ΔΙΑΤΜΗΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΣΤΑ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

ΚΙΝΔΥΝΟΙ ΚΑΙ ΕΛΕΓΧΟΙ ΤΩΝ ΛΟΓΙΣΤΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Φοιτήτρια: Κυριαζοπούλου Χριστιάνα

Επιβλέπων Καθηγητής: Καραγιώργος Θεοφάνης

Θεσσαλονίκη, Φεβρουάριος 2012

Αναγκαιότητα Διπλωματικής Εργασίας

- Τα σύγχρονα ΛΠΣ είναι αυτοματοποιημένες διαδικασίες που χρησιμοποιούν υπολογιστές, διακομιστές και intranet για τη συλλογή, διαχείριση, αποθήκευση, επεξεργασία, ανάκτηση και παρουσίαση των οικονομικών δεδομένων.
- Τα ΛΠΣ κινδυνεύουν συνεχώς να γίνουν στόχος επιθέσεων με απώτερο σκοπό την απόσπαση απόρρητων χρηματοοικονομικών στοιχείων και τη πρόκληση βλάβης στην εύρυθμη λειτουργία της επιχειρηματικής οντότητας.
- Απαιτείται η εξασφάλιση ενός υψηλού επιπέδου ακρίβειας, ακεραιότητας και ασφάλειας στις οικονομικές συναλλαγές και στην καταχώρηση των ημερολογιακών εγγραφών, ώστε να είναι άμεσα διαθέσιμες σε όσους έχουν νόμιμη πρόσβαση σε αυτές.
- Κατά συνέπεια, οι διαδικασίες ελέγχου που υλοποιούνται, προσπαθούν να εντοπίσουν τους κινδύνους που απειλούν το σύστημα και τις ευπάθειες που ενυπάρχουν.

<u>Σκοπός της διπλωματικής εργασίας είναι</u>

η ανάδειξη της σημασίας διαχείρισης του κινδύνου και εφαρμογής των κατάλληλων διαδικασιών ελέγχου στα λογιστικά πληροφοριακά συστήματα

Διάρθρωση Διπλωματικής Εργασίας

- **Το πρώτο κεφάλαιο αποτελεί την εισαγωγή της εργασίας, όπου καταδεικνύεται η αναγκαιότητα της συγγραφής της και η δομή του περιεχομένου της.**
- **Το δεύτερο κεφάλαιο πραγματεύεται τους κινδύνους που απειλούν και εμφανίζονται στα ΛΠΣ, καθώς και την ανάλυση και αξιολόγηση τους.**
- **Στο τρίτο κεφάλαιο αναλύεται λεπτομερώς η βασική ταξινόμηση του ελέγχου σε γενικούς ελέγχους και ελέγχους εφαρμογών.**
- **Στο τέταρτο κεφάλαιο παρατίθενται κάποιες ερευνητικές μελέτες που σχετίζονται με το αντικείμενο που πραγματεύεται η παρούσα εργασία.**
- **Στο πέμπτο κεφάλαιο αναπτύσσεται η προσέγγιση και η μεθοδολογία της έρευνας. Συγκεκριμένα, αναφέρονται το δείγμα του πληθυσμού, ο τρόπος αποστολής των ερωτηματολογίων και το περιεχόμενο τους, καθώς επίσης και η στατιστική μέθοδος ανάλυσης τους.**
- **Στο έκτο κεφάλαιο παρουσιάζονται τα αποτελέσματα των ερωτήσεων με τη χρήση πινάκων και γραφημάτων.**
- **Στο έβδομο κεφάλαιο παρατίθενται τα συμπεράσματα, όπως προκύπτουν από τη βιβλιογραφική επισκόπηση και την ανάλυση των απαντήσεων του ερωτηματολογίου. Τέλος, γίνονται προτάσεις για περαιτέρω έρευνα.**

Κίνδυνοι ΛΠΣ

Ο ISO ορίζει τον κίνδυνο ως την πιθανότητα μια απειλή (threat) να προκαλέσει αδυναμίες (vulnerabilities) στα περιουσιακά στοιχεία (assets) της επιχείρησης, και γενικότερα να έχει αρνητική επίδραση (impact) στη λειτουργία της.

Περιουσιακά στοιχεία: οι πληροφορίες και οι πόροι που έχουν αξία για την επιχείρηση. Διακρίνονται σε απτά και άυλα.

Απειλές: ανεπιθύμητα γεγονότα που μπορεί να έχουν ως αποτέλεσμα την αποκάλυψη, απώλεια και καταστροφή ενός περιουσιακού στοιχείου. Διακρίνονται στις φυσικές, τυχαίες και σκόπιμες απειλές.

Ευπάθειες: ελαττώματα στο σχεδιασμό, στην εφαρμογή, στη λειτουργία ή στη διαχείριση του συστήματος, τα οποία μπορούν να επιτρέψουν τη μη εξουσιοδοτημένη πρόσβαση ενός εισβολέα στους πόρους του.

Διαχείριση κινδύνου: η διαδικασία προσδιορισμού και αξιολόγησης των κινδύνων που εμφανίζονται, ώστε να περιοριστούν σε κάποιο αποδεκτό επίπεδο.

Ανάλυση κινδύνου (Risk analysis): Προσδιορισμός περιουσιακών στοιχείων, Εντοπισμός απειλών, Προσδιορισμός ευπαθειών

Εκτίμηση κινδύνου (Risk evaluation): Ποσοτικές και ποιοτικές μεθοδολογίες

Έλεγχοι ΛΠΣ

Με τον όρο **Έλεγχος ΛΠΣ** εννοούμε τις μεθόδους, τις διαδικασίες και τις πρακτικές που έχουν ως σκοπό (Νικολάου 1999):

- τη διαφύλαξη των περιουσιακών στοιχείων πληροφορικής τεχνολογίας
- τη διασφάλιση της ακρίβειας και της αξιοπιστίας των οικονομικών δεδομένων
- τη διασφάλιση της πολιτικής της επιχείρησης στη διεξαγωγή των εργασιών της
- την εξασφάλιση της αποδοτικότητας των οργανωτικών της δραστηριοτήτων

Ταξινόμηση Ελέγχου:
Με βάση το σκοπό του - **Προληπτικοί έλεγχοι, Διορθωτικοί έλεγχοι, Διαγνωστικοί έλεγχοι**
Με βάση το πεδίο εφαρμογής του **- Γενικοί έλεγχοι, Έλεγχοι εφαρμογών**

Γενικοί Έλεγχοι (General Controls):
Έλεγχοι Διαχείρισης
Έλεγχοι Ανάπτυξης Συστήματος
Έλεγχοι Υλικού
Έλεγχοι Πρόσβασης
Έλεγχοι Αποθήκευσης Δεδομένων
Έλεγχοι στη Μετάδοση Δεδομένων μέσω Δικτύων
Έλεγχοι για τη Προστασία Προσωπικών Υπολογιστών
Έλεγχοι Συνέχειας

Έλεγχοι Εφαρμογών (Application Controls)
Έλεγχοι στο στάδιο Εισόδου Δεδομένων (Data Inputs Controls)
Έλεγχοι στο στάδιο Επεξεργασίας (Processing Controls)
Έλεγχοι στο στάδιο Εξόδου (Outputs Controls)

Επισκόπηση Ερευνών

Ερευνητής	Θέμα	Αποτελέσματα
Ebaid (2011)	Εσωτερικός έλεγχος στις εισηγμένες αιγυπτιακές επιχειρήσεις	Δεν υπάρχει υψηλό επίπεδο ανεξαρτησίας, υποστήριξη από τη διοίκηση, αλληλεπίδραση εσωτερικών και εξωτερικών ελεγκτών, εξειδικευμένο προσωπικό. Επικεντρώνεται κυρίως στον οικονομικό έλεγχο.
Lin and Wang (2011)	Μοντέλο επιλογής και αξιολόγησης του λογισμικού ελέγχου	Κριτήρια επιλογής: λειτουργίες, επεξεργασία δεδομένων, τεχνική υποστήριξη, κόστος. Παράγοντες επιλογής: ακεραιότητα συστήματος, ακρίβεια δεδομένων, τεχνική υποστήριξη, κόστος απόκτησης.
Dang *et al* (2011)	Συνάφεια των λογιστικών πληροφοριών όταν υπάρχουν λάθη ελέγχου	Η συνάφεια είναι μικρής αξίας όταν υπάρχουν σφάλματα, ανεξαρτήτως από τη φήμη του ελεγκτή.
Law (2011)	Παράγοντες πρόληψης της απάτης	Συμβάλλουν στη πρόληψη της απάτης: η αποδοτικότητα της ελεγκτικής επιτροπής και του εσωτερικού ελέγχου, η ανώτερη διοίκηση, οι ηθικές πολιτικές. Το είδος του ελεγκτή και οι προηγούμενες επιτυχίες του δεν αποδείχτηκε ότι συμβάλλουν.
Salehi and Abdipour (2011)	Εμπόδια στην εφαρμογή των ΛΠΣ	Εμπόδια: οι μεσαίοι μάνατζερ, η οργανωσιακή δομή και κουλτούρα, τα οικονομικά προβλήματα, οι ανθρώπινοι πόροι και οι περιβαλλοντικοί παράγοντες.
Morris (2011)	Επίδραση των ERP στην αποδοτικότητα του εσωτερικού ελέγχου	Οι επιχειρήσεις που εφάρμοζαν ERP παρουσίαζαν λιγότερες αδυναμίες εσωτερικού ελέγχου.
Grande *et al* (2011)	Σχέση ανάμεσα στη χρήση ΛΠΣ και στη βελτίωση της απόδοσης και της παραγωγικότητας	Υπάρχει θετική συσχέτιση. Οι επιχειρήσεις που τα εφαρμόζουν, έχουν καλύτερη οικονομική εικόνα σε αντίθεση με εκείνες που δεν το κάνουν.
Abu-Musa (2010)	Επάρκεια του ελέγχου για την προστασία των ΛΠΣ στις τράπεζες της Σαουδικής Αραβίας	Οι τεχνικές ελέγχου που εφαρμόζονταν επαρκούσαν σε ικανοποιητικό βαθμό. Έγιναν προτάσεις βελτίωσης των διαδικασιών ελέγχου.
Sajady *et al* (2008)	Αξιολόγηση αποδοτικότητας των ΛΠΣ	Τα ΛΠΣ συνέβαλλαν στη βελτίωση της λήψης αποφάσεων, του εσωτερικού ελέγχου, της ποιότητας των οικονομικών καταστάσεων και στη διευκόλυνση της διαδικασίας συναλλαγών. Δεν αποδείχθηκε ότι η διαδικασία αξιολόγησης της απόδοσης είχε βελτιωθεί.
Abu-Musa (2006)	Απειλές των ΛΠΣ	Οι συνηθέστεροι τύποι απειλών ήταν η λανθασμένη εισαγωγή δεδομένων, η καταστροφή δεδομένων, η μόλυνση από κακόβουλο λογισμικό, η γνωστοποίηση των κωδικών πρόσβασης και η διανομή πληροφοριών σε μη εξουσιοδοτημένους χρήστες.
Abu-Musa (2006)	Επάρκεια του ελέγχου για την προστασία των ΛΠΣ από παραβιάσεις και επιθέσεις	Εξετάστηκαν οι εξής κατηγορίες ελέγχου: οργανωσιακός, υλικού και φυσικής πρόσβασης, λογισμικού και ηλεκτρονικής πρόσβασης, δεδομένων, προγραμμάτων αποσύνδεσης και backup, χρησιμότητας, παραβίασης της κανονικής πρόσβασης, προγραμματισμού, καταμερισμού των αρμοδιοτήτων και εκροών.
Hayale and Abu Khadra (2006)	Αξιολόγηση του επιπέδου ελέγχου των ΛΠΣ στις τράπεζες της Ιορδανίας	Οι έλεγχοι για πρόληψη της απάτης και περιορισμό σφαλμάτων ήταν αποδοτικοί. Αδυναμίες υπήρχαν σε ελέγχους φυσικής πρόσβασης, λογικής πρόσβασης, ασφάλειας δεδομένων, τεκμηρίωσης προτύπων, αποκατάστασης μετά από καταστροφή, διαδικτύου, επικοινωνίας και εκροών.

Επισκόπηση Ερευνών

Ερευνητής	Θέμα	Αποτελέσματα
Hunton *et al* (2004)	Ικανότητα των οικονομικών ελεγκτών και των ελεγκτών ΠΣ να αξιολογούν τους κινδύνους των ERP	Οι ελεγκτές ΠΣ ενδιαφερόντουσαν περισσότερο για τους κινδύνους και είχαν λιγότερη εμπιστοσύνη στις ικανότητες των οικονομικών ελεγκτών να τους αντιλαμβάνονται.
Ismail *et al* (2003)	Υιοθέτηση των ΛΠΣ σε επιχειρήσεις μικρού και μεσαίου μεγέθους στη βόρεια περιοχή της χερσονήσου της Μαλαισίας	Η απόδοση του συστήματος ήταν συνάρτηση του έτους εισαγωγής του και των ετών λειτουργίας της επιχείρησης. Δεν αποδείχτηκε ότι σχετιζόταν με το μέγεθος της επιχείρησης και τον τύπο ηγεσίας.
Wright and Wright (2002)	Ασφάλεια των ERP συστημάτων σχετικά με τους κινδύνους που τα απειλούν	Η εμφάνιση επιχειρησιακών κινδύνων και λαθών στις οικονομικές καταστάσεις ήταν απόρροια της ελλιπούς εκπαίδευσης των χρηστών. Οι κίνδυνοι ήταν διαφορετικοί στις ARP εφαρμογές. Οι επιχειρήσεις χρησιμοποιούσαν κυρίως τεχνικές ελέγχου παρά δοκιμές επικύρωσης.
Rezaee *et al* (2001)	Έλεγχος ΛΠΣ που επιτρέπουν την on-line και σε πραγματικό χρόνο διαχείριση οικονομικών πληροφοριών στηριζόμενα στην XBRL	Οι ελεγκτές πρέπει να χρησιμοποιούν τον συνεχή ηλεκτρονικό έλεγχο σε ΛΠΣ πραγματικού χρόνου. Επίσης, πρέπει να γνωρίζουν τις επιπτώσεις του συνεχούς ελέγχου και τις διαδικασίες ελέγχου που μπορούν να εφαρμόζουν.
Grabski *et al* (2001)	Κίνδυνοι και έλεγχοι από την εισαγωγή των ERP συστημάτων	Προσδιορίστηκαν οι 5 βασικοί κίνδυνοι και τα στοιχεία που έπρεπε να ελεγχθούν.
Coffin and Patilis (2001)	Ικανότητα των εσωτερικών ελεγκτών να αξιολογούν τους ελέγχους ασφαλείας στα ΛΠΣ	Ο εσωτερικός έλεγχος είναι σημαντικός για τον εντοπισμό των εφαρμοζόμενων τεχνικών ασφαλείας ώστε να προσδιοριστεί η πρόσβαση σε πληροφορίες και η συμμόρφωση με τους ισχύοντες νόμους.
Nikolaou (2000)	Βαθμός συσχέτισης των απαιτήσεων της επιχείρησης με το σχεδιασμό ενός ΛΠΣ	Θετική συσχέτιση σχέση που συνεισέφερε στην αποδοτικότητα του ελέγχου αλλά όχι στην ικανοποίηση των χρηστών.
Furnell and Dowland's (2000)	Προστασία των ΛΠΣ έναντι της μη εξουσιοδοτημένης πρόσβασης από εισβολείς	Οι μέθοδοι πιστοποίησης των χρηστών και ελέγχου της πρόσβασης δεν επαρκούν.
Zviran and Haga (1999)	Κωδικός πρόσβασης: η συνηθέστερη μέθοδος ασφάλειας των ΛΠΣ	Δίνεται ελάχιστη προσοχή στα χαρακτηριστικά της πραγματικής του χρήσης. Συνήθως αποτελούνται από πέντε ή λιγότερους χαρακτήρες, είναι αλφαβητικοί και δεν αλλάζονται συχνά.
Henry (1997)	Φύση και έλεγχος των ΛΠΣ σε επιχειρήσεις του Hampton Roads στη Βιρτζίνια.	Οι βασικές τεχνικές ασφαλείας ήταν τα εφεδρικά αντίγραφα δεδομένων, οι κωδικοί πρόσβασης, οι περιοδικοί έλεγχοι, τα προγράμματα κατά της μόλυνσης από κακόβουλο λογισμικό, η φυσική ασφάλεια, η μέθοδος εξουσιοδότησης για αλλαγές στο σύστημα και η κρυπτογράφηση.
(1996)	Απειλές των ΛΠΣ	Προσδιορίστηκαν οι απειλές που εμφανίζονται στο περιβάλλον των μικροϋπολογιστών, στους κεντρικούς υπολογιστές και σε περιβάλλοντα δικτύων.
Loch *et al* (1992)	Απειλές των ΛΠΣ	Οι βασικοί τύποι απειλών ήταν οι φυσικές καταστροφές, η ακούσια εισαγωγή λανθασμένων δεδομένων, η ακούσια καταστροφή δεδομένων, ο ανεπαρκής έλεγχος των μέσων και η μη εξουσιοδοτημένη πρόσβαση από χάκερς.

Προσέγγιση - Μεθοδολογία Έρευνας

- Το δείγμα πληθυσμού αφορά επιχειρήσεις που εδρεύουν στη Βόρεια Ελλάδα
- Τα ερωτηματολόγια απεστάλησαν σε εισηγμένες και μη επιχειρήσεις στο ΧΑΑ
- Ο κλάδος δραστηριότητας δεν αποτέλεσε περιοριστικό στοιχείο
- Το δείγμα περιλαμβάνει λογιστικά και φοροτεχνικά γραφεία, καθώς και επιχειρήσεις με ενσωματωμένο λογιστήριο και οικονομικό τμήμα.

- Οι ερωτήσεις που χρησιμοποιήθηκαν είναι κλειστού τύπου, πολλαπλής επιλογής και βαθμολογικής κλίμακας Likert (πενταβάθμια κλίμακα).
- Για τη στατιστική επεξεργασία και ανάλυση των απαντήσεων χρησιμοποιήθηκε το στατιστικό πακέτο λογισμικού SPSS.

Το ερωτηματολόγιο απαρτίζεται από τρία μέρη:

- Το **Μέρος Α**, αφορά σε θέματα σχετικά με τους κινδύνους που απειλούν το λογιστικό πληροφοριακό σύστημα και τη διαχείριση τους.
- Το **Μέρος Β**, περιλαμβάνει ερωτήσεις σχετικά με το ρόλο του ελέγχου και την αποδοτικότητα του.
- Στο **Μέρος Γ**, εξετάζεται η λειτουργικότητα του λογιστικού πληροφοριακού συστήματος σχετικά με τα τεχνικά χαρακτηριστικά του και την ακρίβεια των οικονομικών πληροφοριών.

Προσέγγιση - Μεθοδολογία Έρευνας

- Τα ερωτηματολόγια απεστάλησαν σε 200 επιχειρήσεις, από τις οποίες ανταποκρίθηκαν οι 52. Δηλαδή ποσοστό της τάξης του 23% επί του συνόλου.

- Από τις 52 επιχειρήσεις, 4 ανήκουν στον κλάδο της Κλωστοϋφαντουργίας (7,7%), 18 είναι λογιστικά γραφεία (34,6%), 5 ανήκουν στον κλάδο της Υγείας (9,6%), 5 στον κλάδο των Τροφίμων και Ποτών (9,6%), 8 στον κλάδο του Εμπορίου (15,4%), 6 στον κλάδο των Βιομηχανικών Προϊόντων (11,5%), 4 στον Κατασκευαστικό-Τεχνικό κλάδο (7,7%) και 2 στον κλάδο του Πολιτισμού (3,8%).

- Ως προς την ιδιότητα των ερωτηθέντων, 4 δήλωσαν πως είναι διευθυντικά στελέχη (7,7%), 6 Προϊστάμενοι Μηχανοργάνωσης (IT Supervisor) (11,5%), 14 Βοηθοί Λογιστών (26,9%), 10 Λογιστές (19,2%), 16 Προϊστάμενοι Λογιστηρίου (30,8%), και 2 Υπεύθυνοι Logistics (3,8%).

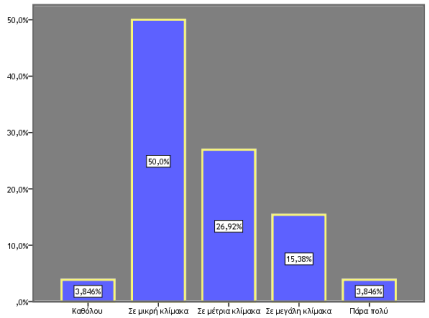
- Σχετικά με το λογιστικό πληροφοριακό σύστημα που χρησιμοποιούν οι επιχειρήσεις, 2 επέλεξαν να εφαρμόσουν το ERP Momentum (3,8%), 8 το X-Line ERP (15,4%), 4 το Singular Eurofasma (7,7%), 2 το Softone ERP (3,8%), 4 το Singular Logic (7,7%), 8 το Entersoft ERP (15,4%), 11 το Epsilon Net (21,2%), 6 το Κεφάλαιο (11,5%) και 7 το Atlantis (13,5%).

Αποτελέσματα Έρευνας (ερωτήσεις 1-3)

Απειλές

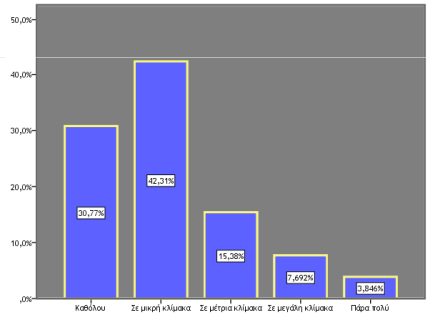
1. **Σε ποιο βαθμό πραγματοποιείται λανθασμένη εισαγωγή δεδομένων από τους εργαζομένους στο σύστημα;**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Καθόλου	2	3,8	3,8	3,8
	Σε μικρή κλίμακα	26	50,0	50,0	53,8
	Σε μέτρια κλίμακα	14	26,9	26,9	80,8
	Σε μεγάλη κλίμακα	8	15,4	15,4	96,2
	Πάρα πολύ	2	3,8	3,8	100,0
	Total	52	100,0	100,0	



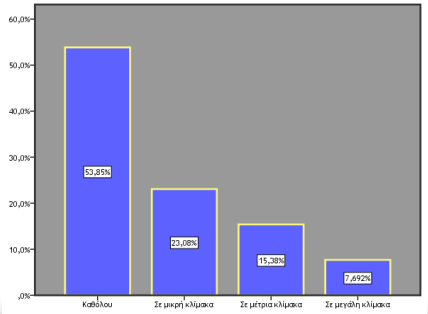
2. **Σε ποιο βαθμό πραγματοποιείται καταστροφή ή διαγραφή δεδομένων από τους εργαζομένους στο σύστημα;**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Καθόλου	16	30,8	30,8	30,8
	Σε μικρή κλίμακα	22	42,3	42,3	73,1
	Σε μέτρια κλίμακα	8	15,4	15,4	88,5
	Σε μεγάλη κλίμακα	4	7,7	7,7	96,2
	Πάρα πολύ	2	3,8	3,8	100,0
	Total	52	100,0	100,0	



3. **Σε ποιο βαθμό πραγματοποιείται μη εξουσιοδοτημένη πρόσβαση σε δεδομένα από εσωτερικούς χρήστες ή εισβολείς;**

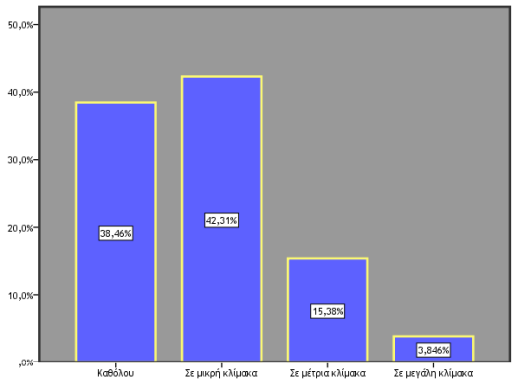
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Καθόλου	28	53,8	53,8	53,8
	Σε μικρή κλίμακα	12	23,1	23,1	76,9
	Σε μέτρια κλίμακα	8	15,4	15,4	92,3
	Σε μεγάλη κλίμακα	4	7,7	7,7	100,0
	Total	52	100,0	100,0	



Αποτελέσματα Έρευνας (ερωτήσεις 4-5)
Απειλές

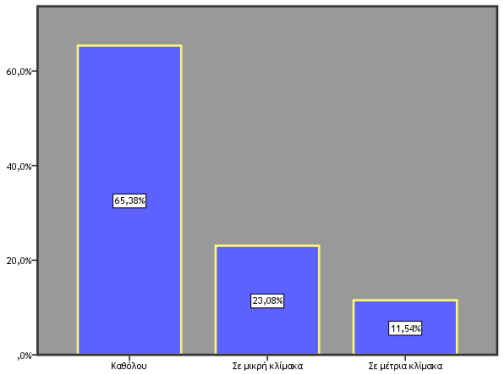
4. **Σε ποιο βαθμό πραγματοποιείται μόλυνση του συστήματος από κακόβουλο λογισμικό;**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Καθόλου	20	38,5	38,5	38,5
	Σε μικρή κλίμακα	22	42,3	42,3	80,8
	Σε μέτρια κλίμακα	8	15,4	15,4	96,2
	Σε μεγάλη κλίμακα	2	3,8	3,8	100,0
	Total	52	100,0	100,0	



5. **Σε ποιο βαθμό πραγματοποιείται κλοπή απόρρητων οικονομικών πληροφοριών από εσωτερικούς χρήστες ή εισβολείς;**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Καθόλου	34	65,4	65,4	65,4
	Σε μικρή κλίμακα	12	23,1	23,1	88,5
	Σε μέτρια κλίμακα	6	11,5	11,5	100,0
	Total	52	100,0	100,0	



Αποτελέσματα Έρευνας (ερωτήσεις 3-4)
Συσχέτιση Pearson

- **Μήτρα συσχέτισης 2x2**
- **Η διαγώνιος της μήτρας δίνει συντελεστή συσχέτισης 1**
- **Η συσχέτιση των μεταβλητών Access και Theft είναι +0,989**
- **Χρησιμοποιήθηκαν 52 ζεύγη τιμών**
- **Το επίπεδο σημαντικότητας δίνεται με τρία δεκαδικά ψηφία (,000) και είναι διπλής ουράς**
- **Η συσχέτιση είναι σημαντική σε επίπεδο σημαντικότητας 0.01 (1%)**

Αποτέλεσμα: θετική σχέση μεταξύ μη εξουσιοδοτημένης πρόσβασης και κλοπής απόρρητων πληροφοριών

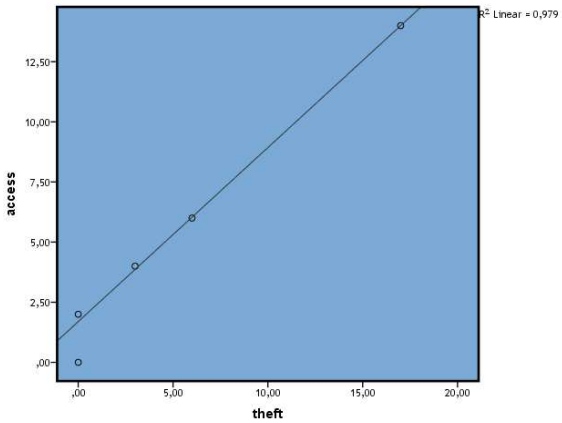
		access	theft
access	Pearson Correlation	1	,989**
	Sig. (2-tailed)		,000
	N	52	52
theft	Pearson Correlation	,989**	1
	Sig. (2-tailed)	,000	
	N	52	52

**. Correlation is significant at the 0.01 level (2-tailed).

Γράφημα Διασποράς

- **Μικρή διασπορά = Μεγάλη συσχέτιση**
- **Η κλίση της διασποράς είναι μια μάλλον ευθεία γραμμή**
- **Η θέση της ευθείας υποδηλώνει θετική συσχέτιση**

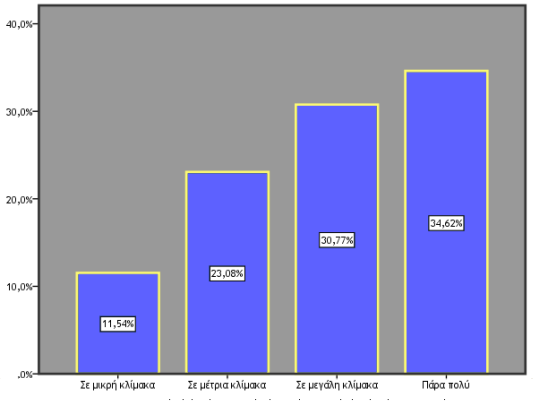
Αποτέλεσμα: δεν υπάρχουν ενδείξεις μη γραμμικής σχέσης ή έντονα αποκλίνουσες τιμές



Αποτελέσματα Έρευνας (ερωτήσεις 6-7)
Ευπάθειες

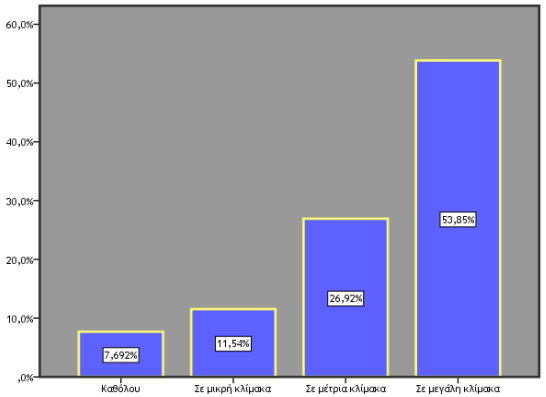
6. Σε ποιο βαθμό διατηρεί η επιχείρηση εφεδρικά αντίγραφα δεδομένων;

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Σε μικρή κλίμακα	6	11,5	11,5	11,5
	Σε μέτρια κλίμακα	12	23,1	23,1	34,6
	Σε μεγάλη κλίμακα	16	30,8	30,8	65,4
	Πάρα πολύ	18	34,6	34,6	100,0
	Total	52	100,0	100,0	



7. Σε ποιο βαθμό η ταχύτητα αποκατάστασης του συστήματος μετά από διακοπή της λειτουργίας του είναι ικανοποιητική;

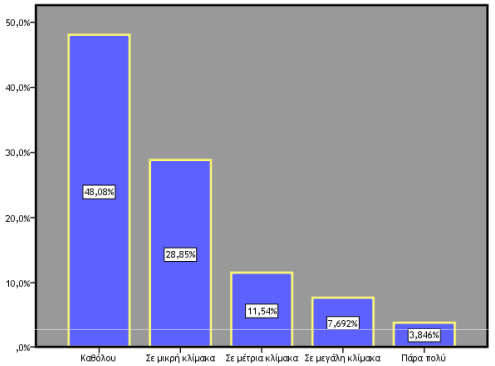
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Καθόλου	4	7,7	7,7	7,7
	Σε μικρή κλίμακα	6	11,5	11,5	19,2
	Σε μέτρια κλίμακα	14	26,9	26,9	46,2
	Σε μεγάλη κλίμακα	28	53,8	53,8	100,0
	Total	52	100,0	100,0	



Αποτελέσματα Έρευνας (ερωτήσεις 8-9)
Ευπάθειες

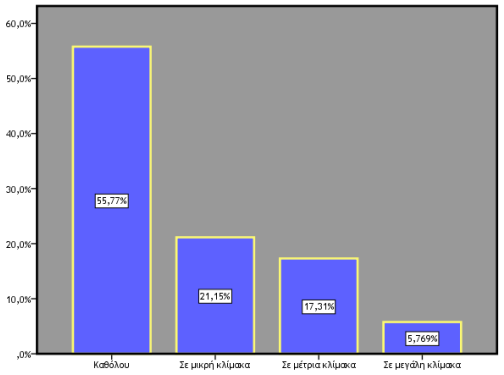
8. Σε ποιο βαθμό πραγματοποιείται άρνηση υπηρεσίας (denial of service) στους εξουσιοδοτημένους χρήστες;

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Καθόλου	25	48,1	48,1	48,1
	Σε μικρή κλίμακα	15	28,8	28,8	76,9
	Σε μέτρια κλίμακα	6	11,5	11,5	88,5
	Σε μεγάλη κλίμακα	4	7,7	7,7	96,2
	Πάρα πολύ	2	3,8	3,8	100,0
	Total	52	100,0	100,0	



9. Σε ποιο βαθμό παρατηρούνται περιστατικά social engineering με σκοπό την αποκάλυψη απόρρητων πληροφοριών ή πιστοποιήσεων χρήστη;

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Καθόλου	29	55,8	55,8	55,8
	Σε μικρή κλίμακα	11	21,2	21,2	76,9
	Σε μέτρια κλίμακα	9	17,3	17,3	94,2
	Σε μεγάλη κλίμακα	3	5,8	5,8	100,0
	Total	52	100,0	100,0	



Αποτελέσματα Έρευνας (ερωτήσεις 6-9)
Περιγραφικά Στατιστικά Στοιχεία

Είναι αριθμοί που υπολογίζονται από τα δεδομένα και η τιμή τους αντιπροσωπεύει κάποια συμπεριφορά ή τάση του δείγματος (Κυριαζόπουλος και Σαμαντά, 2009).

		backups	recovery	denial_of_service	social_engineering
N	Valid	52	52	52	52
	Missing	0	0	0	0
Mean		14,6154	12,5385	5,0385	4,2692
Median		16,0000	14,0000	4,0000	3,0000
Mode		18,00	,00	2,00	,00
Std. Deviation		3,87123	11,66268	3,93557	4,18735
Variance		14,986	136,018	15,489	17,534
Range		12,00	28,00	13,00	11,00
Minimum		6,00	,00	2,00	,00
Maximum		18,00	28,00	15,00	11,00
Sum		760,00	652,00	262,00	222,00

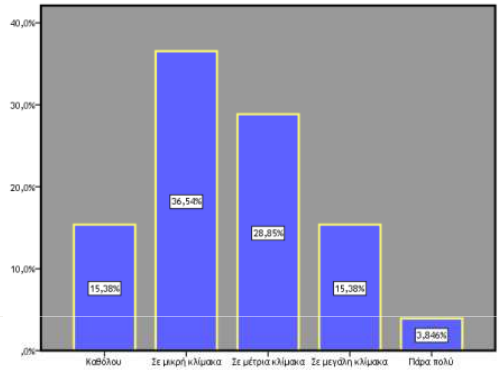
Οι σοβαρότερες αδυναμίες προκαλούνται στο σύστημα από:

1. **Προβλήματα στην ταχύτητα αποκατάστασης μετά από διακοπή της λειτουργίας του**
2. **Περιστατικά κοινωνικής μηχανικής**
3. **Άρνηση παροχής υπηρεσίας**
4. **Έλλειψη εφεδρικών αντιγράφων δεδομένων**

Αποτελέσματα Έρευνας (ερωτήσεις 10-11)
Διαχείριση Κινδύνου

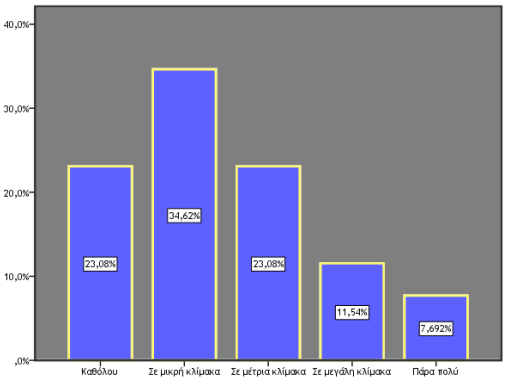
10. Σε ποιο βαθμό ο προσδιορισμός των περιουσιακών στοιχείων, των απειλών και των ευπαθειών πραγματοποιείται σε τακτικά χρονικά διαστήματα;

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Καθόλου	8	15,4	15,4	15,4
	Σε μικρή κλίμακα	19	36,5	36,5	51,9
	Σε μέτρια κλίμακα	15	28,8	28,8	80,8
	Σε μεγάλη κλίμακα	8	15,4	15,4	96,2
	Πάρα πολύ	2	3,8	3,8	100,0
	Total	52	100,0	100,0	



11. Σε ποιο βαθμό η επιχείρηση εφαρμόζει ποσοτικές και ποιοτικές μεθοδολογίες προκειμένου να αξιολογήσει τον κίνδυνο;

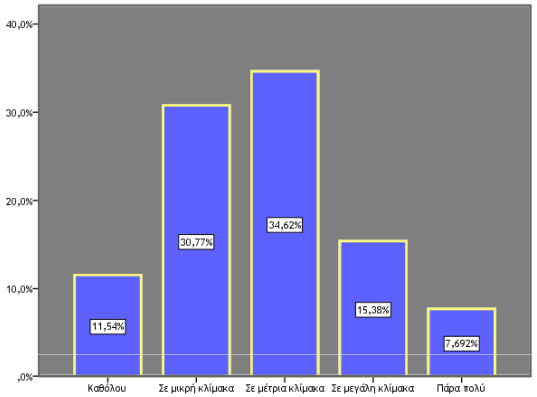
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Καθόλου	12	23,1	23,1	23,1
	Σε μικρή κλίμακα	18	34,6	34,6	57,7
	Σε μέτρια κλίμακα	12	23,1	23,1	80,8
	Σε μεγάλη κλίμακα	6	11,5	11,5	92,3
	Πάρα πολύ	4	7,7	7,7	100,0
	Total	52	100,0	100,0	



Αποτελέσματα Έρευνας (ερωτήσεις 12-13)
Διαχείριση Κινδύνου

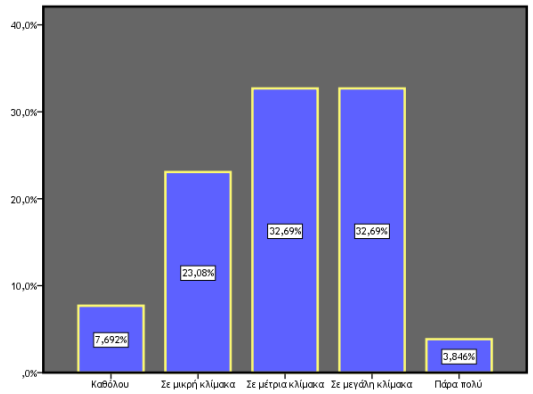
12. Σε ποιο βαθμό η διοίκηση έχει ορίσει αποτελεσματικές διαδικασίες για την αντιμετώπιση των γνωστών και επαναλαμβανόμενων κινδύνων;

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Καθόλου	6	11,5	11,5	11,5
	Σε μικρή κλίμακα	16	30,8	30,8	42,3
	Σε μέτρια κλίμακα	18	34,6	34,6	76,9
	Σε μεγάλη κλίμακα	8	15,4	15,4	92,3
	Πάρα πολύ	4	7,7	7,7	100,0
	Total	52	100,0	100,0	



13. Σε ποιο βαθμό η διαχείριση κινδύνου παρέχει στη διοίκηση τις απαραίτητες πληροφορίες που χρειάζεται ώστε να μειώσει τον κίνδυνο σε ένα αποδεκτό επίπεδο και να εφαρμόσει κατάλληλους μηχανισμούς ασφαλείας για τη διατήρηση του;

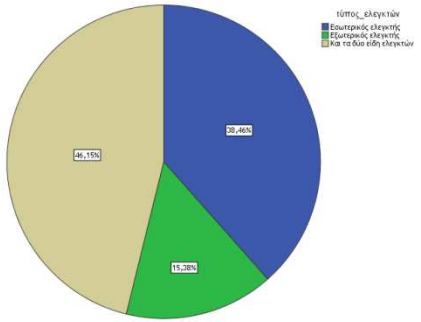
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Καθόλου	4	7,7	7,7	7,7
	Σε μικρή κλίμακα	12	23,1	23,1	30,8
	Σε μέτρια κλίμακα	17	32,7	32,7	63,5
	Σε μεγάλη κλίμακα	17	32,7	32,7	96,2
	Πάρα πολύ	2	3,8	3,8	100,0
	Total	52	100,0	100,0	



Αποτελέσματα Έρευνας (ερωτήσεις 14-16)
Τύποι Ελεγκτών και Αρμόδιοι Ελέγχου

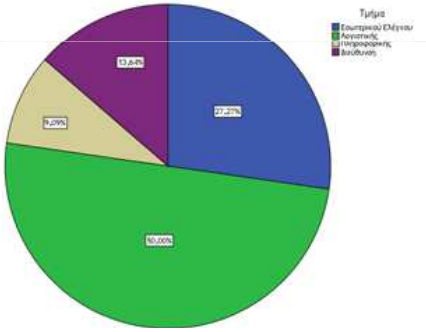
14. Η αξιολόγηση του συστήματος της επιχείρησης πραγματοποιείται από εσωτερικούς ελεγκτές, εξωτερικούς ελεγκτές ή και τα δύο είδη ελεγκτών;

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Εσωτερικός ελεγκτής	20	38,5	38,5	38,5
	Εξωτερικός ελεγκτής	8	15,4	15,4	53,8
	Και τα δύο είδη ελεγκτών	24	46,2	46,2	100,0
	Total	52	100,0	100,0	



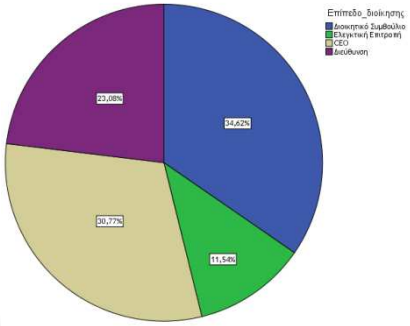
15. Εάν πραγματοποιείται από εσωτερικούς ελεγκτές, τότε υπάρχει ξεχωριστό τμήμα εσωτερικού ελέγχου στην επιχείρηση ή είναι κομμάτι άλλου τμήματος;

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Εσωτερικού Ελέγχου	12	27,3	27,3	27,3
	Λογιστικής	22	50,0	50,0	77,3
	Πληροφορικής	4	9,1	9,1	86,4
	Διεύθυνση	6	13,6	13,6	100,0
	Total	44	100,0	100,0	



16. Σε ποιο επίπεδο διοίκησης αναφέρεται ο ελεγκτής;

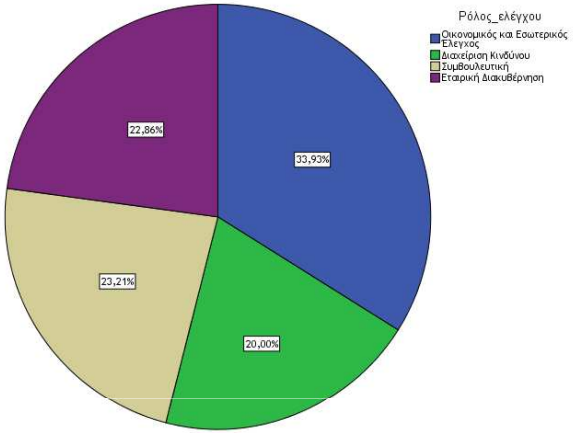
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Διοικητικό Συμβούλιο	18	34,6	34,6	34,6
	Ελεγκτική Επιτροπή	6	11,5	11,5	46,2
	CEO	22	42,3	42,3	88,5
	Ιδιοκτήτης	6	11,5	11,5	100,0
	Total	52	100,0	100,0	



Αποτελέσματα Έρευνας (ερωτήσεις 17-18)
Αντικείμενο και Ρόλος Ελέγχου

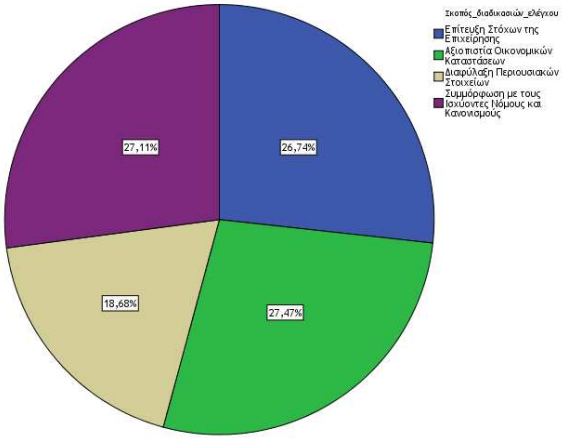
17. Με τι ασχολείται ο έλεγχος στην επιχείρηση σας;

		Percent	Valid Percent	Cumulative Percent
Valid	Οικονομικός και Εσωτερικός Έλεγχος	33,9	33,9	33,9
	Διαχείριση Κινδύνου	20,0	20,0	53,9
	Συμβουλευτική	23,2	23,2	77,1
	Εταιρική Διακυβέρνηση	22,9	22,9	100,0
	Total	100,0	100,0	



18. Οι διαδικασίες ελέγχου που εφαρμόζονται στην επιχείρηση σας έχουν σκοπό να διασφαλίσουν:

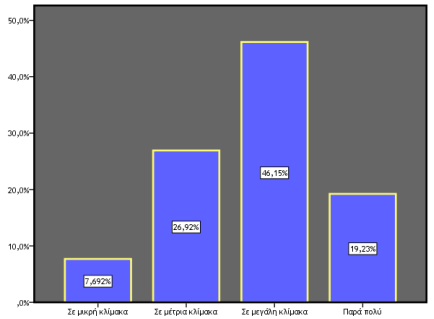
		Percent	Valid Percent	Cumulative Percent
Valid	Επίτευξη Στόχων της Επιχείρησης	26,7	26,7	26,7
	Αξιοπιστία Οικονομικών Καταστάσεων	27,5	27,5	54,2
	Διαφύλαξη Περιουσιακών Στοιχείων	18,7	18,7	72,9
	Συμμόρφωση με τους Ισχύοντες Νόμους και Κανονισμούς	27,1	27,1	100,0
	Total	100,0	100,0	



Αποτελέσματα Έρευνας (ερωτήσεις 19-21)
Αποδοτικότητα Ελέγχου

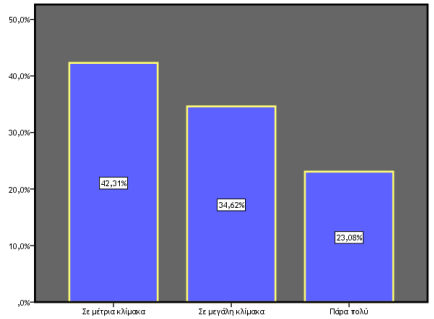
19. Σε ποιο βαθμό ο έλεγχος εντοπίζει τους κινδύνους που ενδέχεται να επηρεάσουν την εύρυθμη λειτουργία της επιχείρησης;

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Σε μικρή κλίμακα	4	7,7	7,7	7,7
	Σε μέτρια κλίμακα	14	26,9	26,9	34,6
	Σε μεγάλη κλίμακα	24	46,2	46,2	80,8
	Πάρα πολύ	10	19,2	19,2	100,0
	Total	52	100,0	100,0	



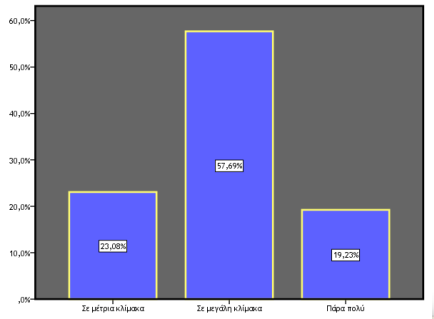
20. Σε ποιο βαθμό η επιχείρηση αξιολογεί την αποδοτικότητα του ελέγχου ούτως ώστε να περιοριστεί ο κίνδυνος;

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Σε μέτρια κλίμακα	22	42,3	42,3	42,3
	Σε μεγάλη κλίμακα	18	34,6	34,6	76,9
	Πάρα πολύ	12	23,1	23,1	100,0
	Total	52	100,0	100,0	



21. Σε ποιο βαθμό η επιχείρηση εφαρμόζει τις υποδείξεις του ελεγκτή;

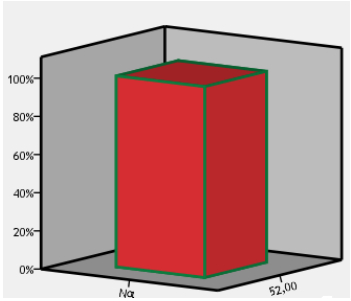
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Σε μέτρια κλίμακα	12	23,1	23,1	23,1
	Σε μεγάλη κλίμακα	30	57,7	57,7	80,8
	Πάρα πολύ	10	19,2	19,2	100,0
	Total	52	100,0	100,0	



Αποτελέσματα Έρευνας (ερωτήσεις 22-25)
Τεχνικά Χαρακτηριστικά ΛΠΣ

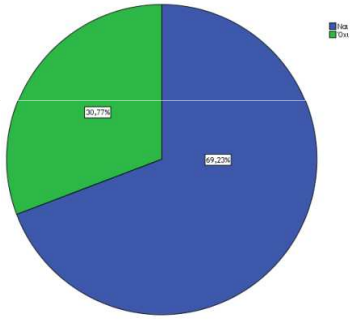
22. Το λογιστικό πληροφοριακό σύστημα έχει αγοραστεί από την επιχείρηση;

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Ναι	52	100,0	100,0	100,0



23. Το λογιστικό πληροφοριακό σύστημα λειτουργεί σε πραγματικό χρόνο;

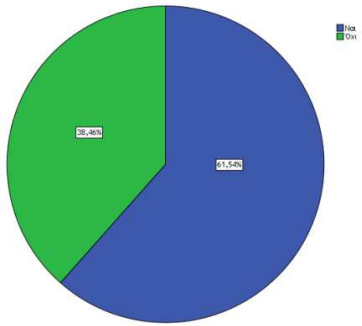
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Ναι	36	69,2	69,2	69,2
	Οχι	16	30,8	30,8	100,0
	Total	52	100,0	100,0	



24. Διαθέτει υπηρεσία για την online παρουσίαση των υπολοίπων των λογαριασμών γενικού καθολικού;

25. Προσφέρει online και σε πραγματικό χρόνο οικονομικές καταστάσεις;

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Ναι	32	61,5	61,5	61,5
	Οχι	20	38,5	38,5	100,0
	Total	52	100,0	100,0	



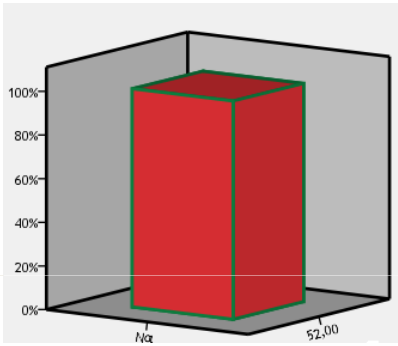
Αποτελέσματα Έρευνας (ερωτήσεις 26-29)
Ακρίβεια, Επικαιρότητα και Ασφάλεια Πληροφοριών

26. Οι οικονομικές πληροφορίες είναι πλήρεις και ακριβείς;

27. Οι οικονομικές καταστάσεις βασίζονται σε ενημερωμένες πληροφορίες;

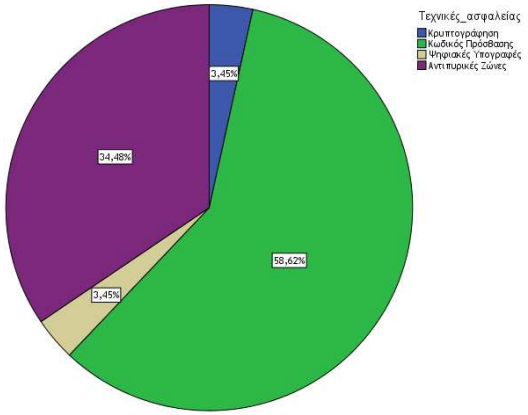
28. Τηρούνται τα χρονοδιαγράμματα για τη σύνταξη των περιοδικών οικονομικών καταστάσεων;

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Ναι	52	100,0	100,0	100,0



29. Ποιες τεχνικές χρησιμοποιούνται για να περιοριστεί η πρόσβαση από μη εξουσιοδοτημένους χρήστες;

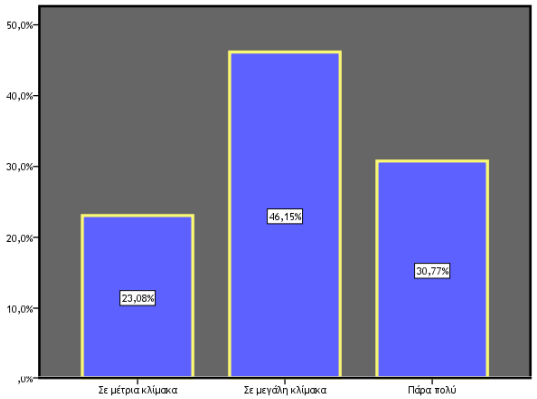
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Κρυπτογράφηση	2	3,4	3,4	3,4
	Κωδικός Πρόσβασης	34	58,6	58,6	62,1
	Ψηφιακές Υπογραφές	2	3,4	3,4	65,5
	Αντιπυρικές Ζώνες	20	34,5	34,5	100,0
	Total	58	100,0	100,0	



Αποτελέσματα Έρευνας (ερωτήσεις 30-31)
Αποδοτικότητα του ΛΠΣ

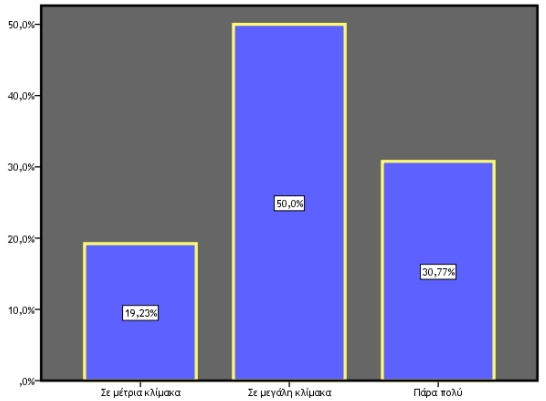
30. Σε ποιο βαθμό το σύστημα είναι φιλικό προς το χρήστη;

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Σε μέτρια κλίμακα	12	23,1	23,1	23,1
	Σε μεγάλη κλίμακα	24	46,2	46,2	69,2
	Πάρα πολύ	16	30,8	30,8	100,0
	Total	52	100,0	100,0	



31. Σε ποιο βαθμό το σύστημα είναι εύκολο στη χρήση;

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Σε μέτρια κλίμακα	10	19,2	19,2	19,2
	Σε μεγάλη κλίμακα	26	50,0	50,0	69,2
	Πάρα πολύ	16	30,8	30,8	100,0
	Total	52	100,0	100,0	



Αποτελέσματα Έρευνας (ερωτήσεις 30-31)
Παλινδρόμηση

- **Το σύμβολο Β δείχνει τη κλίση της ευθείας παλινδρόμησης**
- **Ο συντελεστής μεταξύ της φιλικότητας και της ευκολίας στη χρήση είναι 0,761**
- **Το 95% διάστημα εμπιστοσύνης για τον συντελεστή κυμαίνεται μεταξύ 0,747 και 0,775**
- **Η τεταγμένη α αναφέρεται ως σταθερά από το SPSS και έχει την τιμή 2,065**
- **Το 95% διάστημα εμπιστοσύνης για τη σταθερά είναι 1,924 μέχρι 2,205**
- **Η στήλη Beta δίνει την τιμή 0,999. Αυτός είναι ο συντελεστής συσχέτισης Pearson**
- **Η στήλη Sig περιέχει τα παρατηρηθέντα επίπεδα στατιστικής σημαντικότητας, των παραμέτρων α και β. Οι υποθέσεις που ελέγχονται είναι οι Ho:α=0 H1:α≠0 και Ho:β=0 H1:β≠0. Εφόσον και οι δύο τιμές είναι μικρότερες του 0,05 συμπεραίνουμε ότι και οι δύο μηδενικές υποθέσεις απορρίπτονται.**
- **Η ευθεία της παλινδρόμησης είναι Y = 0,761X + 2,065, δηλαδή**

Φιλικότητα = 0,761 * Ευκολία + 2,065

Variables Entered/Removed[a]

Model	Variables Entered	Variables Removed	Method
1	εύκολο[b]	.	Enter

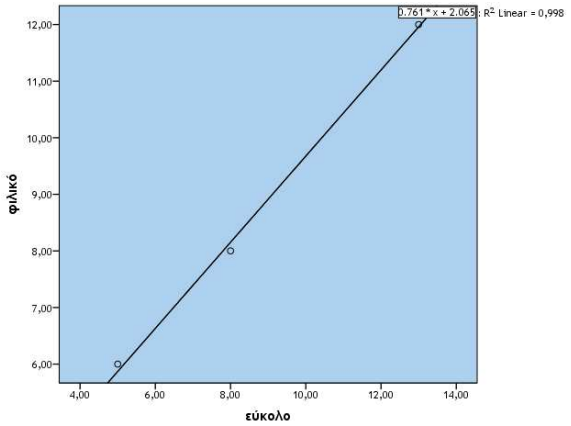
a. Dependent Variable: φιλικό

b. All requested variables entered.

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95,0% Confidence Interval for B	
		B	Std. Error	Beta			Lower Bound	Upper Bound
1	(Constant)	2,065	,068		30,226	,000	1,924	2,205
	εύκολο	,761	,007	,999	113,371	,000	,747	,775

a. Dependent Variable: φιλικό

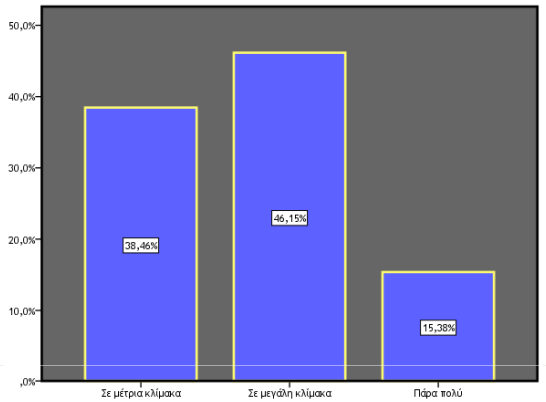


Αποτελέσματα Έρευνας (ερωτήσεις 32-33)

Αποδοτικότητα του ΛΠΣ

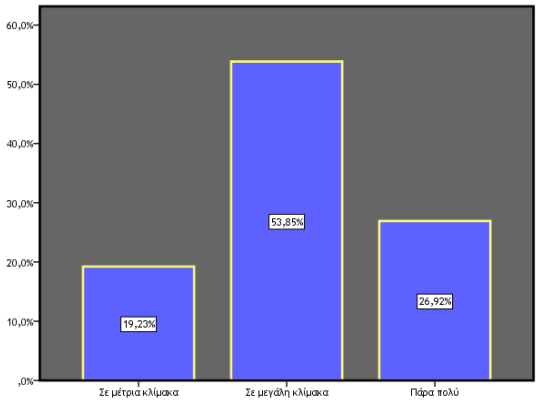
32. Σε ποιο βαθμό η ταχύτητα ανάκτησης των δεδομένων είναι ικανοποιητική;

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Σε μέτρια κλίμακα	20	38,5	38,5	38,5
	Σε μεγάλη κλίμακα	24	46,2	46,2	84,6
	Πάρα πολύ	8	15,4	15,4	100,0
	Total	52	100,0	100,0	



33. Σε ποιο βαθμό οι παρεχόμενες οικονομικές πληροφορίες συμβάλλουν στη λήψη αποφάσεων;

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Σε μέτρια κλίμακα	10	19,2	19,2	19,2
	Σε μεγάλη κλίμακα	28	53,8	53,8	73,1
	Πάρα πολύ	14	26,9	26,9	100,0
	Total	52	100,0	100,0	



Συμπεράσματα

- Οι απειλές είναι απόρροια του ανθρώπινου παράγοντα και κυρίως είναι τυχαίες παρά σκόπιμες.
- Οι ευπάθειες οφείλονται κυρίως σε ελαττώματα στο σχεδιασμό του συστήματος.
- Η διαδικασία της διαχείρισης κινδύνου πραγματοποιείται σε μικρό βαθμό από τις επιχειρήσεις, παρόλο που όλες αναγνωρίζουν τη συνεισφορά της στην επιλογή βέλτιστων μηχανισμών ασφαλείας.

- Η ανάθεση της αξιολόγησης του συστήματος σε εσωτερικούς και εξωτερικούς ελεγκτές απαιτεί συνεχή συνεργασία μεταξύ τους.
- Ξεχωριστό τμήμα εσωτερικού ελέγχου θα ήταν ωφέλιμο να λειτουργεί σε επιχειρήσεις που διαθέτουν εσωτερικό ελεγκτή.
- Η αποδοτικότητα των διαδικασιών ελέγχου στον προσδιορισμό των κινδύνων που εμφανίζονται ή απειλούν το ΛΠΣ κρίνεται ικανοποιητική.
- Οι υποδείξεις του ελεγκτή απαιτείται να εφαρμόζονται πλήρως από τις επιχειρήσεις.

- Η ανάπτυξη ΛΠΣ που να ανταποκρίνεται πλήρως στις ανάγκες της κάθε επιχείρησης, ίσως και να ήταν πιο ωφέλιμη από την αγορά ενός πακέτου λογισμικού.
- Τα συστήματα που λειτουργούν σε πραγματικό χρόνο υπερέχουν στο ότι όλοι οι συνδεδεμένοι και απομακρυσμένοι χρήστες μπορούν να δουν το αποτέλεσμα μιας συναλλαγής την ίδια στιγμή.
- Η χρήση των τεχνικών ασφαλείας της κρυπτογράφησης και των ψηφιακών υπογραφών καλό θα ήταν να διαδοθεί περισσότερο γιατί μπορεί να προσφέρει σημαντική προστασία στο σύστημα.

Προτάσεις για Μελλοντική Έρευνα

- **Περαιτέρω έρευνα** θα μπορούσε να διεξαχθεί για κάθε μέρος του ερωτηματολογίου ξεχωριστά, ώστε να προσδιοριστούν σε βάθος η λειτουργικότητα, οι κίνδυνοι και οι έλεγχοι των λογιστικών πληροφοριακών συστημάτων.

- Επιπλέον, μία **μελλοντική έρευνα** θα μπορούσε να χρησιμοποιήσει πιο εξειδικευμένες στατιστικές μεθόδους, ώστε να εξευρεθούν περισσότερες συσχετίσεις μεταξύ των ερωτήσεων του ερωτηματολογίου.

Εν κατακλείδι

Τόσο η διαχείριση των πιθανών κινδύνων όσο και η εφαρμογή των κατάλληλων διαδικασιών ελέγχου αποτελούν μονόδρομο για την προστασία των λογιστικών πληροφοριακών συστημάτων.

Η εξέρευση των απαραίτητων μηχανισμών ασφαλείας για τη διαφύλαξη της ακεραιότητας και της ακρίβειας των οικονομικών πληροφοριών αποτελεί εχέγγυο για την επιτυχία της οικονομικής μονάδας του σήμερα και του αύριο.

Ερωτήσεις;;;

Σας ευχαριστώ πολύ για την προσοχή σας