

ISACA Athens Chapter

Newsletter

ΠΕΡΙΕΧΟΜΕΝΑ

1. Συνέντευξη

Ανάργυρος Γαλανάκης, Ιδρυτικό Μέλος και 2ος Πρόεδρος του ISACA Athens Chapter 4

2. Αρθρογραφία

"Όταν η ταχύτητα του φωτός δεν είναι αρκετή" 8

3. Νέα του Ινστιτούτου

Τρίτος Academic Advocate του ΙΕΣΠ 11

Αποτελέσματα Έρευνας Μελών ΙΕΣΠ 2010 11

Εκπαιδευτικές Εκδηλώσεις 11

Κοπή Πρωτοχρονιάτικης Πίτας 2011 14

Επαναληπτική Γενική Συνέλευση 09/03/2011 15

Νέα Ομάδων Εργασίας Website και Newsletter 15

Αναμένοντας τα Αποτελέσματα των Αξιολογήσεων του ISACA 15

4. Νέα ISACA International

Σημαντικές Ημερομηνίες για τις Εξετάσεις 16

Ιουνίου CISA, CISM, CGEIT & CRISC

Κλείνει η Διαδικασία CRISC Grandfathering 16

Ο ISACA και το IIA υπέγραψαν Memorandum of Understanding 17

Έρευνα ITGI: Moving from Legacy Systems to Cloud Computing 17

Δέκα Συμβουλές για Διαχείριση της Ιδιωτικότητας 19

Book Reviews: Outsourcing IT και Monitoring 21

Internal Control Systems and IT 21

Αγαπητά μέλη,



Με ιδιαίτερη χαρά σας καλωσορίζουμε στο πρώτο για το 2011 Newsletter του Ινστιτούτου μας. Όπως θα διαπιστώσετε και εσείς τα νέα μας είναι αρκετά, τα θέματα ποικίλουν και η διάθεση για ενημέρωση φανερή.

Συνεχίζουμε τη σειρά των συνεντεύξεων με όλους και όλες τους/τις προέδρους του ΙΕΣΠ. Σε αυτό το τεύχος έχουμε την τιμή να φιλοξενούμε τη συνέντευξη του κ. Ανάργυρου Γαλανάκη. Επίσης, θα θέλαμε να ευχαριστήσουμε το Academic Group του Δημοκρίτειου Πανεπιστημίου Θράκης για το άρθρο που μας έστειλε και το οποίο δημοσιεύουμε στο παρόν τεύχος. Ακόμη, μπορείτε να ενημερωθείτε για τα τελευταία νέα του Ελληνικού Παραρτήματος όπως και του ISACA παγκοσμίως. Επιπλέον, παρουσιάζονται τα εκπαιδευτικά προγράμματα, οι εκδηλώσεις και οι συνεργασίες που έλαβαν ή πρόκειται να λάβουν χώρα και όχι μόνο...

Τέλος, αν θα έπρεπε να περιγράψω με μία λέξη αυτό το Newsletter, αυτή δεν θα ήταν άλλη από τη «Συμμετοχή». Αν και είμαι ένα νέο σχετικά μέλος του Ινστιτούτου και δη της Ομάδας Εργασίας που ασχολείται με την έκδοση του Newsletter, θεωρώ ότι το παρόν είναι το πλέον συμμετοχικό. Η ομάδα μας έχει αυξηθεί και αυτό είναι πολύ ενθαρρυντικό και τιμητικό για όλους μας. Νιώθουμε ότι υπάρχει ανταπόκριση στις προσπάθειές μας όπως φαίνεται και από τα σχόλια που λαμβάνουμε αυτό το διάστημα από μέλη και όχι μόνο του Ινστιτούτου. Στα πλαίσια αυτά, λοιπόν, καλούμε όποιον θέλει και όπως μπορεί να συμμετάσχει με τις ιδέες του, τα άρθρα του, τις ερωτήσεις του ή ακόμη και με την παρουσία του στις προσπάθειες και τις πρωτοβουλίες του Ινστιτούτου (γιατί όχι ξεκινώντας με τη Γενική μας Συνέλευση που πραγματοποιείται αυτές τις μέρες).

Άλλωστε όπως είχε πει και ο Salvador Dali "κάθε συμμετοχή σημαίνει τη γέννηση μιας ανάμνησης..."

Με φιλικούς χαιρετισμούς,

Γιάννης Μπονάτος

Μέλος Ομάδας Εργασίας Newsletter

ΙΕΣΠ - ISACA Athens Chapter

ISACA Athens Chapter Newsletter

Περιεχόμενα (συνέχεια)

5. Η Σελίδα των Μελών

Ζητούνται... άρθρα	23
Επίπεδα Αναγνώρισης Μελών ISACA	23
Έρευνες Μελών και Μη Μελών μέσω του ΙΕΣΠ	23
Σταυρόλεξο	24
Αγγελία Εργασίας	24

6. Σε Τροχιά CobIT

Mapping of ISO/IEC 20000 With COBIT 4.1	25
---	----

7. Εκπαιδευτικά προγράμματα και συνεργασίες

Εκπαιδευτικά Προγράμματα ISACA

Webinar	26
e-Symposium	26
EuroCACS 2011 Conference	26
Virtual Seminar and Tradeshow	27
Επόμενες Εκπαιδευτικές Εκδηλώσεις ISACA Athens Chapter, 06/04 και 04/05/2011	28

Εκπαιδευτικές Συνεργασίες

Cloud Computing Forum	28
Σεμινάρια Προετοιμασίας CISA-CISM	29



COBIT® *The comprehensive IT governance framework that addresses every aspect of IT and integrates all of the main global IT standards.*



ISACA Athens Chapter

Newsletter

Chris enjoys playing sports.

Chris is an IT professional.

Chris is motivated.

Chris gets recognition.

Chris achieves more.

Chris has an ISACA® certification.

www.isaca.org/certification



Certified Information
Systems Auditor



Certified Information
Security Manager



Certified in the
Governance of
Enterprise IT



Certified in Risk
and Information
Systems Control

Recognition • Success • Growth

Για περισσότερες
πληροφορίες
επικοινωνήστε στο
info@isaca.gr

June Exam Date:
11 June 2011

Registration Deadline:
6 April 2011

ISACA®

Εμπιστοσύνη & Αξία από τα Συστήματα Πληροφορικής

Athens Chapter

Newsletter

1. Συνέντευξη

Με τον κ. Ανάργυρο Γαλανάκη, Ιδρυτικό Μέλος και 2ος Πρόεδρος του ISACA Athens Chapter



Καθώς ετοιμάζαμε τη συνέντευξη για το παρόν τεύχος ανατρέξαμε στην όλη επικοινωνία μας με τον κ. Γαλανάκη, από τις αρχές του περασμένου Οκτώβρη. Πέρα από τις απαντήσεις στις ερωτήσεις που του κάναμε, τις αναμνήσεις του για το (τότε) ΕΙΕΣΠ, υπήρξαν

κάποια ακόμη σημεία που μας μετέφεραν σε εκείνη την εποχή που το Ινστιτούτο μας ήταν ακόμη στα σπάργανα. Ξεχωρίσαμε δύο από αυτά τα οποία – Αργύρη επιτρέποντος – μοιραζόμαστε μαζί σας. Το πρώτο ήταν κάποια στιγμή όπου αλληλοεπιβεβαιώναμε «ιστορικά» δεδομένα και ο Αργύρης μας είπε: «Επειδή αφενός τα χρόνια περνούν και οι αριθμοί ξεθωριάζουν και αφετέρου δεν είχα κρατήσει λεπτομερές προσωπικό αρχείο, θα σε παρακαλούσα να μου έστέλνες επιγραμματικά τα σημεία της απάντησης του Φαίδωνα (σ.σ. κ. Χατζησάββα, βλ. προηγούμενο τεύχος), στα σημεία που ενδεχομένως αναφέρονται ημερομηνίες, χρονιές και milestones.». Το δεύτερο είναι το «δίλημμα» που είχαμε αστειευόμενοι αν η φωτογραφία που θα μας έστέλνε θα ήταν πρόσφατη ή της εποχής της Προεδρίας του. Η απάντηση του Αργύρη ήταν άμεση «....μάλλον παλαιά φωτογραφία πρέπει να σας στείλω, αλλά που να τη βρεις». Για την ιστορία, η φωτογραφία είναι πρόσφατη. Αργύρη σε ευχαριστούμε για το χρόνο που μας διέθεσες, τότε και τώρα.

Ο κύριος Γαλανάκης είναι από τα Ιδρυτικά μέλη του ΙΕΣΠ, μέλος της Οργανωτικής Επιτροπής που ανέλαβε και έφερε εις πέρας τη διαδικασία σύστασης

του ΙΕΣΠ Είναι ο Πρόεδρος με την πιο μακροσκελή θητεία, από τον 02/1997 μέχρι τον 02/2002. Ο Ανάργυρος Γαλανάκης γεννήθηκε στον Πειραιά (δεν είναι ...Ολυμπιακός !!), υπήρξε μαθητής στην Ιωνίδειο και σπούδασε Μαθηματικά στην Αθήνα, με παράλληλες σπουδές προγραμματισμού Η/Υ. Κατά τη θητεία του, υπηρέτησε ως καθηγητής μαθηματικών και προπονητής κωπηλασίας σε παραγωγική Σχολή του Πολεμικού Ναυτικού. Από το 1978 εργάστηκε στην Εθνική Τράπεζα ως προγραμματιστής εφαρμογών και συστήματος μετά από εσωτερικό διαγωνισμό. Το 1987 ανέλαβε καθήκοντα ως IS (τότε EDP) auditor στη Διεύθυνση Πληροφορικής και αργότερα στη Διεύθυνση Επιθεώρησης, ενώ από το 2002 προΐστατο της Υποδιεύθυνσης IS Audit του NBG Group. Έχει ασχοληθεί με το μηχανογραφικό έλεγχο σε όλο το φάσμα των συστημάτων πληροφορικής και των εφαρμογών της Εθνικής Τράπεζας και του Ομίλου της, τόσο στην Ελλάδα όσο και στο εξωτερικό. Αποσύρθηκε το 2009 από τη θέση του Manager στην ΕΘΝΟDATA και τώρα ζει μακριά από την Αθήνα, ανακαλύπτοντας τα μονοπάτια του Παρνασσού.

Η πρωτότυπη μεθοδολογία του, με θέμα “Risk assessment in a IT environment” βρίσκεται αναρτημένη από το 2005, στην ιστοσελίδα του διεθνούς Οργανισμού των χρηστών του ISO 17799. Υπήρξε πρωταθλητής στην Κωπηλασία (ΝΑΣ, Ναυτικός Αθλητικός Σύνδεσμος) και αργότερα στην Ιστιοπλοΐα (ΙΟΠ, Ιστιοπλοϊκός Όμιλος Πειραιώς) και μέλος των Εθνικών Ομάδων Ιστιοπλοΐας (“Flying Dutchman” και “Soling”) με συμμετοχές σε Βαλκανικά, Μεσογειακά, Πανευρωπαϊκά και Παγκόσμια Πρωταθλήματα. Ήταν επίσης μόνιμο μέλος του πληρώματος του σκάφους GREEN DRAGON, με πληθώρα διακρίσεων στην Ανοικτή Θάλασσα. Επί σειράν ετών υπήρξε Αντιπρόεδρος και αργότερα Γενικός Γραμματέας του

ISACA Athens Chapter Newsletter

1. Συνέντευξη

ΙΟΠ και διετέλεσε επί δεκαετία Διευθυντής Σπουδών στην εκεί Σχολή Ιστοπλοΐας Ανοικτής Θάλασσας. Υπήρξε ακόμη Αντιπρόεδρος και Γενικός Γραμματέας του ΑΟΦ ΠΟΡΦΥΡΑΣ, την ιστοσελίδα του οποίου συντηρεί και σήμερα.

Πως αποφασίσατε να ασχοληθείτε ενεργά με το Ινστιτούτο Ελέγχου Συστημάτων Πληροφορικής; Ποια χρόνια διετελέσατε Πρόεδρος του ΙΕΣΠ;

Άρχισα να ασχολούμαι με το EDP audit, όπως λεγόταν τότε, το 1987 ως EDP auditor με full job απασχόληση στη Διεύθυνση Πληροφορικής και μετά της Επιθεώρησης της ΕΤΕ, μετά από 10 περίπου χρόνια ως προγραμματιστής εφαρμογών και μηχανικός μηχανογραφικών συστημάτων. Τα προβλήματα ήσαν πολλά, με κυριότερο αυτό της ενημέρωσης καθότι δεν υπήρχε το εύρος της σημερινής, κυρίως μέσω διαδικτύου, πλούσιας πληροφόρησης. Θυμάμαι χαρακτηριστικά με τι προσμονή αναμέναμε τα ανά διμήνο τεύχη της τότε EDPA (Electronic Data Processing Audit Association) και πως κυκλοφορούσαν τα φωτοαντίγραφα τους από χέρι σε χέρι. Θυμάμαι χαρακτηριστικά και τις συζητήσεις μας για την ελληνική ερμηνεία της λέξης “audit”. Μετά ήλθαν οι ορισμοί της Association και ηρεμήσαμε.

Στην Ελλάδα ο κλάδος ήταν στα σπάργανα και υπήρχε μία πανσπερμία των τρόπων αντιμετώπισης των διαδικασιών, των μεθοδολογιών, των πρακτικών εκπαίδευσης και εργασίας για το συγκεκριμένο νέο τομέα. Συγχρόνως ο καθένας μπορούσε να κάνει τον ειδήμονα, χωρίς γνώση προτύπων ελέγχου και κανόνων ασφάλειας και διαδικασιών. Από τα παραπάνω θα πρέπει να εξαιρεθούν λίγα ενήμερα στελέχη των, τότε, Big Six. Τότε δημιουργήθηκε η ανάγκη να ...οργανωθούμε και ξεκίνησε μία πρώτη

προσπάθεια να καταμετρηθούμε. Κατά τη διάρκεια της εν λόγω διαδικασίας ήλθα σε επαφή με τον κ. Φαίδωνα Χατζησάββα, στέλεχος τότε μεγάλης ελεγκτικής εταιρείας.

Η θρυαλλίδα πήρε φωτιά σε ένα πανευρωπαϊκό Συνέδριο της Association το 1990 ή 91 στη Στοκχόλμη, όπου πήγα μαζί με τον κ. Χατζησάββα. Εκεί σε συναντήσεις με τους ιθύνοντες της Association - η Γραμματέας ήταν Ελληνοαμερικανίδα με ποντιακές ρίζες -, πληροφορηθήκαμε ότι ετοιμαζόταν η ένταξη σε αυτή του ...Τουρκικού Chapter (!!!). Αυτό ήταν, αν και εκ των υστέρων καταλήξαμε ότι μάλλον ...μπλοφάρανε. Γυρίζοντας πίσω επιταχύνουμε τις διαδικασίες της ίδρυσης του τοπικού Chapter. Οι δυσκολίες πολλές, καθότι οι νόρμες από την Association για το καταστατικό του τοπικού παραρτήματος ήταν πρωτόγνωρες, και πολλοί συνάδελφοι, κυρίως από τον τότε χώρο του εσωτερικού ελέγχου, μας αντιμετώπιζαν με καχυποψία. Το εν λόγω κλίμα ήταν για πολλά χρόνια τροχοπέδη στις προσπάθειές μας και πέρασε αρκετός καιρός για να το υπερκεράσουμε. Ο ομιλών συμμετείχε σε ουκ ολίγες εισηγήσεις και Συνέδρια του εν λόγω χώρου με σκοπό την περαιτέρω προσέγγιση. Οι δυσκολίες πάντως μας πεισμάτωναν, μας δυνάμωναν και συνεχίζαμε. Με την αρωγή του κ. Χατζησάββα δημιουργήθηκε το πρώτο καταστατικό, με τις όποιες μικροατέλειες, και το νερό μπήκε στο αυλάκι.

Ίσως αυτά φαίνονται σήμερα γραφικά, αλλά έτσι ξεκινήσαμε. Με γενικές συνελεύσεις των 5-7 ατόμων (!!!), με αδυναμία συγκρότησης επί μέρους επιτροπών, με αδυναμία εξεύρεσης ειδικών ομιλητών σε συγκεντρώσεις μας, με υπεροπτική και καχύποπτη αντιμετώπιση από τον κόσμο της πληροφορικής και όχι μόνο. Όπλα μας η πολλή δουλειά, η ενημέρωση

Newsletter

1. Συνέντευξη

από την Association και η ταπεινή και χωρίς τυμπανοκρουσίες προώθηση των βασικών προτύπων μηχανογραφικού ελέγχου. Το 1993 σε ένα πανηγυρικό EUROCACS λόγω του ιωβηλαίου 25ετίας της Association, στο Λονδίνο, ανακοινώθηκε η ίδρυση του Ελληνικού Chapter. Θυμάμαι ακόμη την έκδηλη συγκίνησή μου, όταν κλήθηκα να μιλήσω. Έτσι ξεκινήσαμε. Με τον κ. Χατζησάββα ως Πρόεδρο και τον υπογράφοντα ως Γραμματέα μέχρι το 1997. Τότε ανέλαβα εγώ ως Πρόεδρος μέχρι το 2002. Μετά παρέδωσα το Ινστιτούτο στα σίγουρα χέρια των ...γυναικών (κα Σωτηρίου, κα Χίου).

Σημείωση: ...το Τουρκικό chapter άργησε πολύ να δημιουργηθεί !!

Ποια θεωρείτε πως ήταν η μεγαλύτερη πρόκληση που αντιμετωπίσατε στη θητεία σας ως Πρόεδρος του Ινστιτούτου και πως ανταπεξήλθατε σε αυτήν;

Ξεκινώντας από τον μικρό αριθμό των ιδρυτικών μελών, τη δυσκολία σύνταξης του αρχικού καταστατικού, τις μικροατέλειες που τελικά είχαν παρεισφρήσει σε αυτό, τις δυσκολίες εξεύρεσης στέγης για τις συγκεντρώσεις μας (...έως και τον Ιστιοπλοϊκό Πειραιώς είχαμε χρησιμοποιήσει), τον πολύ μικρό αριθμό ειδικών εισηγητών αλλά και ακροατών, τη μόνιμη αδυναμία συγκρότησης επί μέρους επιτροπών, θα καταλήξω τελικά στη δυσκολία της καθημερινής αναγνώρισης του κύρους του Ινστιτούτου και των προσπαθειών μας από τους συναδέλφους στο μηχανογραφικό αλλά και γενικότερο επιχειρηματικό περιβάλλον. Με άπειρη υπομονή και ατέλειωτη επιμονή, με επικοινωνιακές προσπάθειες και τακτικές, με αगाστή σύμπνοια, με κατανόηση και συμβουλευτική διάθεση, χωρίς ίχνος κομπορημοσύνης και δογματισμού, μπορέσαμε να προχωρήσουμε.

Κάνοντας μια καταγραφή των σημαντικότερων στιγμών στην ιστορία του Ινστιτούτου, ποια θεωρείτε ως τα πιο σημαντικά γεγονότα/επιτεύγματα του ΙΕΣΠ κατά τη θητεία σας ως Πρόεδρος;

Κάτι μικρό και άγνωστο. Όταν άρχισαν οι εξετάσεις για την πιστοποίηση CISA να δίνονται και στην Αθήνα, αλλά και παλαιότερα - ναι, υπήρχαν μέλη που πήγαιναν να δώσουν εξετάσεις στο εξωτερικό -, γινόμουν αποδέκτης παραπόνων ότι αυτές έκλιναν περισσότερο σε εξετάσεις για "American English" και όχι για IT audit. Σε χειμερινή συνάντηση των Προέδρων (Μαδρίτη) των Ευρωπαϊκών Chapters υπογράμμισα έντονα την παρατήρηση σε σχετική Ομάδα εργασίας που συμμετείχα. Αποτέλεσμα ήταν να σταματήσουν οι ερωτήσεις με αρνητικό πυρήνα, αλλά και τα θέματα με σύνθετες αριθμητικές πράξεις.

Αλλά ας μου επιτραπεί μία παρασπονδία. Να φύγουμε από το δοξαστικό και να πάμε στις γκρίζες σελίδες. Θεωρώ ότι το σοβαρότερο θέμα που κληροδοτήσαμε στα επόμενα Διοικητικά Συμβούλια ήταν η αναμόρφωση του Καταστατικού, σύμφωνα με τις -νέες- κατευθύνσεις της Association. Επί αρκετά χρόνια δεν μπορέσαμε, ή δεν θελήσαμε, να την αγγίξουμε. Ως εκ τούτου, σήμερα, δράττομαι της ευκαιρίας να ΣΥΓΧΑΡΩ την κα Σωτηρίου ως Πρόεδρο του επομένου Δ.Σ. και την Ομάδα Εργασίας που επελήφθη του τόσο σοβαρού και ακανθώδους θέματος και ιδιαίτερα τον κ. Ζαν Αράζ, ως τον επικεφαλής της σχετικής Ομάδας. Ήταν, όπως αποδεικνύεται, ένα σημαντικό σημείο στροφής και βασικός μοχλός για την περαιτέρω εξάπλωση του Chapter.

ISACA Athens Chapter Newsletter

1. Συνέντευξη

Ποιος είναι ο ρόλος του επαγγελματία στο χώρο της Πληροφορικής και ιδιαίτερα εκείνου στη γνωστική περιοχή της Ασφάλειας και Ελέγχου Πληροφοριακών Συστημάτων στην Ελλάδα σήμερα και ποια θεωρείτε πως είναι τα απαιτούμενα εφόδια/χαρακτηριστικά που θα πρέπει να διαθέτει;

Θα έλεγε κανείς ότι η «ηρωική» εποχή ξεπεράστηκε. Σήμερα, με πληθώρα προτύπων και τυποποιημένων διαδικασιών ελέγχου, πολλοί θα πουν ότι η δουλειά του IT auditor περιορίζεται σε απλή συμπλήρωση διαφόρων check lists. Παρά ταύτα, επιτρέψτε μου να διαφωνήσω, καθώς και σήμερα απαιτούνται εγρήγορση, προσοχή, οξυδέρκεια, εμπειρίες, αντίληψη, ικανότητα προσαρμογής, γνώσεις για να μπορέσουμε να εστιάσουμε σε κάθε περίπτωση και σε σύνθετα μηχανογραφικά περιβάλλοντα, τις αρχές και τα πρότυπα των μηχανογραφικών ελέγχων με σκοπό να εντοπίσουμε αδυναμίες και κινδύνους. Μην ξεχνάτε ότι υπογράφουμε γι' αυτό. Όπως συνηθίζω να λέω: “Θεωρητικά η θεωρία δεν διαφέρει από την πράξη. Πρακτικά διαφέρει.” Ως εκ τούτου, ανεξάρτητα από γνώσεις, πιστοποιήσεις κλπ. απαιτούνται και άλλες ιδιότητες, ικανότητες και κλίσεις. Πράγματι ο ρόλος του ως άνω επαγγελματία εξακολουθεί να είναι σημαντικός και απαραίτητος και μάλιστα με αυξανόμενο ρυθμό και βαθμιαία κλιμάκωση.

Ποιο είναι το μεγαλύτερο όφελος που αποκομίζατε από τη συμμετοχή σας στο ΙΕΣΠ;

Όλο αυτό το “ταξίδι” για το τότε ΕΙΕΣΠ με έκανε πλουσιότερο σε συγκινήσεις, σε εμπειρίες, σε “μαθήματα” και σε καλούς φίλους εδώ και στο

εξωτερικό. Ήταν κάτι πέρα από επαγγελματική καταξίωση και αναγνώριση. Ήμουν από τους “τυχερούς”.

Τι έχετε να πείτε σε κάποιον/α που σκέφτεται σήμερα αφενός για το αν θα πρέπει να γίνει μέλος στο Ινστιτούτο και αφετέρου να συμμετάσχει στο Δ.Σ. ή σε κάποια από τις Ομάδες Εργασίας;

Με τις ανάγκες που καλύπτει σήμερα η Association, και αν αγαπάει το IT audit, κάποια μέρα θα οδηγηθεί να γίνει μέλος. Με εμπειρίες και γνώσεις μέσα από διάφορες Ομάδες Εργασίας θα κτίσει σιγά-σιγά ένα στέρεο υπόβαθρο για να ασχοληθεί και με το Δ.Σ. του Ινστιτούτου. Αγάπη για το αντικείμενο, όρεξη και μεράκι για δουλειά να υπάρχει.



ISACA Athens Chapter Newsletter

2. Αρθρογραφία

Όταν η ταχύτητα του φωτός δεν είναι αρκετή



Από τους κ. κ. Βασίλη Κάτο, CHFI,
ISACA Academic Advocate
Δημοκρίτειο Πανεπιστήμιο Θράκης

και



Ιωάννη Κόρνιο μέλος του ISACA
Student Group στο Δημοκρίτειο
Πανεπιστήμιο Θράκης

Η σημερινή εποχή της πληροφορίας μπορεί να χαρακτηριστεί από την εκθετική ανάπτυξη των Τεχνολογιών Πληροφορίας & Επικοινωνιών (ΤΠΕ) με ανάγκες διαβίβασης πληροφορίας που καταλήγουν ότι η σταθερά c (η ταχύτητα του φωτός) είναι μικρή. Ένα παράδειγμα είναι το χρηματιστήριο της Νέας Υόρκης όπου ένας μεγάλος όγκος συναλλαγών πραγματοποιείται αποκλειστικά από υπολογιστικά συστήματα τα οποία υλοποιούν αλγόριθμους θεωρίας παιγνίων με αποτέλεσμα να εκδίδονται εντολές περίπου κάθε 30ms. Ένας κόμβος εγκατεστημένος στην Αθήνα θα εθεωρείτο “καθυστερημένος” διότι το roundrip time με τη Νέα Υόρκη είναι της τάξης των 100ms και επομένως θα είχε σημαντική υστέρηση στις διαδικασίες λήψης αποφάσεων.

Το πρόβλημα, ωστόσο, δεν περιορίζεται στις επίγειες επικοινωνίες. Αντίστοιχα, οι μεγάλοι χρόνοι καθυστέρησης που επικρατούν στο Διάστημα έχουν σημαντική επίπτωση στην απόδοση των διαστημικών επικοινωνιών. Οι μεγάλες καθυστερήσεις διάδοσης, σε

συνδυασμό με τη διακοπτόμενη επικοινωνία, τους υψηλούς ρυθμούς σφαλμάτων και τα ασύμμετρα κανάλια επικοινωνίας (αφού ο όγκος των δεδομένων που συλλέγονται στη Γη είναι πολλαπλάσιος των δεδομένων-εντολών που αποστέλλονται στα διαστημικά στοιχεία) περιορίζουν τις δυνατότητες των διαστημικών επικοινωνιών. Για το λόγο αυτό, άλλωστε, οι σημερινές διαστημικές επικοινωνίες παραμένουν στατικές και χαρακτηρίζονται από χειροκίνητες διαδικασίες και περιορισμένες λειτουργίες, αξιοποιώντας μόνο προκαθορισμένα κανάλια επικοινωνίας και συγκεκριμένες διαδρομές χωρίς τη δυνατότητα δυναμικής δρομολόγησης.

Λόγω των ιδιαιτεροτήτων του εν λόγω περιβάλλοντος αποκλείεται μια σημαντική κατηγορία κρυπτογραφικών πρωτοκόλλων. Πιο συγκεκριμένα τα διαδραστικά πρωτόκολλα αυθεντικοποίησης (interactive protocols) που κυριαρχούν σε διαδικτυακές εφαρμογές και πιστοποιούν δικτυακές οντότητες και απομακρυσμένους χρήστες δεν μπορούν να συμπεριληφθούν στις επιλογές σχεδιασμού πλαισίου αυθεντικοποίησης. Οι μεγάλες αποστάσεις καθιστούν συστήματα “κλειστού βρόγχου” απαγορευτικά. Ας θεωρήσουμε ενδεικτικά το πρωτόκολλο δημοσίου κλειδιού Needham-Schroeder το οποίο έχει μελετηθεί εκτενώς και είναι αναγνωρισμένο για την απλότητα και μινιμαλισμό μηνυμάτων:

1. Ο Α στέλνει στον Β το Χ
2. Ο Β στέλνει στον Α το Υ
3. Ο Α στέλνει στον Β το Ζ

όπου Χ,Υ,Ζ μικρά (σχετικά) κρυπτογραφημένα μηνύματα. Εάν ο Α βρίσκεται στη Γη ενώ ο Β βρίσκεται στον Άρη, η διαδικασία θα ολοκληρωθεί το νωρίτερο σε $3 \times 3 = 9$ λεπτά και το αργότερο σε $3 \times 22 = 66$ λεπτά, εφόσον η επικοινωνία είναι εφικτή.

2. Αρθρογραφία

Επίσης, το παραπάνω σενάριο προϋποθέτει αδιάκοπη συνδεσιμότητα μεταξύ των δυο κόμβων, υπόθεση η οποία δεν ισχύει στο Διάστημα. Η συνδεσιμότητα εξαρτάται από την τροχιακή κίνηση των πλανητών και, ακόμη και αν κάποιος δημιουργήσει το χάρτη συνδεσιμότητας αξιοποιώντας πληροφορίες σχετικά με τη θέση και τη κίνηση των πλανητών, δεν μπορούν να προβλεφθούν φαινόμενα όπως μια ηλιακή καταιγίδα ή η παρεμβολή ενός κομήτη στη γραμμή επικοινωνίας (line-of-sight) ανάμεσα σε δύο κόμβους. Ακόμη και μικρής διάρκειας διακοπές συνδεσιμότητας δημιουργούν σημαντικά προβλήματα στην επικοινωνία, καταλήγοντας σε χαμηλή απόδοση.

Οι φυσικοί περιορισμοί που προσβάλλουν τη διαθεσιμότητα του καναλιού επικοινωνίας σε συνδυασμό με το συνεχώς αυξανόμενο πλήθος των διαστημικών στοιχείων παρότρυναν τους ερευνητές διαδικτυακών πρωτοκόλλων να σχεδιάσουν εναλλακτικά πρωτόκολλα και δικτυακές υποδομές οι οποίες θα μπορούν να υποστηρίξουν μια νέα εποχή “διαστημικής διαδικτύωσης”. Πρωτοπόρο ρόλο στη νέα αυτή εποχή έχει η τεχνολογία των Δικτύων Ανεκτικών προς τη Καθυστέρηση (DTN - Delay Tolerant Networking), η οποία βρίσκεται ήδη σε φάση προτυποποίησης από την Επιτροπή Διαστημικών Προτύπων (CCSDS - Consultative Committee for Space Data Systems). Σκοπός της νέας τεχνολογίας είναι η καλύτερη αξιοποίηση των διαθέσιμων διαστημικών στοιχείων για δυναμικές και ευέλικτες επικοινωνίες. Οι χειροκίνητες διαδικασίες αντικαθίστανται από αυτοματοποιημένες και οι σταθερές διαδρομές από δυναμική δρομολόγηση ανάμεσα σε κόμβους και αξιοποίηση εναλλακτικών διαδρομών.

Η χρήση διαφορετικών μονοπατιών για τη μεγιστοποίηση της χρήσης της υποδομής απαιτεί διαλειτουργικότητα μεταξύ των διαφορετικών φορέων (π.χ. NASA, ESA, JAXA, κλπ.). Η νέα τεχνολογία DTN πετυχαίνει αυτή τη διαλειτουργικότητα χρησιμοποιώντας ένα νέο κοινό δικτυακό στρώμα πάνω από τα υπάρχοντα. Με τον τρόπο αυτό, δεν απαιτούνται αλλαγές στα πρωτόκολλα επιπέδου σύνδεσης που χρησιμοποιεί η κάθε διαστημική υπηρεσία. Για παράδειγμα, σήμερα η NASA χρησιμοποιεί το πρωτόκολλο σύνδεσης AOS (Advanced Orbiting Systems), ενώ η ESA χρησιμοποιεί τα πρωτόκολλα TM/TC για τις ίδιες λειτουργίες. Η τεχνολογία DTN, λειτουργώντας ως στρώμα επικάλυψης (overlay), επιτρέπει την επικοινωνία μεταξύ κόμβων που σήμερα χρησιμοποιούν διαφορετικά πρωτόκολλα και δεν μπορούν να επικοινωνήσουν.

Η νέα τεχνολογία παρέχει το πλεονέκτημα της επικοινωνίας μεταξύ ενός μεγάλου πλήθους κόμβων, δημιουργώντας ταυτόχρονα τις εξής προκλήσεις στην ασφάλεια και διαπίστευση πληροφοριών:

- Πολιτικές ασφάλειας για τη θεσμοθετημένη συνεργασία και διαλειτουργικότητα των φορέων
- Μοντέλα εμπιστοσύνης (trust models) και δυνατότητα υλοποίησης αυτών από τους εμπλεκόμενους κόμβους
- Διαδικασίες διαπίστευσης και ελέγχου (audit & assurance) όλων των μηχανισμών ασφάλειας, συμπεριλαμβανομένων και των διαδικασιών αναβάθμισης λειτουργικού (firmware upgrade) των διαστημικών συσκευών, καθώς μια ενδεχόμενη αποτυχία αναβάθμισης θα καθιστούσε τη συσκευή εκτός λειτουργίας (bricked), κάτι το οποίο δεν είναι καθόλου επιθυμητό στο διάστημα!

Newsletter

2. Αρθρογραφία

Το Κέντρο Διαστημικής Διαδικτύωσης (SPICE - Space Internetworking Center) με έδρα την Ξάνθη πρωτοπορεί σε πανευρωπαϊκό επίπεδο στον τομέα των Δικτύων Ανεκτικών στη Καθυστέρηση, εκπροσωπώντας την Ευρωπαϊκή Διαστημική Υπηρεσία (ESA) στην επιτροπή προτύπων CCSDS σε θέματα που αφορούν το DTN και έχοντας αναλάβει χρηματοδότηση από την ΕΕ για το σχεδιασμό δρομολογητών που διαχειρίζονται διαστημικά δεδομένα, χρησιμοποιώντας ως πυρήνα την τεχνολογία DTN [FP7-SPACE].

Ο Δρ. Βασίλης Κάτος, CHFI είναι Επίκουρος Καθηγητής στην Ασφάλεια Υπολογιστικών και Επικοινωνιακών Συστημάτων στο Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Δημοκρίτειου Πανεπιστημίου Θράκης. Κατέχει πιστοποίηση Computer Hacking Forensic Investigator (CHFI) και έχει διατελέσει ειδικός σύμβουλος και εμπειρογνώμων σε θέματα ασφάλειας πληροφοριακών συστημάτων σε ποινικό δικαστήριο στη Μεγάλη Βρετανία. Τα ερευνητικά του ενδιαφέροντα εστιάζονται στην εγκληματολογική ανάλυση ψηφιακών τεκμηρίων, ασφάλεια πληροφοριών και απόκριση περιστατικών ασφάλειας.

Ο κ. Ιωάννης Κόμνιος είναι υποψήφιος διδάκτωρ στο τμήμα Η.Μ.Μ.Υ. του Δημοκρίτειου Πανεπιστημίου Θράκης με ερευνητικό αντικείμενο τα δίκτυα υπολογιστών. Παράλληλα εργάζεται ως ερευνητής στο Κέντρο Διαστημικής Διαδικτύωσης (SPICE). Τα ερευνητικά του ενδιαφέροντα περιλαμβάνουν θέματα αξιοπιστίας σε διάφορα δικτυακά επίπεδα και δρομολόγηση σε δίκτυα ανεκτικά στην καθυστέρηση (DTN).

The Business Model for Information Security

A holistic and business-oriented approach to managing information security, and a common language for information security and business management to talk about information protection.



www.isaca.org/bmls

ISACA
Serving IT Governance Professionals

ISACA Athens Chapter Newsletter

3. Νέα του Ινστιτούτου

Τρίτος Academic Advocate του ΙΕΣΠ



Μετά τους κ. κ. Δημήτρη Γκρίτζαλη (Ο.Π.Α.) και Βασίλη Κάτο (Δ.Π.Θ.) τον περασμένο χρόνο, το ΙΕΣΠ στα πλαίσια της συνεχούς του συνεργασίας με Πανεπιστήμια και Κολλέγια βρίσκεται στην ευχάριστη θέση να ανακοινώσει τον τρίτο

academic advocate του, τον κ. Ιωάννη Μαυρίδη στο Πανεπιστήμιο Μακεδονίας. Του ευχόμαστε καλή αρχή στην ενεργό συμμετοχή του στα δρώμενα του ISACA.

Ο Δρ. Ιωάννης Μαυρίδης είναι Επίκουρος Καθηγητής Πληροφοριακών Συστημάτων Ασφαλείας του Τμήματος Εφαρμοσμένης Πληροφορικής του Πανεπιστημίου Μακεδονίας. Κατέχει δίπλωμα Μηχανικού Ηλεκτρονικών Υπολογιστών και Πληροφορικής από το Πανεπιστήμιο Πατρών και διδακτορικό (PhD) σε Ασφάλεια Φορητών Υπολογιστών από το Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης. Είναι μέλος της Ομάδας Εργασίας 11.3 σχετικά με θέματα ασφάλειας βάσης δεδομένων της Διεθνούς Ομοσπονδίας Επεξεργασίας Πληροφοριών (IFIP). Έχει συμμετάσχει σε αρκετά ερευνητικά προγράμματα στο χώρο της ασφάλειας Τεχνολογίας Πληροφοριών. Τα ερευνητικά του ενδιαφέροντα περιλαμβάνουν τους τομείς της αξιοπιστίας και της ασφάλειας των πληροφοριών, της ιδιωτικής ζωής και του έλεγχου της πρόσβασης καθώς και την ασφάλεια στον κυβερνοχώρο.

Περισσότερες πληροφορίες για το πρόγραμμα Academic Advocate μπορείτε να βρείτε στη σχετική [ιστοσελίδα](#) του ISACA.

Αποτελέσματα Έρευνας Μελών ΙΕΣΠ 2010

Σας ενημερώνουμε ότι τα αποτελέσματα από την πρόσφατη έρευνα μελών του Ινστιτούτου μας έχουν αναρτηθεί στην [ιστοσελίδα](#) μας, ενώ επίσης θα γίνει μία σχετική παρουσίαση στην ετήσια Γενική Συνέλευση. Η συμμετοχή σας ήταν ιδιαίτερα υψηλή, καθώς στην έρευνα απάντησαν 110 μέλη. Σας ευχαριστούμε!

Εκπαιδευτικές Εκδηλώσεις σε IT Governance και Continuous Assurance

Με μεγάλη επιτυχία διεξήχθησαν οι εκπαιδευτικές εκδηλώσεις του ΙΕΣΠ, με θέμα «IT Governance: Theory, Implementation and the Internal Auditor's View» και «Continuous Assurance» που διοργανώθηκαν αντίστοιχα στις 09/12/2010 και 19/01/2011 το απόγευμα στην Ελληνοαμερικανική Ένωση. Μάλιστα, η δεύτερη εκδήλωση συνδιοργανώθηκε με το Ελληνικό Ινστιτούτο Εσωτερικών Ελεγκτών.

IT Governance

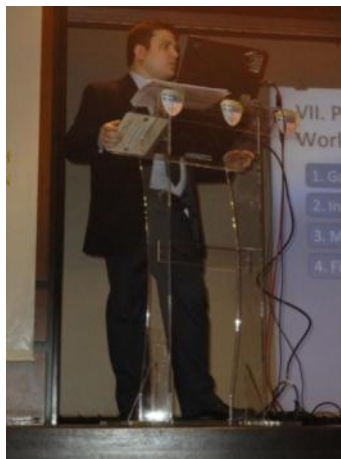
Η μεν πρώτη εκδήλωση ήταν χωρισμένη σε δύο ενότητες. Στην πρώτη ενότητα, εισηγητές ήταν κατά σειρά παρουσίασης ο Πρόεδρος του ISACA Athens Chapter, κ. Ανέστης Δημόπουλος, Manager Συμβουλευτικών Υπηρεσιών της Ernst & Young, καθώς και ο κ. Ιωάννης Φίλος, επίκουρος καθηγητής του Παντείου Πανεπιστημίου. Ο κ. Δημόπουλος ξεκίνησε την εκδήλωση αναλύοντας το πλαίσιο διακυβέρνησης πληροφοριακών συστημάτων του ISACA, τα κύρια χαρακτηριστικά του όπως και τις επιμέρους θεματικές περιοχές καθώς και τη συσχέτισή του με το διεθνές πρότυπο ISO 38500. Επιπρόσθετα, παρουσίασε πως μπορεί να χρησιμοποιηθεί το πλαίσιο CobiT ως μέσο εφαρμογής ενός αποτελεσματικού πλαισίου διακυβέρνησης πληροφοριακών συστημάτων όπως και σχετικές μελέτες περίπτωσης (case-studies).

3. Νέα του Ινστιτούτου

Στη συνέχεια ο κ. Φίλος ανέπτυξε έναν τρόπο προσέγγισης με τον οποίο μπορούν οι εσωτερικοί ελεγκτές – οι οποίοι δεν έχουν εξειδικευμένες γνώσεις στον έλεγχο της μηχανογράφησης – να προσεγγίσουν τη μηχανογράφηση (και συγκεκριμένα την οργάνωση, τη διοίκηση και τη λειτουργία της) κυρίως μέσα στα πλαίσια του περιεχομένου ενός Κανονισμού Εσωτερικής Λειτουργίας σε σχέση με το IT και το πρόγραμμα ελέγχου κάθε περιοχής. Στη δεύτερη ενότητα, ακολούθησε συζήτηση επί των θεμάτων που παρουσιάστηκαν με μορφή πάνελ στο οποίο συμμετείχαν οι κεντρικοί εισηγητές καθώς και τα παρακάτω μέλη του ΙΕΣΠ, Δρ. Βασίλειος Τσούμας, Σύμβουλος Γ. Γραμματέα Επικοινωνιών και κ. Γεώργιος Παπούλιας, Senior Project Manager Εθνικής Τράπεζας.

Continuous Assurance

Η θεματολογία της δεύτερης εκδήλωσης κινήθηκε γύρω από τις σύγχρονες τάσεις και το πλαίσιο του ISACA για “Continuous Auditing and Monitoring” (οδηγία G42 και Monitoring Internal Controls Systems and IT). Επίσης, έγιναν αναφορές σε θέματα που άπτονται του continuous assurance και τα οποία απασχολούν τις επιχειρήσεις και τον Εσωτερικό Έλεγχο σε σχέση με την ασφάλεια των πληροφοριακών συστημάτων. Εισηγητές της εκπαιδευτικής εκδήλωσης κατά σειρά παρουσίασης ήταν οι κ. κ. Παναγιώτης Δρούκας, μέλος Δ.Σ του ISACA Athens Chapter και Ελεγκτής Πληροφοριακών Συστημάτων στην Τράπεζα της Ελλάδος, ο Ιωάννης Λευκάκης Αντιπρόεδρος του ISACA Athens Chapter και σύμβουλος Διοίκησης στην Εθνική Τράπεζα της Ελλάδος και ο κ. Νότης Ηλιόπουλος, μέλος της επιτροπής εκπαιδευτικών θεμάτων του ISACA Athens Chapter και Διευθυντής Τεχνολογίας στην IntelliSolutions.



Συγκεκριμένα, ο κ. Δρούκας προχώρησε σε μία εισαγωγή για το continuous assurance και πως αυτό διαφοροποιείται από τον παραδοσιακό τρόπο ελέγχου των πληροφοριακών συστημάτων υπό το πρίσμα της σχετικής οδηγίας G42 του ISACA ενώ παρουσίασε τις νέες

απαιτήσεις που προκύπτουν από την υιοθέτηση μίας τέτοιας προσέγγισης όπως και το ρόλο και τις ευθύνες του ελεγκτή.



Στη συνέχεια, ο κ. Λευκάκης παρουσίασε τις τρέχουσες προσεγγίσεις του ISACA στο γνωστικό περιβάλλον του “continuous assurance” δίνοντας ιδιαίτερη έμφαση στην πρωτοβουλία που αφορά το “Monitoring Internal Control Systems and IT”

και παρουσιάζοντας μία μελέτη περίπτωσης (case study).

ISACA Athens Chapter Newsletter

3. Νέα του Ινστιτούτου

Τέλος, ο κ. Ηλιόπουλος στην παρουσίασή του έδωσε έμφαση στο continuous auditing και πως αυτό προσαρμόζεται στη γνωστική περιοχή της ασφάλειας πληροφοριών. Ακόμη, προχώρησε στην παρουσίαση ενός πλαισίου συνεχούς ελέγχου και παρακολούθησης όπως και σχετικών συμπερασμάτων και απαιτήσεων υλοποίησης.

Οι παρουσιάσεις των εισηγητών έχουν αναρτηθεί στην ενότητα «Εκπαίδευση», του ιστοτόπου του ΙΕΣΠ. Τέλος, θα θέλαμε να ευχαριστήσουμε το Ινστιτούτο Εσωτερικών Ελεγκτών για τη συνεργασία και όλους τους συμμετέχοντες - μέλη και μη - που μας τίμησαν με την παρουσία τους. Σύμφωνα με τα στοιχεία μας, τις εκδηλώσεις παρακολούθησαν 32 άτομα (28 εξ' αυτών μέλη) και 66 (30 εξ' αυτών μέλη) ενώ ο βαθμός ικανοποίησης που προέκυψε από τις αξιολογήσεις σας έφτασε το 81% και 79% αντιστοίχως.



Academic Advocate

Enrich Your Students' Careers.
Enhance Your Professional Resources.
Grow the Profession.



3. Νέα του Ινστιτούτου

Κοπή Πρωτοχρονιάτικης Πίτας 2011

Την Πέμπτη 3 Φεβρουαρίου 2011 είχαμε τη χαρά να γιορτάσουμε την κοπή της πρωτοχρονιάτικης πίτας του Ινστιτούτου. Η καθιερωμένη ετήσια γιορτή φιλοξενήθηκε και φέτος στο πάρα πολύ όμορφο roof garden της Ελληνοαμερικανικής Ένωσης. Αν και ο καιρός δυστυχώς δεν διευκόλυνε τη προσέλευση των μελών μας, παρόλα αυτά αρκετοί ήταν εκείνοι που απήφησαν την κακοκαιρία και κατάφεραν τελικά να έρθουν.

Η εκδήλωση ξεκίνησε με χαιρετισμό από τον πρόεδρο του ISACA Athens Chapter, τον κ. Ανέστη Δημόπουλο. Σε αυτό το σημείο αξίζει να σημειωθεί ότι είχαμε να την τιμή να φιλοξενήσουμε στην εκδήλωση και αρκετά διεθνή στελέχη του ISACA τα οποία βρίσκονταν στην Αθήνα στο πλαίσιο εργασιών για το CobiT. Ο κ. Χρήστος Δημητριάδης, International Vice President και μέλος του ISACA Athens Chapter και κα Shannon Donahue, Director of Information Security Practices, απεύθυναν χαιρετισμό και μια σύντομη ενημέρωση για τις τρέχουσες εξελίξεις και πρωτοβουλίες του ISACA.

Μέσα σε ένα άνετο και ζεστό χώρο και με τη συνοδεία κρασιού και εδεσμάτων και έχοντας θέα την Ακρόπολη, τα μέλη μας είχαν τη δυνατότητα να συνομιλήσουν, να ανταλλάξουν απόψεις και να εκφράσουν προβληματισμούς τόσο μεταξύ τους όσο και με τα διεθνή στελέχη του ISACA. Τέλος, όπως κάθε χρόνο, διεξήχθη και κλήρωση δώρων μεταξύ των παρευρισκομένων μελών. Τα δώρα ήταν μία συμμετοχή σε προπαρασκευαστικό σεμινάριο CISA ή CISM και δύο προσκλήσεις στο 6ο συνέδριο βέλτιστων πρακτικών για Project Management, προσφορά της Ελληνοαμερικανικής Ένωσης.

Ευχαριστούμε όλα τα μέλη που παρευρέθησαν και μας τίμησαν με την παρουσία του και ευχόμαστε σε όλους σας να είσαστε καλά και του χρόνου!!! Και με καλύτερο καιρό!!!



3. Νέα του Ινστιτούτου

Επαναληπτική Γενική Συνέλευση, 09/03/2011

Σας υπενθυμίζουμε ότι αυτή την Τετάρτη 9 Μαρτίου 2011 και ώρα 18:30 θα διεξαχθεί η επαναληπτική ετήσια Γενική Συνέλευση του Ινστιτούτου μας λόγω μη απαρτίας κατά την πρώτη σύγκλησή της. Επισημαίνεται ότι ο τόπος διεξαγωγής της επαναληπτικής Γενικής Συνέλευσης θα είναι η έδρα του Ινστιτούτου, Μασσαλίας 22, Αθήνα (Ελληνοαμερικανική Ένωση) και όπως προβλέπεται από το Καταστατικό θα είναι και οριστική. Τα θέματα της ημερησίας διατάξεως είναι τα ακόλουθα:

- Παρουσίαση των αποτελεσμάτων από την έρευνα μελών του Ινστιτούτου σχετικά με το βαθμό ικανοποίησης των μελών του καθώς και τις εκπαιδευτικές ανάγκες αυτών.
- Οικονομικός Απολογισμός 2010 και Προϋπολογισμός 2011
- Έκθεση Εξελεγκτικής Επιτροπής επί της οικονομικής διαχείρισης του Διοικητικού Συμβουλίου για το διάστημα αυτό
- Πεπραγμένα του Διοικητικού Συμβουλίου

Δικαίωμα συμμετοχής στη Γενική Συνέλευση έχει κάθε ταμειακώς ενήμερο μέλος. Τέλος, σημειώνεται ότι στους κατόχους των επαγγελματικών πιστοποιήσεων θα δοθούν βεβαιώσεις για αναγνώριση δύο (2) CPEs.

Νέα Ομάδων Εργασίας Website και Newsletter

Η Ομάδα Εργασίας του Website σε συνεργασία με την Ομάδα Εργασίας που ασχολείται με τα Εκπαιδευτικά Θέματα έχει αναλάβει το έργο ανασχεδιασμού της ιστοσελίδας του Ινστιτούτου όσον αφορά τη θεματική ενότητα που σχετίζεται με την εκπαίδευση. Στόχος είναι τα μέλη μας να έχουν αφενός ευκολότερη πρόσβαση και αφετέρου περισσότερο διαθέσιμο υλικό και παρουσιάσεις που θα αφορούν είτε εκδηλώσεις που διοργάνωσε το Ινστιτούτο σε προηγούμενα χρόνια ή εκδηλώσεις τρίτων φορέων στις οποίες συμμετείχαν ως ομιλητές, εκπρόσωποι του Ινστιτούτου. Για το τελευταίο έχει ήδη δημιουργηθεί η υπό-ενότητα «Συμμετοχές σε Συνέδρια».

Σε ότι αφορά την Ομάδα Εργασίας του Newsletter έχει ήδη προχωρήσει ο καθορισμός αρμοδιοτήτων μεταξύ των μελών της και η οριστικοποίηση της ανανεωμένης δομής για τα newsletters μας. Ελπίζουμε να έχετε προσέξει και να σας άρεσαν οι αλλαγές!!! Επίσης, θα θέλαμε να καλωσορίσουμε τα δύο νέα μέλη της Ομάδας Εργασίας μας, τους κ. κ. Νίκο Μπούμπουλη και Σταμάτη Πασσά.

Αναμένοντας τα Αποτελέσματα των Αξιολογήσεων του ISACA

Είμαστε στην ευχάριστη θέση να σας ανακοινώσουμε ότι ο ISACA έχει ξεκινήσει τις διαδικασίες αξιολόγησης των καλύτερων website και newsletter των ανά τον κόσμο Παραρτημάτων του. Αισιοδοξούμε, ευχόμαστε τα καλύτερα (γιατί όχι και την πρωτιά...) και ευχαριστούμε θερμά όσους έχουν βοηθήσει και στις δύο αυτές προσπάθειες, αλλά και όλα τα μέλη που υποστηρίζουν το ΙΕΣΠ με τη δική τους συμμετοχή στις δραστηριότητές μας.

ISACA Athens Chapter Newsletter

4. Νέα ISACA International

Σημαντικές Ημερομηνίες για τις Εξετάσεις Ιουνίου 2011 CISA, CISM, CGEIT, CRISC

Καθώς πλησιάζει η τελική προθεσμία για την εγγραφή στις εξετάσεις όλων των πιστοποιήσεων του ISACA τον προσεχή Ιούνιο σας υπενθυμίζουμε τις σχετικές ημερομηνίες:

Final Registration: 6 Απριλίου 2011

Exam: 11 Ιουνίου 2011

Κλείνει η Διαδικασία Grandfathering για το CRISC

Σας υπενθυμίζουμε ότι η περίοδος απόκτησης της νέας πιστοποίησης του ISACA χωρίς εξετάσεις λήγει τον Μάρτιο του 2011. Όσοι ενδιαφέρονται και πληρούν τις απαραίτητες προϋποθέσεις μπορούν να συμπληρώσουν τη σχετική αίτηση στην ιστοσελίδα του ISACA.

Η νέα πιστοποίηση, CRISC, απευθύνεται σε επαγγελματίες του κλάδου της πληροφορικής που ασχολούνται με την διαχείριση κινδύνων κατά την ανάπτυξη, υλοποίηση και συντήρηση πληροφοριακών συστημάτων

Μετά την πάροδο του grandfathering, οι ενδιαφερόμενοι μπορούν να αποκτήσουν την πιστοποίηση μέσω γραπτών εξετάσεων, οι οποίες θα πραγματοποιηθούν για πρώτη φορά τον Ιούνιο του 2011.



Recognition • Success • Growth



4. Νέα ISACA International

Ο ISACA και το IIA υπέγραψαν Memorandum of Understanding

Ο ISACA υπέγραψε Memorandum of Understanding (MoU) με το Ινστιτούτο Εσωτερικών Ελεγκτών (IIA). Το MoU δημιουργεί τις βάσεις για συνεργασία και σύμπραξη ανάμεσα στον ISACA και το Ινστιτούτο Εσωτερικών Ελεγκτών με σκοπό την πρόοδο του επαγγέλματος των Εσωτερικών Ελεγκτών παγκοσμίως μέσω της αμοιβαίας ανταλλαγής γνώσεων, εμπειριών και βέλτιστων πρακτικών. Και οι δυο οργανώσεις αναγνωρίζουν τις μεγάλες δυνατότητες και προοπτικές αυτής της σχέσης. Αν και η λίστα των πιθανών δραστηριοτήτων που θα μπορούσαν να πραγματοποιηθούν είναι σχεδόν ατελείωτη, ορισμένες από τις δυνατότητες που μπορούν να προσδιορισθούν από αυτό το MoU ανάμεσα στους δυο οργανισμούς είναι οι εξής:

- Η αμοιβαία συμμετοχή σε ομιλίες και παρουσιάσεις σε συνέδρια, σεμινάρια και εκδηλώσεις που διοργανώνονται είτε από τον ISACA είτε από το IIA.
- Η δημιουργία εκδηλώσεων με κοινή χορηγία.
- Η αμοιβαία αναγνώριση, όπου απαιτείται, των αντίστοιχων προγραμμάτων συνεχούς εκπαίδευσης του ISACA και του IIA, για την συνεχή παροχή εκπαιδευτικών μονάδων (CPEs) με στόχο την επαρκή κάλυψη των απαιτήσεων των πιστοποιήσεων.
- Η ενθάρρυνση για παρόμοια συνεργασία και σύμπραξη ανάμεσα στα τοπικά chapters του ISACA και του IIA (μια δραστηριότητα που ήδη αναπτύσσεται και ευδοκimeί σε πολλές περιοχές σε ολόκληρο τον κόσμο).
- Ο προσδιορισμός ευκαιριών για κοινά έργα που προωθούν παγκοσμίως το επάγγελμα του Εσωτερικού Ελεγκτή και το επαγγελματικό κύρος των μελών των δυο οργανισμών.

- Η συμμετοχή σε περιοδικές συζητήσεις σχετικά με θέματα δημόσιας πολιτικής που επηρεάζουν το επάγγελμα του Εσωτερικού Ελεγκτή.
- Όπου απαιτείται, ο συντονισμός και η προώθηση ενιαίων μηνυμάτων και ανταποκρίσεων προς τους ρυθμιστές προτύπων/οδηγιών συνολικά, και παρέχοντας τους πληροφορίες σχετικά με τις βέλτιστες επαγγελματικές πρακτικές.

Ο ISACA αναμένει με ενδιαφέρον την ευκαιρία να παρέχει πρόσθετα οφέλη και υποστήριξη στα μέλη του και στα λοιπά συστατικά μέρη του μέσω αυτής της συνεργασίας και όλων των υπόλοιπων σχέσεων που θα δημιουργηθούν.

Να προσθέσουμε ότι το ISACA Athens Chapter ήδη υλοποιεί με επιτυχία όσα από τα παραπάνω άπτονται σε θέματα εκδηλώσεων, εκπαίδευσεων και πιστοποιήσεων σε συνεργασία με το Hellenic Institute of Internal Auditors.

Έρευνα ITGI: Moving from Legacy Systems to Cloud Computing

Σύμφωνα με μια έρευνα που διεξήγε το Ινστιτούτο Διακυβέρνησης Πληροφορικής (IT Governance Institute, μη κερδοσκοπικό Ινστιτούτο το οποίο ιδρύθηκε από τον ISACA το 1998) το 35% των στελεχών Πληροφορικής αναφέρουν σημαντικές επενδύσεις σε υποδομές, ως αίτιο μη υιοθέτησης του cloud computing. Η έρευνα διεξήχθη στα πλαίσια της τέταρτης παγκόσμιας έκθεσης προόδου σχετικά με τη διακυβέρνηση IT (GEIT) –για το έτος 2011.

4. Νέα ISACA International

Ενώ πάνω από 40% των ερωτηθέντων χρησιμοποιούν ή σχεδιάζουν να χρησιμοποιήσουν το cloud computing για κρίσιμες υπηρεσίες πληροφορικής & πληροφόρησης, εκείνοι που δεν σκοπεύουν να χρησιμοποιήσουν το cloud computing καταγράφουν λίστα “μπελάδων” σε θέματα ασφάλειας και ιδιωτικότητας, τα οποία έχουν ως αποτέλεσμα επενδύσεις σε υποδομές, οι οποίες προβάλλουν ως εμπόδια για την υιοθέτηση τέτοιων τεχνικών (cloud computing). Οι οργανισμοί ολοένα στρέφονται σε απασχόληση εργατικού δυναμικού με εξωτερική ανάθεση (outsourcing), δίδοντας πολλές φορές σε αυτό, το 93% των IT δραστηριοτήτων τους.

«Οι αναδυόμενες τεχνολογίες όπως το cloud computing και η εξωτερική ανάθεση μπορούν να διαχειριστούν αποτελεσματικά, με την ενσωμάτωση μιας χρήσιμης και λειτουργικής διακυβέρνησης στο IT. Οι οργανισμοί πρέπει να υιοθετήσουν νέα μοντέλα παροχής υπηρεσιών ώστε να παραμείνουν ανταγωνιστικοί» δήλωσε ο Ken Vander Wal, CISA, CPA, Διεθνής Αντιπρόεδρος του ISACA. «Η εκτίμηση της αξίας των τρεχουσών επενδύσεων, η δημιουργία συναίνεσης μεταξύ των ενδιαφερομένων μερών και η μείωση των κινδύνων με τους προμηθευτές, όλα αυτά απαιτούν ένα συνολικό πλαίσιο διακυβέρνησης για τους οργανισμούς ώστε να είναι βέβαιοι ότι κάνουν τα σωστά πράγματα ή ακόμα καλύτερα να κάνουν τα πράγματα σωστά».

Η μελέτη του Ινστιτούτου καθώς και οι τρεις προηγούμενες εκδόσεις διατίθενται δωρεάν προς λήψη ([download](#)). Στη μελέτη του 2011 ρωτήθηκαν 834 στελέχη από 21 χώρες, ήταν δε μοιρασμένη σχεδόν ισομερώς μεταξύ των στελεχών των

επιχειρήσεων (CEOs, CFOs και COOs) και των στελεχών IT (CIOs και τους επικεφαλείς της πληροφορικής). Η μελέτη αναλύει το βαθμό στον οποίο η έννοια της Διακυβέρνηση της Πληροφορικής είναι αποδεκτή από στελέχη C-suite και καθορίζει τα επίπεδα ωριμότητας της Διακυβέρνησης της Πληροφορικής, την αναγνώριση πλαισίων, που απαιτούνται ή είναι επιθυμητές οι πιστοποιήσεις, και διάφορα άλλα θέματα γύρω από τη διακυβέρνηση της πληροφορικής.

Μεταξύ ανωτάτων στελεχών (C-suite) που ρωτήθηκαν, το 95% θεωρούν τη διακυβέρνηση της επιχείρησης αρκετά σημαντική. Αυτό αποκαλύπτει μια σχεδόν καθολικά κοινή αντίληψη της πληροφορικής ως κρίσιμος παράγοντας για την συνολική επιχειρηματική στρατηγική.

«Η συντριπτική συναίνεση σχετικά με τη σημασία διακυβέρνησης της πληροφορικής είναι ενθαρρυντική. Καθώς το 2011 οι πρωτοβουλίες που δρομολογούνται έρχονται αντιμέτωπες με το οικονομικό σκηνικό που συνεχίζει να είναι ασταθές, η ικανότητα ενός οργανισμού να ισορροπήσει και να δημιουργήσει αξία, η διαχείριση των κινδύνων και η βελτιστοποίηση των πόρων θα είναι κρίσιμης και υψίστης σημασίας», λέει χαρακτηριστικά το μέλος της ομάδας έργου Nicky Tiesenga, CISA, CISM, CGEIT, ο οποίος δουλεύει για την εταιρεία IBM στις ΗΠΑ.

4. Νέα ISACA International

Η μελέτη αυτής της χρονιάς δείχνει ότι οι κύριες τακτικές που χρησιμοποιήθηκαν για τη μάχη της οικονομικής ύφεσης ήταν η μείωση προσωπικού του προμηθευτή όπως και μόνιμου προσωπικού και η ενοποίηση των υποδομών. Σύμφωνα με την παγκόσμια έκθεση προόδου σχετικά με τη διακυβέρνηση IT, οι διαδικασίες διακυβέρνησης IT μπορούν να διασφαλίσουν την ισορροπία, με στόχο τις επενδύσεις οι οποίες με τη σειρά τους μπορούν να δημιουργήσουν εξοικονόμηση κόστους και τελικά να γίνουν από μόνες τους μοχλοί αυτοχρηματοδότησης.

Η επιτυχής υλοποίηση διαδικασιών διακυβέρνησης IT εξαρτάται από την αποτελεσματική διαχείριση των αλλαγών, την επικοινωνία, την οριοθέτηση του πεδίου και τον προσδιορισμό των εφικτών στόχων. Τα αποτελέσματα περιλαμβάνουν βραχυπρόθεσμα οφέλη, όπως μείωση του κόστους και μακροπρόθεσμα οφέλη, όπως η βελτιωμένη διαχείριση των τεχνολογιών πληροφορικής που σχετίζονται με τον κίνδυνο, τη βελτίωση των σχέσεων μεταξύ επιχειρήσεων και πληροφορικής, καθώς και την αύξηση της ανταγωνιστικότητας των επιχειρήσεων. Τα πιο σημαντικά οφέλη που παρατίθενται στη φετινή μελέτη είναι η βελτίωση της διαχείρισης κινδύνου των Τεχνολογιών Πληροφορικής (αναφέρθηκε από 42% των ερωτηθέντων) και η καλύτερη επικοινωνία και σχέσεις μεταξύ επιχειρήσεων και της πληροφορικής (αναφέρθηκε από 37% των ερωτηθέντων).

Για περισσότερες πληροφορίες, επισκεφθείτε τη σχετική [ιστοσελίδα](#) του ISACA.

Δέκα Συμβουλές για Διαχείριση της Ιδιωτικότητας

Από τον Victor Chapela

Η διαχείριση της ιδιωτικότητας στην πραγματικότητα αφορά κυρίως τη διαχείριση της εμπιστοσύνης. Τα παρακάτω είναι σημαντικά και θα πρέπει να λαμβάνονται υπόψη όταν κάποιος ασχολείται με τη διαχείριση της ιδιωτικότητας.

1. Για να διαχειριστείς με επιτυχία την ιδιωτικότητα, χρειάζεται να αναγνωρίσεις κάθε άτομο ως τον κάτοχο των προσωπικών του δεδομένων. Για αυτό το λόγο απαιτείται να επικοινωνήσεις και να ζητήσεις ρητώς από τον καθένα τη συγκατάθεση του/ της πριν προχωρήσεις στη χρήση των προσωπικών του δεδομένων.

2. Κάθε άτομο θα πρέπει να μπορεί να προσδιορίσει και να περιορίσει την αποθήκευση, την επεξεργασία και τη χρήση των δεδομένων εκείνων που με κάποιον τρόπο μπορούν να τον αναγνωρίσουν.

3. Κάθε χώρα έχει διαφορετική προσέγγιση σε θέματα προστασίας της ιδιωτικότητας. Όμως, στις περισσότερες περιπτώσεις, ευαίσθητα δεδομένα ορίζονται εκείνα τα δεδομένα που μπορούν να χρησιμοποιηθούν για διακρίσεις. Παραδείγματα αυτών είναι το φύλλο ή η καταγωγή, το ιατρικό ιστορικό, θρησκευτικές, φιλοσοφικές ή πολιτικές πεποιθήσεις και σεξουαλικές προτιμήσεις.

4. Νέα ISACA International

4. Προσωπικά δεδομένα, όπως τα παραδείγματα που αναφέρθηκαν παραπάνω είναι σε γενικές γραμμές καλά προστατευμένα. Παρόλα αυτά, τα δεδομένα εκείνα που οδηγούν στην ταυτοποίηση των ατόμων που δεν προστατεύονται αυστηρώς από τη νομοθεσία μπορεί να έχουν τους ίδιους ή και μεγαλύτερους κινδύνους για τις επιχειρήσεις αλλά και τους υπαλλήλους. Τέτοιου είδους δεδομένα είναι οι αριθμοί αστυνομικών ταυτοτήτων, τα συνθηματικά και οι λογαριασμοί πρόσβασης, αριθμοί πιστωτικών και χρεωστικών καρτών.

5. Τα δεδομένα που οδηγούν στην ταυτοποίηση των ατόμων θεωρούνται υψηλής αξίας και αναζητούνται από το οργανωμένο έγκλημα για τη διεξαγωγή απάτης. Αυτού του είδους τα δεδομένα θα πρέπει να κατηγοριοποιούνται βάσει του επιπέδου απειλής (δηλ. η αξία των δεδομένων για τους εγκληματίες ή τους ανταγωνιστές) και όχι βάσει της αξίας που έχουν για την εταιρία (που σε ορισμένες περιπτώσεις μπορεί να είναι και μηδενική).

6. Η σωστή διαχείριση της ιδιωτικότητας μπορεί να συνεισφέρει στην κάλυψη των απαιτήσεων ασφάλεια πληροφοριών. Τόσο η ασφάλεια όσο και η ιδιωτικότητα μπορούν να διαχειρισθούν καλύτερα μέσω της κατάταξης και διαχείρισης των δεδομένων βάσει επιπέδων κινδύνου.

7. Η κατηγοριοποίηση των δεδομένων θα πρέπει να λάβει υπόψη της τις δύο διαφορετικές συνιστώσες: την ανάλυση επίπτωσης ιδιωτικότητας (συμμόρφωση με ισχύουσα νομοθεσία) και την ανάλυση απειλών στα ίδια τα δεδομένα (προσδιορίζοντας τα επίπεδα κινδύνου βάσει της αξίας που έχουν τα δεδομένα).

8. Για κάθε επίπεδο κατηγοριοποίησης κινδύνου, ο πλήρης κύκλος των δεδομένων θα πρέπει να αναλυθεί από τη σύλληψη τους ή τη δημιουργία τους μέχρι την καταστροφή τους. Μία πολιτική ιδιωτικότητας και τα πρότυπα για κάθε επίπεδο κινδύνου θα πρέπει να προσδιορίζονται στην ανάλυση.

9. Για κάθε επίπεδο κατηγοριοποίησης αντίστοιχες νομικές, οργανωσιακές αλλά και τεχνολογικές δικλείδες ασφαλείας θα πρέπει να σχεδιασθούν και να υλοποιηθούν βάσει των πληροφοριακών αγαθών και των επιμέρους ομάδων.

10. Η ιδιωτικότητα δεν έχει σχέση μόνο με τη συμμόρφωση. Μέσω της ιδιωτικότητας, μπορείς να εγγυηθείς τα δικαιώματα του κάθε ατόμου και με αυτό τον τρόπο να αυξήσεις την εμπιστοσύνη των ενδιαφερομένων μερών.

Ο Victor Chapela είναι ιδρυτής και Διευθύνων Σύμβουλος της εταιρείας «Sm4rt Security Services». Συμμετείχε στη συγγραφή του βιβλίου για τα στάδια εξέλιξης του κινδύνου και είναι συχνά ομιλητής σε συνέδρια παγκοσμίως.

ISACA Athens Chapter Newsletter

4. Νέα ISACA International

Book Reviews:

Outsourcing IT - A Governance Guide

από τον Rupert Kendrick



Ο σκοπός του συγγραφέα είναι να δημιουργήσει ένα βιβλίο αναφοράς που θα παρουσιάζει τα μέσα, τη μεθοδολογία, και τις παραμέτρους εκείνες που θα πρέπει να ληφθούν υπόψη στην απόφαση για το αν πρέπει ή όχι μία επιχείρηση να εκχωρήσει τις λειτουργίες της πληροφορικής σε εξωτερικούς συνεργάτες (outsourcing).

Η αύξηση της σημασίας της τεχνολογίας και της πληροφορικής στις σύγχρονες επιχειρήσεις, ο αυξανόμενος ανταγωνισμός για νέα, ολοένα και πιο καινοτόμα προϊόντα και υπηρεσίες, τα ασφυκτικά χρονοδιαγράμματα, η εξέλιξη της τεχνολογίας και η απαίτηση για αυξημένα επίπεδα ποιότητας, συνθέτουν το πλαίσιο των προκλήσεων που έχουν να αντιμετωπίσουν οι επιχειρήσεις στο πεδίο της διαχείρισης της τεχνολογίας και ειδικότερα της πληροφορικής. Σε αυτό το πλαίσιο, τίθεται όλο και πιο επιτακτικά το ερώτημα, κατά πόσο, και υπό ποιες προϋποθέσεις, μία επιχείρηση θα μπορούσε να εκχωρήσει τις λειτουργίες της πληροφορικής σε μία εξωτερική εταιρεία.

Το βιβλίο, αναλύει τα κριτήρια και τις προϋποθέσεις που απαιτούνται για μία τέτοια απόφαση, από την οπτική του στελέχους διοίκησης. Καθορίζει τις βασικές

αρχές και τις πολιτικές διαχείρισης σε ένα outsourced IT, ενώ παράλληλα, περιγράφει τα βήματα που θα πρέπει να ακολουθήσουν οι διοικούντες ενός οργανισμού για τη μετάβαση σε ένα τέτοιο σχήμα διακυβέρνησης.

Το βιβλίο εκδόθηκε το 2009, έχει 336 σελίδες και διατίθεται από το βιβλιοπωλείο του ISACA στην τιμή των \$ 72 για τα μέλη (Product Code: 21TO).

Monitoring Internal Control Systems and IT: A Primer for Business Executives, Managers and Auditors on How to Embrace and Advance Best Practices

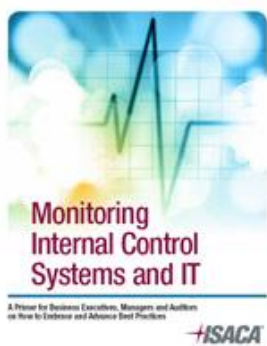
Από τον ISACA και το ITGI

Το συγκεκριμένο βιβλίο αποτελεί ένα χρήσιμο οδηγό βέλτιστων πρακτικών για όλα τα στελέχη μιας επιχείρησης, τους επαγγελματίες στο χώρο του IT και τους υπεύθυνους της οργάνωσης των διαδικασιών μέσα σε μια εταιρεία, για το πώς μπορεί να γίνει ο σχεδιασμός και η διαχείριση των διεργασιών εκείνων για την παρακολούθηση μηχανισμών ελέγχου μέσω των πληροφοριακών συστημάτων.

Το σημαντικότερο που επιτυγχάνεται μέσω της έκδοσης αυτής, είναι πώς γίνεται μια παρουσίαση εργαλείων τα οποία προσεγγίζονται μέσα από διάφορες περιπτώσεις και ποικίλα παραδείγματα έτσι ώστε να μπορέσει ο αναγνώστης να καταλάβει σε βάθος την χρησιμότητα τους και να κατανοήσει πώς η παραμετροποίηση των αυτοματοποιημένων αυτών εργαλείων είναι απαραίτητη και θα πρέπει να προσαρμόζεται κάθε φορά στις διαφορετικές ανάγκες κάθε επιχείρησης.

Newsletter

4. Νέα ISACA International



Σημαντικό κομμάτι του βιβλίου είναι επίσης η αναφορά που γίνεται και η προσπάθεια επέκτασης των δυνατοτήτων του “2009 COSO Οδηγός για Παρακολούθηση του Εσωτερικού Ελέγχου”. Για περισσότερες πληροφορίες επισκεφτείτε τη σχετική ιστοσελίδα του ISACA.

Το βιβλίο εκδόθηκε το 2010, έχει 124 σελίδες και διατίθεται δωρεάν σε ηλεκτρονική μορφή για τα μέλη. Επίσης είναι διαθέσιμο σε hard copy από το βιβλιοπωλείο του ISACA στην τιμή των \$55 για τα μέλη (Product Code: MIC).

Develop Your Professional Identity
Become a Student Member of ISACA®

ISACA®
Trust us, and value from information applies

5. Η Σελίδα των Μελών

Ζητούνται... άρθρα

Όπως σας έχουμε αναφέρει στο προηγούμενο newsletter μας προσπαθούμε να εξασφαλίσουμε την ύπαρξη ενός άρθρου από τα μέλη μας σε κάθε τεύχος. Για να το πετύχουμε αυτό χρειαζόμαστε την ενεργή συμμετοχή σας. Γι' αυτό σας καλούμε να μας στείλετε τα άρθρα σας στη νέα μας διεύθυνση, newsletter@isaca.gr, όπου η Ομάδα Εργασίας του Newsletter θα έρθει σε επαφή μαζί σας για τη δημοσίευσή τους. Απαραίτητη προϋπόθεση είναι να μην διαφημίζουν/προωθούν προϊόντα και υπηρεσίες εταιρειών και φορέων (πλην του ISACA). Το επιθυμητό μέγεθος των άρθρων έχει οριστεί μέχρι δύο σελίδες Word. Και να μην ξεχνάμε ότι η συγγραφή άρθρων περιλαμβάνεται στις δραστηριότητες που χορηγούνται CPEs σύμφωνα με την εν ισχύ πολιτική του ISACA.

Επίπεδα Αναγνώρισης Μελών ISACA – 4 Platinum Members του ΙΕΣΠ

Η συντονιστική επιτροπή του ISACA σχετικά με την ανάπτυξη και τη διατήρηση των μελών του (Membership Growth and Retention Committee) πρότεινε τη δημιουργία ενός διεθνούς προγράμματος αναγνώρισης. Την 1η Νοεμβρίου 2010, ο Οργανισμός ISACA ξεκίνησε επισήμως το πρόγραμμα σχετικά με την αναγνώριση των μελών του σύμφωνα με τα χρόνια που είναι εγγεγραμμένα σε συνεχή βάση, προσφέροντας αναγνώριση σε τέσσερα επίπεδα (Member Level Program):

- **Πλατινένιο** επίπεδο μέλους – Προσφέρεται σε όσους έχουν 15 ή περισσότερα συνεχόμενα χρόνια συμμετοχής ως μέλη του Οργανισμού
- **Χρυσό** επίπεδο μέλους – Προσφέρεται σε όσους έχουν από 10 ως 14 συνεχόμενα χρόνια συμμετοχής ως μέλη του Οργανισμού
- **Ασημένιο** επίπεδο μέλους – Προσφέρεται σε όσους έχουν από πέντε ως εννέα συνεχόμενα χρόνια συμμετοχής ως μέλη του Οργανισμού
- **Χάλκινο** επίπεδο μέλους – Προσφέρεται σε όσους έχουν από τρία ως τέσσερα συνεχόμενα χρόνια συμμετοχής ως μέλη του Οργανισμού

Με στοιχεία της 1^{ης} Μαρτίου, το ΙΕΣΠ έχει στο δυναμικό του **4 platinum level members**, τον κ. **Χριστόδουλο Σεφέρη**, τον κ. **Παναγιώτη Κροντήρη**, την κα **Ελένη Σωτηρίου** και τον κ. **Εμμανουήλ Λαγούβαρδο**, τους οποίους και ευχαριστεί θερμά για την πολυετή υποστήριξή τους. Επιπλέον έχει 25 gold level members, 89 silver level members και 92 bronze level members σε σύνολο 356 μελών.

Έρευνες Μελών και Μη Μελών μέσω του ΙΕΣΠ

Κατά την έκδοση αυτού του newsletter, βρίσκονται σε εξέλιξη δύο έρευνες. Η πρώτη έρευνα έχει σαν θέμα «[Η εφαρμογή της τηλεργασίας στις ελληνικές επιχειρήσεις](#)» και διεξάγεται από μέλος του ΙΕΣΠ ενώ η δεύτερη αφορά «[IT Governance, Regulation & Compliance through VAL IT framework– The case of Greece](#)» και διεξάγεται από μεταπτυχιακό φοιτητή στο Πρόγραμμα Σπουδών M.B.A. του Τμήματος Διοίκησης Επιχειρήσεων του Πανεπιστημίου Αιγαίου. Παρακαλούνται όσα μέλη το επιθυμούν να συμβάλλουν στις παραπάνω έρευνες συμπληρώνοντας τα ερωτηματολόγια αυτά.

ISACA Athens Chapter Newsletter

5. Η Σελίδα των Μελών

Σταυρόλεξο

Από τον Σταμάτη Πασσά, Μέλος της Ομάδας Εργασίας Newsletter

Με στόχο να γίνει το newsletter μας διαδραστικό, δημιουργήσαμε το παρακάτω σταυρόλεξο, αντλώντας πληροφορίες από το CISA Exam Preparation (Michael Gregg, Que Publishing 2007). Οι δέκα πρώτοι που θα το συμπληρώσουν σωστά θα λάβουν μία πρόσκληση για τις επόμενες δύο εκπαιδευτικές εκδηλώσεις του ΙΕΣΠ (πέντε προσκλήσεις για την εκδήλωση της 6/4 και πέντε για της 4/5) προκειμένου να τις διαθέσουν σε μη μέλη του Ινστιτούτου. Οι απαντήσεις πρέπει να σταλούν με e-mail στο newsletter@isaca.gr

ΟΡΙΖΟΝΤΙΩΣ

2 - .. identification is the task of identifying all the organization's assets.

3 - .. 9001 allows the company to identify shortcomings that must be addressed to obtain certification.

5 - .. sampling. It records deviations by measuring the rate of occurrence that a sample has a certain attribute.

7 - Written Procedures.

8 - .. of duties usually falls into four areas of control (authorization, custody, record keeping, reconciliation).

9 Control Category (attempts to prevent problems).

ΚΑΘΕΤΩΣ

1 This document specifies requirements that are considered mandatory.

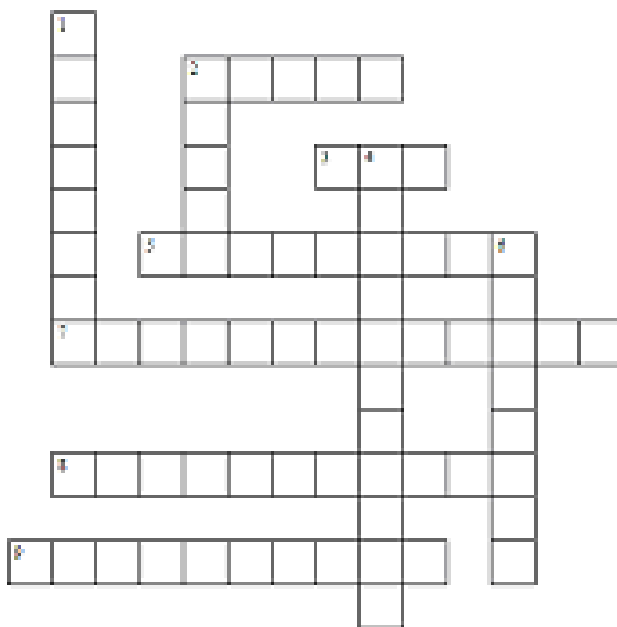
2 - The audit report might contain a material error and the auditor did not detect. This is an ... risk.

4 - .. testing. Sometimes called transaction integrity.

6 - .. is any information the auditor obtains that can be used to aid in rendering an opinion.

Αγγελία Εργασίας

Μέσα από αυτό το κομμάτι του Newsletter, θα σας ενημερώνουμε για τυχόν αγγελίες που προκύπτουν και πιθανώς να ενδιαφέρουν μέλη του Ινστιτούτου τα οποία βρίσκονται σε αναζήτηση εργασίας ή ακόμα και μέλη που επιθυμούν να αλλάξουν εργασία. Θα θέλαμε λοιπόν να σας ενημερώσουμε ότι στον όμιλο ΑΛΦΑ ΒΗΤΑ ΒΑΣΙΛΟΠΟΥΛΟΣ, έχει προκύψει μία θέση για IT Auditor / Data Analyst που θα ασχολείται με τον έλεγχο των πληροφοριακών συστημάτων του ομίλου. Επιπρόσθετο προσόν θα θεωρηθεί η κατοχή της επαγγελματικής πιστοποίησης CISA του ISACA. Για περισσότερες πληροφορίες όσον αφορά το προφίλ της επιχείρησης και του υποψηφίου και τις απαιτήσεις της θέσης, μπορείτε να ανατρέξετε στο σχετικό [link](#) στον ιστότοπο του ΙΕΣΠ



(Οι σωστές απαντήσεις θα ανακοινωθούν στο επόμενο τεύχος)

6. Σε Τροχιά CobiT

Mapping of ISO/IEC 20000 With COBIT 4.1



Ο ISACA πρόσφατα έκδωσε μελέτη για την αντιστοίχιση του προτύπου ISO/IEC 20000 με το COBIT 4.1.

Η σειρά ISO/IEC 20000 δίνει τη δυνατότητα σε όσους παρέχουν υπηρεσίες, να αντιληφθούν πώς να βελτιώσουν την ποιότητα των υπηρεσιών που παρέχουν τόσο τους εσωτερικούς όσο και στους εξωτερικούς πελάτες τους. Η μελέτη περιλαμβάνει σε υψηλό επίπεδο την αντιστοίχιση των δύο προτύπων και συγκεκριμένα των στόχων του ISO/IEC 20000:2005 με τις διαδικασίες ελέγχου του COBIT.

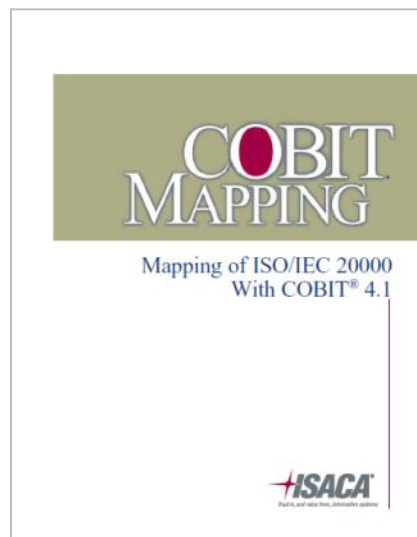
Πιο συγκεκριμένα το πρότυπο ISO/IEC 20000-1:2005 διαχωρίστηκε σε επιμέρους τμήματα τα οποία αντιστοιχήθηκαν σε έναν ή περισσότερους αντικειμενικούς σκοπούς σημείων ελέγχου (control objectives) του COBIT. Αυτά τα τμήματα έχουν ορισθεί ως απαιτήσεις πληροφορίας (information requirements).

Στη συνέχεια οι απαιτήσεις πληροφορίας αντιστοιχήθηκαν στους αντικειμενικούς σκοπούς σημείων ελέγχου του COBIT ως ακολούθως:

- a) Πραγματοποιήθηκε αντιστοίχιση 1:1 για τις απαιτήσεις πληροφορίας που ταίριαζαν με έναν αντικειμενικό σκοπό σημείου ελέγχου.
- b) Πραγματοποιήθηκε αντιστοίχιση 1:n για τις απαιτήσεις πληροφορίας που ταίριαζουν σε περισσότερους αντικειμενικούς σκοπούς σημείων ελέγχου.

- c) Αν η απαίτηση καλύπτει μία ολοκληρωμένη διαδικασία του COBIT, τότε αντιστοιχίζεται στην εν λόγω διαδικασία (σκοπός σημείου ελέγχου n.n, π.χ., DS5.1).
- d) Εάν κανένα από τα a, b, και c δεν καλύπτονται, τότε το COBIT δεν καλύπτει τη συγκεκριμένη απαίτηση πληροφορίας. Επιλέχθηκε η πιο κατάλληλη διαδικασία και η απαίτηση πληροφορίας αντιστοιχήθηκε σε (μη – υπάρχον) σκοπό σημείου ελέγχου της διαδικασίας.

Οι απαιτήσεις που περιγράφονται από τις απαιτήσεις πληροφορίας ήταν λεπτομερείς (από το ISO/IEC 20000-1:2005), και το αποτέλεσμα ταξινομήθηκε όπως ορίζεται από το πλαίσιο COBIT. Θα πρέπει να τονισθεί ότι το ISO/IEC 20000:2005 δρα συμπληρωματικά ως προς τα υπόλοιπα πρότυπα ISO και αντιστρόφως. Η αντιστοίχιση είναι διαθέσιμη για download από τα μέλη του ISACA (απαιτείται login) μέσω της σχετικής [ιστοσελίδας](#).



Newsletter

7. Εκπαιδευτικά Προγράμματα & Συνεργασίες

ΕΚΠΑΙΔΕΥΤΙΚΑ ΠΡΟΓΡΑΜΜΑΤΑ ISACA

ISACA Webinar, 10/03/2011



Ο ISACA διοργανώνει στις **10 Μαρτίου 2011** webinar με τίτλο [“Address Regulatory Mandates for Data Encryption without Changing Your Applications”](#) (11:00am CST

/ 9:00am PST / 12:00pm EST / 17:00pm UTC).

Αντικείμενο του σεμιναρίου θα αποτελέσει το λογισμικό Oracle Advanced Security για την κρυπτογράφηση των δεδομένων προκειμένου να προστατευθούν οι προσωπικές πληροφορίες (personally identifiable information (PII)). Το σεμινάριο θα περιλαμβάνει το case study της εταιρίας TransUnion Interactive, η οποία διαχειρίζεται πληροφορίες για 500 εκατομμύρια πελατών παγκοσμίως, σχετικά με το πώς κάλυψε τις απαιτήσεις κρυπτογράφησης του προτύπου PCI DSS χρησιμοποιώντας βάση δεδομένων Oracle 11g και αξιοποιώντας τις δυνατότητες του λογισμικού Oracle Advanced Security.

Για περισσότερες πληροφορίες και εγγραφή μπορείτε να επισκεφτείτε τη σχετική [ιστοσελίδα](#) του ISACA.

ISACA e-Symposium, 22/03/2011



Ο ISACA διοργανώνει στις **22 Μαρτίου 2011** e-symposium με τίτλο “A 360 Degree Approach to a Data Breach” (11:00am-14:00pm EST, 16:00pm-19:00pm UTC), όπου θα αναλυθούν περιστατικά

παραβίασης δεδομένων από πολλές διαφορετικές οπτικές γωνίες, απειλές και τρωτά σημεία, το πραγματικό κόστος των παραβιάσεων των δεδομένων, καθώς και τον τρόπο αντιμετώπισης των συνεπειών της παραβίασης. Οι συμμετέχοντες μπορούν να λάβουν 3 CPEs υπό την προϋπόθεση της επιτυχούς ολοκλήρωσης σχετικού τεστ (70% και άνω σε quiz 10 ερωτήσεων). Για περισσότερες πληροφορίες και εγγραφή μπορείτε να επισκεφτείτε τη σχετική ιστοσελίδα του ISACA.

EuroCACS 2011 Conference, 20-23/03/2011

20-23 Μαρτίου 2011, Μάντσεστερ, Αγγλία. Ο ISACA διοργανώνει το ετήσιο συνέδριο για την ασφάλεια, διακυβέρνηση και έλεγχο των συστημάτων πληροφορικής. Οι περιοχές του συνεδρίου θα καλύψουν επίκαιρα θέματα αναφορικά με νέες τεχνολογίες και μεθοδολογίες συστημάτων, εντοπίζοντας κινδύνους και ευκαιρίες. Οι συμμετέχοντες μπορούν να λάβουν έως και 40 CPEs. Για περισσότερες πληροφορίες μπορείτε να επισκεφτείτε τη σχετική [ιστοσελίδα](#) του ISACA.



Newsletter

7. Εκπαιδευτικά Προγράμματα & Συνεργασίες

Virtual Seminar and Tradeshow, 08/03/2011

Ο ISACA διοργανώνει στις **8 Μαρτίου 2011** ολόήμερη εκδήλωση (9:00am – 4:30pm EST, GMT-5) με τίτλο “[Best Practices For Electronic Health Records](#)”. Αντικείμενο της ημερίδας θα αποτελέσουν οι στρατηγικές που θα πρέπει να ακολουθήσουν οι οργανισμοί για την συμμόρφωση τους με τις απαιτήσεις του κανονιστικού και νομοθετικού πλαισίου HITECH Act αναφορικά με την ασφάλεια και την εμπιστευτικότητα των ηλεκτρονικών δεδομένων υγείας. Οι συμμετέχοντες δικαιούνται να λάβουν 4 CPEs. Για περισσότερες πληροφορίες αναφορικά με το πρόγραμμα της εκδήλωσης και εγγραφή μπορείτε να επισκεφτείτε τη σχετική [ιστοσελίδα](#) του ISACA.



ISACA's Virtual Seminar and Tradeshow

ISACA
Career Centre

**Narrow your search,
expand your choices.**

ISACA Athens Chapter Newsletter

7. Εκπαιδευτικά Προγράμματα & Συνεργασίες

Επόμενες Εκπαιδευτικές Εκδηλώσεις ISACA Athens Chapter, 06/04 και 04/05/2011

Το Ινστιτούτο Ελέγχου Συστημάτων Πληροφορικής έχει ήδη προγραμματίσει τις επόμενες δύο απογευματινές εκπαιδευτικές εκδηλώσεις. Η πρώτη θα διεξαχθεί την Τετάρτη **6 Απριλίου 2011** και θα αφορά «**Μια επισκόπηση των δραστηριοτήτων του ENISA (Ευρωπαϊκός Οργανισμός Ασφάλειας Δικτύων και Πληροφοριών) στην περιοχή Απορρήτου Λογοδοσίας και Εμπιστοσύνης**» κάνοντας μία συνοπτική παρουσίαση του Οργανισμού, του ρόλου του, των περιοχών στις οποίες δραστηριοποιείται και κάποιων από τις δράσεις του στην περιοχή Απορρήτου Λογοδοσίας και Εμπιστοσύνης. Εισηγητής θα είναι ο κ. Δημοσθένης Οικονόμου, Senior Expert στο τμήμα εργαλείων και αρχιτεκτονικών ασφαλείας του ENISA.

Η δεύτερη προγραμματίζεται για την Τετάρτη **4 Μαΐου 2011** με θεματική ενότητα σχετική με **νομικά ζητήματα που αναφέρονται για την ασφάλεια των προσωπικών δεδομένων** και την ευθύνη που έχουν όσοι διαχειρίζονται τα θέματα αυτά για λογαριασμό των εταιρειών τους. Εισηγήτρια θα είναι η δικηγόρος και lecturer στο Athens Information Technology, κα Μίνα Ζούλοβιτς.

Και οι δύο εκδηλώσεις θα διεξαχθούν στην Ελληνοαμερικανική Ένωση (Μασσαλίας 22) στο αμφιθέατρο του 2ου ορόφου και ώρες 18:30-20:30. Για κάθε εκδήλωση θα αποσταλεί περαιτέρω ενημέρωση μέσω e-mail ενώ επίσης θα αναρτηθεί το σχετικό πρόγραμμα στο www.isaca.gr

ΕΚΠΑΙΔΕΥΤΙΚΕΣ ΣΥΝΕΡΓΑΣΙΕΣ

Cloud Computing Forum, 09/03/2011

Το περιοδικό netweek και η Boussias Communications διοργανώνουν την Τετάρτη 9 Μαρτίου 2011 στο ξενοδοχείο Μεγάλη Βρετανία το 1ο ανεξάρτητο συνέδριο για το Cloud Computing. Το ΙΕΣΠ ως υποστηρικτής του συνεδρίου εξασφάλισε έκπτωση 10% για τα μέλη του στην αρχική τιμή συμμετοχής, διαμορφώνοντάς τη στα 135 ευρώ πλέον Φ.Π.Α.

Εφόσον σας ενδιαφέρει να δηλώσετε συμμετοχή, θα πρέπει να σημειώσετε πάνω στη φόρμα ότι είστε μέλος του ISACA Athens Chapter και να τη στείλετε με fax στο 210 6617778. Επιπλέον μπορείτε να επισκεφθείτε το www.cloudforum.gr και να δηλώσετε συμμετοχή online. Για οποιεσδήποτε διευκρινίσεις, μπορείτε να επικοινωνήσετε με τον κ. Στέλιο Κιοσσέ στη Boussias Communications, τηλ. 210 6617777 (ext 149), skiosses@boussias.com.



7. Εκπαιδευτικά Προγράμματα & Συνεργασίες

Σεμινάρια Προετοιμασίας CISA - CISM

Σας ενημερώνουμε για τα προπαρασκευαστικά προγράμματα για τις πιστοποιήσεις CISA και CISM που θα λάβουν χώρα τους προσεχείς μήνες για την εξεταστική περίοδο του Ιουνίου:

CISA

28-30 Μαρτίου 2011, [Ελληνοαμερικανική Ένωση](#). Το σεμινάριο διάρκειας 24 ωρών θα λάβει χώρα στο συνεδριακό χώρο της Ελληνοαμερικανικής Ένωσης (Μασσαλίας 22, Αθήνα). Τα μέλη του ISACA Athens Chapter δικαιούνται έκπτωση με βάση την οποία το κόστος του σεμιναρίου ανέρχεται στο ποσό των € 890. Για περισσότερες πληροφορίες μπορείτε να επισκεφτείτε τη σχετική [ιστοσελίδα](#) της Ελληνοαμερικανικής Ένωσης.

06-08, 13-15 & 27-29 Μαΐου 2011, [PwC's Training Services](#). Το σεμινάριο διάρκειας 48 ωρών θα λάβει χώρα στο εκπαιδευτικό κέντρο της PwC's Training Services (Ζαλοκώστα 42, Χαλάνδρι). Το κόστος παρακολούθησης ανέρχεται στα € 990 όπου τα μέλη του ISACA Athens Chapter δικαιούνται έκπτωση 10%. Πλέον αυτού του κόστους υπάρχει και ένα κόστος ύψους € 90 για τη σχετική ύλη. Για περισσότερες πληροφορίες μπορείτε να επισκεφτείτε τη σχετική [ιστοσελίδα](#) της PwC.

14 - 18 Μαρτίου 2011. Η [Q-Training](#) προσφέρει σεμινάρια προετοιμασίας CISA. Το κόστος του σεμιναρίου ποικίλει ανάλογα με τη διάρκεια που θα επιλέξει ο συμμετέχων, 2, 3 ή 5 ημέρες, από €675 έως €1260, συμπεριλαμβανομένης έκπτωσης 10% για τα μέλη ISACA. Περισσότερες πληροφορίες μπορείτε να δείτε στην ιστοσελίδα της [Q-Training](#).

CISM

30/03-02/04/2011, [Ελληνοαμερικανική Ένωση](#). Το σεμινάριο διάρκειας 24 ωρών θα λάβει χώρα στο συνεδριακό χώρο της Ελληνοαμερικανικής Ένωσης (Μασσαλίας 22, Αθήνα). Τα μέλη του ISACA Athens Chapter δικαιούνται έκπτωση με βάση την οποία το κόστος του σεμιναρίου ανέρχεται στο ποσό των €890. Για περισσότερες πληροφορίες μπορείτε να επισκεφτείτε τη σχετική [ιστοσελίδα](#) της Ελληνοαμερικανικής Ένωσης.



ISACA Athens Chapter

Newsletter

Ινστιτούτο Ελέγχου Συστημάτων Πληροφορικής (ΙΕΣΠ) - ISACA Athens Chapter

Μασσαλίας 22, Αθήνα,
GR -10680
www.isaca.gr
newsletter@isaca.gr
Τηλ: +30 210-28 86 041
Fax: +30 210 28 86 901

Το Ινστιτούτο Ελέγχου Συστημάτων
Πληροφορικής – ISACA Athens Chapter
δραστηριοποιείται στην Ελλάδα από το 1994
και αποτελεί το Ελληνικό παράρτημα του
διεθνούς οργανισμού
ISACA
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443

© 2011 Ινστιτούτο Ελέγχου Συστημάτων
Πληροφορικής (ISACA Athens Chapter) και ISACA
International.

ISACA®, CISA®, CISM®, CGEIT®, CRISC®, COBIT® 3rd
Edition®, COBIT®, COBIT Quickstart™, COBIT
Online™, K-NET®, IT Governance Institute®, ITGI®,
CACSSM, Information Systems Audit and Control
Association® and Information Systems Control
Journal®
are registered trademarks of ISACA International

Διοικητικό Συμβούλιο ΙΕΣΠ - ISACA Athens Chapter

Πρόεδρος:	Ανέστης Δημόπουλος
Αντιπρόεδρος:	Ιωάννης Λευκάκης
Γραμματέας:	Γεώργιος Ράικος
Ταμίας:	Αντώνιος Γκινόπουλος
Μέλη Δ.Σ.	Ιωάννης Δρακούλης Παναγιώτης Δρούκας Παναγιώτης Μερκούρης

Συντονιστής Πιστοποιήσεων:

Ανέστης Δημόπουλος
Membership & Marketing Director:
Ιωάννης Δρακούλης
Επικεφαλές Εκπαιδευτικής Επιτροπής:
Παναγιώτης Μερκούρης
Ιωάννης Λευκάκης
Υπεύθυνος Δικτυακού Τύπου:
Παναγιώτης Δρούκας
Συντονιστής Ακαδημαϊκών Θεμάτων:
Παναγιώτης Μερκούρης

Ομάδα Σύνταξης Ενημερωτικού Δελτίου:

Ιωάννης Λευκάκης
Παναγιώτης Μερκούρης
Ιωάννης Μπονάτος
Γιώργος Ταναμπασίδης
Χρήστος Βιδάκης
Σταμάτης Πασσάς
Νίκος Μπούμπουλης

Περισσότερες πληροφορίες και στοιχεία επικοινωνίας
στο www.isaca.gr ή www.isaca.org