018	Παντελής Παπαστάθης
		Μεθοδολογία Εσωτερικού Ελέγχου	Μάκης Σολομών
		Τεχνικες Δειματοληπτικου Ελέγχου	Γιώργος Πελεκανάκης
		It Audit	Νικόλαος Φράγκος
		Αξιολόγηση Κινδύνων και Κατάρτιση Ετήσιου Προγράμματος Ελέγχου	Οδυσσέας Ζαχαράκης
		Απάτη, Αξιολόγηση Κινδύνων και Ελεγχος	Οδυσσέας Ζαχαράκης
		Αποτελεσματικές Συνεντεύξεις	Χρήστος Νομικός
2		CIA - Part I	Joseph Kassapis
		CIA - Part II	
		CIA - Part III	
3		Certified Financial Services Auditor (CFSA) Training	Ανδρέας Κουτούπης
4	ΝΕΟ	Intelligent Cost Reduction: The role of Internal Audit	Ανδρέας Κουτούπης
5	ΝΕΟ	Auditing Culture	Γεράσιμος Στανίτσας
6	ΝΕΟ	Έλεγχος Ανθρώπινου Δυναμικού	Λάμπρος Κληρονόμος
7		Business Continuity Management	Σπύρος Αλεξίου
8	ΝΕΟ	Ηθικές όψεις της Χρηματοοικονομικής Διοίκησης	Γιώργος Ηλιού
9	ΝΕΟ	Ο Κώδικας Δεοντολογίας των Εσωτερικών Ελεγκτών: Από τη Θεωρία στην Πράξη	Ευαγγελία Παππά
10	ΝΕΟ	"Ένας για όλους και όλοι για έναν Αναπτύσσοντας ομάδες Υψηλών Επιδόσεων (High Performing Team)"	Δημήτρης Τσούχλος
11	ΝΕΟ	Κερδίζεις; Κερδίζω! Χάνεις; Χάνω! Οδηγός διαπραγματεύσεων με πειθώ και επιρροή	Νάνσυ Παπαθανασίου
12	ΝΕΟ	Διενέργεια Εσωτερικής Ποιοτικής Αξιολόγησης (Internal Quality Assessment Process) της Ελεγκτικής Δραστηριότητας	Σταυρούλα Ανδρικοπούλου
13		Reports with Impact	Sara I. James
14	ΝΕΟ	Root Cause Analysis for auditors	John Chesshire
15	ΝΕΟ	Anti fragility theory	Silvio De Girolamo
16	ΝΕΟ	Έλεγχος έργων - Μελετών - Σύνταξη ερωτηματολογίων ελέγχου	Κωνσταντία Γκιουλεντζή
17	ΝΕΟ	Ελεγκτικά Πρότυπα - IPPF	Βασίλης Μονογυιός
18	ΝΕΟ	Το πλαίσιο χειραγώγησης περι κατάχρησης (MAR II) & τεχνικές χειραγώγησης	Στάθης Πετρόπουλος
19	ΝΕΟ	Creative Thinking Techniques	Αγγελίνα Μιχαηλίδου Βασιλακοπούλου
20		Λογιστικά για Εσωτερικούς Ελεγκτές.Ειδικά Θεματα λογιστικής και χρηματοικονομικης διοίκησης για ΕΣ- ΕΛ	Ανδρέας Παπαδάκης
21	ΝΕΟ	Έλεγχος πιστοδοτήσεων (δανείων και πιστώσεων) σε καθυστέρηση (Θεωρητική και πρακτική προσέγγιση)	Μιχαήλ Ε. Αγγελάκης
22	ΝΕΟ	Creating a State of the Art Audit Universe and Risk Assessment	Μάρκος Δασκαλάκης
23	ΝΕΟ	Finance & IFRS Accounting for Internal Auditors	Μάρκος Δασκαλάκης
24	ΝΕΟ	Εισαγωγή στο Διεθνές Εμπόριο για Εσωτερικούς Ελεγκτές - Risk & Fraud in International trade	Ελένη Σταθάτου
25	ΝΕΟ	Advanced cases Risk & Fraud in international trade - Part 2 (documentary credits, demand guarantee etc.)	Ελένη Σταθάτου
26	ΝΕΟ	Εξωδικαστικός Συμβιβασμός Ρύθμισης Επιχειρηματικών Οφειλών	Πετρος Παπαζαχαρίου
27	ΝΕΟ	Cyber Security	σε συνεργασία με το ISACA
28	ΝΕΟ	GDPR Προσωπικά Δεδομένα	σε συνεργασία με το ISACA
29		Κανονιστική Συμμόρφωση	Δημητριάδης Άρης

Γνωρίστε τους συντελεστές έκδοσης

Δ. Στάβαρης (MBA) – Υπεύθυνος Επιτροπής Δημοσίων Σχέσεων

Υποδιευθυντής στη Διεύθυνση Εσωτερικού Ελέγχου του Ομίλου της Εθνικής Τράπεζας και μέλος του Δ.Σ. του IEEE, αρμόδιος για θέματα Εκπαίδευσης & Δημοσίων Σχέσεων. Με πολυετή (από το 1996) εμπειρία σε Ελέγχους Κεντρικών Υπηρεσιών της Τράπεζας και θυγατρικών εταιριών του Ομίλου της, στο εσωτερικό και το εξωτερικό, καθώς και σε καταστήματα του δικτύου της ΕΤΕ. Πτυχιούχος Οικονομολόγος, από το Πανεπιστήμιο Αθηνών και κάτοχος Μεταπτυχιακού τίτλου MBA in Banking, από το ALBA.

Λάμπρος Κληρονόμος (MSc, QMS, ISMS, CICA) Συντονιστής Έκδοσης Newsletter

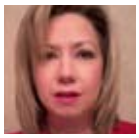
Εργάζεται ως Chief Internal Audit Officer στην Intralot SA, με 15ετή ελεγκτική προϋπηρεσία, στους κλάδους της βιομηχανίας, ασφαλιστικής, νοσοκομείου και τυχερών παιχνιδιών.

Έφη Κόκκα

Εργάζεται ως Διοικητική Διευθύντρια του Ινστιτούτου Εσωτερικών Ελεγκτών Ελλάδας (IIA Ελλάδας), με εμπειρία 15 ετών στο χώρο του Marketing και των Πωλήσεων σε εταιρίες του κλάδου ενέργειας. ISO 9001 Lead Auditor Certification.

Γεώργιος Βουσινάς (MSc, MBA, CICA)

Εργάζεται στην Alpha Bank ως Εσωτερικός Ελεγκτής και διαθέτει πολυετή εμπειρία στον τραπεζικό κλάδο σε θέματα Εσωτερικού Ελέγχου και αντιμετώπισης απάτης. Είναι κάτοχος Μεταπτυχιακών τίτλων στα Χρηματοοικονομικά, στις Τηλεπικοινωνίες και στη Διοίκηση Επιχειρήσεων, ενώ σήμερα είναι υποψήφιος Διδάκτωρ στο Εθνικό Μετσόβιο Πολυτεχνείο. Είναι συγγραφέας του βιβλίου «The history of Internet & the birth of InfoCom industry. IT & Economic Performance» και έχει πληθώρα δημοσιεύσεων σε διεθνή επιστημονικά περιοδικά, καθώς και παρουσιάσεις σε συνέδρια τόσο στην Ελλάδα όσο και στο εξωτερικό.



Λίλη Ζαφείρη

Εργάζεται ως εξειδικευμένο προσωπικό στον Όμιλο ΟΤΕ από το 1998, ενώ από το 2014 είναι στέλεχος στη Διεύθυνση Κανονιστικής Συμμόρφωσης, Διαχείρισης Εταιρικών Κινδύνων & Ασφάλισης Ομίλου ΟΤΕ. Είναι κάτοχος πτυχίου Οικονομικών Επιστημών του Πανεπιστημίου Αθηνών και κατέχει μεταπτυχιακούς τίτλους στα Οικονομικά από το Πανεπιστήμιο Paris 7 και στο Marketing από το Οικονομικό Πανεπιστήμιο Αθηνών.

Ιωάννης Μιχαλόπουλος (CIA)

Εργάζεται ως διευθυντής Εσωτερικού Ελέγχου στην Εταιρεία Διανομής Αερίου Θεσσαλονίκης & Θεσσαλίας (ΕΔΑ ΘΕΣΣ), με 15ετή εμπειρία στους κλάδους των κατασκευών, του αλουμινίου και των εταιρειών ενέργειας.

Αλεξάνδρα Μουλαβασίλη (BSc, ACCA Advanced Diploma in Accounting and Business)

Εργάζεται ως Internal Audit Supervisor στην Intralot SA, με 6ετή προϋπηρεσία στον εσωτερικό και εξωτερικό έλεγχο.

Ελένη Νικολάντου

Εργάζεται ως Υπεύθυνη Εσωτερικού Ελέγχου στην εταιρεία ΣΙΔΜΑ (όμιλος ΒΙΟΧΑΛΚΟ). Διαθέτει 15ετή εμπειρία στον εσωτερικό και εξωτερικό έλεγχο. Είναι κάτοχος επαγγελματικής πιστοποίησης από το Σώμα Ορκωτών Ελεγκτών-Λογιστών καθώς και πτυχίου διαχείρισης κινδύνου από το Institute of Risk Management, UK.

Μαρία Σουρή (CIA)

Εσωτερικός Ελεγκτής της εταιρίας Ελληνικά Χρηματιστήρια – Χρηματιστήριο Αθηνών Α.Ε., με μακρόχρονη εμπειρία στον εσωτερικό έλεγχο και πρότερη στον εξωτερικό σε μία από τις 5 μεγάλες διεθνείς ελεγκτικές εταιρίες (big five). Μέλος Επιτροπής Δημοσίων Σχέσεων IEEE

Εύη Φωτιάδου

Είναι απόφοιτος του τμήματος Οικονομικών Επιστημών του Πανεπιστημίου Μακεδονίας και κάτοχος μεταπτυχιακού στην Τραπεζική και Χρηματοοικονομική από το Διεθνές Πανεπιστήμιο Ελλάδος. Εργάζεται στη Διεύθυνση Κανονιστικής Συμμόρφωσης, Διαχείρισης Εταιρικών Κινδύνων και Ασφάλισης του Ομίλου ΟΤΕ.

Graphic Design: Αντωνιάδου Δώρα | antoniadoudora@gmail.com