The Institute of Internal Auditors Greece

«Ασφάλεια της Πληροφορίας & Εσωτερικός Έλεγχος» Προσέγγιση της Ασφάλειας της Πληροφορίας σύμφωνα με το πρότυπο ISO 27001

Χρίστος Κόζιαρης

Στόχος Σεμιναρίου

Αξιοποιώντας την πολύτιμη εμπειρία που έχει αποκτηθεί, στο σεμινάριο θα παρουσιαστούν τα κύρια σημεία του προτύπου ασφαλείας πληροφοριών ISO 27001 και θα ξεκαθαριστούν βασικά θέματα για την εφαρμογή του σε οργανισμούς και επιχειρήσεις. Η παρακολούθηση του συγκεκριμένου σεμιναρίου επιτρέπει στους συμμετέχοντες την απόκτηση των βασικών γνώσεων του προτύπου, της εφαρμογής του και μιά εισαγωγή σε θεμελιώδη θέματα ασφάλειας και ιδιωτικότητας δεδομένων. Με μιά σειρά πραγματικών παραδειγμάτων και περιστατικών θα εμπεδωθεί και θα συζητηθεί η εφαρμογή του προτύπου αλλά και των θεμάτων ασφάλειας και φυσικά του εσωτερικού ελέγχου.

Σε ποιους απευθύνεται

- εσωτερικους ή εξωτερικού ελεγκτές του ιδιωτικού/δημοσίου τομέα,
- υποψήφιους ή εν ενεργεία DPO (Υπεύθυνους Προστασίας Προσωπικών Δεδομένων),
- σε συμβούλους επιχειρήσεων,
- σε κάθε στέλεχος που επιθυμεί να ενημερωθεί σε θέματα ασφάλειας δεδομένων
- σε Υπευθύνους Ασφάλειας Πληροφοριών,
- Στελέχη Διασφάλισης Ποιότητας,
- Υπεύθυνους και Στελέχη Λειτουργιών IT,
- εμπλεκόμενα Στελέχη στον Σχεδιασμό και στη Λειτουργία IT Συστημάτων,
- αλλά και στους Γενικούς Διευθυντές και ιδιοκτήτες Επιχειρήσεων που επιθυμούν να ενημερωθούν για τις σύγχρονες πρακτικές στον ασφαλή και αποτελεσματικό τρόπο Διαχείρισης Πληροφοριών.

Οι συμμετέχοντες θα μπορούν:

- Να κατανοήσουν τις βασικές αρχές Ασφάλειας Πληροφοριών
- Να γνωρίζουν τη μεθοδολογία Ανάλυσης και Διαχείρισης Κινδύνων
- Να γνωρίζουν τις απαιτήσεις του Προτύπου ISO 27001:2013
- Να γνωρίζουν τρόπους κάλυψης των απαιτήσεων του Προτύπου στην Επιχείρησή τους
- Να Ελέγχουν – Αξιολογούν αποτελεσματικά τη Λειτουργία ενός Συστήματος Ασφάλειας Πληροφοριών με τα κατάλληλα Εργαλεία
- Να γνωρίζουν τη Μεθοδολογία ανάπτυξης Συστήματος Διαχείρισης Ασφάλειας μέχρι και την πιστοποίησή του
- Να προσαρμόσουν το Υπόδειγμα Ολοκληρωμένου Συστήματος κατά ISO 27001, που δίνεται σε ηλεκτρονική μορφή, στα Δεδομένα της Επιχείρησης τους

Περιγραφή Σεμιναρίου

(α) Εισαγωγή – IT Risk Management

- Εισαγωγή στο IT Security και στο ISO 27001
- Μεθοδολογίες αξιολόγησης Κινδύνων IT
- Εργαλεία αξιολόγησης Κινδύνων
- Απαιτήσεις αξιολόγησης Κινδύνων με βάση το Πρότυπο ISO 27001

(β) Ειδικές εφαρμογές

- Φυσική Ασφάλεια Χώρων: Συστήματα ελέγχου πρόσβασης σε διαβαθμισμένους χώρους, Προστασία από απειλές, Πολιτική clear desk / clear screen
- Ασφάλεια Υποδομών – Εξοπλισμού: Αποδεκτή χρήση – ιδιοκτησία, Επιστροφή εξοπλισμού μετά από χρήση, Απόρριψη – καταστροφή εξοπλισμού, Ασφάλεια εξοπλισμού εκτός Εταιρείας, Ασφάλεια φορητού εξοπλισμού / μέσων (media)
- Ασφάλεια Συστημάτων: Capacity Management, Ασφάλεια κατά την εγκατάσταση / τροποποίηση Συστημάτων, Αξιολόγηση τεχνικών αδυναμιών (technical vulnerabilities) Συστημάτων, Ασφάλεια Δικτύων – προστασία από εξωτερικές απειλές, Συστήματα backup, Malware controls, IT Systems Change Management, Emails Management
- Ασφάλεια Πρόσβασης: Πολιτικές προσβάσεων σε Δίκτυα και Υπηρεσίες (network services), Συστήματα Ελέγχου Πρόσβασης (access control systems), Διαδικασίες user registration / rights / authentication / log on, Διαχείριση κωδικών

Κόστος
€ 270
€ 170 (Μέλη IEEE)

Τόπος διεξαγωγής
τηλε-συνδιάσκεψη

CPE's: 7

Πρόσβασης, Κρυπτογραφικοί Έλεγχοι
- Ασφάλεια στην Ανάπτυξη Συστημάτων: Αξιολόγηση – καταγραφή απαιτήσεων (specification analysis), Ασφάλεια Περιβάλλοντος Ανάπτυξης, System Security Tests and Acceptance

- IT Business Continuity: Διαχείριση Περιστατικών Ασφάλειας. Υπευθυνότητες – Διαδικασίες, Business Continuity, Disaster Recovery Plans
- Ασφάλεια Πληροφοριακών Στοιχείων (Assets): Πνευματική Ιδιοκτησία, Συμβάσεις, Υπεργολάβοι – Εξωτερικοί Συνεργάτες, Ασφάλεια κατά τις προσλήψεις – μετακινήσεις – αποχωρήσεις

(γ) IT Audit
- Ο σχεδιασμός του Audit
- Checklist IT Auditing
- Ο μηχανισμός βελτιώσεων βάσει των ευρημάτων

(δ) Θέματα Ασφάλειας Δεδομένων
- Μελέτες Περιπτώσεων Ασφάλειας Προσωπικών Δεδομένων (Από Ελλάδα και Κύπρο)
- Πρακτικές Risk Management

Βιογραφικό Εισηγητή

Χρήστος Νομικός

Μηχανικός Πληροφορικής, με μεταπτυχιακές σπουδές στη Διοίκηση Επιχειρήσεων (i-MBA) από το Οικονομικό Πανεπιστήμιο και MSc στην Ασφάλεια και Διαχείριση Κινδύνων από το Πανεπιστήμιο του Leicester.

Είναι πιστοποιημένος στην Διαχείριση Κινδύνων Πληροφοριακών Συστημάτων (CRISC: Certified in Risk and Information Systems Control) και στο Σχεδιασμό και Υλοποίηση Λύσεων Ιδιωτικότητας Δεδομένων CDPSE (Certified Data Privacy Solutions Engineer) από τον οργανισμό ISACA, στον οποίο διατελεί εκλεγμένο μέλος του Δ.Σ στην Ελλάδα από το 2016 και υπεύθυνος σε θέματα εκπαίδευσης. Είναι πιστοποιημένος Data Protection Officer από την TUV Austria.

Εργάζεται από το 1987 στο αντικείμενο της πληροφορικής, εκ των οποίων 16 χρόνια στην Vodafone σε διοικητικές θέσεις πληροφορικής, διαχείρισης των συστημάτων τιμολόγησης, όσο και στη διαχείριση κινδύνων και διασφάλισης εσόδων. Διαθέτει σημαντική εμπειρία στον κλάδο των τηλεπικοινωνιών, του e-επιχειρείν, στην ανάπτυξη και διαχείριση εφαρμογών και υλικού, στην ολοκλήρωση συστημάτων, διαχείριση έργων και προϋπολογισμού, την βελτίωση διεργασιών και ελεγκτικών μηχανισμών, κ.α. Τέλος έχει συμμετάσχει σε προγράμματα συμμόρφωσης κανονιστικών πλαισίων (SOX, ISOs, BCP, Information Security, Quality Management, GDPR, κ.α.). Είναι πιστοποιημένος DPO (Data Protection Officer) από την TUV Austria.

Εργάζεται σαν σύμβουλος επιχειρήσεων αλλά και εισηγητής, επικεντρωμένος σε θέματα ασφάλειας δεδομένων με τα σχετικό και νομικό κανονιστικό πλαίσιο.