



**ΤΜΗΜΑ ΟΡΓΑΝΩΣΗΣ ΚΑΙ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ**

***ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ***

***“ΔΙΟΙΚΗΣΗ ΕΠΙΧΕΙΡΗΣΕΩΝ”***

**ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ**

“Η συμβολή του εσωτερικού ελέγχου στην ασφάλεια της ηλεκτρονικής διακυβέρνησης  
σε δήμους στην Ελλάδα”

Υποψήφια: Ιωάννα Γκεντσούδη, ΑΕΜ 392

Επιβλέπων καθηγητής :

Δρ. Παζάρσκης Μιχαήλ, Αναπληρωτής Καθηγητής

Σέρρες, 04/05/2023

## Περίληψη

Ο εσωτερικός έλεγχος και η κυβερνοασφάλεια αποκτούν ολοένα και μεγαλύτερη σημασία στον δημόσιο τομέα, ιδιαίτερα για τους δήμους, καθώς προσπαθούν να προστατεύσουν ευαίσθητα δεδομένα και να διατηρήσουν την εμπιστοσύνη του κοινού. Ως κύριο συμπέρασμα της παρούσας εργασίας μπορεί να υπογραμμιστεί η σημασία των παραπάνω πτυχών στην λειτουργία της τοπικής αυτοδιοίκησης. Σκοπός της εργασίας είναι η ανάλυση του ρόλου του εσωτερικού ελέγχου και των διαστάσεων του στην κυβερνοασφάλεια του δημόσιου τομέα και ειδικά των Δήμων. Για τον λόγο αυτό, πρωτογενής έρευνα με την χρήση ερωτηματολογίου έλαβε χώρα με δείγμα 83 δημοτικούς υπαλλήλους σε διάφορους δήμους της χώρας. Σε σχέση με την συσχέτιση της έλλειψης ασφάλειας με τις δραστηριότητες εσωτερικού ελέγχου φάνηκε ότι η ανάγκη για πληροφόρηση, εκπαίδευση και εγκαθίδρυση πολιτικών εσωτερικού ελέγχου έρχονται μάλλον ως απάντηση στον κίνδυνο έλλειψης της κυβερνοασφάλειας (αφού αυτός ενδεχομένως έχει πρώτα εκφραστεί με αύξηση των κυβερνοεπιθέσεων το τελευταίο διάστημα) και όχι προληπτικά και εξαρχής. Η έρευνα υπογράμμισε την ανάγκη για τους ελεγκτές ειδικά στο δημόσιο τομέα, να εμπλουτίσουν τις γνώσεις τους όσον αναφορά την ασφάλεια στον κυβερνοχώρο προκειμένου να επιτύχουν την αποτελεσματικότητα των ελέγχων αυτών.

## **Abstract**

Internal auditing and cybersecurity are becoming increasingly important in the public sector, particularly for municipalities, as they strive to protect sensitive data and maintain public trust. As a main conclusion of this thesis, the importance of the above aspects in the function of the local government can be underlined. The purpose of this thesis was to analyze the role of internal auditing and its dimensions in the cyber security of the public sector and especially of Municipalities. For this reason, primary research using a questionnaire took place with a sample of 83 municipal employees in various municipalities of the country. In relation to the correlation of the lack of security with internal auditing activities, it appeared that the need for information, training and the establishment of internal auditing policies come rather as a response to the risk of a lack of cyber security (since this may have first been expressed with an increase in cyber-attacks recently) and not proactively and from the beginning. The research highlighted the need for auditors to enrich their knowledge of cyber security in order to achieve the effectiveness of these audits.

## Περιεχόμενα

Εισαγωγή .....	10
1. Η σημασία του Εσωτερικού Ελέγχου με έμφαση στο δημόσιο τομέα .....	12
1.1 Η έννοια και η χρησιμότητα των ελέγχων, γενικά.....	12
1.1.1 Ορισμός, σημασία και τύπου ελέγχων .....	12
1.1.2 Ελεγκτικά Πρότυπα .....	14
1.1.3 Διαδικασία Ελέγχου .....	16
1.1.4 Τύποι δοκιμών ελέγχου .....	18
1.2. Εσωτερικός έλεγχος .....	20
1.2.1 Γενικά στοιχεία για τον Εσωτερικό Έλεγχο .....	20
1.2.2. Πλαίσιο και Πρότυπα Εσωτερικού Ελέγχου.....	22
1.2.3 Λειτουργίες και Εξειδικεύσεις του Εσωτερικού Ελέγχου.....	24
1.3 Η έννοια του Εσωτερικού Ελέγχου στο Δημόσιο Τομέα .....	26
1.3.1 Ορισμός και Στόχοι Εσωτερικού Ελέγχου του Δημόσιου Τομέα .....	26
1.3.2 Πλαίσια και Πρότυπα Εσωτερικού Ελέγχου του Δημόσιου Τομέα .....	28
1.3.3 Προκλήσεις και Ευκαιρίες για τον Εσωτερικό Έλεγχο του Δημόσιου Τομέα .....	30
2. Η κυβερνο-ασφάλεια και η σύνδεσή της με τον εσωτερικό έλεγχο. Η περίπτωση του δημόσιου τομέα και των Δήμων.....	34
2.1. Η έννοια της Κυβερνοασφάλειας με έμφαση στον δημόσιο τομέα και τους δήμους.....	34
2.2 Τύποι και περιπτώσεις παραβίασης της κυβερνοασφάλειας σε δήμους.....	36
2.3 Εσωτερικός έλεγχος και κυβερνοασφάλεια .....	38
2.4 Διαστάσεις του εσωτερικού ελέγχου που σχετίζονται με την κυβερνοασφάλεια .....	40
2.4.1 Συμβουλευτικός Ρόλος Εσωτερικών Ελέγχων στην Κυβερνοασφάλεια για τους Δήμους .....	40
2.4.2 Ο ρόλος των εσωτερικών ελέγχων στην ενίσχυση της τεχνολογικής γνώσης και της κυβερνοασφάλειας στους δήμους.....	42
2.4.3. Ρόλος των Εσωτερικών Ελέγχων στην Ενίσχυση της Συνεργασίας που σχετίζεται με την Κυβερνοασφάλεια στους Δήμους .....	43

2.4.4. Ο ρόλος των εσωτερικών ελέγχων στην αξιολόγηση και την ενίσχυση των πολιτικών και προτύπων κυβερνοασφάλειας στους δήμους.....	44
2.4.5 Ενημέρωση και εκπαίδευση.....	45
3. Μεθοδολογία έρευνας.....	46
3.1. Σκοπός της έρευνας.....	46
3.2 Τα ερευνητικά ερωτήματα .....	46
3.3 Το ερωτηματολόγιο και το δείγμα της έρευνας .....	46
3.4 Στατιστικές μέθοδοι επεξεργασίας δεδομένων .....	48
4. Τα αποτελέσματα της έρευνας .....	49
4.1 Δημογραφικά στοιχεία και στοιχεία δήμων .....	49
4.2 Ερωτήσεις σχετικά με την κυβερνο-ασφάλεια των δήμων.....	52
4.3 Η διάσταση του συμβουλευτικού ρόλου .....	55
4.4 Η διάσταση της τεχνολογικής γνώσης .....	58
4.5 Η διάσταση της συνεργασίας .....	61
4.6 Πολιτικές και πρότυπα.....	65
4.7 Πληροφόρηση και εκπαίδευση .....	70
4.8 Οι συνολικές διαστάσεις του ερωτηματολογίου.....	74
4.9 Συσχετίσεις μεταξύ των διαστάσεων .....	75
4.10 Η στατιστικά σημαντική επίδραση των δημογραφικών χαρακτηριστικών .....	79
4.11 Η στατιστικά σημαντική επίδραση των χαρακτηριστικών των δήμων.....	79
Συμπεράσματα .....	83
Βιβλιογραφία .....	86
Παράρτημα.....	93

## Κατάλογος Πινάκων

Πίνακας 1. Έλεγχος αξιοπιστίας ερωτηματολογίου .....	47
Πίνακας 2. Φύλο .....	49
Πίνακας 3. Ηλικία .....	50
Πίνακας 4. Ποιος είναι, προσεγγιστικά, ο ετήσιος κύκλος εργασιών (απολογισμός) του δήμου.....	51
Πίνακας 5. Ποιος είναι, προσεγγιστικά, ο πληθυσμός του δήμου σας;.....	52
Πίνακας 6. Έχει δεχτεί ο οργανισμός σας επιθέσεις κυβερνο-ασφάλειας τους τελευταίους 12 μήνες;.....	53
Πίνακας 7. Πόσα από τα παραπάνω περιστατικά εντοπίστηκαν σε σχέση με την εμφάνιση λειτουργικών προβλημάτων, οικονομικών απωλειών ή απώλειας φήμης ..	54
Πίνακας 8. Θεωρείτε ότι τα περιστατικά κυβερνο-επιθέσεων έχουν αυξηθεί τα τελευταία τρία χρόνια; .....	55
Πίνακας 9. Σε ποιο βαθμό οι εσωτερικοί ελεγκτές συμβουλεύουν διαφορετικά τμήματα (όπως το τμήμα πληροφορικής) σχετικά με την κερδοφορία τους; .....	56
Πίνακας 10. Σε ποιο βαθμό οι εσωτερικοί ελεγκτές ενεργούν ως “παίκτες” μιας ομάδας και όχι ως υπηρεσίες επιβολής του νόμου; .....	57
Πίνακας 11. Σε ποιο βαθμό οι εσωτερικοί ελεγκτές εμπλέκονται στην ασφάλεια των πληροφοριών και των πληροφοριακών συστημάτων; .....	58
Πίνακας 12. Σε ποιο βαθμό συνεργάζονται οι ειδικοί σε θέματα ασφάλειας πληροφοριών με εσωτερικούς ελεγκτές για να διασφαλίσουν την ασφάλεια των συστημάτων πληροφοριών; .....	59
Πίνακας 13. Σε ποιο βαθμό είναι περιορισμένη η τριβή μεταξύ εμπειρογνομόνων ασφάλειας πληροφοριών και εσωτερικών ελεγκτών; .....	60
Πίνακας 14. Σε ποιο βαθμό η σχέση μεταξύ ειδικών σε θέματα ασφάλειας πληροφοριών και εσωτερικών ελεγκτών χαρακτηρίζεται ως στενή;.....	61
Πίνακας 15. Σε ποιο βαθμό γνωρίζουν οι εσωτερικοί ελεγκτές την ασφάλεια των πληροφοριακών συστημάτων; .....	62
Πίνακας 16. Σε ποιο βαθμό οι εσωτερικοί ελεγκτές έχουν εξειδικευμένη τεχνολογική γνώση των πληροφοριακών συστημάτων που χρησιμοποιούν;.....	63
Πίνακας 17. Σε ποιο βαθμό υπάρχει εκπαίδευση για εσωτερικούς ελεγκτές σχετικά με την ασφάλεια των πληροφοριακών συστημάτων; .....	63

Πίνακας 18. Σε ποιο βαθμό οι εσωτερικοί ελεγκτές διαθέτουν την πιστοποίηση Certified Information Systems Auditor (CISA);.....	64
Πίνακας 19. Σε ποιο βαθμό υπάρχει καταγεγραμμένη Πολιτική Ασφάλειας Πληροφοριών;.....	66
Πίνακας 20. Σε ποιο βαθμό ο δήμος σας χρησιμοποιεί κάποιο από τα πρότυπα ISO (ISO 27001, 27005, κ.λπ.); .....	66
Πίνακας 21. Πόσο χρησιμοποιεί ο δήμος σας τα Πρότυπα για την Επαγγελματική Εφαρμογή του Εσωτερικού Ελέγχου;.....	67
Πίνακας 22. Σε ποιο βαθμό ο δήμος σας χρησιμοποιεί συγκεκριμένα πλαίσια (όπως το Πρόγραμμα Αξιολόγησης και Βελτίωσης Ποιότητας);.....	68
Πίνακας 23. Σε ποιο βαθμό οι εσωτερικοί ελεγκτές αξιολογούν τη συμμόρφωση με τις πολιτικές-και τα πρότυπα ασφαλείας; .....	69
Πίνακας 24. Σε ποιο βαθμό ο δήμος σας διαθέτει συγκεκριμένους οδηγούς που περιγράφουν τι επιτρέπεται να κάνουν οι εργαζόμενοι με τους υπολογιστές τους; ....	70
Πίνακας 25. Σε ποιο βαθμό ο δήμος σας παρέχει εκπαίδευση για να βοηθήσει τους υπαλλήλους του να βελτιώσουν τις γνώσεις τους σε θέματα ασφάλειας πληροφοριών; .....	71
Πίνακας 26. Σε ποιο βαθμό το προσωπικό γνωρίζει την πολιτική ασφάλειας πληροφοριών;.....	72
Πίνακας 27. Σε ποιο βαθμό οι εσωτερικοί ελεγκτές διασφαλίζουν ότι οι ενημερώσεις ασφαλείας του προσωπικού είναι επωφελείς;.....	73
Πίνακας 28. Οι συνολικές διαστάσεις του ερωτηματολογίου .....	74
Πίνακας 29. Συσχετίσεις μεταξύ των χαρακτηριστικών του εσωτερικού ελέγχου.....	76
Πίνακας 30. Συσχετίσεις μεταξύ των χαρακτηριστικών του εσωτερικού ελέγχου και της ασφάλειας .....	77
Πίνακας 31. Η στατιστικά σημαντική επίδραση του φύλου.....	79
Πίνακας 32. Η στατιστικά σημαντική επίδραση του κύκλου εργασιών των δήμων ...	79
Πίνακας 33. Τα αποτελέσματα του posthoc test LSD.....	80

## Κατάλογος Διαγραμμάτων

Διάγραμμα 1. Φύλο.....	49
Διάγραμμα 2. Ηλικία .....	50
Διάγραμμα 3. Ποιος είναι, προσεγγιστικά, ο ετήσιος κύκλος εργασιών (απολογισμός) του.....	51
Διάγραμμα 4. Ποιος είναι ,προσεγγιστικά, ο πληθυσμός του δήμου σας; .....	52
Διάγραμμα 5. Έχει δεχτεί ο οργανισμός σας επιθέσεις κυβερνο-ασφάλειας τους τελευταίους 12 μήνες;.....	53
Διάγραμμα 6. Πόσα από τα παραπάνω περιστατικά εντοπίστηκαν σε σχέση με την εμφάνιση λειτουργικών προβλημάτων, οικονομικών απωλειών ή απώλειας φήμης ..	54
Διάγραμμα 7. Θεωρείτε ότι τα περιστατικά κυβερνο-επιθέσεων έχουν αυξηθεί τα τελευταία τρία χρόνια; .....	55
Διάγραμμα 8. Σε ποιο βαθμό οι εσωτερικοί ελεγκτές συμβουλεύουν διαφορετικά τμήματα (όπως το τμήμα πληροφορικής) σχετικά με την κερδοφορία τους; .....	56
Διάγραμμα 9. Σε ποιο βαθμό οι εσωτερικοί ελεγκτές ενεργούν ως “παίκτες” μιας ομάδας και όχι ως υπηρεσίες επιβολής του νόμου; .....	57
Διάγραμμα 10. Σε ποιο βαθμό οι εσωτερικοί ελεγκτές εμπλέκονται στην ασφάλεια των πληροφοριών και των πληροφοριακών συστημάτων; .....	58
Διάγραμμα 11. Σε ποιο βαθμό συνεργάζονται οι ειδικοί σε θέματα ασφάλειας πληροφοριών με εσωτερικούς ελεγκτές για να διασφαλίσουν την ασφάλεια των συστημάτων πληροφοριών; .....	59
Διάγραμμα 12. Σε ποιο βαθμό είναι περιορισμένη η τριβή μεταξύ εμπειρογνομόνων ασφάλειας πληροφοριών και εσωτερικών ελεγκτών; .....	60
Διάγραμμα 13. Σε ποιο βαθμό η σχέση μεταξύ ειδικών σε θέματα ασφάλειας πληροφοριών και εσωτερικών ελεγκτών χαρακτηρίζεται ως στενή;.....	61
Διάγραμμα 14. Σε ποιο βαθμό γνωρίζουν οι εσωτερικοί ελεγκτές την ασφάλεια των πληροφοριακών συστημάτων; .....	62
Διάγραμμα 15. Σε ποιο βαθμό οι εσωτερικοί ελεγκτές έχουν εξειδικευμένη τεχνολογική γνώση των πληροφοριακών συστημάτων που χρησιμοποιούν;.....	63
Διάγραμμα 16. Σε ποιο βαθμό υπάρχει εκπαίδευση για εσωτερικούς ελεγκτές σχετικά με την ασφάλεια των πληροφοριακών συστημάτων; .....	64



Διάγραμμα 17. Σε ποιο βαθμό οι εσωτερικοί ελεγκτές διαθέτουν την πιστοποίηση Certified Information Systems Auditor (CISA);.....	65
Διάγραμμα 18. Σε ποιο βαθμό υπάρχει καταγεγραμμένη Πολιτική Ασφάλειας Πληροφοριών;.....	66
Διάγραμμα 19. Σε ποιο βαθμό ο δήμος σας χρησιμοποιεί κάποιο από τα πρότυπα ISO (ISO 27001, 27005, κ.λπ.); .....	67
Διάγραμμα 20. Πόσο χρησιμοποιεί ο δήμος σας τα Πρότυπα για την Επαγγελματική Εφαρμογή του Εσωτερικού Ελέγχου;.....	68
Διάγραμμα 21. Σε ποιο βαθμό ο δήμος σας χρησιμοποιεί συγκεκριμένα πλαίσια (όπως το Πρόγραμμα Αξιολόγησης και Βελτίωσης Ποιότητας);.....	69
Διάγραμμα 22. Σε ποιο βαθμό οι εσωτερικοί ελεγκτές αξιολογούν τη συμμόρφωση με τις πολιτικές-και τα πρότυπα ασφαλείας; .....	70
Διάγραμμα 23. Σε ποιο βαθμό ο δήμος σας διαθέτει συγκεκριμένους οδηγούς που περιγράφουν τι επιτρέπεται να κάνουν οι εργαζόμενοι με τους υπολογιστές τους; ....	71
Διάγραμμα 24. Σε ποιο βαθμό ο δήμος σας παρέχει εκπαίδευση για να βοηθήσει τους υπαλλήλους του να βελτιώσουν τις γνώσεις τους σε θέματα ασφάλειας πληροφοριών; .....	72
Διάγραμμα 25. Σε ποιο βαθμό το προσωπικό γνωρίζει την πολιτική ασφαλείας πληροφοριών;.....	73
Διάγραμμα 26. Σε ποιο βαθμό οι εσωτερικοί ελεγκτές διασφαλίζουν ότι οι ενημερώσεις ασφαλείας του προσωπικού είναι επωφελείς; .....	74
Διάγραμμα 27. Οι συνολικές διαστάσεις του ερωτηματολογίου.....	75
Διάγραμμα 28. Διαγραμματική απεικόνιση της πρώτης στατιστικά σημαντικής διαφοράς του κύκλου εργασιών των δήμων .....	82
Διάγραμμα 29. Διαγραμματική απεικόνιση της πρώτης στατιστικά σημαντικής διαφοράς του κύκλου εργασιών των δήμων .....	82

## Εισαγωγή

Με το πέρασμα του χρόνου, ο τρόπος λειτουργίας των επιχειρήσεων έχει εξελιχθεί, λόγω των συνεχιζόμενων αλλαγών σε οικονομικούς, τεχνολογικούς και άλλους παράγοντες. Αυτές οι αλλαγές απαιτούν την εφαρμογή εσωτερικών ελέγχων για τους παρόχους υπηρεσιών. Στον σημερινό κόσμο, καλά ενημερωμένα ενδιαφερόμενα μέρη με εξειδίκευση στους τομείς τους μπορούν να συμβάλουν στις στρατηγικές μιας εταιρείας για βελτιωμένη απόδοση. Ως αποτέλεσμα, οι γνώστες των ενδιαφερομένων και οι αποτελεσματικές πρακτικές ανταλλαγής πληροφοριών μπορούν να βοηθήσουν στη δημιουργία ευέλικτων και ανταγωνιστικών στρατηγικών.

Σε ένα απρόβλεπτο επιχειρηματικό τοπίο, οι οργανισμοί πρέπει να αντιμετωπίσουν τους κινδύνους που αντιμετωπίζουν, με τον εσωτερικό έλεγχο να διαδραματίζει κρίσιμο ρόλο. Ένας σημαντικός σύγχρονος κίνδυνος είναι η διασφάλιση της κυβερνοασφάλειας, μια ανησυχία που έχει προκύψει λόγω της ευρείας υιοθέτησης ψηφιακών συστημάτων πληροφοριών. Ωστόσο, η εκτεταμένη αυτή χρήση μπορεί να οδηγήσει σε αρνητικά αποτελέσματα σε ενδεχόμενες παραβιάσεις στον κυβερνοχώρο τόσο στον επιχειρηματικό κόσμο όσο και στον δημόσιο τομέα. Επιπλέον, οι κυβερνοεπιθέσεις γίνονται όλο και πιο συχνές, προκαλώντας σημαντικές απώλειες. Κατά συνέπεια, ο εσωτερικός έλεγχος, ο οποίος έχει αναλάβει ευρύτερο ρόλο λόγω των πρόσφατων μετασχηματισμών, πρέπει να συμμετέχει ενεργά στην προστασία της ασφάλειας των διαδικτυακών υπηρεσιών και διαδικασιών.

Για τον λόγο αυτό, πρωτογενής έρευνα με την χρήση ερωτηματολογίου έλαβε χώρα με δείγμα 83 δημοτικούς υπαλλήλους σε διάφορους δήμους της χώρας. Προκειμένου να αναδειχθεί εξάλλου, το τελικό συμπέρασμα της εργασίας, αυτή δομείται, εκτός από αυτό το εισαγωγικό κεφάλαιο, από τα παρακάτω κεφάλαια.

Το πρώτο κεφάλαιο είναι αφιερωμένο στην έννοια και την σημασία των ελέγχων και ειδικότερα των εσωτερικών ελέγχων, ενώ έμφαση δίνεται στον δημόσιο τομέα και στους δήμους ειδικότερα. Στο δεύτερο κεφάλαιο αναλύεται η έννοια της κυβερνοασφάλειας με την έμφαση και πάλι να δίνεται στους Δήμους, ενώ ταυτόχρονα λαμβάνει χώρα και η σύνδεση της έννοιας αυτής με τον εσωτερικό έλεγχο, τις διαδικασίες και τις διαστάσεις του. Το τρίτο κεφάλαιο περιλαμβάνει το σύνολο των

μεθόδων που έκανε χρήση η έρευνα, τα ευρήματα της οποίας παρουσιάζονται αναλυτικά στο τέταρτο και τελευταίο κεφάλαιο.

# **1. Η σημασία του Εσωτερικού Ελέγχου με έμφαση στο δημόσιο τομέα**

## **1.1 Η έννοια και η χρησιμότητα των ελέγχων, γενικά.**

### **1.1.1 Ορισμός, σημασία και τύπου ελέγχων**

Ο έλεγχος είναι μια συστηματική διαδικασία που αναλαμβάνουν οι ελεγκτές για να εξετάσουν και να αξιολογήσουν τα οικονομικά αρχεία, τις συναλλαγές, τους εσωτερικούς ελέγχους και τα λογιστικά συστήματα ενός οργανισμού, με πρωταρχικό στόχο την παροχή μιας αμερόληπτης άποψης σχετικά με την ορθότητα των οικονομικών καταστάσεων (Hayes, Dassen , Schilder, &Wallage, 2014; Pazarskisetal., 2022). Με τον τρόπο αυτό θα ενισχυθεί και η εμπιστοσύνη των διαφόρων ενδιαφερομένων όπως των επενδυτών, των πιστωτών, των ρυθμιστικών αρχών αλλά και γενικότερα του ευρύ κοινού στη χρηματοοικονομική αναφορά του οργανισμού (Mihret&Yismaw, 2007; Galanisetal., 2023).

Η σημασία του ελέγχου δεν μπορεί να υποεκτιμηθεί, καθώς διαδραματίζει κρίσιμο ρόλο στη διατήρηση της ακεραιότητας του συστήματος χρηματοοικονομικής αναφοράς και στην ενίσχυση της διαφάνειας στο επιχειρηματικό περιβάλλον. Εντοπίζοντας αποκλίσεις, λάθη και πιθανή απάτη, οι ελεγκτές μπορούν να βοηθήσουν τους οργανισμούς να αντιμετωπίσουν τις αδυναμίες στους εσωτερικούς ελέγχους και τις λογιστικές πρακτικές τους, μειώνοντας έτσι τον κίνδυνο οικονομικών ανακρίβειών και προωθώντας την καλή εταιρική διακυβέρνηση (Arens, Elder, &Beasley, 2014; Nerantzidisetal., 2022). Επιπλέον, οι έλεγχοι μπορούν να βελτιώσουν τη διαδικασία λήψης αποφάσεων των ενδιαφερομένων παρέχοντάς τους αξιόπιστες και ακριβείς οικονομικές πληροφορίες που αντικατοπτρίζουν την πραγματική οικονομική απόδοση και την οικονομική θέση του οργανισμού (Knechel, Salterio, &Ballou, 2019).

Οι έλεγχοι μπορούν γενικά να ταξινομηθούν σε τρεις κύριους τύπους: εσωτερικούς, εξωτερικούς και κυβερνητικούς ελέγχους. Οι εσωτερικοί έλεγχοι διενεργούνται από τους εσωτερικούς ελεγκτές του ίδιου του οργανισμού, οι οποίοι

αξιολογούν την αποτελεσματικότητα των εσωτερικών ελέγχων, τις πρακτικές διαχείρισης κινδύνου καθώς όμως και τη συμμόρφωση με νόμους και κανονισμούς (Spencer&Marsden, 2016). Ο πρωταρχικός στόχος των εσωτερικών ελέγχων είναι η παροχή συστάσεων για βελτιώσεις στο περιβάλλον λειτουργικής αποτελεσματικότητας και ελέγχου του οργανισμού, προσθέτοντας έτσι αξία στον οργανισμό (Arena&Azzone, 2009).

Οι εξωτερικοί έλεγχοι, από την άλλη πλευρά, διενεργούνται από ανεξάρτητους εξωτερικούς ελεγκτές που δεν συνδέονται με τον οργανισμό που ελέγχεται. Ο πρωταρχικός στόχος των εξωτερικών ελέγχων είναι η έκφραση γνώμης σχετικά με τη δικαιοσύνη και την ακρίβεια των οικονομικών καταστάσεων του οργανισμού, η οποία βοηθά τους ενδιαφερόμενους στη λήψη τεκμηριωμένων αποφάσεων (Cohen&Knechel, 2017). Οι εξωτερικοί ελεγκτές ακολουθούν καθιερωμένα πρότυπα και κατευθυντήριες γραμμές ελέγχου, όπως τα “Γενικά Αποδεκτά Πρότυπα Ελέγχου” (“Generally Accepted Auditing Standards”, GAAS) ή τα “Διεθνή Πρότυπα Ελέγχου” (“International Standards on Auditing”, ISA), για να διασφαλίσουν την ποιότητα και τη συνέπεια του ελεγκτικού τους έργου (Humphrey, Loft, & Woods, 2009).

Οι κρατικοί έλεγχοι είναι μια εξειδικευμένη μορφή ελέγχου που επικεντρώνεται στην αξιολόγηση των χρηματοοικονομικών δραστηριοτήτων και των επιδόσεων των φορέων του δημόσιου τομέα, όπως κυβερνητικοί φορείς, τμήματα και προγράμματα (Rahaman, 2010). Αυτοί οι έλεγχοι διενεργούνται συνήθως από διορισμένους από την κυβέρνηση ελεγκτές ή ανεξάρτητες ελεγκτικές εταιρείες και έχουν σχεδιαστεί για να διασφαλίζουν τη σωστή χρήση των δημόσιων πόρων, τη συμμόρφωση με τις νομικές και κανονιστικές απαιτήσεις και την επίτευξη των στόχων δημόσιας πολιτικής (Ouda, 2008; Pazarskis et al., 2020).

Ο έλεγχος είναι μια ζωτικής σημασίας διαδικασία που ενισχύει την αξιοπιστία των χρηματοοικονομικών πληροφοριών και συμβάλλει στη συνολική σταθερότητα και διαφάνεια του επιχειρηματικού περιβάλλοντος (Pazarskis et al., 2023). Εξετάζοντας τα οικονομικά αρχεία και τους εσωτερικούς ελέγχους, οι ελεγκτές διαδραματίζουν κρίσιμο ρόλο στη διασφάλιση των συμφερόντων των διαφόρων ενδιαφερομένων και στην προώθηση της χρηστής εταιρικής διακυβέρνησης. Οι διαφορετικοί τύποι ελέγχων, συμπεριλαμβανομένων των εσωτερικών, εξωτερικών και

κυβερνητικών ελέγχων, εξυπηρετούν διαφορετικούς σκοπούς και καλύπτουν τις μοναδικές ανάγκες των οργανισμών και των ενδιαφερομένων τους.

### 1.1.2 Ελεγκτικά Πρότυπα

Τα ελεγκτικά πρότυπα παρέχουν ένα πλαίσιο στους ελεγκτές ώστε να διενεργούν ελέγχους υψηλής ποιότητας, διασφαλίζοντας τη συνέπεια και την αξιοπιστία στο έργο τους. Αυτά τα πρότυπα είναι χρήσιμα για την εξασφάλιση της εμπιστοσύνης του κοινού στη χρηματοοικονομική αναφορά και για την προώθηση της διαφάνειας στο επιχειρηματικό περιβάλλον. Αυτή η ενότητα εξετάζει τα “Γενικά Αποδεκτά Ελεγκτικά Πρότυπα” (GAAS), τα “Διεθνή Πρότυπα Ελέγχου” (ISA) και τα “Πρότυπα του Συμβουλίου Εποπτείας Λογιστικών Εταιρειών” (“Public Company Accounting Oversight Board”, PCAOB).

- ✓ Γενικά Αποδεκτά Ελεγκτικά Πρότυπα (GAAS): Τα GAAS είναι ένα σύνολο κατευθυντήριων γραμμών και αρχών που θεσπίστηκαν από το “Αμερικανικό Ινστιτούτο Ορκωτών Λογιστών” (“American Institute of Certified Public Accountants”, AICPA) τις οποίες πρέπει να τηρούν οι ελεγκτές όταν διενεργούν ελέγχους οικονομικών καταστάσεων στις Ηνωμένες Πολιτείες (Arens, Elder, & Beasley, 2014). Το GAAS περιλαμβάνει δέκα βασικά πρότυπα που είναι οργανωμένα σε τρεις κατηγορίες: γενικά πρότυπα, πρότυπα επιτόπιας εργασίας και πρότυπα αναφοράς (Carmichael, 2004). Τα γενικά πρότυπα επικεντρώνονται στην ικανότητα, την ανεξαρτησία και την επαγγελματική φροντίδα του ελεγκτή, ενώ τα πρότυπα της επιτόπιας εργασίας δίνουν έμφαση στον σχεδιασμό του ελέγχου, στην κατανόηση των εσωτερικών ελέγχων του πελάτη και στη συλλογή επαρκών ελεγκτικών τεκμηρίων. Τα πρότυπα αναφοράς περιγράφουν την ευθύνη του ελεγκτή να εκφράσει γνώμη επί των οικονομικών καταστάσεων με βάση τα ευρήματα του ελέγχου (Arens et al., 2014).
- ✓ Διεθνή Πρότυπα Ελέγχου (ISA): Το ISA, που αναπτύχθηκε και εκδόθηκε από το “International Auditing and Assurance Standards Board” (IAASB), αντιπροσωπεύει ένα παγκοσμίως αναγνωρισμένο σύνολο ελεγκτικών προτύπων που στοχεύουν στην εναρμόνιση των ελεγκτικών πρακτικών σε

διάφορες δικαιοδοσίες (Humphrey, Loft, & Woods, 2009). Ο κύριος στόχος του ISA είναι να βελτιώσει την ποιότητα και τη συνέπεια των ελέγχων, προωθώντας έτσι το διεθνές εμπόριο και τις επενδύσεις αυξάνοντας την αξιοπιστία των χρηματοοικονομικών πληροφοριών (Gómez-Aguilar, Humphrey, & Moizer, 2019). Το ISA καλύπτει διάφορες πτυχές της διαδικασίας ελέγχου (IAASB, 2018). Καθώς περισσότερες χώρες υιοθετούν το ISA, η συγκρισιμότητα των διασυνοριακών οικονομικών καταστάσεων αναμένεται να βελτιωθεί, διευκολύνοντας τις διασυνοριακές επενδύσεις και την οικονομική συνεργασία (Simnett & Huggins, 2015).

- ✓ Πρότυπα του Συμβουλίου Εποπτείας Λογιστικών Εταιρειών (PCAOB): Το PCAOB, που ιδρύθηκε με τον νόμο Sarbanes-Oxley του 2002 ως απάντηση σε σκάνδαλα εταιρικής λογιστικής υψηλού προφίλ, είναι ένας μη κερδοσκοπικός οργανισμός που επιβλέπει τους ελέγχους των δημοσίων εταιρειών και των ενδιάμεσων στις Ηνωμένες Πολιτείες (PCAOB, 2018). Το PCAOB εκδίδει ελεγκτικά πρότυπα, γνωστά ως Πρότυπα PCAOB, τα οποία είναι υποχρεωτικά για τους ελεγκτές των δημοσίων εταιρειών των ΗΠΑ και χρησιμεύουν για την προστασία των επενδυτών και την προώθηση της ακεραιότητας της χρηματοοικονομικής αναφοράς (Rezaee, 2004). Τα πρότυπα PCAOB έχουν δημιουργηθεί έτσι ώστε να συμπληρώνουν το GAAS και να τονίζουν την αυτονομία του ελεγκτή, τον επαγγελματικό σκεπτικισμό και τον ποιοτικό έλεγχο στη διαδικασία ελέγχου (Gendron, Bedard, & Gosselin, 2004). Επιπλέον, το PCAOB διενεργεί επιθεωρήσεις εγγεγραμμένων ελεγκτικών εταιρειών για να αξιολογήσει τη συμμόρφωσή τους με τα ελεγκτικά πρότυπα και να επιβάλει πειθαρχικά μέτρα όταν είναι απαραίτητο (Daugherty, Tervo, & Dickins, 2012).

Εν κατακλείδι, τα ελεγκτικά πρότυπα όπως τα πρότυπα GAAS, ISA και PCAOB παρέχουν στους ελεγκτές τη βάση για τη διεξαγωγή ποιοτικών, συνεπών και αξιόπιστων ελέγχων. Με την τήρηση αυτών των προτύπων, οι ελεγκτές μπορούν να ενισχύσουν την αξιοπιστία της χρηματοοικονομικής αναφοράς και να προωθήσουν τη διαφάνεια στο επιχειρηματικό περιβάλλον.

### 1.1.3 Διαδικασία Ελέγχου

Η διαδικασία ελέγχου είναι μια συστηματική προσέγγιση για την εξέταση των οικονομικών καταστάσεων, των εσωτερικών ελέγχων και των διαδικασιών διαχείρισης κινδύνου ενός οργανισμού. Αυτή η ενότητα εξετάζει τα βασικά στοιχεία της διαδικασίας ελέγχου, συμπεριλαμβανομένου του σχεδιασμού ελέγχου, της αξιολόγησης κινδύνου, της αξιολόγησης εσωτερικού ελέγχου, των τεστ ελέγχου και της υποβολής εκθέσεων και τεκμηρίωσης.

#### 1. Σχεδιασμός Ελέγχου

Ο σχεδιασμός του ελέγχου είναι η αρχική φάση της διαδικασίας ελέγχου, όπου οι ελεγκτές αναπτύσσουν μια συνολική στρατηγική για τη διεξαγωγή του ελέγχου αποτελεσματικά και αποδοτικά (Arens, Elder, & Beasley, 2014). Αυτό περιλαμβάνει την απόκτηση κατανόησης του επιχειρηματικού περιβάλλοντος, του κλάδου και του ρυθμιστικού περιβάλλοντος του πελάτη, καθώς και τον εντοπισμό σημαντικών περιοχών ελέγχου, τον καθορισμό επιπέδων σημαντικότητας και την κατανομή των πόρων ελέγχου (Mock, Turner, & Vasarhelyi, 2013). Ο σωστός σχεδιασμός ελέγχου βοηθά τους ελεγκτές να εστιάσουν τις προσπάθειές τους σε τομείς υψηλού κινδύνου, να εντοπίζουν έγκαιρα πιθανά ζητήματα ελέγχου και να κατανέμουν κατάλληλα τους πόρους, βελτιώνοντας τελικά την ποιότητα του ελέγχου (Knechel, Salterio, & Ballou, 2019).

#### 2. Εκτίμηση Κινδύνου

Η αξιολόγηση και η εκτίμηση του κινδύνου είναι ένα κρίσιμο στοιχείο της διαδικασίας ελέγχου, όπου οι ελεγκτές αξιολογούν τους πιθανούς κινδύνους που μπορεί να επηρεάσουν την ακρίβεια και την αξιοπιστία των οικονομικών καταστάσεων ενός οργανισμού (Hayes, Dassen, Schilder, & Wallage, 2014). Αυτό περιλαμβάνει την αξιολόγηση των εγγενών κινδύνων και των κινδύνων ελέγχου που σχετίζονται με κάθε ισχυρισμό των οικονομικών καταστάσεων, καθώς και του κινδύνου ουσιώδους ανακρίβειας λόγω απάτης (Johnstone & Bedard, 2004). Με βάση την εκτίμηση του κινδύνου, οι ελεγκτές αναπτύσσουν μια προσαρμοσμένη προσέγγιση ελέγχου για την αντιμετώπιση των εντοπισθέντων κινδύνων και τη λήψη



επαρκών ελεγκτικών τεκμηρίων για τη στοιχειοθέτηση της έκφρασης γνώμης ελέγχου (Knecheletal., 2019).

### *3. Αξιολόγηση Εσωτερικού Ελέγχου*

Η αξιολόγηση των εσωτερικών ελέγχων ενός οργανισμού είναι μια κρίσιμη πτυχή της διαδικασίας ελέγχου, καθώς οι αποτελεσματικοί εσωτερικοί έλεγχοι συμβάλλουν στην πρόληψη και τον εντοπισμό ουσιωδών ανακρίβειων στη χρηματοοικονομική αναφορά (Mihret&Yismaw, 2007). Η πλήρης κατανόηση των εσωτερικών ελέγχων του πελάτη επιτρέπει στους ελεγκτές να εντοπίζουν ελλείψεις ελέγχου και να αναπτύσσουν συστάσεις για βελτίωση, συμβάλλοντας έτσι στη συνολική αποτελεσματικότητα και αποδοτικότητα του οργανισμού (Rahaman, 2010).

### *4. Τεστ Ελέγχου*

Τα τεστ ελέγχου είναι η διαδικασία συλλογής ελεγκτικών τεκμηρίων για την αξιολόγηση της ακρίβειας και της πληρότητας των οικονομικών καταστάσεων ενός οργανισμού και την αξιολόγηση της αποτελεσματικότητας των εσωτερικών ελέγχων (Arensetal., 2014). Τα τεστ ελέγχου περιλαμβάνει διάφορες διαδικασίες, όπως αναλυτικές διαδικασίες, δοκιμές ελέγχων και ουσιαστικές δοκιμές (Hayesetal., 2014). Οι αναλυτικές διαδικασίες περιλαμβάνουν τη σύγκριση των οικονομικών δεδομένων με προσδοκίες που βασίζονται σε προηγούμενη εμπειρία, σημεία αναφοράς του κλάδου ή ισχυρισμούς της διοίκησης (Glover&Prawitt, 2014). Οι δοκιμές ελέγχων αξιολογούν κατά πόσο ήταν αποτελεσματικοί οι εσωτερικοί έλεγχοι του πελάτη, ενώ οι ουσιαστικοί έλεγχοι παρέχουν άμεσες αποδείξεις αναφορικά με την ακρίβεια των ισχυρισμών των οικονομικών καταστάσεων (Arensetal., 2014). Η φύση, ο χρόνος και η έκταση της δοκιμής ελέγχου εξαρτώνται από την εκτίμηση κινδύνου του ελεγκτή και το εκτιμώμενο επίπεδο κινδύνου ελέγχου (Knecheletal., 2019).

### *5. Αναφορά και Τεκμηρίωση*

Το τελικό στάδιο της διαδικασίας ελέγχου περιλαμβάνει την υποβολή εκθέσεων και την τεκμηρίωση. Η έκθεση ελέγχου κοινοποιεί τη γνώμη του ελεγκτή για τυχόν εντοπισμένες ελλείψεις ελέγχου ή ουσιώδεις ανακρίβειες (Hayesetal., 2014). Επιπλέον, οι ελεγκτές απαιτείται να διατηρούν επαρκή τεκμηρίωση ελέγχου συμπεριλαμβανομένου του σχεδίου ελέγχου, της αξιολόγησης κινδύνου, των δοκιμών ελέγχων και των ουσιαστικών διαδικασιών (Johnstone&Bedard, 2004). Η κατάλληλη

τεκμηρίωση ελέγχου διευκολύνει τον ποιοτικό έλεγχο του ελέγχου, ενισχύει τη λογοδοσία του ελεγκτή και επιτρέπει την αποτελεσματική επικοινωνία με τον πελάτη και άλλα ενδιαφερόμενα μέρη (Singleton&Singleton, 2010).

Συμπερασματικά, η διαδικασία ελέγχου είναι μια συστηματική προσέγγιση για την εξέταση των οικονομικών καταστάσεων, των εσωτερικών ελέγχων και των διαδικασιών διαχείρισης κινδύνου ενός οργανισμού. Ακολουθώντας μια δομημένη διαδικασία που περιλαμβάνει σχεδιασμό ελέγχου, εκτίμηση κινδύνου, αξιολόγηση εσωτερικού ελέγχου, δοκιμές ελέγχου και υποβολή εκθέσεων και τεκμηρίωσης, οι ελεγκτές μπορούν να παρέχουν γνώμη ότι οι οικονομικές καταστάσεις δεν έχουν κάποια σημαντική(ουσιώδη) ανακρίβεια, ενισχύοντας τελικά την αξιοπιστία της χρηματοοικονομικής αναφοράς και ενισχύοντας την εμπιστοσύνη του κοινού στο χρηματοπιστωτικό σύστημα.

#### **1.1.4 Τύποι δοκιμών ελέγχου**

Οι δοκιμές ελέγχου πραγματοποιούνται από ελεγκτές για τη συλλογή αποδεικτικών στοιχείων επί των οικονομικών καταστάσεων, την οργάνωση των εσωτερικών ελέγχων και τη συμμόρφωση του οργανισμού με τη σχετική νομοθεσία και διαφόρων ειδών κανονιστικές διατάξεις. Αυτή η ενότητα εξετάζει τους βασικούς τύπους δοκιμών ελέγχου, συμπεριλαμβανομένων των ουσιαστικών δοκιμών, των δοκιμών συμμόρφωσης, των αναλυτικών διαδικασιών και των δοκιμών διπλού σκοπού.

- ✓ Ουσιαστικός Έλεγχος: Ο ουσιαστικός έλεγχος είναι μια διαδικασία ελέγχου που στοχεύει στη λήψη άμεσων αποδεικτικών στοιχείων σχετικά με την ακρίβεια και την πληρότητα των ισχυρισμών των οικονομικών καταστάσεων (Arens, Elder, &Beasley, 2014). Αυτός ο τύπος ελέγχου περιλαμβάνει την εξέταση συναλλαγών, υπολοίπων λογαριασμών και γνωστοποιήσεων για την επαλήθευση της ορθότητάς τους, συχνά μέσω τεχνικών όπως η βεβαίωση, η ανίχνευση και οι επιβεβαιώσεις (Glover&Prawitt, 2014). Ο ουσιαστικός έλεγχος μπορεί να πραγματοποιηθεί χρησιμοποιώντας μια δοκιμή λεπτομερειών, όπου οι ελεγκτές εξετάζουν μεμονωμένα στοιχεία σε έναν

λογαριασμό ή μέσω ουσιαστικών αναλυτικών διαδικασιών, οι οποίες περιλαμβάνουν σύγκριση οικονομικών δεδομένων με προσδοκίες που βασίζονται σε προηγούμενη εμπειρία, δείκτες αναφοράς του κλάδου ή ισχυρισμούς της διοίκησης (Knechel, Salterio, & Μπάλλου, 2019).

- ✓ Έλεγχος Συμμόρφωσης: Ο έλεγχος συμμόρφωσης, γνωστός και ως δοκιμές ελέγχων, αξιολογεί την αποτελεσματικότητα των εσωτερικών ελέγχων ενός οργανισμού στην πρόληψη ή τον εντοπισμό ουσιωδών ανακρίβειων (Arens et al., 2014). Αυτός ο τύπος ελέγχου περιλαμβάνει την εξέταση του σχεδιασμού και της λειτουργίας των δραστηριοτήτων ελέγχου, όπως η εξουσιοδότηση, ο διαχωρισμός καθηκόντων και οι διαδικασίες “συμφιλίωσης”. Με την έννοια της συμφιλίωσης νοείται η διαδικασία σύγκρισης των συναλλαγών και της δραστηριότητας με την τεκμηρίωση. Επιπλέον, η συμφιλίωση περιλαμβάνει την επίλυση τυχόν αποκλίσεων που μπορεί να έχουν ανακαλυφθεί. (Hayes, Dassen, Schilder, & Wallage, 2014). Ο έλεγχος συμμόρφωσης βοηθά τους ελεγκτές να εκτιμήσουν το επίπεδο του κινδύνου ελέγχου και να προσδιορίσουν την έκταση των ουσιαστικών ελέγχων που απαιτούνται στον έλεγχο (Johnstone & Bedard, 2004). Εάν ο ελεγκτής καταλήξει στο συμπέρασμα ότι οι εσωτερικοί έλεγχοι λειτουργούν αποτελεσματικά, μπορεί να μειώσουν την έκταση των ουσιαστικών ελέγχων, με αποτέλεσμα μια πιο αποτελεσματική προσέγγιση ελέγχου (Knechelet al., 2019).
- ✓ Αναλυτικές Διαδικασίες: Περιλαμβάνουν την αξιολόγηση των οικονομικών πληροφοριών μέσω της ανάλυσης εύλογων αλληλεπίδρασης μεταξύ χρηματοοικονομικών και μη χρηματοοικονομικών δεδομένων (Arens et al., 2014). Αυτός ο τύπος ελέγχου μπορεί να χρησιμοποιηθεί σε διάφορα στάδια του ελέγχου, όπως η αξιολόγηση κινδύνου, ο ουσιαστικός έλεγχος και η συνολική αναθεώρηση (Glover & Prawitt, 2014). Οι αναλυτικές διαδικασίες μπορεί να περιλαμβάνουν ανάλυση τάσεων, ανάλυση αριθμοδεικτών και σύγκριση των πραγματικών αποτελεσμάτων με προϋπολογισμούς, προβλέψεις ή αποτελέσματα προηγούμενης περιόδου (Knechelet al., 2019). Εντοπίζοντας απροσδόκητες σχέσεις ή διακυμάνσεις, οι αναλυτικές διαδικασίες μπορούν να βοηθήσουν τους ελεγκτές να εντοπίσουν πιθανές ανακρίβειες, να αξιολογήσουν το εύλογο των ισχυρισμών της διοίκησης και να κατευθύνουν την προσοχή τους σε τομείς υψηλού κινδύνου (Hayes et al., 2014).

- ✓ Δοκιμές διπλού σκοπού (Dual-Purpose Testing): Οι δοκιμές διπλού σκοπού αναφέρονται σε ελεγκτικές διαδικασίες που έχουν σχεδιαστεί για την επίτευξη τόσο ουσιαστικών στόχων, όσο και στόχων συμμόρφωσης (Arensetal., 2014). Αυτός ο τύπος ελέγχου επιτρέπει στους ελεγκτές να συλλέγουν στοιχεία σχετικά με την ακρίβεια των ισχυρισμών των οικονομικών καταστάσεων, ενώ παράλληλα αξιολογούν την αποτελεσματικότητα των εσωτερικών ελέγχων (Glover&Prawitt, 2014). Ο έλεγχος διπλού σκοπού μπορεί να αυξήσει την αποτελεσματικότητα του ελέγχου μειώνοντας την ανάγκη για χωριστές δοκιμές ελέγχων και δοκιμές ουσίας, καθώς ο ελεγκτής μπορεί να βασιστεί στα αποτελέσματα της δοκιμής διπλού σκοπού για να συναγάγει συμπεράσματα τόσο για τη δομή εσωτερικού ελέγχου όσο και για τους ισχυρισμούς των οικονομικών καταστάσεων. Knecheletal., 2019).

Συμπερασματικά, οι δοκιμές ελέγχου είναι απαραίτητα εργαλεία για τους ελεγκτές για τη συλλογή αποδεικτικών στοιχείων και τη συμμόρφωση του οργανισμού ή της εκάστοτε επιχείρησης με τους σχετικούς νόμους, ερμηνευτικές εγκυκλίους και κανονισμούς. Χρησιμοποιώντας έναν συνδυασμό ουσιαστικών δοκιμών, δοκιμών συμμόρφωσης, αναλυτικών διαδικασιών και δοκιμών διπλού σκοπού, οι ελεγκτές μπορούν να αποκτήσουν μια ολοκληρωμένη κατανόηση της οικονομικής θέσης του οργανισμού και του περιβάλλοντος εσωτερικού ελέγχου, ενισχύοντας τελικά την αξιοπιστία της χρηματοοικονομικής αναφοράς και ενισχύοντας την εμπιστοσύνη του κοινού στα χρηματοοικονομικά Σύστημα.

## **1.2. Εσωτερικός έλεγχος**

### **1.2.1 Γενικά στοιχεία για τον Εσωτερικό Έλεγχο**

Ο εσωτερικός έλεγχος είναι μια βασική λειτουργία εντός των οργανισμών που παρέχει ανεξάρτητες, αντικειμενικές υπηρεσίες διασφάλισης και συμβουλευτικής για τη βελτίωση των λειτουργιών ενός οργανισμού. Αυτή η ενότητα παρουσιάζει μια επισκόπηση του ορισμού, του ρόλου, της σημασίας, των στόχων και της εξέλιξης του εσωτερικού ελέγχου.

Ο εσωτερικός έλεγχος ορίζεται από το Ινστιτούτο Εσωτερικών Ελεγκτών (IIA) ως “μια ανεξάρτητη, αντικειμενική δραστηριότητα διασφάλισης και συμβουλευτικής που έχει σχεδιαστεί για να προσθέτει αξία και να βελτιώνει τις λειτουργίες ενός οργανισμού” (IIA, 2017). Οι εσωτερικοί ελεγκτές είναι υπεύθυνοι για την αξιολόγηση των εσωτερικών ελέγχων, της διαχείρισης κινδύνων και των διαδικασιών διακυβέρνησης ενός οργανισμού και για την παροχή συστάσεων για βελτίωση (Mihret, 2010).

Ο πρωταρχικός ρόλος του εσωτερικού ελέγχου είναι να παρέχει διαβεβαίωση στη διοίκηση και στο διοικητικό συμβούλιο (ή σε ισοδύναμο διοικητικό όργανο) ότι οι εσωτερικοί έλεγχοι, η διαχείριση κινδύνου και οι διαδικασίες διακυβέρνησης του οργανισμού είναι αποτελεσματικοί και αποδοτικοί (Arena&Azzone, 2009). Συμβάλλει να πετύχουν τους στόχους τους οι οργανισμοί, εντοπίζοντας κινδύνους, αξιολογώντας το σχεδιασμό και τη λειτουργία των εσωτερικών ελέγχων και παρακολουθώντας τη συμμόρφωση με νόμους, κανονισμούς και οργανωτικές πολιτικές (Sarens&Beelde, 2006). Η ύπαρξη του εσωτερικού ελέγχου έχει γίνει πιο αναγκαία τον τελευταίο καιρό λόγω των αυξημένων κανονιστικών απαιτήσεων, της αυξανόμενης πολυπλοκότητας των επιχειρηματικών λειτουργιών και του αυξημένου δημόσιου ελέγχου της εταιρικής διακυβέρνησης (Pickett, 2011).

Οι πρωταρχικοί στόχοι του εσωτερικού ελέγχου είναι η παροχή υπηρεσιών διασφάλισης και συμβουλευτικής που βοηθούν τους οργανισμούς να επιτύχουν τους στόχους τους, να βελτιώσουν τους εσωτερικούς ελέγχους και να διατηρήσουν τη συμμόρφωση με τους νόμους και τους κανονισμούς (IIA, 2017). Οι υπηρεσίες διασφάλισης περιλαμβάνουν την αξιολόγηση της αποτελεσματικότητας των διαδικασιών διαχείρισης κινδύνου, ελέγχου και διακυβέρνησης, ενώ οι συμβουλευτικές υπηρεσίες επικεντρώνονται στην παροχή συμβουλών και συστάσεων για τη βελτίωση αυτών των διαδικασιών (Mihret, 2010). Με την επίτευξη αυτών των στόχων, οι εσωτερικοί ελεγκτές συμβάλλουν στη συνολική αποτελεσματικότητα και αποδοτικότητα του οργανισμού, ενισχύοντας τελικά την εμπιστοσύνη και την εμπιστοσύνη των ενδιαφερομένων.

Το επάγγελμα του εσωτερικού ελέγχου εξάλλου, έχει εξελιχθεί σημαντικά τις τελευταίες δεκαετίες ως απάντηση στο μεταβαλλόμενο επιχειρηματικό περιβάλλον, στις κανονιστικές απαιτήσεις και στις προσδοκίες των ενδιαφερομένων. Ιστορικά, οι

εσωτερικοί ελεγκτές επικεντρώθηκαν κυρίως στον οικονομικό έλεγχο και τον έλεγχο συμμόρφωσης, με μεγάλη έμφαση στον εντοπισμό και την πρόληψη της απάτης (Pickett, 2011). Ωστόσο, ο ρόλος του εσωτερικού ελέγχου έχει επεκταθεί για να συμπεριλάβει ένα ευρύτερο φάσμα αρμοδιοτήτων, συμπεριλαμβανομένης της διαχείρισης λειτουργικού και στρατηγικού κινδύνου, του ελέγχου τεχνολογίας πληροφοριών και περιβαλλοντικών, κοινωνικών και διακυβέρνησης (Ziegenfuss&Gilsdorf, 1997).

Η αυξανόμενη σημασία του εσωτερικού ελέγχου έχει επίσης οδηγήσει στην ανάπτυξη επαγγελματικών προτύπων και καθοδήγησης, όπως το Διεθνές Πλαίσιο Επαγγελματικών Πρακτικών της ΙΑ (International Professional Practices Framework, IPPF) και ο Κώδικας Δεοντολογίας της ΙΑ (ΙΑ, 2017). Αυτά τα πλαίσια παρέχουν μια βάση για τους εσωτερικούς ελεγκτές ώστε να διατηρούν τα υψηλότερα επίπεδα επαγγελματισμού, ανεξαρτησίας και αντικειμενικότητας και να βελτιώνουν συνεχώς τις δεξιότητες και τις ικανότητές τους ως απάντηση στο μεταβαλλόμενο επιχειρηματικό τοπίο (Mihret, 2010).

Εν κατακλείδι, ο εσωτερικός έλεγχος είναι μια ζωτική λειτουργία εντός των οργανισμών που παρέχει ανεξάρτητες, αντικειμενικές υπηρεσίες διασφάλισης και συμβουλευτικής για τη βελτίωση των λειτουργιών ενός οργανισμού. Οι εσωτερικοί ελεγκτές διαδραματίζουν κρίσιμο ρόλο στην αξιολόγηση των εσωτερικών ελέγχων, της διαχείρισης κινδύνων και των διαδικασιών διακυβέρνησης και στην παροχή συστάσεων για βελτίωση. Καθώς το επιχειρηματικό περιβάλλον συνεχίζει να εξελίσσεται, το επάγγελμα του εσωτερικού ελεγκτή πρέπει να προσαρμοστεί για να αντιμετωπίσει νέες προκλήσεις και ευκαιρίες, διασφαλίζοντας ότι οι οργανισμοί παραμένουν ανθεκτικοί και αποτελεσματικοί στην επίτευξη των στόχων τους.

### **1.2.2. Πλαίσιο και Πρότυπα Εσωτερικού Ελέγχου**

Το επάγγελμα του εσωτερικού ελέγχου καθοδηγείται από ένα ολοκληρωμένο σύνολο πλαισίων, προτύπων και καθοδήγησης που καθιερώνουν μια συνεπή και υψηλής ποιότητας προσέγγιση στον εσωτερικό έλεγχο. Αυτή η ενότητα εξετάζει το Ινστιτούτο Εσωτερικών Ελεγκτών (ΙΑ), το “Διεθνές Πλαίσιο Επαγγελματικών

Πρακτικών” (IPPF), τον “Κώδικα Δεοντολογίας Εσωτερικού Ελέγχου”, τα πρότυπα και τις οδηγίες εσωτερικού ελέγχου και τον εσωτερικό έλεγχο βάσει κινδύνου.

- ✓ Ινστιτούτο Εσωτερικών Ελεγκτών (ΙΑ) και το Διεθνές Πλαίσιο Επαγγελματικών Πρακτικών (IPPF): Η ΙΑ είναι μια παγκόσμια επαγγελματική ένωση που εκπροσωπεί εσωτερικούς ελεγκτές και θέτει τα πρότυπα για το επάγγελμα του εσωτερικού ελέγχου (ΙΑ, 2021). Η ΙΑ ανέπτυξε το Διεθνές Πλαίσιο Επαγγελματικών Πρακτικών (IPPF), ένα ολοκληρωμένο σύνολο επαγγελματικών πρακτικών, προτύπων και καθοδήγησης για εσωτερικούς ελεγκτές (Ramamoortietal., 2009). Το IPPF έχει σχεδιαστεί για να διασφαλίζει ότι οι εσωτερικοί ελεγκτές διαθέτουν τις απαραίτητες γνώσεις, δεξιότητες και τεχνογνωσία για να εκτελούν αποτελεσματικά τα καθήκοντά τους και να συμβάλλουν στη συνολική επιτυχία των οργανισμών τους (Pickett, 2011).
- ✓ Κώδικας Δεοντολογίας Εσωτερικού Ελέγχου: Θεσπίζει τις ηθικές αρχές και τις προσδοκίες για τους εσωτερικούς ελεγκτές, προωθώντας ένα περιβάλλον εμπιστοσύνης, ακεραιότητας και επαγγελματισμού (ΙΑ, 2021). Ο Κώδικας Δεοντολογίας βασίζεται σε τέσσερις βασικές αρχές: ακεραιότητα, αντικειμενικότητα, εμπιστευτικότητα και ικανότητα (ΙΑ, 2021). Οι εσωτερικοί ελεγκτές αναμένεται να τηρούν αυτές τις αρχές κατά την εκτέλεση των καθηκόντων τους, διασφαλίζοντας ότι διατηρούν τα υψηλότερα επίπεδα επαγγελματισμού, ανεξαρτησίας και αντικειμενικότητας στην εργασία τους (Mihret, 2010).
- ✓ Πρότυπα και Οδηγίες Εσωτερικού Ελέγχου: Τα Διεθνή Πρότυπα της ΙΑ για την Επαγγελματική Πρακτική του Εσωτερικού Ελέγχου (Πρότυπα) παρέχουν ένα πλαίσιο για την εκτέλεση και την προώθηση υψηλής ποιότητας υπηρεσιών εσωτερικού ελέγχου (ΙΑ, 2021). Τα Πρότυπα καλύπτουν διάφορες πτυχές του εσωτερικού ελέγχου, συμπεριλαμβανομένου του σχεδιασμού, της εκτέλεσης, της επικοινωνίας και της παρακολούθησης των αποτελεσμάτων των εργασιών ελέγχου (Pickett, 2011). Επιπλέον, η ΙΑ εκδίδει καθοδήγηση για συγκεκριμένα θέματα που σχετίζονται με τον εσωτερικό έλεγχο, όπως η ανίχνευση απάτης, η διαχείριση κινδύνου και ο έλεγχος τεχνολογίας πληροφοριών (Ramamoortietal., 2009). Αυτά τα πρότυπα και τα έγγραφα καθοδήγησης προορίζονται να βοηθήσουν τους εσωτερικούς ελεγκτές να

αναπτύξουν και να διατηρήσουν τις απαραίτητες γνώσεις, δεξιότητες και τεχνογνωσία για να εκτελούν αποτελεσματικά τα καθήκοντά τους και να συμβάλλουν στη συνολική επιτυχία των οργανισμών τους.

- ✓ Εσωτερικός έλεγχος βάσει κινδύνου: Ο εσωτερικός έλεγχος βάσει κινδύνου (Risk-Based Internal Auditing, RBIA) είναι μια προσέγγιση που εστιάζει στην αξιολόγηση της αποτελεσματικότητας των διαδικασιών διαχείρισης κινδύνου ενός οργανισμού και στη διαχείριση βασικών κινδύνων (Arenas&Azzone, 2009). Ο RBIA δίνει τη δυνατότητα στους εσωτερικούς ελεγκτές να ιεραρχήσουν τις προσπάθειες και τους πόρους τους με βάση το προφίλ κινδύνου του οργανισμού, διασφαλίζοντας ότι οι πιο σημαντικοί κίνδυνοι αντιμετωπίζονται πρώτα (Sarens&Beelde, 2006). Υιοθετώντας μια προσέγγιση βασισμένη στον κίνδυνο, οι εσωτερικοί ελεγκτές μπορούν να παρέχουν πιο έγκαιρες και σχετικές υπηρεσίες διασφάλισης και συμβουλευτικής, ενισχύοντας τελικά την ικανότητα του οργανισμού να διαχειρίζεται τους κινδύνους και να επιτυγχάνει τους στόχους του (Knecheletal., 2013).

Συμπερασματικά, το επάγγελμα του εσωτερικού ελέγχου καθοδηγείται από ένα ολοκληρωμένο σύνολο πλαισίων, προτύπων και καθοδήγησης που καθιερώνουν μια συνεπή και υψηλής ποιότητας προσέγγιση στον εσωτερικό έλεγχο. Το ΠΑ και το IPPF χρησιμεύουν ως βάση για αυτές τις πρακτικές, διασφαλίζοντας ότι οι εσωτερικοί ελεγκτές διαθέτουν τις απαραίτητες γνώσεις, δεξιότητες και τεχνογνωσία για να εκτελούν αποτελεσματικά τα καθήκοντά τους και να συμβάλλουν στη συνολική επιτυχία των οργανισμών τους. Με την τήρηση όλων αυτών που αναφέρθηκαν παραπάνω οι εσωτερικοί ελεγκτές μπορούν να διατηρήσουν τα υψηλότερα επίπεδα επαγγελματισμού, ανεξαρτησίας και αντικειμενικότητας στο έργο τους. Επιπλέον, υιοθετώντας μια προσέγγιση βάσει κινδύνου στον εσωτερικό έλεγχο, οι εσωτερικοί ελεγκτές μπορούν να παρέχουν πιο έγκαιρες και σχετικές υπηρεσίες διασφάλισης και συμβουλευτικής, ενισχύοντας τελικά την ικανότητα του οργανισμού να διαχειρίζεται τους κινδύνους και να επιτυγχάνει τους στόχους του.

### **1.2.3 Λειτουργίες και Εξειδικεύσεις του Εσωτερικού Ελέγχου**



Οι λειτουργίες του εσωτερικού ελέγχου καλύπτουν ένα ευρύ φάσμα εξειδικευμένων τομέων, επιτρέποντας στους οργανισμούς να αντιμετωπίζουν διάφορους κινδύνους και προκλήσεις που σχετίζονται με τις δραστηριότητές τους. Αυτή η ενότητα εξετάζει πέντε βασικούς τύπους εσωτερικού ελέγχου: οικονομικούς ελέγχους, λειτουργικούς ελέγχους, ελέγχους συμμόρφωσης, ελέγχους τεχνολογίας πληροφοριών και ελέγχους απάτης.

Οι οικονομικοί έλεγχοι επικεντρώνονται στην ακρίβεια και την αξιοπιστία των οικονομικών αναφορών ενός οργανισμού και στην αποτελεσματικότητα των εσωτερικών ελέγχων του στη χρηματοοικονομική αναφορά (Mocketal., 2013). Αυτοί οι έλεγχοι βοηθούν να διασφαλιστεί ότι οι οικονομικές καταστάσεις συντάσσονται σύμφωνα με τα ισχύοντα λογιστικά πρότυπα και τις κανονιστικές απαιτήσεις, παρέχοντας στους ενδιαφερόμενους αξιόπιστες και ακριβείς πληροφορίες για τη λήψη αποφάσεων (DeZoortetal., 2012).

Οι λειτουργικοί έλεγχοι αξιολογούν την αποδοτικότητα και την αποτελεσματικότητα των επιχειρηματικών διαδικασιών, των λειτουργιών και των πρακτικών διαχείρισης ενός οργανισμού (Sarens&Beelde, 2006). Αυτοί οι έλεγχοι εντοπίζουν τομείς προς βελτίωση, βοηθώντας τους οργανισμούς να βελτιστοποιήσουν τις λειτουργίες τους, να μειώσουν το κόστος και να βελτιώσουν τη συνολική απόδοση (Cohen&Sayag, 2010).

Οι έλεγχοι συμμόρφωσης αξιολογούν τη συμμόρφωση ενός οργανισμού στους ισχύοντες νόμους, κανονισμούς, πολιτικές και διαδικασίες (Cohen&Sayag, 2010). Αυτοί οι έλεγχοι βοηθούν τους οργανισμούς να εντοπίσουν και να αντιμετωπίσουν πιθανούς κινδύνους συμμόρφωσης, διασφαλίζοντας ότι παραμένουν σε καλή κατάσταση με τις ρυθμιστικές αρχές και άλλους ενδιαφερόμενους φορείς (DeZoortetal., 2012).

Οι έλεγχοι τεχνολογίας πληροφοριών (IT) αξιολογούν την αποτελεσματικότητα των συστημάτων πληροφορικής, των διαδικασιών και των ελέγχων ενός οργανισμού στη διαχείριση και τη διαφύλαξη των πληροφοριών του (Schneider, 2012). Αυτοί οι έλεγχοι επικεντρώνονται σε τομείς όπως η ακεραιότητα των δεδομένων, η ασφάλεια του συστήματος και η διακυβέρνηση IT, βοηθώντας τους οργανισμούς να προστατεύουν τα κρίσιμα στοιχεία πληροφοριών τους και να

διασφαλίζουν την αξιοπιστία των συστημάτων πληροφορικής τους (DaVeiga&Eloff, 2010).

Οι έλεγχοι απάτης τέλος, στοχεύουν στον εντοπισμό, την πρόληψη και την αποτροπή δόλιων δραστηριοτήτων εντός ενός οργανισμού (Wells, 2011). Αυτοί οι έλεγχοι συνήθως περιλαμβάνουν τη χρήση εξειδικευμένων τεχνικών και εργαλείων, όπως η ανάλυση δεδομένων, για τον εντοπισμό πιθανών δεικτών απάτης και τη διερεύνηση ύποπτων συναλλαγών ή δραστηριοτήτων (Singletonetal., 2006).

Συμπερασματικά, οι λειτουργίες εσωτερικού ελέγχου καλύπτουν ένα ευρύ φάσμα εξειδικευμένων τομέων, αντιμετωπίζοντας διάφορους κινδύνους και προκλήσεις που σχετίζονται με τις λειτουργίες ενός οργανισμού. Κάθε τύπος εσωτερικού ελέγχου εξυπηρετεί έναν ξεχωριστό σκοπό, βοηθώντας τους οργανισμούς να επιτύχουν τους στόχους τους, να διαχειριστούν τους κινδύνους και να διατηρήσουν τη συμμόρφωση με τους ισχύοντες νόμους και κανονισμούς.

Με την υιοθέτηση μιας ολοκληρωμένης προσέγγισης για τον εσωτερικό έλεγχο που περιλαμβάνει αυτούς τους εξειδικευμένους τομείς, οι οργανισμοί μπορούν να διαχειριστούν καλύτερα τους κινδύνους, να βελτιώσουν τη λειτουργική αποτελεσματικότητα και να διατηρήσουν τη συμμόρφωση με τους ισχύοντες νόμους και κανονισμούς. Αυτή η ολιστική προσέγγιση διασφαλίζει ότι οι οργανισμοί είναι καλά εξοπλισμένοι για να αντιμετωπίσουν τις δυναμικές προκλήσεις και τους κινδύνους που αντιμετωπίζουν στο σημερινό πολύπλοκο επιχειρηματικό περιβάλλον.

## **1.3 Η έννοια του Εσωτερικού Ελέγχου στο Δημόσιο Τομέα**

### **1.3.1 Ορισμός και Στόχοι Εσωτερικού Ελέγχου του Δημοσίου Τομέα**

Ο εσωτερικός έλεγχος του δημόσιου τομέα είναι ένα κρίσιμο στοιχείο της διακυβέρνησης του δημόσιου τομέα, παρέχοντας ανεξάρτητες και αντικειμενικές αξιολογήσεις των λειτουργιών, των προγραμμάτων και των δραστηριοτήτων των κυβερνητικών οργανισμών. Αυτή η ενότητα παρέχει μια επισκόπηση αυτού του

ελέγχου, συμπεριλαμβανομένου του ορισμού και των στόχων του, του ρόλου και της σημασίας του, των βασικών διαφορών από τον εσωτερικό έλεγχο του ιδιωτικού τομέα και του εξελισσόμενου ρόλου στους δημόσιους τομείς.

Ο εσωτερικός έλεγχος του δημόσιου τομέα μπορεί να οριστεί ως μια ανεξάρτητη, αντικειμενική δραστηριότητα διασφάλισης και συμβουλευτικής που έχει σχεδιαστεί για να προσθέτει αξία και να βελτιώνει τις λειτουργίες των κυβερνητικών οργανισμών (IIA, 2019). Οι στόχοι του εσωτερικού ελέγχου του δημόσιου τομέα περιλαμβάνουν την αξιολόγηση της αποτελεσματικότητας, της αποδοτικότητας και της οικονομίας των κρατικών λειτουργιών, την αξιολόγηση της συμμόρφωσης με τους ισχύοντες νόμους, κανονισμούς και πολιτικές, την ανίχνευση και πρόληψη απάτης, σπατάλης και κατάχρησης και την προώθηση της διαφάνειας και της λογοδοσίας στους κυβερνητικούς οργανισμούς.

Ο εσωτερικός έλεγχος του δημόσιου τομέα διαδραματίζει κρίσιμο ρόλο στη διασφάλιση ότι οι κυβερνητικοί οργανισμοί λειτουργούν αποτελεσματικά, αποδοτικά και σε συμμόρφωση με τους ισχύοντες νόμους, κανονισμούς και πολιτικές. Οι εσωτερικοί ελεγκτές παρέχουν πολύτιμες υπηρεσίες διασφάλισης και συμβουλευτικής σε κυβερνητικούς οργανισμούς, βοηθώντας στον εντοπισμό πιθανών κινδύνων, στη βελτίωση των λειτουργιών και στη βελτίωση της λογοδοσίας και της διαφάνειας (Braun&Freytag, 2016). Επιπλέον, ο εσωτερικός έλεγχος απαιτείται συχνά από νόμους ή κανονισμούς στον δημόσιο τομέα, υπογραμμίζοντας τη σημασία του ως βασικό στοιχείο της χρηστής διακυβέρνησης.

Ενώ υπάρχουν ομοιότητες μεταξύ του εσωτερικού ελέγχου σε υπηρεσίες και φορείς του δημοσίου και σε ιδιωτικές επιχειρήσεις, υπάρχουν επίσης βασικές διαφορές που αντικατοπτρίζουν τις μοναδικές προκλήσεις και προτεραιότητες του δημόσιου τομέα. Για παράδειγμα, στο δημόσιο οι ελεγκτές πρέπει να πλοηγούνται σε πολύπλοκα νομικά και ρυθμιστικά πλαίσια, να διαχειρίζονται τον πολιτικό και δημόσιο έλεγχο και να λειτουργούν σε μια αποκεντρωμένη και συχνά απομονωμένη οργανωτική δομή (IIA, 2019). Επιπλέον, ο εσωτερικός έλεγχος σε αυτούς τους φορείς πρέπει να εξισορροπεί την ανάγκη τόσο για λογοδοσία όσο και για αποτελεσματικότητα, συχνά με περιορισμένους πόρους και ανταγωνιστικές απαιτήσεις.

Ο ρόλος του εσωτερικού ελέγχου του δημόσιου τομέα εξελίσσεται, καθοδηγούμενος από την πρόοδο της τεχνολογίας, τις μεταβαλλόμενες προσδοκίες των ενδιαφερόμενων μερών και τους αναδυόμενους κινδύνους και προκλήσεις. Για παράδειγμα, η υιοθέτηση της ανάλυσης δεδομένων γίνεται όλο και περισσότερο βασικό συστατικό του εσωτερικού ελέγχου του δημόσιου τομέα, βοηθώντας τους εσωτερικούς ελεγκτές να εντοπίζουν πιο αποτελεσματικά τους κινδύνους και τις ευκαιρίες για βελτίωση (Swartz, 2016). Επιπλέον, ο εσωτερικός έλεγχος του δημόσιου τομέα ενσωματώνεται περισσότερο με άλλους τομείς διακυβέρνησης, όπως η διαχείριση κινδύνου, η διαχείριση απόδοσης και ο στρατηγικός σχεδιασμός, αντανακλώντας την αυξανόμενη αναγνώριση της ανάγκης για μια ολιστική προσέγγιση στη διακυβέρνηση του δημόσιου τομέα (Behn, 2001).

Εν κατακλείδι, ο εσωτερικός έλεγχος στους δημοσίου οργανισμούς είναι ένα κρίσιμο συστατικό της χρηστής διακυβέρνησης σε κυβερνητικούς οργανισμούς, παρέχοντας ανεξάρτητες και αντικειμενικές αξιολογήσεις λειτουργιών, προγραμμάτων και δραστηριοτήτων. Ο εσωτερικός έλεγχος του δημόσιου τομέα έχει μοναδικές προκλήσεις και προτεραιότητες σε σύγκριση με τον εσωτερικό έλεγχο του ιδιωτικού τομέα, αλλά διαδραματίζει ουσιαστικό ρόλο στην προώθηση της διαφάνειας, της λογοδοσίας και της χρηστής διακυβέρνησης στον δημόσιο τομέα. Ο εξελισσόμενος ρόλος του εσωτερικού ελέγχου του δημόσιου τομέα αντανακλά την ανάγκη προσαρμογής στους αναδυόμενους κινδύνους και προκλήσεις και την υιοθέτηση νέων εργαλείων και προσεγγίσεων που θα συμβάλλουν στην επίτευξη στόχων με την χαμηλότερη δυνατή επιβάρυνση στον κρατικό προϋπολογισμό.

### **1.3.2 Πλαίσια και Πρότυπα Εσωτερικού Ελέγχου του Δημόσιου Τομέα**

Ο εσωτερικός έλεγχος του δημόσιου τομέα διαδραματίζει κρίσιμο ρόλο στην προώθηση της διαφάνειας, της λογοδοσίας και της χρηστής διακυβέρνησης. Για να διασφαλιστεί η συνέπεια και η αποτελεσματικότητα, οι εσωτερικοί ελεγκτές του δημόσιου τομέα τηρούν διάφορα πλαίσια και πρότυπα. Αυτή η ενότητα θα συζητήσει το Διεθνές Πλαίσιο Επαγγελματικών Πρακτικών (IPPF) στον δημόσιο τομέα, τα Διεθνή Πρότυπα των Ανώτατων Ελεγκτικών Οργανισμών (ISSAI), τον Κώδικα

Δεοντολογίας Εσωτερικού Ελέγχου του Δημόσιου Τομέα και τον εσωτερικό έλεγχο βάσει κινδύνου στο δημόσιο τομέα.

- ✓ INTOSAI και τα Διεθνή Πρότυπα Ανώτατων Ελεγκτικών Οργανισμών (ISSAI): Ο Διεθνής Οργανισμός Ανώτατων Ιδρυμάτων Ελέγχου (INTOSAI) είναι ένας διεθνής επαγγελματικός οργανισμός που στοχεύει να ενισχύσει τον έλεγχο του δημόσιου τομέα παγκοσμίως. Η INTOSAI αναπτύσσει και προωθεί τα Διεθνή Πρότυπα των Ανώτατων Ελεγκτικών Ιδρυμάτων (ISSAI), τα οποία παρέχουν ένα πλαίσιο για τον εξωτερικό και εσωτερικό έλεγχο του δημόσιου τομέα (INTOSAI, 2010). Το πλαίσιο ISSAI περιλαμβάνει διάφορες πτυχές του ελέγχου του δημόσιου τομέα, όπως οικονομικούς ελέγχους, ελέγχους επιδόσεων και ελέγχους συμμόρφωσης, και έχει σχεδιαστεί για να διασφαλίζει υψηλής ποιότητας πρακτικές ελέγχου του δημόσιου τομέα (Dye&Stapenhurst, 1998).
- ✓ Κώδικας Δεοντολογίας Εσωτερικού Ελέγχου Δημόσιου Τομέα: Αποτελεί αναπόσπαστο μέρος του IPPF, παρέχοντας καθοδήγηση σχετικά με τις ηθικές αρχές και συμπεριφορές που αναμένονται από τους εσωτερικούς ελεγκτές στο δημόσιο τομέα. Ο Κώδικας Δεοντολογίας τονίζει τη σημασία ορισμένων αρχών όπως της εμπιστευτικότητας, της αντικειμενικότητας, της ακεραιότητας και της ικανότητας στον εσωτερικό έλεγχο (IIA, 2017). Η τήρηση αυτών των ηθικών αρχών συμβάλλει στην ενίσχυση της αξιοπιστίας και του επαγγελματισμού των εσωτερικών ελεγκτών του δημόσιου τομέα και διασφαλίζει ότι μπορούν να υποστηρίξουν αποτελεσματικά τους οργανισμούς τους στην επίτευξη των στόχων τους (VanPeurse, 2005).
- ✓ Εσωτερικός έλεγχος βάσει κινδύνου στο Δημόσιο Τομέα: Ο εσωτερικός έλεγχος που βασίζεται στον κίνδυνο είναι μια ευρέως αναγνωρισμένη προσέγγιση που εστιάζει στον εντοπισμό και την αντιμετώπιση των πιο σημαντικών κινδύνων που αντιμετωπίζει ένας οργανισμός (Knecheletal., 2013). Στον δημόσιο τομέα, ο εσωτερικός έλεγχος βάσει κινδύνου είναι όλο και πιο σημαντικός, δεδομένων των πολυάριθμων κινδύνων και προκλήσεων που συνδέονται με την παροχή δημόσιων υπηρεσιών και τη διαχείριση των δημόσιων πόρων (Barrett, 2007). Ο εσωτερικός έλεγχος βάσει κινδύνου επιτρέπει στους εσωτερικούς ελεγκτές του δημόσιου τομέα να παρέχουν πιο έγκαιρες και σχετικές υπηρεσίες διασφάλισης και συμβουλευτικής

υποστήριξης, υποστηρίζοντας τους οργανισμούς τους στην επίτευξη των στόχων τους και τη διαχείριση των κινδύνων αποτελεσματικά (Simnettetal., 2009).

Συμπερασματικά, τα πλαίσια και τα πρότυπα εσωτερικού ελέγχου στους δημόσιους φορείς είναι απαραίτητα για να προωθούν την διαφάνεια, την λογοδοσία και την χρηστή διακυβέρνηση. Το Διεθνές Πλαίσιο Επαγγελματικών Πρακτικών (IPPF) και τα Διεθνή Πρότυπα Ανώτατων Ελεγκτικών Ιδρυμάτων (ISSAI) παρέχουν ολοκληρωμένη καθοδήγηση στους εσωτερικούς ελεγκτές του δημόσιου τομέα, διασφαλίζοντας συνέπεια και αποτελεσματικότητα στις πρακτικές τους. Η τήρηση του Κώδικα Δεοντολογίας Εσωτερικού Ελέγχου του Δημόσιου Τομέα είναι ζωτικής σημασίας για τη διατήρηση της αξιοπιστίας και του επαγγελματισμού των εσωτερικών ελεγκτών. Επιπλέον, η υιοθέτηση μιας προσέγγισης εσωτερικού ελέγχου βάσει κινδύνου βοηθά τους οργανισμούς του δημόσιου τομέα να αντιμετωπίζουν αποτελεσματικά τους κινδύνους και να επιτυγχάνουν τους στόχους τους.

Ακολουθώντας αυτά τα πλαίσια και τα πρότυπα, οι εσωτερικοί ελεγκτές του δημόσιου τομέα μπορούν να υποστηρίξουν καλύτερα τις οργανώσεις τους στην παροχή δημόσιων υπηρεσιών υψηλής ποιότητας και στη διαχείριση των δημοσίων πόρων με υπευθυνότητα. Επιπλέον, η εφαρμογή αυτών των πλαισίων και προτύπων συμβάλλει στη συνεχή βελτίωση και εξέλιξη των πρακτικών εσωτερικού ελέγχου του δημόσιου τομέα, ενισχύοντας τελικά την αξία και τον αντίκτυπο του εσωτερικού ελέγχου στο δημόσιο τομέα.

### **1.3.3 Προκλήσεις και Ευκαιρίες για τον Εσωτερικό Έλεγχο του Δημόσιου Τομέα**

Οι εσωτερικοί ελεγκτές του δημόσιου τομέα αντιμετωπίζουν πολυάριθμες προκλήσεις και ευκαιρίες στον ρόλο τους να παρέχουν υπηρεσίες διασφάλισης και συμβουλευτικής σε κυβερνητικούς οργανισμούς. Αυτή η ενότητα εξετάζει μερικές από τις κύριες προκλήσεις και ευκαιρίες που αντιμετωπίζει ο εσωτερικός έλεγχος του δημόσιου τομέα, συμπεριλαμβανομένης της διασφάλισης της ανεξαρτησίας και της αντικειμενικότητας, της ανάπτυξης ικανοτήτων και της επαγγελματικής ανάπτυξης, της συνεργασίας και του συντονισμού με εξωτερικούς ελεγκτές, της αξιοποίησης της

τεχνολογίας και της ανάλυσης δεδομένων και της προώθησης της διαφάνειας, της λογοδοσίας και της χρηστής διακυβέρνησης .

Μία από τις πρωταρχικές προκλήσεις για τον εσωτερικό έλεγχο του δημόσιου τομέα είναι η διασφάλιση της ανεξαρτησίας και της αντικειμενικότητας στο έργο τους. Ως δημόσιοι υπάλληλοι, οι εσωτερικοί ελεγκτές μπορεί να αντιμετωπίσουν πιέσεις ή συγκρούσεις συμφερόντων που θα μπορούσαν να θέσουν σε κίνδυνο την ικανότητά τους να παρέχουν αμερόληπτες και αντικειμενικές αξιολογήσεις των λειτουργιών των οργανισμών τους (Kirkpatrick, 2003). Για την αντιμετώπιση αυτής της πρόκλησης, οι εσωτερικοί ελεγκτές πρέπει να τηρούν τα ηθικά πρότυπα και να διατηρούν επαγγελματική απόσταση από τη διοίκηση των οργανισμών τους (Morales-Sánchez&García-Sánchez, 2016). Επιπρόσθετα, οι εσωτερικοί ελεγκτές είναι αναγκαίο να είναι ελεύθεροι να χρησιμοποιήσουν και να κάνουν ευρέως γνωστά τα ευρήματά και τις συστάσεις τους χωρίς φόβο αντιποίνων και η εργασία τους πρέπει να υπόκειται σε κατάλληλη επίβλεψη και επανεξέταση (IAASB, 2013).

Μια άλλη πρόκληση για τον εσωτερικό έλεγχο του δημόσιου τομέα είναι η οικοδόμηση και η διατήρηση της ικανότητας και της εμπειρογνομosύνης που απαιτούνται για την αποτελεσματική εκπλήρωση των ρόλων τους. Οι οργανισμοί του δημόσιου τομέα αντιμετωπίζουν συχνά περιορισμούς πόρων, συμπεριλαμβανομένων περιορισμένων προϋπολογισμών και προσωπικού, που μπορεί να εμποδίσουν την ικανότητα των εσωτερικών ελεγκτών να διενεργούν ελέγχους και να παρέχουν συστάσεις προστιθέμενης αξίας (Borgonovoetal., 2016). Για να ξεπεραστεί αυτή η πρόκληση, οι εσωτερικοί ελεγκτές του δημόσιου τομέα πρέπει να συμμετέχουν σε συνεχή επαγγελματική ανάπτυξη και κατάρτιση για να παραμένουν ενήμεροι για τα αναδυόμενα ζητήματα, τις τεχνολογίες και τις βέλτιστες πρακτικές στον τομέα τους (IIA, 2019). Επιπλέον, οι οργανισμοί του δημόσιου τομέα πρέπει να δώσουν προτεραιότητα στους απαραίτητους πόρους για τη δημιουργία και τη διατήρηση μιας ικανής και αποτελεσματικής λειτουργίας εσωτερικού ελέγχου.

Οι εσωτερικοί ελεγκτές του δημόσιου τομέα πρέπει επίσης να συντονίζονται και να συνεργάζονται αποτελεσματικά με εξωτερικούς ελεγκτές, όπως οι νομοθετικοί ελεγκτές, για να αποφευχθεί η αλληλεπικάλυψη των προσπαθειών και να διασφαλιστεί ότι τα ευρήματα και οι συστάσεις του ελέγχου είναι συνεπείς και περιεκτικές (Hendriksen&VanBreda, 2013). Η αποτελεσματική συνεργασία μπορεί

επίσης να βοηθήσει στον εντοπισμό ευκαιριών για μόχλευση πόρων εξωτερικού ελέγχου, όπως εξειδικευμένη τεχνογνωσία ή τεχνολογία, για την ενίσχυση της αποτελεσματικότητας και της αποδοτικότητας του έργου εσωτερικού ελέγχου (Vinten, 2015).

Επιπλέον, οι εξελίξεις στην τεχνολογία και στην ανάλυση δεδομένων προσφέρουν σημαντικές ευκαιρίες για τον εσωτερικό έλεγχο του δημόσιου τομέα για τη βελτίωση της αποτελεσματικότητας και της αποδοτικότητάς τους (IIA, 2018). Αξιοποιώντας εργαλεία τεχνολογίας και ανάλυση δεδομένων, οι εσωτερικοί ελεγκτές μπορούν να αναλύσουν μεγάλους όγκους δεδομένων, να εντοπίσουν πρότυπα και ανωμαλίες και να αποκτήσουν γνώσεις για πιθανούς κινδύνους και τομείς προς βελτίωση (Swartz, 2016). Ωστόσο, η υιοθέτηση της τεχνολογίας και της ανάλυσης δεδομένων παρουσιάζει επίσης προκλήσεις, συμπεριλαμβανομένης της ανάγκης για εξειδικευμένες δεξιότητες, κατάλληλη εκπαίδευση και επαρκείς πόρους για την εφαρμογή και τη διατήρηση τεχνολογικών λύσεων.

Τέλος, ο εσωτερικός έλεγχος του δημόσιου τομέα διαδραματίζει κρίσιμο ρόλο στην προώθηση της διαφάνειας, της λογοδοσίας και της χρηστής διακυβέρνησης στους κυβερνητικούς οργανισμούς. Οι εσωτερικοί ελεγκτές πρέπει να κοινοποιούν τα ευρήματά τους και τις συστάσεις τους με σαφήνεια και αποτελεσματικότητα στη διοίκηση των οργανισμών τους και σε άλλα ενδιαφερόμενα μέρη (IAASB, 2013). Με αυτόν τον τρόπο, μπορούν να συμβάλουν στην οικοδόμηση της εμπιστοσύνης του κοινού στην αποτελεσματικότητα και αποδοτικότητα των κυβερνητικών λειτουργιών, ενισχύοντας τη λογοδοσία και τη διαφάνεια των οργανισμών του δημόσιου τομέα.

Συμπερασματικά, ο εσωτερικός έλεγχος του δημόσιου τομέα αντιμετωπίζει διάφορες προκλήσεις και ευκαιρίες στον ρόλο του να παρέχει υπηρεσίες διασφάλισης και συμβουλευτικής σε κυβερνητικούς οργανισμούς. Αυτές οι προκλήσεις περιλαμβάνουν τη διασφάλιση της ανεξαρτησίας και της αντικειμενικότητας, την οικοδόμηση και διατήρηση ικανότητας και εμπειρογνωμοσύνης, τον συντονισμό και τη συνεργασία με εξωτερικούς ελεγκτές, την υιοθέτηση τεχνολογίας και ανάλυσης δεδομένων και την προώθηση της διαφάνειας, της λογοδοσίας και της χρηστής διακυβέρνησης. Αντιμετωπίζοντας αυτές τις προκλήσεις και αξιοποιώντας αυτές τις ευκαιρίες, είναι δυνατό να ενισχυθεί η αποτελεσματικότητά των εσωτερικών ελεγκτών έτσι ώστε να συνεισφέρουν ουσιαστικά στους οργανισμούς τους. Αυτές οι



προσπάθειες μπορούν τελικά να συμβάλουν στη βελτίωση της ποιότητας, της αποδοτικότητας και της αποτελεσματικότητας των κυβερνητικών λειτουργιών.

## **2. Η κυβερνο-ασφάλεια και η σύνδεσή της με τον εσωτερικό έλεγχο. Η περίπτωση του δημόσιου τομέα και των Δήμων.**

### **2.1. Η έννοια της Κυβερνοασφάλειας με έμφαση στον δημόσιο τομέα και τους δήμους**

Η κυβερνοασφάλεια έχει αναδειχθεί ως κρίσιμη ανησυχία για τον δημόσιο τομέα, με τις κυβερνήσεις σε όλα τα επίπεδα να αναγνωρίζουν την ανάγκη προστασίας της ψηφιακής τους υποδομής, των ευαίσθητων δεδομένων και του απορρήτου των πολιτών (Alcaraz&Zeadally, 2015). Η σημασία της κυβερνοασφάλειας για τους δήμους δεν μπορεί να υποκτιμηθεί, καθώς οι τοπικές κυβερνήσεις συχνά διαθέτουν πλήθος ευαίσθητων πληροφοριών και παρέχουν βασικές υπηρεσίες στους πολίτες τους (Harrison&Guerrero, 2019). Οι δήμοι είναι υπεύθυνοι για τη διατήρηση της ασφάλειας των κοινοτήτων τους, και στον σημερινό διασυνδεδεμένο ψηφιακό κόσμο, αυτό περιλαμβάνει προστασία έναντι των απειλών στον κυβερνοχώρο (Kshetri&Voas, 2017; Galanis&Pazarskis, 2022).

Η ανάγκη για ισχυρά μέτρα κυβερνοασφάλειας έχει γίνει ολοένα και πιο εμφανής καθώς οι δήμοι σε όλο τον κόσμο έχουν βιώσει περιστατικά στον κυβερνοχώρο υψηλού προφίλ κινδύνου (Gordon, 2020). Αυτά τα περιστατικά έχουν διαταράξει βασικές υπηρεσίες, έχουν θέσει σε κίνδυνο ευαίσθητα δεδομένα και έχουν οδηγήσει σε σημαντικές οικονομικές ζημιές (Romanoskyetal., 2019). Ο δημόσιος τομέας, ιδιαίτερα σε δημοτικό επίπεδο, στοχεύεται συχνά λόγω των πολύτιμων πληροφοριών που διαθέτει και της αντιληπτής ευαλωτότητάς του, καθώς πολλές τοπικές κυβερνήσεις έχουν περιορισμένους πόρους και τεχνογνωσία για να αμυνθούν σε εξελιγμένες κυβερνοεπιθέσεις (Finklea&Jaikaran, 2017).

Μία από τις βασικές προκλήσεις που αντιμετωπίζουν οι δήμοι για την αντιμετώπιση της κυβερνοασφάλειας είναι η απόλυτη πολυπλοκότητα του τοπίου των απειλών (Savageetal., 2015). Οι εγκληματίες του κυβερνοχώρου αναπτύσσουν συνεχώς νέες τεχνικές και τακτικές, οι οποίες μπορεί να δυσκολέψουν τους οργανισμούς του δημόσιου τομέα να παραμείνουν μπροστά από τις αναδυόμενες απειλές (Shackelford, 2016). Επιπλέον, η ευρεία υιοθέτηση της ψηφιακής

τεχνολογίας έχει επεκτείνει το εύρος της επίθεσης για εγκληματίες του κυβερνοχώρου (Cavelty, 2018). Ως αποτέλεσμα, οι δήμοι πρέπει τώρα να εξασφαλίσουν μια συνεχώς αυξανόμενη σειρά ψηφιακών στοιχείων, από διαδικτυακές πύλες και έξυπνες υποδομές πόλεων έως συστήματα αποθήκευσης και απομακρυσμένης εργασίας που βασίζονται σε cloud (Ανθόπουλος, 2017).

Μια άλλη πρόκληση που αντιμετωπίζουν οι δήμοι είναι η έλλειψη επαρκών δεξιοτήτων και τεχνογνωσίας στον τομέα της κυβερνοασφάλειας εντός των οργανισμών τους (Boin&Rhinar, 2018). Ο δημόσιος τομέας έχει παλέψει ιστορικά να προσελκύσει και να διατηρήσει ειδικευμένους επαγγελματίες στον τομέα της κυβερνοασφάλειας, οι οποίοι συχνά έλκονται από πιο προσοδοφόρες ευκαιρίες στον ιδιωτικό τομέα (Egan, 2017). Αυτό το κενό δεξιοτήτων μπορεί να αφήσει τους δήμους ανεπαρκείς για τη διαχείριση των ολοένα και πιο εξελιγμένων απειλών που αντιμετωπίζουν και να εμποδίσει την ικανότητά τους να αναπτύσσουν και να εφαρμόζουν αποτελεσματικές στρατηγικές κυβερνοασφάλειας (Kesanel., 2017).

Ένα σχετικό ζήτημα είναι η ανάγκη για μεγαλύτερη συνεργασία και ανταλλαγή πληροφοριών μεταξύ των οργανισμών του δημόσιου τομέα (Kesanel., 2017). Οι δήμοι μπορούν να επωφεληθούν από την ανταλλαγή βέλτιστων πρακτικών, πληροφοριών σχετικά με τις απειλές και διδάγματα που αντλήθηκαν από περιστατικά στον κυβερνοχώρο (Savageetal., 2015). Ωστόσο, ανησυχίες σχετικά με το απόρρητο και την ασφάλεια των δεδομένων, καθώς και τα γραφειοκρατικά και οργανωτικά εμπόδια, μπορεί μερικές φορές να εμποδίσουν μια τέτοια συνεργασία (Boin&Rhinar, 2018). Η ενθάρρυνση της μεγαλύτερης συνεργασίας, τόσο εντός του δημόσιου τομέα όσο και με εταίρους του ιδιωτικού τομέα, είναι ζωτικής σημασίας για την ενίσχυση της ανθεκτικότητας των δήμων στον κυβερνοχώρο (Kesanel., 2017).

Η χρηματοδότηση είναι μια άλλη σημαντική πρόκληση για τους δήμους καθώς προσπαθούν να ενισχύσουν τη στάση τους στον κυβερνοχώρο (Harrison&Guerrero, 2019). Η εφαρμογή ισχυρών μέτρων κυβερνοασφάλειας μπορεί να είναι δαπανηρή και πολλές τοπικές κυβερνήσεις αντιμετωπίζουν δημοσιονομικούς περιορισμούς που περιορίζουν την ικανότητά τους να επενδύσουν στην απαραίτητη τεχνολογία, προσωπικό και εκπαίδευση (Finklea&Jaikaran, 2017). Αυτή η έλλειψη πόρων μπορεί να αφήσει τους δήμους ευάλωτους σε απειλές στον κυβερνοχώρο και

να τους δυσκολέψει να ανταποκριθούν αποτελεσματικά όταν συμβαίνουν περιστατικά (Romanoskyetal., 2019).

Τέλος, είναι σημαντικό να αναγνωριστεί ο ρόλος της εμπλοκής και της ευαισθητοποίησης των πολιτών στην ενίσχυση της δημοτικής κυβερνοασφάλειας (Kshetri&Voas, 2017). Οι πολίτες είναι συχνά η πρώτη γραμμή άμυνας έναντι των απειλών στον κυβερνοχώρο, καθώς μπορούν να βοηθήσουν στον εντοπισμό και την αναφορά ύποπτης δραστηριότητας (Ανθόπουλος, 2017). Ωστόσο, πολλοί άνθρωποι αγνοούν τους κινδύνους που συνδέονται με τις απειλές στον κυβερνοχώρο και τα βήματα που μπορούν να λάβουν για να προστατεύσουν τον εαυτό τους και τις κοινότητές τους (Ανθόπουλος, 2017). Οι δήμοι πρέπει επομένως να επενδύσουν σε πρωτοβουλίες εκπαίδευσης και ευαισθητοποίησης στον τομέα της κυβερνοασφάλειας για να καλλιεργήσουν μια κουλτούρα επαγρύπνησης και ετοιμότητας μεταξύ των πολιτών τους (Kshetri&Voas, 2017).

Συμπερασματικά, η σημασία της κυβερνοασφάλειας για τους δήμους δεν μπορεί να υποεκτιμηθεί, καθώς είναι υπεύθυνοι για την προστασία ευαίσθητων πληροφοριών και την παροχή βασικών υπηρεσιών στις κοινότητές τους (Harrison&Guerrero, 2019). Η αντιμετώπιση των βασικών προκλήσεων που αντιμετωπίζει ο δημόσιος τομέας, όπως η πολυπλοκότητα του τοπίου της απειλής, το χάσμα δεξιοτήτων και οι περιορισμένοι πόροι, θα είναι ζωτικής σημασίας για την ενίσχυση της ανθεκτικότητας στον κυβερνοχώρο των τοπικών κυβερνήσεων και την προστασία των πολιτών που εξυπηρετούν (Kesanetal., 2017).

## **2.2 Τύποι και περιπτώσεις παραβίασης της κυβερνοασφάλειας σε δήμους**

Οι δήμοι σε όλο τον κόσμο αντιμετωπίζουν ένα ποικίλο και εξελισσόμενο φάσμα απειλών στον κυβερνοχώρο που θέτουν σημαντικές προκλήσεις για τις δραστηριότητές τους και την ακεραιότητα ευαίσθητων δεδομένων (Gordon, 2020). Η κατανόηση του τοπίου των απειλών στον κυβερνοχώρο είναι απαραίτητη για τις τοπικές κυβερνήσεις να αναπτύξουν και να εφαρμόσουν αποτελεσματικές

στρατηγικές κυβερνοασφάλειας για την προστασία των ψηφιακών τους περιουσιακών στοιχείων και τη διατήρηση της εμπιστοσύνης του κοινού (Alcaraz&Zeadally, 2015).

Οι συνήθεις τύποι απειλών στον κυβερνοχώρο που επηρεάζουν τους δήμους περιλαμβάνουν ransomware, phishing, επιθέσεις κατανεμημένης άρνησης υπηρεσίας (DDoS) και παραβιάσεις δεδομένων (Kshetri&Voas, 2017). Οι επιθέσεις ransomware, ειδικότερα, έχουν γίνει όλο και πιο διαδεδομένες και ενοχλητικές, καθώς οι εγκληματίες του κυβερνοχώρου κρυπτογραφούν κρίσιμα δεδομένα και συστήματα, απαιτώντας πληρωμή σε αντάλλαγμα για κλειδιά αποκρυπτογράφησης (Romanoskyetal., 2019). Αυτές οι επιθέσεις μπορεί να έχουν σοβαρές συνέπειες για τις τοπικές κυβερνήσεις, οδηγώντας σε απώλεια ευαίσθητων δεδομένων, οικονομικό κόστος και διακοπές σε βασικές υπηρεσίες (Gordon, 2020).

Οι επιθέσεις phishing, μια άλλη κοινή απειλή, εκμεταλλεύονται τα ανθρώπινα τρωτά σημεία χρησιμοποιώντας παραπλανητικές τακτικές για να εξαπατήσουν τα άτομα ώστε να αποκαλύψουν ευαίσθητες πληροφορίες ή να κάνουν κλικ σε κακόβουλους συνδέσμους (Savageetal., 2015). Οι δημοτικοί υπάλληλοι στοχοποιούνται συχνά σε αυτές τις επιθέσεις, καθώς μπορεί να έχουν πρόσβαση σε πολύτιμα δεδομένα ή συστήματα (Shackelford, 2016). Οι επιθέσεις DDoS, από την άλλη πλευρά, περιλαμβάνουν τη συντριβή του δικτύου ή του διακομιστή ενός στόχου, καθιστώντας τον απρόσιτο στους νόμιμους χρήστες (Alcaraz&Zeadally, 2015). Οι παραβιάσεις δεδομένων περιλαμβάνουν μη εξουσιοδοτημένη πρόσβαση ή αποκάλυψη ευαίσθητων δεδομένων, η οποία μπορεί να οδηγήσει σε βλάβη της φήμης, οικονομικές απώλειες και νομικές συνέπειες (Romanoskyetal., 2019).

Αρκετές περιπτωσιολογικές μελέτες δείχνουν τον αντίκτυπο των περιστατικών κυβερνοασφάλειας στους δήμους. Η επίθεση ransomwareWannaCry του 2017, για παράδειγμα, επηρέασε πολλούς οργανισμούς του δημόσιου τομέα παγκοσμίως, συμπεριλαμβανομένων νοσοκομείων, σχολείων και τοπικών κυβερνήσεων (Finklea&Jaikaran, 2017). Η επίθεση εκμεταλλεύτηκε μια ευπάθεια στα Microsoft Windows και κρυπτογραφημένα δεδομένα στα επηρεαζόμενα συστήματα, προκαλώντας εκτεταμένες διακοπές στις υπηρεσίες και σημαντικό οικονομικό κόστος (Finklea&Jaikaran, 2017). Ένα άλλο αξιοσημείωτο παράδειγμα είναι η κυβερνοεπίθεση του 2018 στην πόλη της Ατλάντα στις Ηνωμένες Πολιτείες, όπου το SamSamransomware κρυπτογραφούσε δεδομένα της πόλης και ζήτησε πληρωμή

λύτρων (Harrison&Guerrero, 2019). Η επίθεση διέκοψε βασικές υπηρεσίες, συμπεριλαμβανομένων των διαδικτυακών συστημάτων πληρωμών της πόλης, των δικαστικών υπηρεσιών και των αστυνομικών επιχειρήσεων, και είχε ως αποτέλεσμα εκατομμύρια δολάρια σε κόστος ανάκτησης (Harrison&Guerrero, 2019).

Μια άλλη μελέτη περίπτωσης περιλαμβάνει μια σειρά επιθέσεων DDoS εναντίον ιστοσελίδων αρκετών δήμων της Εσθονίας το 2007, οι οποίες αποδόθηκαν σε χάκερ (Cavelty, 2018). Αυτές οι επιθέσεις διέκοψαν τις διαδικτυακές υπηρεσίες και προκάλεσαν μια εθνική προσπάθεια για την ενίσχυση της υποδομής και της ανθεκτικότητας στον κυβερνοχώρο της Εσθονίας (Cavelty, 2018). Τέλος, η παραβίαση του Γραφείου Διαχείρισης Προσωπικού (OPM) του 2016 στις Ηνωμένες Πολιτείες, αν και δεν αφορά συγκεκριμένο δήμο, προσφέρει πληροφορίες για τους κινδύνους που σχετίζονται με παραβιάσεις δεδομένων στον δημόσιο τομέα (Kesanetal., 2017). Η παραβίαση αποκάλυψε ευαίσθητες προσωπικές πληροφορίες εκατομμυρίων νυν και πρώην ομοσπονδιακών υπαλλήλων, υπογραμμίζοντας την πιθανότητα σημαντικής βλάβης όταν διακυβεύονται τα δεδομένα του δημόσιου τομέα (Kesanetal., 2017).

Συμπερασματικά, το τοπίο απειλών στον κυβερνοχώρο για τους δήμους είναι περίπλοκο και συνεχώς εξελίσσεται, με ransomware, phishing, επιθέσεις DDoS και παραβιάσεις δεδομένων που θέτουν σημαντικές προκλήσεις για τις τοπικές κυβερνήσεις (Kshetri&Voas, 2017). Κατανοώντας τη φύση και τον αντίκτυπο αυτών των απειλών, όπως φαίνεται από διάφορες περιπτώσιολογικές μελέτες, οι δήμοι μπορούν να αναπτύξουν πιο αποτελεσματικές στρατηγικές κυβερνοασφάλειας για να προστατεύσουν τα ψηφιακά τους στοιχεία, τα ευαίσθητα δεδομένα και τις κοινότητες που εξυπηρετούν (Alcaraz&Zeadally, 2015).

### **2.3 Εσωτερικός έλεγχος και κυβερνοασφάλεια**

Ο εσωτερικός έλεγχος διαδραματίζει κρίσιμο ρόλο βοηθώντας τους δήμους να διαχειριστούν το τοπίο της κυβερνοαπειλής αξιολογώντας την αποτελεσματικότητα των ελέγχων τους στον κυβερνοχώρο, εντοπίζοντας τρωτά σημεία και προτείνοντας βελτιώσεις (Beresfordetal., 2018). Καθώς οι τοπικές κυβερνήσεις βασίζονται όλο και

περισσότερο στις ψηφιακές τεχνολογίες για την παροχή υπηρεσιών και τη διαχείριση ευαίσθητων πληροφοριών, οι λειτουργίες εσωτερικού ελέγχου πρέπει να προσαρμοστούν για την αντιμετώπιση των μοναδικών κινδύνων και προκλήσεων που σχετίζονται με τις απειλές στον κυβερνοχώρο (Kshetri&Voas, 2017).

Μία από τις βασικές αρμοδιότητες των εσωτερικών ελεγκτών στο πλαίσιο της κυβερνοασφάλειας είναι η αξιολόγηση της επάρκειας των πολιτικών και διαδικασιών ασφάλειας πληροφοριών ενός οργανισμού (Beresfordetal., 2018). Αυτό περιλαμβάνει την αξιολόγηση της εφαρμογής των ελέγχων ασφαλείας, όπως η κρυπτογράφηση, οι έλεγχοι πρόσβασης και τα σχέδια αντιμετώπισης περιστατικών, και η διασφάλιση ότι είναι ευθυγραμμισμένα με τις βέλτιστες πρακτικές του κλάδου και τις κανονιστικές απαιτήσεις (Alcaraz&Zeadally, 2015). Οι εσωτερικοί ελεγκτές μπορούν επίσης να βοηθήσουν τους δήμους να εντοπίσουν πιθανούς τομείς αδυναμίας στη στάση τους στον κυβερνοχώρο, όπως το ξεπερασμένο λογισμικό, η ανεπαρκής εκπαίδευση των εργαζομένων ή η ανεπαρκής τμηματοποίηση του δικτύου (Gordon, 2020).

Εκτός από την αξιολόγηση της αποτελεσματικότητας των υφιστάμενων ελέγχων, οι εσωτερικοί ελεγκτές διαδραματίζουν κρίσιμο ρόλο στην προώθηση μιας κουλτούρας συνειδητοποίησης και ετοιμότητας για την ασφάλεια στον κυβερνοχώρο εντός των δήμων (Shackelford, 2016). Αυτό περιλαμβάνει την παροχή καθοδήγησης σχετικά με τις αναδυόμενες απειλές στον κυβερνοχώρο και τη σύσταση στρατηγικών για τον μετριασμό τους, όπως η εφαρμογή ελέγχου ταυτότητας πολλαπλών παραγόντων, η διεξαγωγή τακτικών αξιολογήσεων ευπάθειας και η παροχή εκπαίδευσης εργαζομένων στις βέλτιστες πρακτικές κυβερνοασφάλειας (Savageetal., 2015). Οι εσωτερικοί ελεγκτές μπορούν επίσης να διευκολύνουν την ανταλλαγή πληροφοριών και τη συνεργασία μεταξύ διαφορετικών τμημάτων ενός δήμου για να εξασφαλίσουν μια συντονισμένη και ολοκληρωμένη προσέγγιση στην ασφάλεια στον κυβερνοχώρο (Beresfordetal., 2018).

Επιπλέον, οι εσωτερικοί ελεγκτές μπορούν να υποστηρίξουν τους δήμους στη διαχείριση των κινδύνων που σχετίζονται με τρίτους προμηθευτές, μια κοινή πηγή απειλών στον κυβερνοχώρο (Romanoskyetal., 2019). Διενεργώντας αξιολογήσεις δέουσας επιμέλειας και παρακολουθώντας τις πρακτικές κυβερνοασφάλειας των πωλητών, οι εσωτερικοί ελεγκτές μπορούν να βοηθήσουν τους δήμους να

διασφαλίσουν ότι οι αλυσίδες εφοδιασμού τους είναι ασφαλείς και ότι τα ευαίσθητα δεδομένα προστατεύονται επαρκώς (Kesanel., 2017).

Αρκετές περιπτωσιολογικές μελέτες καταδεικνύουν τη σημασία του εσωτερικού ελέγχου για την αντιμετώπιση του τοπίου της κυβερνοαπειλής για τους δήμους. Στον απόηχο της επίθεσης ransomware WannaCry του 2017, οι εσωτερικοί ελεγκτές είχαν καίρια θέση καθώς βοήθησαν τους επηρεαζόμενους οργανισμούς να εκτιμήσουν τη ζημιά, να εντοπίσουν τρωτά σημεία στους ελέγχους κυβερνοασφάλειάς τους και να αναπτύξουν στρατηγικές για την πρόληψη μελλοντικών συμβάντων (Finklea&Jaikaran, 2017). Ομοίως, μετά την κυβερνοεπίθεση του 2018 στην πόλη της Ατλάντα, οι εσωτερικοί ελεγκτές έπαιξαν καθοριστικό ρόλο στη διεξαγωγή μιας συνολικής ανασκόπησης της στάσης της πόλης στον κυβερνοχώρο και στην πρόταση βελτιώσεων για την πρόληψη μελλοντικών επιθέσεων (Harrison&Guerrero, 2019).

Συμπερασματικά, ο εσωτερικός έλεγχος είναι απαραίτητος για τους δήμους οι οποίοι επιδιώκουν να περιηγηθούν στο περίπλοκο και εξελισσόμενο τοπίο απειλών στον κυβερνοχώρο (Beresfordetal., 2018). Αξιολογώντας την αποτελεσματικότητα των ελέγχων κυβερνοασφάλειας, προωθώντας μια κουλτούρα ετοιμότητας και βοηθώντας στη διαχείριση κινδύνων τρίτων, οι εσωτερικοί ελεγκτές μπορούν να υποστηρίξουν τις τοπικές κυβερνήσεις στην ενίσχυση της ανθεκτικότητάς τους στον κυβερνοχώρο και στην προστασία των ευαίσθητων δεδομένων και των βασικών υπηρεσιών που παρέχουν (Kshetri&Voas, 2017).

## **2.4 Διαστάσεις του εσωτερικού ελέγχου που σχετίζονται με την κυβερνοασφάλεια**

### **2.4.1 Συμβουλευτικός Ρόλος Εσωτερικών Ελέγχων στην Κυβερνοασφάλεια για τους Δήμους**

Οι εσωτερικοί έλεγχοι μπορούν να διαδραματίσουν ζωτικό συμβουλευτικό ρόλο για την ενίσχυση της κυβερνοασφάλειας εντός των δήμων παρέχοντας



ανεξάρτητη διασφάλιση και συστάσεις σχετικά με την αποτελεσματικότητα των πολιτικών, διαδικασιών και ελέγχων στον κυβερνοχώρο του οργανισμού (Alles, 2018). Οι εσωτερικοί ελεγκτές μπορούν να βοηθήσουν τους δήμους να εντοπίσουν πιθανές ευπάθειες και τομείς για βελτίωση της στάσης τους στον κυβερνοχώρο, διασφαλίζοντας την προστασία των ευαίσθητων πληροφοριών και την ανθεκτικότητα των κρίσιμων συστημάτων.

Μια βασική πτυχή του συμβουλευτικού ρόλου των εσωτερικών ελέγχων στην κυβερνοασφάλεια είναι η αξιολόγηση της συμμόρφωσης του δήμου με σχετικούς νόμους, κανονισμούς και πρότυπα, όπως ο “Γενικός Κανονισμός για την Προστασία Δεδομένων της ΕΕ” (GDPR) (Voigt&vondemBussche, 2017). Οι εσωτερικοί ελεγκτές μπορούν να επανεξετάσουν τις πολιτικές και τις πρακτικές προστασίας δεδομένων του οργανισμού για να διασφαλίσουν τη συμμόρφωση, να εντοπίσουν πιθανά κενά και να παρέχουν συστάσεις για την αντιμετώπιση αυτών των θεμάτων.

Η διαχείριση κινδύνων είναι ένας άλλος τομέας όπου η συμβολή των εσωτερικών ελεγκτών είναι πολύτιμη για την ασφάλεια στον κυβερνοχώρο. Με τον εντοπισμό, την αξιολόγηση και την ιεράρχηση των κινδύνων στον κυβερνοχώρο, οι εσωτερικοί ελεγκτές μπορούν να βοηθήσουν τους δήμους να αναπτύξουν αποτελεσματικές στρατηγικές μετριασμού και αντιμετώπισης του κινδύνου, διασφαλίζοντας την ετοιμότητα του οργανισμού για πιθανές απειλές στον κυβερνοχώρο (Alles, 2018). Αυτή η διαδικασία μπορεί να περιλαμβάνει την αξιολόγηση της αποτελεσματικότητας των υφιστάμενων πρακτικών διαχείρισης κινδύνου και την πρόταση βελτιώσεων με βάση τις βέλτιστες πρακτικές και τα πρότυπα του κλάδου.

Εκτός από τη διαχείριση κινδύνου, οι εσωτερικοί ελεγκτές μπορούν να υποστηρίξουν τους δήμους στην ανάπτυξη και εφαρμογή πολιτικών και διαδικασιών κυβερνοασφάλειας, διασφαλίζοντας μια ολοκληρωμένη προσέγγιση για την προφύλαξη της ψηφιακής περιουσίας και των υποδομών του οργανισμού (Alles, 2018). Αυτό μπορεί να περιλαμβάνει την παροχή καθοδήγησης για την υιοθέτηση πλαισίων ασφαλείας, όπως το Πλαίσιο Κυβερνοασφάλειας NIST, και βοήθεια στην ανάπτυξη σχεδίων αντιμετώπισης περιστατικών για να διασφαλιστεί η ταχεία και συντονισμένη απόκριση σε πιθανά συμβάντα στον κυβερνοχώρο (Siponen, 2016).

Τέλος, οι εσωτερικοί ελεγκτές μπορούν να διαδραματίσουν κρίσιμο ρόλο στην προώθηση μιας κουλτούρας ευαισθητοποίησης και κατάρτισης για την ασφάλεια στον κυβερνοχώρο στους δήμους. Με την αξιολόγηση της αποτελεσματικότητας των υφιστάμενων προγραμμάτων εκπαίδευσης στον κυβερνοχώρο και την παροχή συστάσεων για βελτίωση, οι εσωτερικοί ελεγκτές μπορούν να βοηθήσουν να διασφαλιστεί ότι οι εργαζόμενοι είναι καλά εξοπλισμένοι για τον εντοπισμό, την πρόληψη και την ανταπόκριση σε απειλές στον κυβερνοχώρο (Alles, 2018).

#### **2.4.2 Ο ρόλος των εσωτερικών ελέγχων στην ενίσχυση της τεχνολογικής γνώσης και της κυβερνοασφάλειας στους δήμους**

Οι εσωτερικοί έλεγχοι διαδραματίζουν κρίσιμο ρόλο στην ενίσχυση της τεχνολογικής γνώσης και της κυβερνοασφάλειας στους δήμους παρέχοντας ανεξάρτητες υπηρεσίες διασφάλισης και συμβουλευτικής σχετικά με την αποτελεσματικότητα των τεχνολογικών πρωτοβουλιών και τα σχετικά μέτρα ασφαλείας τους (Alles, 2018, Spathis&Ananiadis, 2015). Οι εσωτερικοί ελεγκτές μπορούν να βοηθήσουν τους δήμους να εντοπίσουν πιθανά κενά στην τεχνολογική γνώση και την ασφάλεια στον κυβερνοχώρο, να προτείνουν βέλτιστες πρακτικές για την ασφαλή υιοθέτηση νέων τεχνολογιών και να διασφαλίσουν ότι οι τεχνολογικές επενδύσεις ευθυγραμμίζονται με τους οργανωτικούς στόχους και στόχους (Weistroffer, Smith, & Narula, 2016).

Ένας τρόπος με τον οποίο οι εσωτερικοί ελεγκτές συμβάλλουν στην ενίσχυση της τεχνολογικής γνώσης και της ασφάλειας στον κυβερνοχώρο είναι μέσω της αξιολόγησης της δομής διακυβέρνησης της πληροφορικής του δήμου, συμπεριλαμβανομένης της ενσωμάτωσης των πολιτικών για την κυβερνοασφάλεια (Weistrofferetal., 2016). Αξιολογώντας την αποτελεσματικότητα του πλαισίου διακυβέρνησης, οι εσωτερικοί ελεγκτές μπορούν να παρέχουν συστάσεις για τη βελτίωση των διαδικασιών λήψης αποφάσεων, την καλλιέργεια μιας κουλτούρας συνεχούς βελτίωσης και τη διασφάλιση της σωστής κατανομής των πόρων τόσο για πρωτοβουλίες τεχνολογίας όσο και για πρωτοβουλίες κυβερνοασφάλειας (Alles, 2018).

Οι εσωτερικοί ελεγκτές μπορούν επίσης να υποστηρίξουν τους δήμους στην υλοποίηση και διαχείριση τεχνολογικών έργων, λαμβάνοντας παράλληλα υπόψη τους κινδύνους για την ασφάλεια στον κυβερνοχώρο. Παρέχοντας καθοδήγηση σχετικά με τις βέλτιστες πρακτικές διαχείρισης έργων και διασφαλίζοντας ότι τα μέτρα κυβερνοασφάλειας ενσωματώνονται σε όλο τον κύκλο ζωής του έργου, οι εσωτερικοί ελεγκτές μπορούν να βοηθήσουν τους δήμους να ελαχιστοποιήσουν τον κίνδυνο καθυστερήσεων έργων, υπέρβασης κόστους και παραβιάσεων ασφάλειας (Spathis&Ananiadis, 2015; Alles, 2018).

Τέλος, οι εσωτερικοί ελεγκτές μπορούν να διαδραματίσουν ζωτικό ρόλο στην προώθηση μιας κουλτούρας μάθησης και συνεχούς βελτίωσης εντός των δήμων όσον αφορά τόσο την τεχνολογική γνώση όσο και την ευαισθητοποίηση για την ασφάλεια στον κυβερνοχώρο (Alles, 2018). Με την αξιολόγηση της αποτελεσματικότητας των υφιστάμενων προγραμμάτων κατάρτισης, τον εντοπισμό κενών δεξιοτήτων και την παροχή συστάσεων για βελτίωση, οι εσωτερικοί ελεγκτές μπορούν να βοηθήσουν να διασφαλιστεί ότι οι εργαζόμενοι είναι καλά εξοπλισμένοι να υιοθετούν, να χρησιμοποιούν και να διασφαλίζουν αποτελεσματικά τις νέες τεχνολογίες (Mergel, 2016).

#### **2.4.3. Ρόλος των Εσωτερικών Ελέγχων στην Ενίσχυση της Συνεργασίας που σχετίζεται με την Κυβερνοασφάλεια στους Δήμους**

Οι εσωτερικοί έλεγχοι διαδραματίζουν σημαντικό ρόλο στην ενίσχυση της συνεργασίας που σχετίζεται με την κυβερνοασφάλεια εντός των δήμων παρέχοντας ανεξάρτητες υπηρεσίες διασφάλισης και συμβουλευτικής που προάγουν τη διαφάνεια, τη λογοδοσία και τη συνεργασία μεταξύ διαφορετικών τμημάτων, φορέων και ενδιαφερομένων (Alles, 2018). Μέσω των ελέγχων τους, οι εσωτερικοί ελεγκτές μπορούν να βοηθήσουν στον εντοπισμό πιθανών εμποδίων στη συνεργασία, να προτείνουν στρατηγικές για βελτιωμένη συνεργασία και να διασφαλίσουν ότι οι πολιτικές και οι διαδικασίες κυβερνοασφάλειας ενθαρρύνουν μια κουλτούρα συνεργασίας (Gordonetal., 2015).

Ένας τρόπος με τον οποίο οι εσωτερικοί ελεγκτές μπορούν να συμβάλουν στην ενισχυμένη συνεργασία που σχετίζεται με την κυβερνοασφάλεια εντός των δήμων είναι η αξιολόγηση της αποτελεσματικότητας των μηχανισμών ανταλλαγής πληροφοριών και των συνεργατικών πρωτοβουλιών (Kshetri, 2018). Εντοπίζοντας πιθανά κενά και παρέχοντας συστάσεις για τη βελτίωση της ανταλλαγής πληροφοριών και των κοινών προσπάθειών στον τομέα της κυβερνοασφάλειας, οι εσωτερικοί ελεγκτές μπορούν να συμβάλουν στην ενίσχυση ενός πιο συνεργατικού περιβάλλοντος στο οποίο όλοι οι ενδιαφερόμενοι μπορούν να συμβάλουν στην ανάπτυξη και εφαρμογή αποτελεσματικών μέτρων ασφαλείας

Επιπλέον, οι εσωτερικοί ελεγκτές μπορούν να διαδραματίσουν ζωτικό ρόλο στην προώθηση της ανταλλαγής γνώσεων και στην ανάπτυξη βέλτιστων πρακτικών που σχετίζονται με την κυβερνοασφάλεια σε διάφορα τμήματα και φορείς εντός των δήμων. Ακόμη, μπορούν να βοηθήσουν τους δήμους να αξιοποιήσουν τη συλλογική τους τεχνογνωσία για να αναπτύξουν καινοτόμες λύσεις σε περίπλοκες προκλήσεις ασφαλείας στον κυβερνοχώρο (Gordonetal., 2015).

#### **2.4.4. Ο ρόλος των εσωτερικών ελέγχων στην αξιολόγηση και την ενίσχυση των πολιτικών και προτύπων κυβερνοασφάλειας στους δήμους**

Μέσω των ελέγχων τους, οι εσωτερικοί ελεγκτές μπορούν να βοηθήσουν στον εντοπισμό πιθανών κενών στη συμμόρφωση με τις πολιτικές, να προτείνουν στρατηγικές για βελτίωση και να διασφαλίσουν ότι οι πολιτικές και τα πρότυπα κυβερνοασφάλειας εφαρμόζονται με συνέπεια σε ολόκληρο τον οργανισμό (Σπαθής&Ανανιάδης, 2015).

Οι εσωτερικοί ελεγκτές μπορούν να υποστηρίξουν τους δήμους στην ανάπτυξη και εφαρμογή νέων πολιτικών και προτύπων κυβερνοασφάλειας, ιδιαίτερα σε τομείς όπως η διαχείριση κινδύνου, η αντιμετώπιση περιστατικών και η προστασία δεδομένων (Kshetri, 2018). Παρέχοντας καθοδήγηση για την ανάπτυξη ολοκληρωμένων πολιτικών και προτύπων που αντιμετωπίζουν τις αναδυόμενες προκλήσεις και διασφαλίζουν βέλτιστες πρακτικές, οι εσωτερικοί ελεγκτές μπορούν

να βοηθήσουν τους δήμους να βελτιώσουν τη στάση τους στον κυβερνοχώρο και να επιτύχουν τους στρατηγικούς τους στόχους (Daskalopoulos&Tseles, 2017).

#### **2.4.5 Ενημέρωση και εκπαίδευση**

Τα αποτελεσματικά προγράμματα ενημέρωσης και κατάρτισης είναι απαραίτητα για την εύρυθμη λειτουργία των δήμων και του ευρύτερου δημόσιου τομέα, καθώς συμβάλλουν στην οικοδόμηση των απαραίτητων γνώσεων, δεξιοτήτων και ικανοτήτων των εργαζόμενων έτσι ώστε να εκτελούν τα καθήκοντά τους αποτελεσματικά και αποτελεσματικά (Hossainetal., 2019). Στην Ευρώπη και την Ελλάδα, η επένδυση σε προγράμματα ενημέρωσης και κατάρτισης είναι ζωτικής σημασίας για την προώθηση της διαφάνειας, την ενίσχυση της λογοδοσίας, την προώθηση της καινοτομίας και τη διασφάλιση της συμμόρφωσης με νόμους, κανονισμούς και πρότυπα

Ένας τρόπος με τον οποίο οι εσωτερικοί ελεγκτές μπορούν να συμβάλουν στην ενίσχυση των προγραμμάτων ενημέρωσης και κατάρτισης εντός των δήμων είναι με την αξιολόγηση της αποτελεσματικότητας των υφιστάμενων προγραμμάτων στην επίτευξη των επιδιωκόμενων αποτελεσμάτων, όπως η βελτίωση της απόδοσης των εργαζομένων, η συμμόρφωση με νόμους και κανονισμούς ή η αυξημένη καινοτομία (Hossainetal., 2019 ). Εντοπίζοντας πιθανές ελλείψεις και παρέχοντας συστάσεις για βελτίωση, οι εσωτερικοί ελεγκτές μπορούν να βοηθήσουν τους δήμους να ευθυγραμμίσουν τα προγράμματα ενημέρωσης και κατάρτισης με τους στρατηγικούς τους στόχους και στόχους.

Οι εσωτερικοί ελεγκτές μπορούν επίσης να υποστηρίξουν τους δήμους στην ανάπτυξη και εφαρμογή νέων προγραμμάτων ενημέρωσης και κατάρτισης, ιδιαίτερα σε τομείς όπως η διαχείριση κινδύνων, η διακυβέρνηση πληροφορικής και η οικονομική διαχείριση (Hossainetal., 2019). Παρέχοντας καθοδήγηση για την ανάπτυξη ολοκληρωμένων προγραμμάτων που αντιμετωπίζουν τις αναδυόμενες προκλήσεις και διασφαλίζουν βέλτιστες πρακτικές, οι εσωτερικοί ελεγκτές μπορούν να βοηθήσουν τους δήμους να βελτιώσουν τις διαδικασίες τους και να επιτύχουν τους στρατηγικούς τους στόχους.

### **3. Μεθοδολογία έρευνας**

#### **3.1. Σκοπός της έρευνας**

Σκοπός της έρευνας που πραγματοποιήθηκε στα πλαίσια εκπόνησης της παρούσας διπλωματικής εργασίας είναι η διερεύνηση των μεταβλητών που επηρεάζουν την ασφάλεια στον κυβερνοχώρο και οι οποίες, ταυτόχρονα, σχετίζονται με τον εσωτερικό έλεγχο.. Για την ικανοποίηση του σκοπού αυτού, διατυπώθηκαν τα παρακάτω ερευνητικά ερωτήματα.

#### **3.2 Τα ερευνητικά ερωτήματα**

Τα ερευνητικά ερωτήματα διατυπώνονται ως εξής.

- ✓ Ποιες είναι οι απόψεις των ερωτώμενων σχετικά με την συχνότητα της κυβερνοασφάλειας στους δήμους που απασχολούνται;
- ✓ Ποιες είναι οι απόψεις των ερωτώμενων σχετικά με την συχνότητα των διαστάσεων της σχέσης ανάμεσα στον εσωτερικό έλεγχο και την κυβερνοασφάλεια;
- ✓ Ποια είναι η συσχέτιση των μεταβλητών αυτών με τα επίπεδα κυβερνοασφάλειας στους δήμους;
- ✓ Επηρεάζονται και με ποιον τρόπο οι απόψεις των ερωτώμενων από τα ειδικά δημογραφικά χαρακτηριστικά τους;
- ✓ Επηρεάζονται και με ποιον τρόπο οι απόψεις των ερωτώμενων από τα χαρακτηριστικά των δήμων τους;

#### **3.3 Το ερωτηματολόγιο και το δείγμα της έρευνας**

Το ερωτηματολόγιο που χρησιμοποιήθηκε για την έρευνα στηρίχτηκε σε αυτό των Lois et al. (2021) με μικρές τροποποιήσεις και απαρτίζεται από 26 ερωτήσεις στο σύνολο οι οποίες είναι χωρισμένες σε επτά τμήματα. Το πρώτο αποτελείται από 4 ερωτήσεις που σχετίζονται με τα δημογραφικά χαρακτηριστικά του δείγματος και τα χαρακτηριστικά των δήμων. Το δεύτερο τμήμα του ερωτηματολογίου εξέταζε τις γνώμες των ατόμων που συμμετείχαν στην έρευνα αναφορικά με την κυβερνοασφάλεια των δήμων και αποτελούνταν από 3 ερωτήσεις. Το τρίτο μέρος διερευνούσε τις απαντήσεις των ερωτώμενων σχετικά με την διάσταση του συμβουλευτικού ρόλου του εσωτερικού ελέγχου και αποτελούνταν από 3 ερωτήσεις. Το τέταρτο μέρος σχετιζόταν με την διάσταση της τεχνολογικής γνώσης του εσωτερικού ελέγχου και αποτελούνταν από 3 ερωτήσεις. Το πέμπτο μέρος του ερωτηματολογίου αναφερόταν στην διάσταση της συνεργασίας του εσωτερικού ελέγχου και αποτελούνταν από 4 ερωτήσεις. Το έκτο αφορούσε τις Πολιτικές και τα πρότυπα του εσωτερικού ελέγχου και αποτελούνταν από 5 ερωτήσεις. Τέλος ακολουθούσε ένα εξίσου σημαντικό μέρος του ερωτηματολογίου το έβδομο που διερευνούσε τις απαντήσεις των ερωτώμενων σχετικά με την πληροφόρηση και την εκπαίδευση και αποτελούνταν από 4 ερωτήσεις.

Στη συνέχεια ακολουθεί πίνακας αποτελεσμάτων του ελέγχου αξιοπιστίας α του Cronbach για το σύνολο του ερωτηματολογίου και τα επιμέρους τμήματα του εκτός του τμήματος Α. Σε όλες τις περιπτώσεις οι ληφθείσες τιμές είναι μεγαλύτερες από 0,6.

Πίνακας 1. Έλεγχος αξιοπιστίας ερωτηματολογίου

Τμήμα ερωτηματολογίου	Αριθμός επιμέρους ερωτήσεων	Τιμή Cronbach's α
Τμήματα Β έως Ζ	19	0,951
Τμήμα Β	3	0,660
Τμήμα Γ	3	0,738
Τμήμα Δ	3	0,749
Τμήμα Ε	4	0,898

Τμήμα Στ	5	0,936
Τμήμα Ζ	4	0,858

Το ερωτηματολόγιο εστάλη ηλεκτρονικά μέσω googledrive σε 160 άτομα που εργάζονταν σε διάφορους δήμους στην Ελλάδα. Η χρονική περίοδος υλοποίησης της έρευνας ήταν από Φεβρουάριο μέχρι και Μάρτιο 2023. Σε αυτά απάντησαν 83 άτομα, άρα το ποσοστό ανταπόκρισης ανήλθε σε 51,8%.

### **3.4 Στατιστικές μέθοδοι επεξεργασίας δεδομένων**

Τα ερωτηματολόγια επεξεργάστηκαν μετά από τη σύνθεση τους σε υπολογιστικά φύλλα στο στατιστικό πρόγραμμα spss για περαιτέρω αναλύσεις και συσχετίσεις μεταξύ αυτών. Χρησιμοποιήθηκε επίσης ο συντελεστής συσχέτισης Pearson. Διάστημα εμπιστοσύνης επιλέχθηκε κατά 95% για το δείγμα.



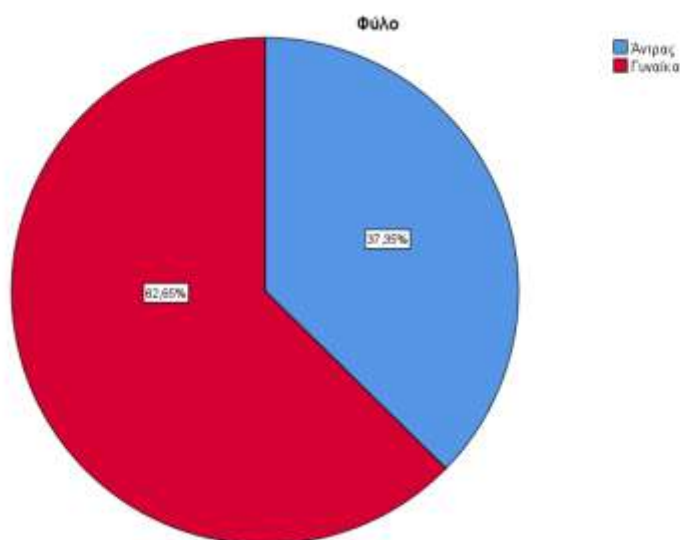
## 4. Τα αποτελέσματα της έρευνας

### 4.1 Δημογραφικά στοιχεία και στοιχεία δήμων

Αρχικά παρουσιάζονται τα αποτελέσματα των δημογραφικών χαρακτηριστικών των συμμετεχόντων και τα χαρακτηριστικά των δήμων τους. Αναφορικά με το φύλο και με βάση το παρακάτω πινακάκι η πλειοψηφία του δείγματος αποτελείται από γυναίκες (62,7%), όταν οι άνδρες αποτελούν το 37,3% του δείγματος.

Πίνακας 2. Φύλο

Ερώτηση A1	Απόλυτες Συχνότητες	Σχετικές Συχνότητες
Άντρας	31	37,30
Γυναίκα	52	62,70
Σύνολο	83	100,00

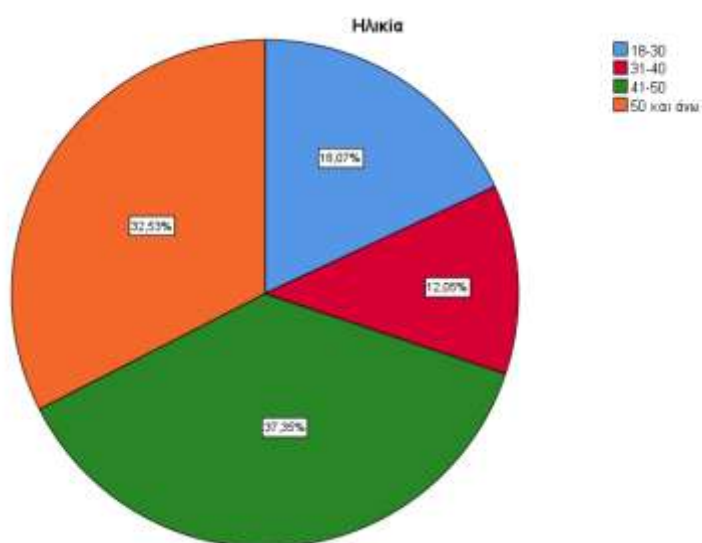


Διάγραμμα 1. Φύλο

Η επόμενη από αυτές τις ερωτήσεις εξέταζε την ηλικία των ερωτώμενων, όπου παρατηρήθηκε ότι το μεγαλύτερο ποσοστό από το δείγμα αποτελείται από άτομα ηλικίας από 41 ετών και πάνω (69,8%), όταν τα άτομα μικρότερης ηλικίας αποτελούν το 30,2% του δείγματος.

Πίνακας 3. Ηλικία

Ερώτηση Α.2	Απόλυτες Συχνότητες	Σχετικές Συχνότητες
18-30	15	18,10
31-40	10	12,10
41-50	31	37,30
50 και άνω	27	32,50
Συνολικό ποσό	83	100,00

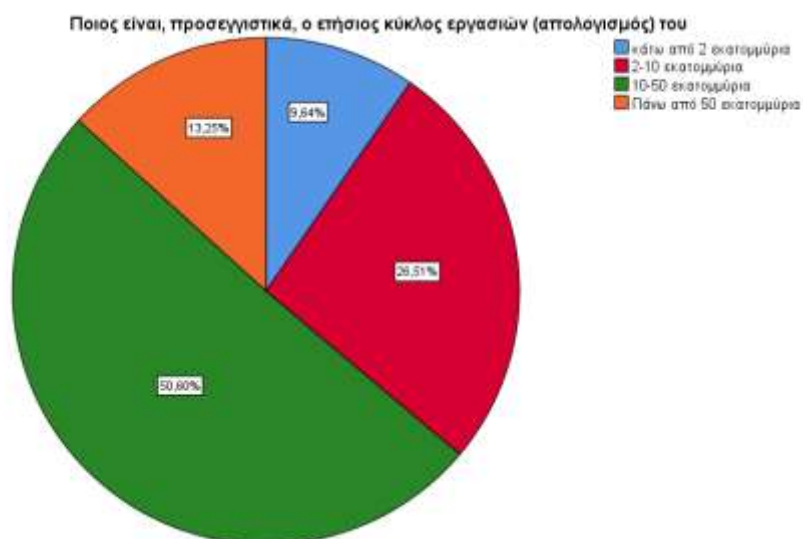


Διάγραμμα 2. Ηλικία

Ακολουθούσε η ερώτηση για τον ετήσιο κύκλο εργασιών του δήμου στον οποίο εργάζονταν τα άτομα που απάντησαν το ερωτηματολόγιο. Το 9,6% των συμμετεχόντων ανήκουν σε δήμους με τζίρους κάτω των 2 εκατομμυρίων ευρώ, το 26,5% των συμμετεχόντων ανήκουν σε δήμους με κύκλους εργασιών από 2 έως 10 εκατομμυρίων ευρώ και το 63,9% των συμμετεχόντων ανήκουν σε δήμους με κύκλους εργασιών μεγαλύτερους των 10 εκατομμυρίων ευρώ.

Πίνακας 4. Ποιος είναι, προσεγγιστικά, ο ετήσιος κύκλος εργασιών (απολογισμός) του δήμου

Ερώτηση Α3	Απόλυτες Συχνότητες	Σχετικές Συχνότητες
κάτω από 2 εκατομμύρια	8	9,6
2-10 εκατομμύρια	22	26,5
10-50 εκατομμύρια	42	50,6
Πάνω από 50 εκατομμύρια	11	13,3
Σύνολο	83	100,0

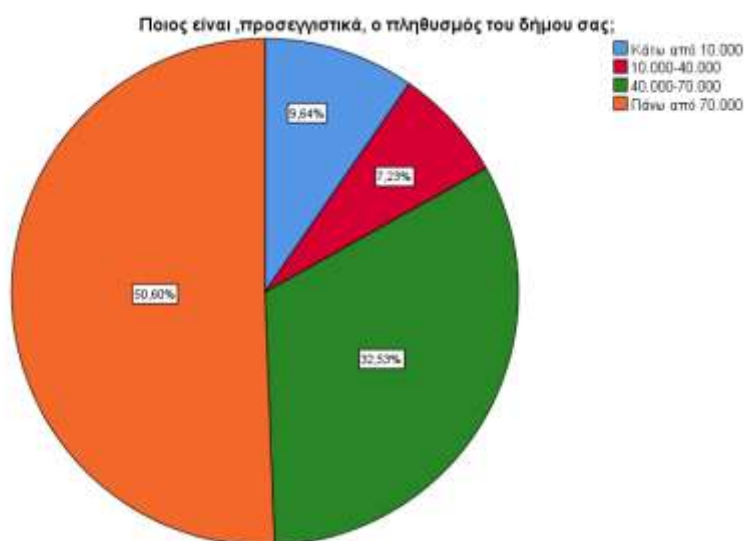


Διάγραμμα 3. Ποιος είναι, προσεγγιστικά, ο ετήσιος κύκλος εργασιών (απολογισμός) του

Η τέταρτη και τελευταία ερώτηση διερευνούσε τον πληθυσμό του δήμου των συμμετεχόντων στην έρευνα. Παρατηρήθηκε ότι, το 9,6% αυτών ανήκουν σε δήμους με πληθυσμό κάτω των 10 χιλιάδων κατοίκων, το 7,2% των συμμετεχόντων ανήκουν με πληθυσμό από 10 έως 40 χιλιάδων κατοίκων και το 83,1% των συμμετεχόντων ανήκουν σε δήμους άνω των 40 χιλιάδων κατοίκων.

Πίνακας 5. Ποιος είναι,προσεγγιστικά, ο πληθυσμός του δήμου σας;

Ερώτηση Α4	Απόλυτες Συχνότητες	Σχετικές Συχνότητες
Κάτω από 10.000	8	9,6
10.000-40.000	6	7,2
40.000-70.000	27	32,5
Πάνω από 70.000	42	50,6
Σύνολο	83	100,0



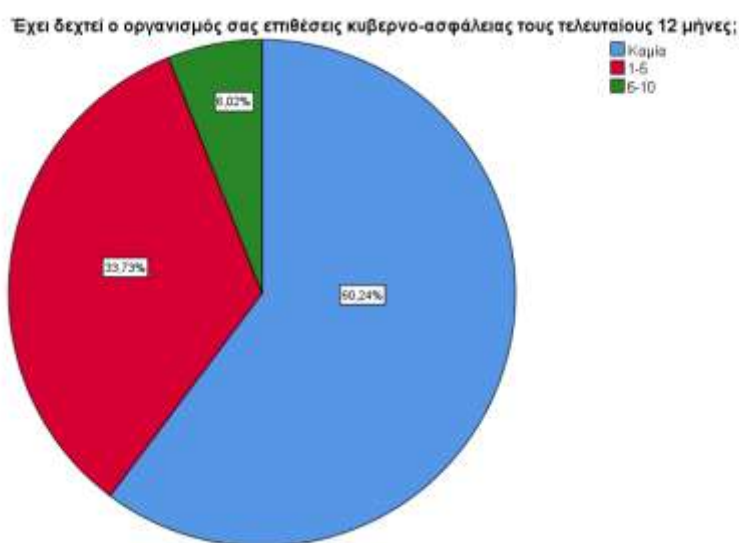
Διάγραμμα 4. Ποιος είναι ,προσεγγιστικά, ο πληθυσμός του δήμου σας;

#### 4.2 Ερωτήσεις σχετικά με την κυβερνο-ασφάλεια των δήμων.

Το δεύτερο τμήμα του ερωτηματολογίου διερευνούσε το ζήτημα της κυβερνο-ασφάλειας στους δήμους. Η πρώτη από αυτές αφορούσε την συχνότητα με την οποία έχει δεχτεί ο δήμος επιθέσεις κυβερνο-ασφάλειας τους τελευταίους 12 μήνες, όπου το 60,2% των ατόμων του δείγματος δηλώνει μηδενικές επιθέσεις, το 33,7% δηλώνει από 1 έως 5 επιθέσεις και το 6% δηλώνει 6- 10 επιθέσεις το τελευταίο 12μηνο.

Πίνακας 6. Έχει δεχτεί ο οργανισμός σας επιθέσεις κυβερνο-ασφάλειας τους τελευταίους 12 μήνες;

Ερώτηση B1	Απόλυτες Συχνότητες	Σχετικές Συχνότητες
Καμία	50	60,2
1-5	28	33,7
6-10	5	6,0
Πάνω από 10	0	0
Σύνολο	83	100,0



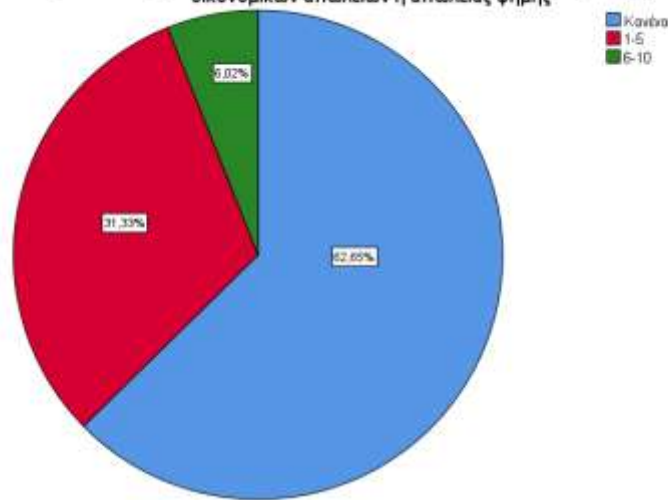
Διάγραμμα 5. Έχει δεχτεί ο οργανισμός σας επιθέσεις κυβερνο-ασφάλειας τους τελευταίους 12 μήνες;

Η δεύτερη από αυτές διερευνούσε τον αριθμό αυτών των περιστατικών που εντοπίστηκαν σε σχέση με την εμφάνιση λειτουργικών προβλημάτων, οικονομικών απωλειών ή απώλειας φήμης. Παρακάτω φαίνεται ότι , το 31,3% δηλώνει από 1 έως 5 περιστατικά και το 6% δηλώνει 6- 10 περιστατικά το τελευταίο 12μηνο.

Πίνακας 7. Πόσα από τα παραπάνω περιστατικά εντοπίστηκαν σε σχέση με την εμφάνιση λειτουργικών προβλημάτων, οικονομικών απωλειών ή απώλειας φήμης

Ερώτηση B2	Απόλυτες Συχνότητες	Σχετικές Συχνότητες
Κανένα	52	62,7
1-5	26	31,3
6-10	5	6,0
Πάνω από 10	0	0
Σύνολο	83	100,0

Πόσα από τα παραπάνω περιστατικά εντοπίστηκαν σε σχέση με την εμφάνιση λειτουργικών προβλημάτων, οικονομικών απωλειών ή απώλειας φήμης

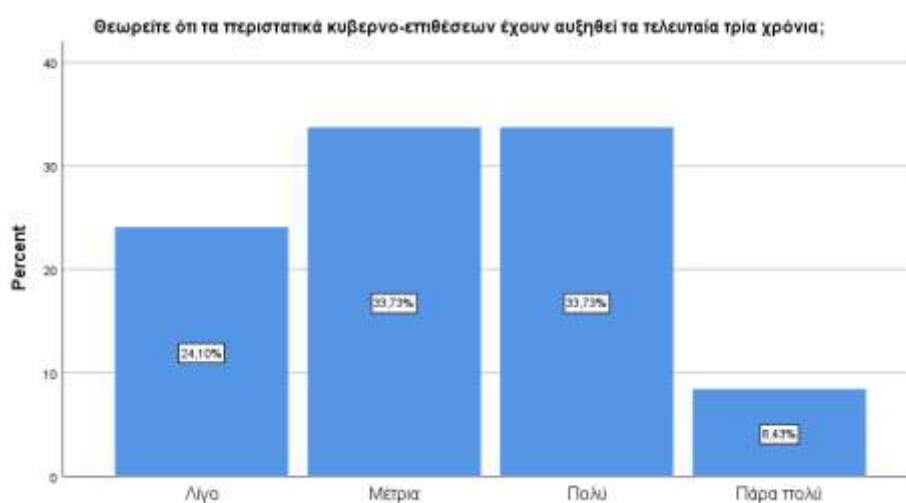


Διάγραμμα 6. Πόσα από τα παραπάνω περιστατικά εντοπίστηκαν σε σχέση με την εμφάνιση λειτουργικών προβλημάτων, οικονομικών απωλειών ή απώλειας φήμης

Η τρίτη και τελευταία έδειχνε εάν και κατά πόσο τα περιστατικά κυβερνο-επιθέσεων έχουν αυξηθεί τα τελευταία τρία χρόνια. Με βάση τα αποτελέσματα της έρευνας, το 24,1% από το δείγμα πιστεύει ότι αυτό συνέβη «λίγο», ενώ «πολύ» και «πάρα πολύ» θεωρεί ότι συνέβη το 42,1%, όπως φαίνεται στον πίνακα και το σχετικό διάγραμμα που ακολουθεί.

Πίνακας 8. Θεωρείτε ότι τα περιστατικά κυβερνο-επιθέσεων έχουν αυξηθεί τα τελευταία τρία χρόνια;

Ερώτηση B3	Απόλυτες Συχνότητες	Σχετικές Συχνότητες
Καθόλου	0	0
Λίγο	20	24,1
Μέτρια	28	33,7
Πολύ	28	33,7
Πάρα πολύ	7	8,4
Σύνολο	83	100,0



Διάγραμμα 7. Θεωρείτε ότι τα περιστατικά κυβερνο-επιθέσεων έχουν αυξηθεί τα τελευταία τρία χρόνια;

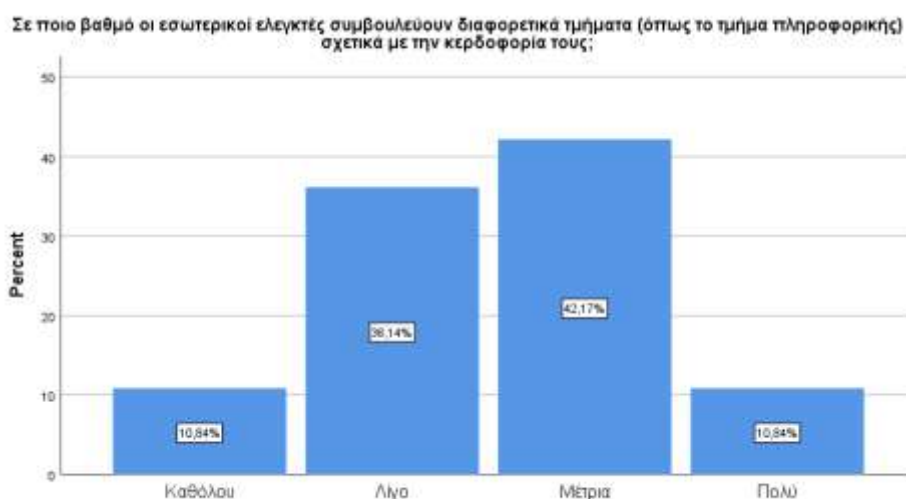
#### 4.3 Η διάσταση του συμβουλευτικού ρόλου του εσωτερικού ελέγχου

Το τρίτο τμήμα από το ερωτηματολόγιο συγκέντρωνε τις απόψεις των ερωτώμενων αναφορικά με την διάσταση του συμβουλευτικού ρόλου του εσωτερικού ελέγχου. Αρχικά διερευνήθηκε ο βαθμός στον οποίο οι εσωτερικοί ελεγκτές συμβουλεύουν διαφορετικά τμήματα (όπως της πληροφορικής) σχετικά με την κερδοφορία τους. Με βάση τα αποτελέσματα της έρευνας, όπως αυτά παρουσιάζονται αναλυτικά στον παρακάτω πίνακα και το αντίστοιχο διάγραμμα, το 24,1% του

δείγματος δηλώνει ότι αυτό συμβαίνει «λίγο», όταν «πολύ» ή «πάρα πολύ» δηλώνει ότι συνέβη το 42,1% του δείγματος.

Πίνακας 9. Σε ποιο βαθμό οι εσωτερικοί ελεγκτές συμβουλεύουν διαφορετικά τμήματα (όπως το τμήμα πληροφορικής) σχετικά με την κερδοφορία τους;

Ερώτηση Γ1	Απόλυτες Συχνότητες	Σχετικές Συχνότητες
Καθόλου	0	0
Λίγο	20	24,1
Μέτρια	28	33,7
Πολύ	28	33,7
Πάρα πολύ	7	8,4
Σύνολο	83	100,0



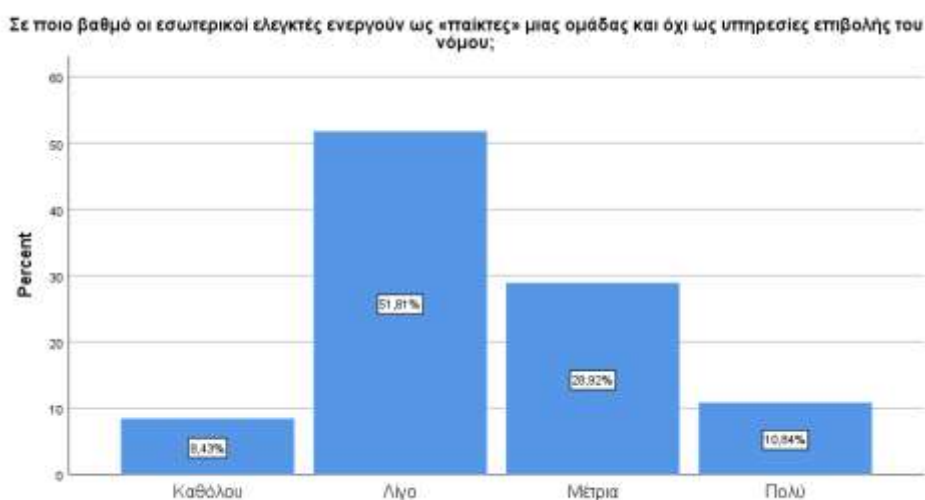
Διάγραμμα 8. Σε ποιο βαθμό οι εσωτερικοί ελεγκτές συμβουλεύουν διαφορετικά τμήματα (όπως το τμήμα πληροφορικής) σχετικά με την κερδοφορία τους;

Η δεύτερη από αυτές διερευνούσε τον βαθμό στον οποίο οι εσωτερικοί ελεγκτές ενεργούν ως “παίκτες” μιας ομάδας και όχι ως υπηρεσίες επιβολής του νόμου. Με βάση τα αποτελέσματα της έρευνας, όπως αυτά παρουσιάζονται αναλυτικά στον παρακάτω πίνακα και το αντίστοιχο διάγραμμα, το 60,2% του δείγματος δηλώνει ότι αυτό συμβαίνει «καθόλου» ή «λίγο», όταν «πολύ» δηλώνει ότι συνέβη το 10,8% του δείγματος.



Πίνακας 10. Σε ποιο βαθμό οι εσωτερικοί ελεγκτές ενεργούν ως “παίκτες” μιας ομάδας και όχι ως υπηρεσίες επιβολής του νόμου;

Ερώτηση Γ2	Απόλυτες Συχνότητες	Σχετικές Συχνότητες
Καθόλου	7	8,4
Λίγο	43	51,8
Μέτρια	24	28,9
Πολύ	9	10,8
Πάρα πολύ	0	0
Σύνολο	83	100,0



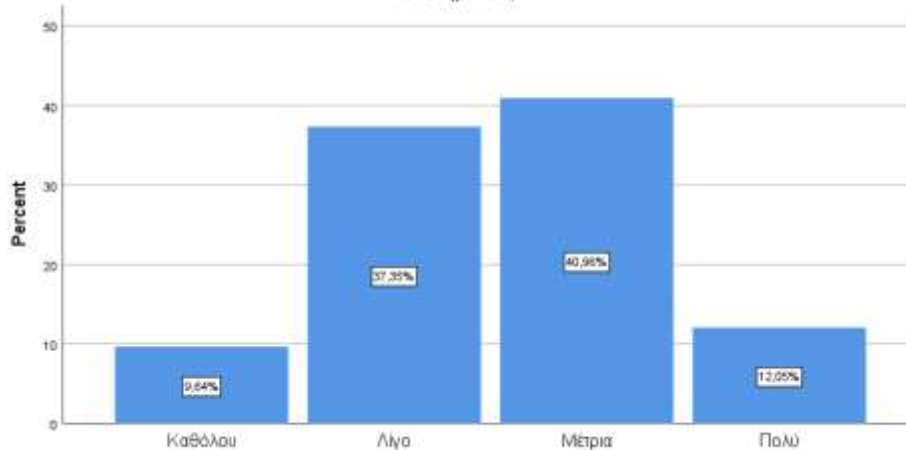
Διάγραμμα 9. Σε ποιο βαθμό οι εσωτερικοί ελεγκτές ενεργούν ως «παίκτες» μιας ομάδας και όχι ως υπηρεσίες επιβολής του νόμου;

Η τρίτη και τελευταία από αυτές διερευνούσε κατά πόσο οι εσωτερικοί ελεγκτές εμπλέκονται στην ασφάλεια των πληροφοριών και των πληροφοριακών συστημάτων. Με βάση τα ευρήματα της έρευνας, το 46,9% δηλώνει ότι αυτό συμβαίνει «καθόλου» ή «λίγο», όταν «πολύ» δηλώνει ότι συνέβη το 12% του δείγματος.

Πίνακας 11. Σε ποιο βαθμό οι εσωτερικοί ελεγκτές εμπλέκονται στην ασφάλεια των πληροφοριών και των πληροφοριακών συστημάτων;

Ερώτηση Γ3	Απόλυτες Συχνότητες	Σχετικές Συχνότητες
Καθόλου	8	9,6
Λίγο	31	37,3
Μέτρια	34	41,0
Πολύ	10	12,0
Πάρα πολύ	0	0
Σύνολο	83	100,0

Σε ποιο βαθμό οι εσωτερικοί ελεγκτές εμπλέκονται στην ασφάλεια των πληροφοριών και των πληροφοριακών συστημάτων;



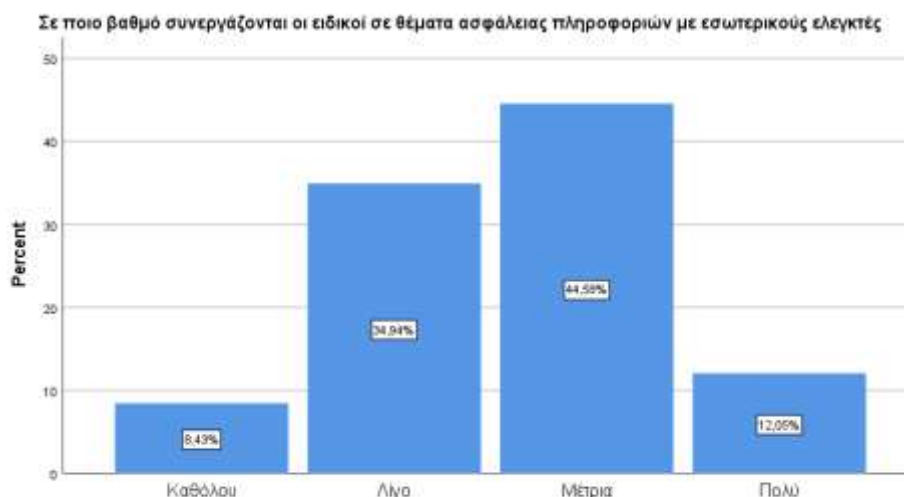
Διάγραμμα 10. Σε ποιο βαθμό οι εσωτερικοί ελεγκτές εμπλέκονται στην ασφάλεια των πληροφοριών και των πληροφοριακών συστημάτων;

#### 4.4 Η διάσταση της τεχνολογικής γνώσης του εσωτερικού ελέγχου

Το τέταρτο κομμάτι από το ερωτηματολόγιο σχετιζόταν με την διάσταση της τεχνολογικής γνώσης του εσωτερικού ελέγχου. Αρχικά, διερευνούσε τον βαθμό στον οποίο οι εσωτερικοί ελεγκτές συνεργάζονται με τους ειδικούς σε θέματα ασφάλειας πληροφοριών να διασφαλίσουν την ασφάλεια των συστημάτων πληροφοριών. Με βάση τον πίνακα και το διάγραμμα που ακολουθεί, γίνεται κατανοητό ότι το 43,3% του δείγματος δηλώνει ότι αυτό συμβαίνει «λίγο», όταν «πολύ» ή «πάρα πολύ» δηλώνει ότι συνέβη το 12% του δείγματος.

Πίνακας 12. Σε ποιο βαθμό συνεργάζονται οι ειδικοί σε θέματα ασφάλειας πληροφοριών με εσωτερικούς ελεγκτές για να διασφαλίσουν την ασφάλεια των συστημάτων πληροφοριών;

Ερώτηση Δ1	Απόλυτες Συχνότητες	Σχετικές Συχνότητες
Καθόλου	7	8,4
Λίγο	29	34,9
Μέτρια	37	44,6
Πολύ	10	12,0
Πάρα πολύ	0	0
Σύνολο	83	100,0

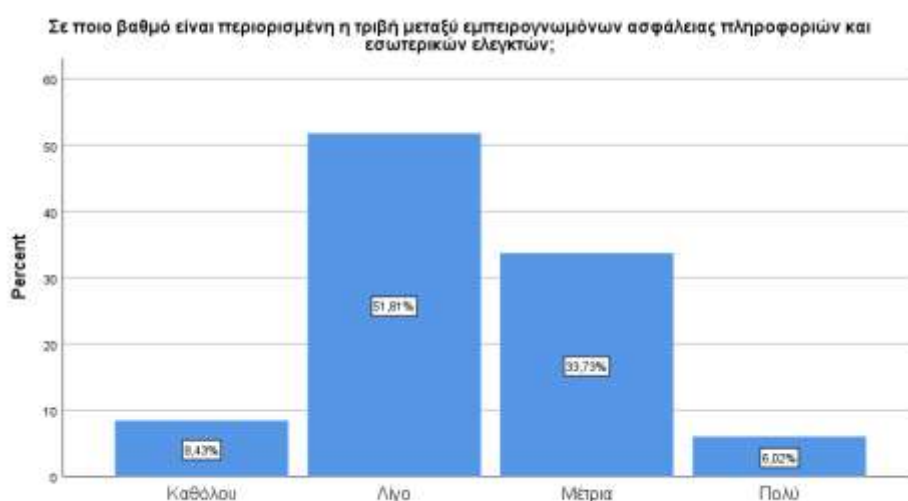


Διάγραμμα 11. Σε ποιο βαθμό συνεργάζονται οι ειδικοί σε θέματα ασφάλειας πληροφοριών με εσωτερικούς ελεγκτές για να διασφαλίσουν την ασφάλεια των συστημάτων πληροφοριών;

Η δεύτερη εξέταζε κατά πόσο είναι περιορισμένη η τριβή μεταξύ εμπειρογνομώνων ασφάλειας πληροφοριών και εσωτερικών ελεγκτών. Με βάση τα αποτελέσματα της έρευνας, το 43,3% του δείγματος δηλώνει ότι αυτό συμβαίνει «καθόλου» ή «λίγο», όταν «πολύ» δηλώνει ότι συνέβη το 6% του δείγματος.

Πίνακας 13. Σε ποιο βαθμό είναι περιορισμένη η τριβή μεταξύ εμπειρογνομόνων ασφάλειας πληροφοριών και εσωτερικών ελεγκτών;

Ερώτηση Δ2	Απόλυτες Συχνότητες	Σχετικές Συχνότητες
Καθόλου	7	8,4
Λίγο	43	51,8
Μέτρια	28	33,7
Πολύ	5	6,0
Πάρα πολύ	0	0
Σύνολο	83	100,0

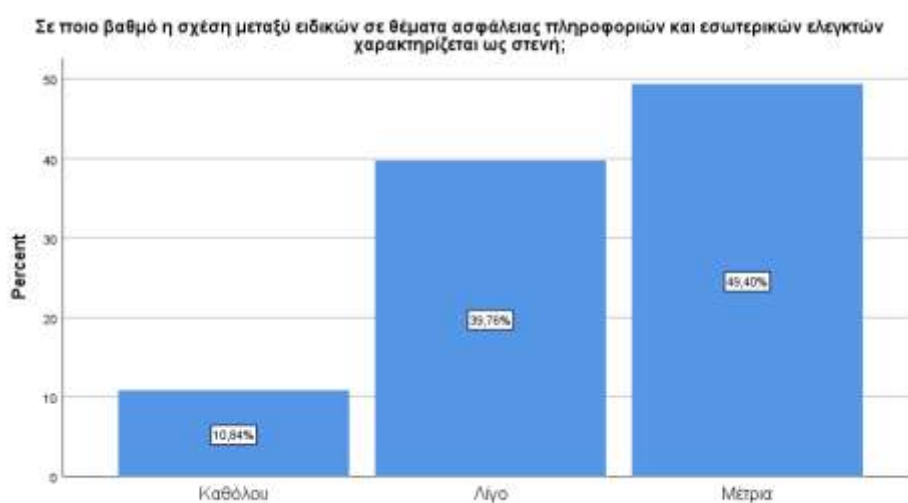


Διάγραμμα 12. Σε ποιο βαθμό είναι περιορισμένη η τριβή μεταξύ εμπειρογνομόνων ασφάλειας πληροφοριών και εσωτερικών ελεγκτών;

Η τρίτη και τελευταία από αυτές διερευνούσε εάν και σε τι κλίμακα η σχέση μεταξύ ειδικών σε θέματα ασφάλειας πληροφοριών και εσωτερικών ελεγκτών μπορεί να χαρακτηριστεί ως στενή. Από τα παρακάτω αποτελέσματα, γίνεται φανερό ότι τα περισσότερα άτομα που συμμετείχαν στην έρευνα(49,4%) χαρακτηρίζουν την σχέση «μέτρια», ενώ το υπόλοιπο(50,6%) δηλώνει ότι αυτό ισχύει «καθόλου» ή έστω «λίγο».

Πίνακας 14. Σε ποιο βαθμό η σχέση μεταξύ ειδικών σε θέματα ασφάλειας πληροφοριών και εσωτερικών ελεγκτών χαρακτηρίζεται ως στενή;

Ερώτηση Δ3	Απόλυτες Συχνότητες	Σχετικές Συχνότητες
Καθόλου	9	10,8
Λίγο	33	39,8
Μέτρια	41	49,4
Πολύ	0	0
Πάρα πολύ	0	0
Σύνολο	83	100,0



Διάγραμμα 13. Σε ποιο βαθμό η σχέση μεταξύ ειδικών σε θέματα ασφάλειας πληροφοριών και εσωτερικών ελεγκτών χαρακτηρίζεται ως στενή;

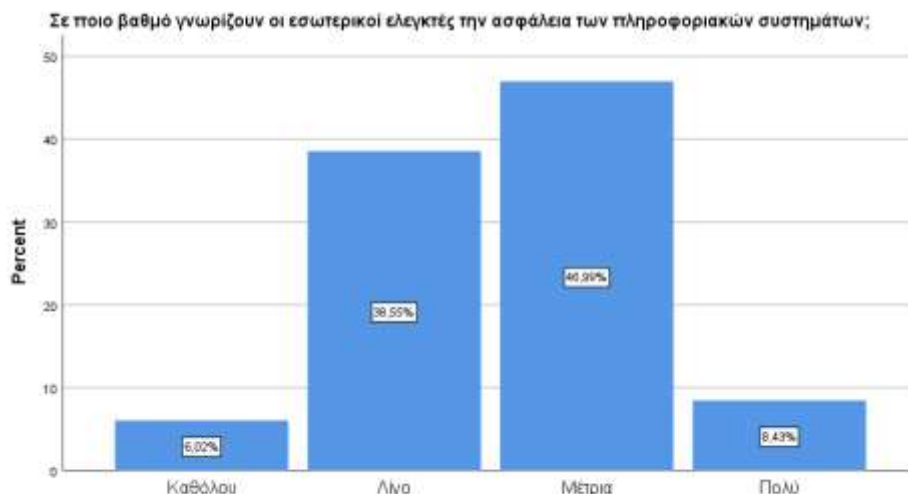
#### 4.5 Η διάσταση της συνεργασίας του εσωτερικού ελέγχου

Το πέμπτο μέρος του ερωτηματολογίου διερευνούσε τις απαντήσεις των ερωτώμενων σχετικά με την διάσταση της συνεργασίας του εσωτερικού ελέγχου. Η πρώτη από αυτές διερευνούσε τον βαθμό στον οποίο γνωρίζουν οι εσωτερικοί ελεγκτές την ασφάλεια των πληροφοριακών συστημάτων. Με βάση τα αποτελέσματα της έρευνας, όπως αυτά παρουσιάζονται αναλυτικά στον παρακάτω πίνακα και το αντίστοιχο διάγραμμα, το 44,6% του δείγματος δηλώνει ότι αυτό

συμβαίνει «καθόλου» ή «λίγο», όταν «πολύ» δηλώνει ότι συνέβη το 8,4% του δείγματος.

Πίνακας 15. Σε ποιο βαθμό γνωρίζουν οι εσωτερικοί ελεγκτές την ασφάλεια των πληροφοριακών συστημάτων;

Ερώτηση E1	Απόλυτες Συχνότητες	Σχετικές Συχνότητες
Καθόλου	5	6,0
Λίγο	32	38,6
Μέτρια	39	47,0
Πολύ	7	8,4
Πάρα πολύ	0	0
Σύνολο	83	100,0

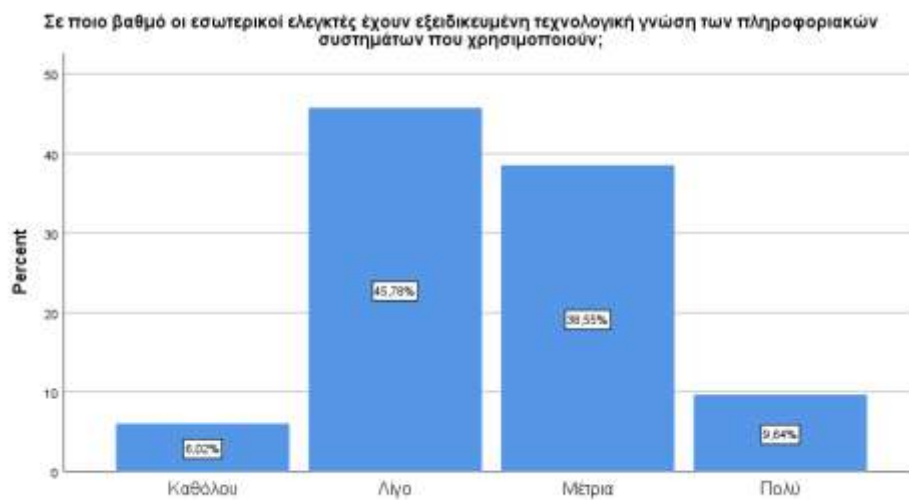


Διάγραμμα 14. Σε ποιο βαθμό γνωρίζουν οι εσωτερικοί ελεγκτές την ασφάλεια των πληροφοριακών συστημάτων;

Η δεύτερη από αυτές διερευνούσε τον βαθμό στον οποίο οι εσωτερικοί ελεγκτές έχουν εξειδικευμένη τεχνολογική γνώση των πληροφοριακών συστημάτων που χρησιμοποιούν. Με βάση τα αποτελέσματα της έρευνας, όπως αυτά παρουσιάζονται αναλυτικά στον παρακάτω πίνακα και το αντίστοιχο διάγραμμα, το 51,8% του δείγματος δηλώνει ότι αυτό συμβαίνει «καθόλου» ή «λίγο», όταν «πολύ» δηλώνει ότι συνέβη το 9,6% του δείγματος.

Πίνακας 16. Σε ποιο βαθμό οι εσωτερικοί ελεγκτές έχουν εξειδικευμένη τεχνολογική γνώση των πληροφοριακών συστημάτων που χρησιμοποιούν;

Ερώτηση E2	Απόλυτες Συχνότητες	Σχετικές Συχνότητες
Καθόλου	5	6,0
Λίγο	38	45,8
Μέτρια	32	38,6
Πολύ	8	9,6
Πάρα πολύ	0	0
Σύνολο	83	100,0

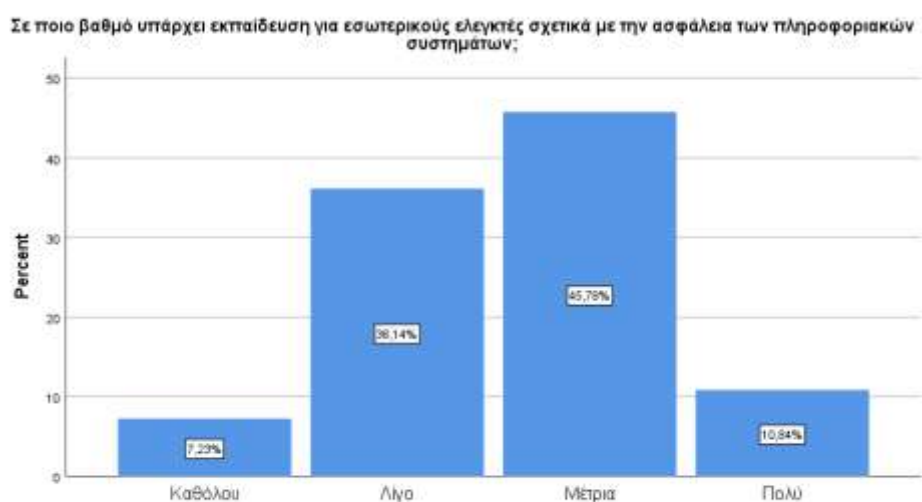


Διάγραμμα 15. Σε ποιο βαθμό οι εσωτερικοί ελεγκτές έχουν εξειδικευμένη τεχνολογική γνώση των πληροφοριακών συστημάτων που χρησιμοποιούν;

Η τρίτη από αυτές διερευνούσε τον βαθμό στον οποίο υπάρχει εκπαίδευση για εσωτερικούς ελεγκτές σχετικά με την ασφάλεια των πληροφοριακών συστημάτων. Με βάση τα αποτελέσματα της έρευνας, όπως αυτά παρουσιάζονται αναλυτικά στον παρακάτω πίνακα και το αντίστοιχο διάγραμμα, το 43,3% του δείγματος δηλώνει ότι αυτό συμβαίνει «καθόλου» ή «λίγο», όταν «πολύ» δηλώνει ότι συνέβη το 10,8% του δείγματος.

Πίνακας 17. Σε ποιο βαθμό υπάρχει εκπαίδευση για εσωτερικούς ελεγκτές σχετικά με την ασφάλεια των πληροφοριακών συστημάτων;

Ερώτηση E3	Απόλυτες Συχνότητες	Σχετικές Συχνότητες
Καθόλου	6	7,2
Λίγο	30	36,1
Μέτρια	38	45,8
Πολύ	9	10,8
Πάρα πολύ	0	0
Σύνολο	83	100,0



Διάγραμμα 16. Σε ποιο βαθμό υπάρχει εκπαίδευση για εσωτερικούς ελεγκτές σχετικά με την ασφάλεια των πληροφοριακών συστημάτων;

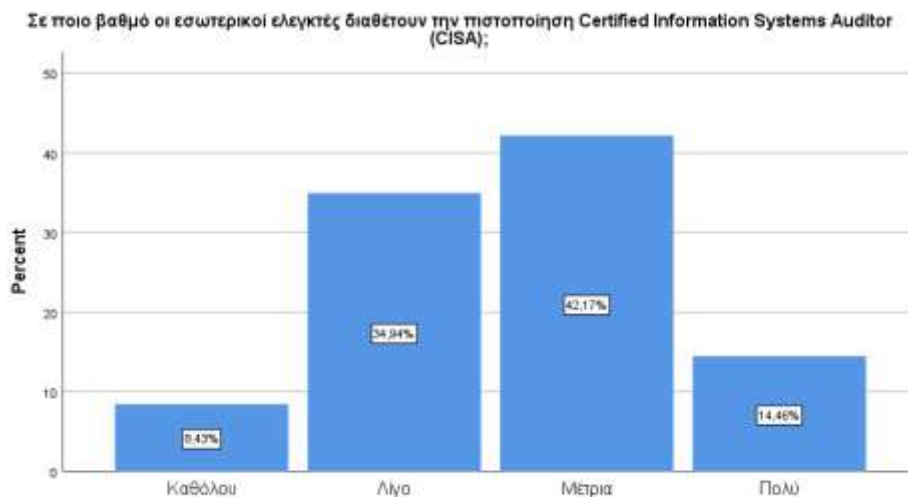
Η τέταρτη και τελευταία από αυτές διερευνούσε τον βαθμό στον οποίο οι εσωτερικοί ελεγκτές διαθέτουν την πιστοποίηση “Certified Information Systems Auditor” (CISA). Με βάση τα αποτελέσματα της έρευνας, όπως αυτά παρουσιάζονται αναλυτικά στον παρακάτω πίνακα και το αντίστοιχο διάγραμμα, το 43,3% του δείγματος δηλώνει ότι αυτό συμβαίνει «καθόλου» ή «λίγο», όταν «πολύ» δηλώνει ότι συνέβη το 14,5% του δείγματος.

Πίνακας 18. Σε ποιο βαθμό οι εσωτερικοί ελεγκτές διαθέτουν την πιστοποίηση Certified Information Systems Auditor (CISA);

Ερώτηση E4	Απόλυτες Συχνότητες	Σχετικές Συχνότητες
------------	---------------------	---------------------



Καθόλου	7	8,4
Λίγο	29	34,9
Μέτρια	35	42,2
Πολύ	12	14,5
Πάρα πολύ	0	0
Σύνολο	83	100,0



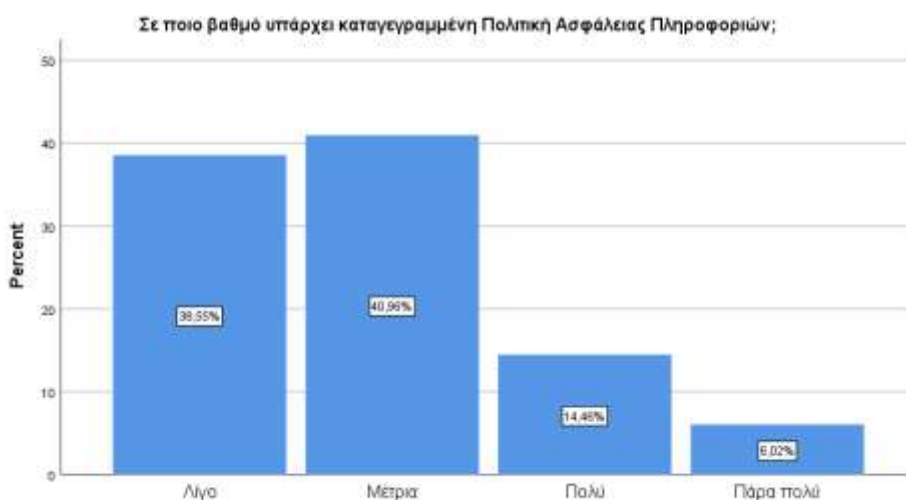
Διάγραμμα 17. Σε ποιο βαθμό οι εσωτερικοί ελεγκτές διαθέτουν την πιστοποίηση Certified Information Systems Auditor (CISA);

#### 4.6 Πολιτικές και πρότυπα

Το έκτο μέρος του ερωτηματολογίου διερευνούσε τις απαντήσεις των ερωτώμενων σχετικά με τις Πολιτικές και τα πρότυπα του εσωτερικού ελέγχου. Η πρώτη από αυτές διερευνούσε τον βαθμό στον οποίο υπάρχει καταγεγραμμένη Πολιτική Ασφάλειας Πληροφοριών. Με βάση τα αποτελέσματα της έρευνας, όπως αυτά παρουσιάζονται αναλυτικά στον παρακάτω πίνακα και το αντίστοιχο διάγραμμα, το 38,6% του δείγματος δηλώνει ότι αυτό συμβαίνει «καθόλου», όταν «πολύ» ή «πάρα πολύ» δηλώνει ότι συνέβη το 20,5% του δείγματος.

Πίνακας 19. Σε ποιο βαθμό υπάρχει καταγεγραμμένη Πολιτική Ασφάλειας Πληροφοριών;

Ερώτηση ΣΤ1	Απόλυτες Συχνότητες	Σχετικές Συχνότητες
Καθόλου	0	0
Λίγο	32	38,6
Μέτρια	34	41,0
Πολύ	12	14,5
Πάρα πολύ	5	6,0
Σύνολο	83	100,0



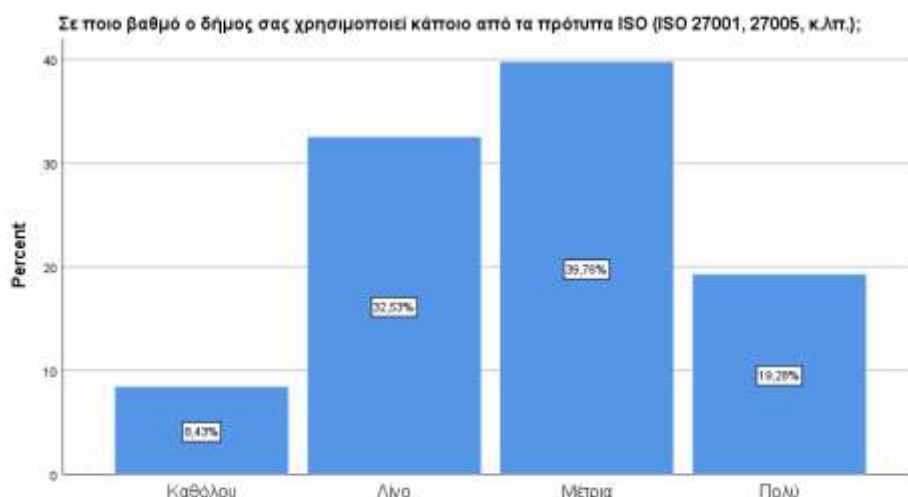
Διάγραμμα 18. Σε ποιο βαθμό υπάρχει καταγεγραμμένη Πολιτική Ασφάλειας Πληροφοριών;

Η δεύτερη από αυτές διερευνούσε τον βαθμό στον οποίο ο δήμος των ερωτώμενων χρησιμοποιεί κάποιο από τα πρότυπα ISO. Με βάση τα αποτελέσματα της έρευνας, όπως αυτά παρουσιάζονται αναλυτικά στον παρακάτω πίνακα και το αντίστοιχο διάγραμμα, το 40,9% του δείγματος δηλώνει ότι αυτό συμβαίνει «καθόλου» ή «λίγο», όταν «πολύ» δηλώνει ότι συνέβη το 19,3% του δείγματος.

Πίνακας 20. Σε ποιο βαθμό ο δήμος σας χρησιμοποιεί κάποιο από τα πρότυπα ISO (ISO 27001, 27005, κ.λπ.);

Ερώτηση ΣΤ2	Απόλυτες Συχνότητες	Σχετικές Συχνότητες
-------------	---------------------	---------------------

Καθόλου	7	8,4
Λίγο	27	32,5
Μέτρια	33	39,8
Πολύ	16	19,3
Πάρα πολύ	0	0
Σύνολο	83	100,0



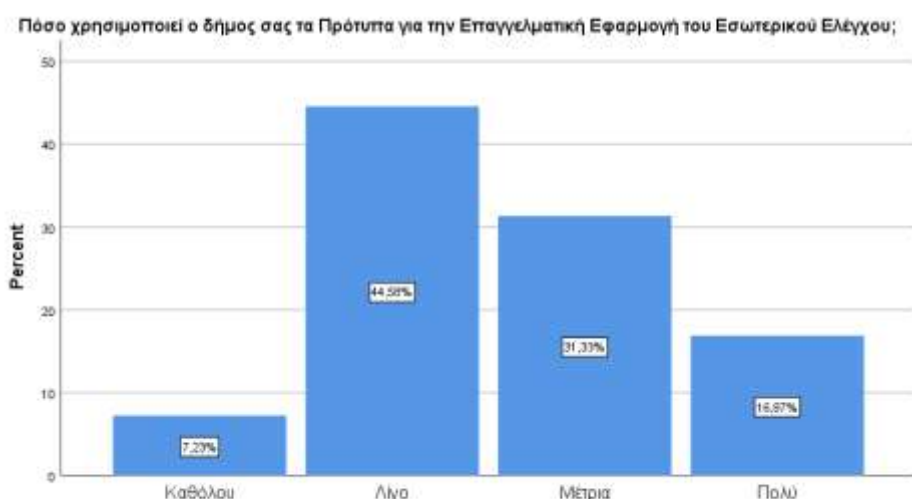
Διάγραμμα 19. Σε ποιο βαθμό ο δήμος σας χρησιμοποιεί κάποιο από τα πρότυπα ISO (ISO 27001, 27005, κ.λπ.);

Η τρίτη από αυτές διερευνούσε τον βαθμό στον οποίο ο δήμος των ερωτώμενων χρησιμοποιεί τα Πρότυπα για την Επαγγελματική Εφαρμογή του Εσωτερικού Ελέγχου. Με βάση τα αποτελέσματα της έρευνας, όπως αυτά παρουσιάζονται αναλυτικά στον παρακάτω πίνακα και το αντίστοιχο διάγραμμα, το 51,8% του δείγματος δηλώνει ότι αυτό συμβαίνει «καθόλου» ή «λίγο», όταν «πολύ» δηλώνει ότι συνέβη το 16,9% του δείγματος.

Πίνακας 21. Πόσο χρησιμοποιεί ο δήμος σας τα Πρότυπα για την Επαγγελματική Εφαρμογή του Εσωτερικού Ελέγχου;

Ερώτηση ΣΤ3	Απόλυτες Συχνότητες	Σχετικές Συχνότητες
Καθόλου	6	7,2

Λίγο	37	44,6
Μέτρια	26	31,3
Πολύ	14	16,9
Πάρα πολύ	0	0
Σύνολο	83	100,0



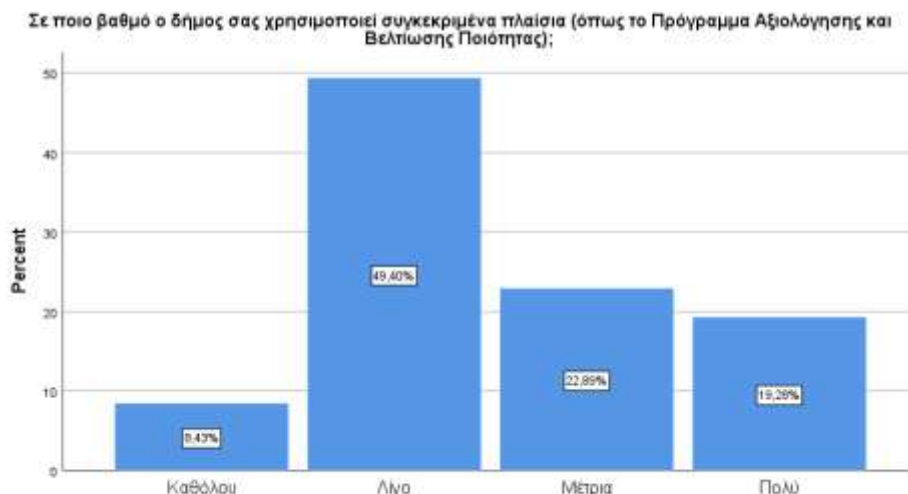
Διάγραμμα 20. Πόσο χρησιμοποιεί ο δήμος σας τα Πρότυπα για την Επαγγελματική Εφαρμογή του Εσωτερικού Ελέγχου;

Η τέταρτη από αυτές διερευνούσε τον βαθμό στον οποίο ο δήμος των ερωτώμενων χρησιμοποιεί συγκεκριμένα πλαίσια (όπως το Πρόγραμμα Αξιολόγησης και Βελτίωσης Ποιότητας). Με βάση τα αποτελέσματα της έρευνας, όπως αυτά παρουσιάζονται αναλυτικά στον παρακάτω πίνακα και το αντίστοιχο διάγραμμα, το 57,8% του δείγματος δηλώνει ότι αυτό συμβαίνει «καθόλου» ή «λίγο», όταν «πολύ» δηλώνει ότι συνέβη το 19,3% του δείγματος.

Πίνακας 22. Σε ποιο βαθμό ο δήμος σας χρησιμοποιεί συγκεκριμένα πλαίσια (όπως το Πρόγραμμα Αξιολόγησης και Βελτίωσης Ποιότητας);

Ερώτηση ΣΤ4	Απόλυτες Συχνότητες	Σχετικές Συχνότητες
Καθόλου	7	8,4
Λίγο	41	49,4

Μέτρια	19	22,9
Πολύ	16	19,3
Πάρα πολύ	0	0
Σύνολο	83	100,0



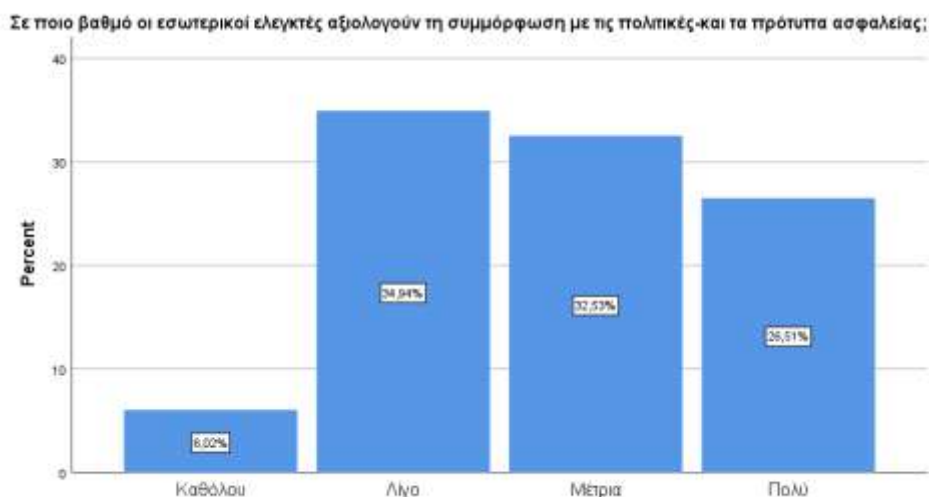
Διάγραμμα 21. Σε ποιο βαθμό ο δήμος σας χρησιμοποιεί συγκεκριμένα πλαίσια (όπως το Πρόγραμμα Αξιολόγησης και Βελτίωσης Ποιότητας);

Η πέμπτη και τελευταία από αυτές διερευνούσε τον βαθμό οι εσωτερικοί ελεγκτές αξιολογούν τη συμμόρφωση με τις πολιτικές-και τα πρότυπα ασφαλείας. Με βάση τα αποτελέσματα της έρευνας, όπως αυτά παρουσιάζονται αναλυτικά στον παρακάτω πίνακα και το αντίστοιχο διάγραμμα, το 40,9% του δείγματος δηλώνει ότι αυτό συμβαίνει «καθόλου» ή «λίγο», όταν «πολύ» δηλώνει ότι συνέβη το 26,5% του δείγματος.

Πίνακας 23. Σε ποιο βαθμό οι εσωτερικοί ελεγκτές αξιολογούν τη συμμόρφωση με τις πολιτικές-και τα πρότυπα ασφαλείας;

Ερώτηση ΣΤ5	Απόλυτες Συχνότητες	Σχετικές Συχνότητες
Καθόλου	5	6,0
Λίγο	29	34,9
Μέτρια	27	32,5

Πολύ	22	26,5
Πάρα πολύ	0	0
Σύνολο	83	100,0



Διάγραμμα 22. Σε ποιο βαθμό οι εσωτερικοί ελεγκτές αξιολογούν τη συμμόρφωση με τις πολιτικές-και τα πρότυπα ασφαλείας;

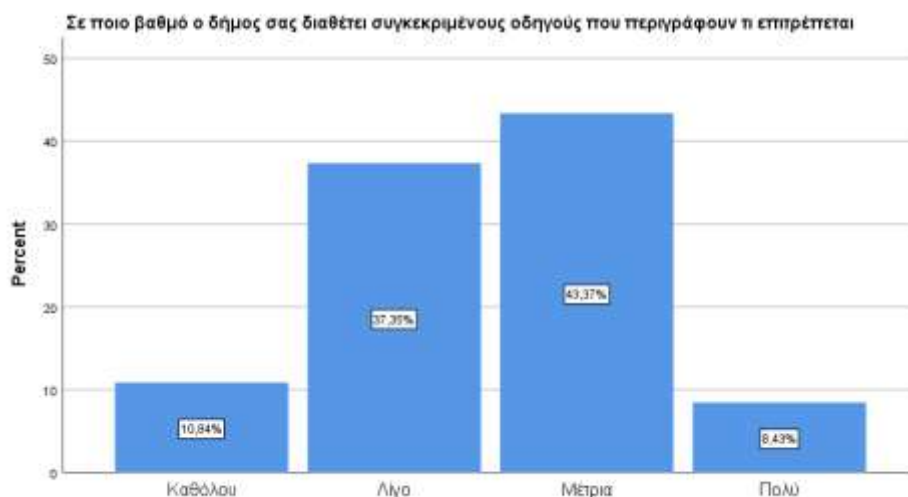
#### 4.7 Πληροφόρηση και εκπαίδευση

Το έβδομο και τελευταίο μέρος του ερωτηματολογίου διερευνούσε τις απαντήσεις των ερωτώμενων σχετικά με την πληροφόρηση και την εκπαίδευση. Η πρώτη από αυτές διερευνούσε τον βαθμό στον οποίο ο δήμος διαθέτει συγκεκριμένους οδηγούς που περιγράφουν τι επιτρέπεται να κάνουν οι εργαζόμενοι με τους υπολογιστές τους. Με βάση τα αποτελέσματα της έρευνας, όπως αυτά παρουσιάζονται αναλυτικά στον παρακάτω πίνακα και το αντίστοιχο διάγραμμα, το 48,1% του δείγματος δηλώνει ότι αυτό συμβαίνει «καθόλου» ή «λίγο», όταν «πολύ» δηλώνει ότι συνέβη το 8,4% του δείγματος.

Πίνακας 24. Σε ποιο βαθμό ο δήμος σας διαθέτει συγκεκριμένους οδηγούς που περιγράφουν τι επιτρέπεται να κάνουν οι εργαζόμενοι με τους υπολογιστές τους;

Ερώτηση Z1	Απόλυτες Συχνότητες	Σχετικές Συχνότητες
Καθόλου	9	10,8

Λίγο	31	37,3
Μέτρια	36	43,4
Πολύ	7	8,4
Πάρα πολύ	0	0
Σύνολο	83	100,0



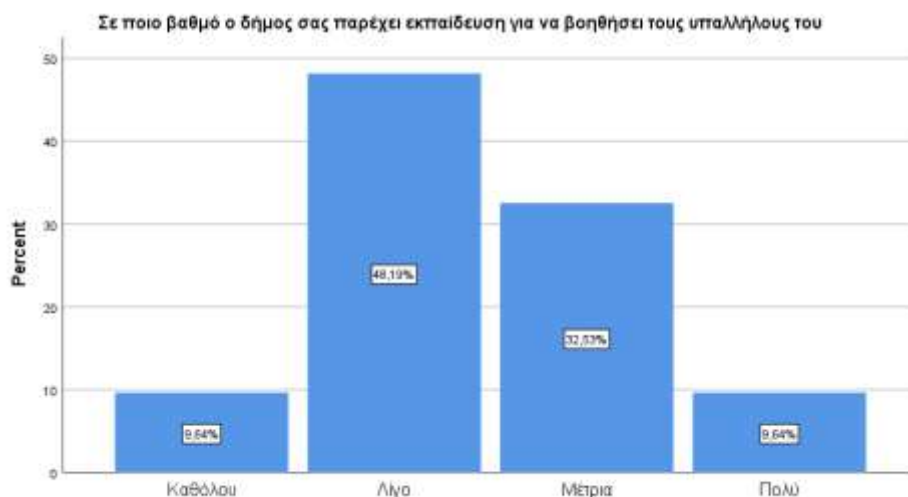
Διάγραμμα 23. Σε ποιο βαθμό ο δήμος σας διαθέτει συγκεκριμένους οδηγούς που περιγράφουν τι επιτρέπεται να κάνουν οι εργαζόμενοι με τους υπολογιστές τους;

Η δεύτερη από αυτές διερευνούσε τον βαθμό στον οποίο ο δήμος παρέχει εκπαίδευση για να βοηθήσει τους υπαλλήλους του να βελτιώσουν τις γνώσεις τους σε θέματα ασφάλειας πληροφοριών. Με βάση τα αποτελέσματα της έρευνας, όπως αυτά παρουσιάζονται αναλυτικά στον παρακάτω πίνακα και το αντίστοιχο διάγραμμα, το 57,8% του δείγματος δηλώνει ότι αυτό συμβαίνει «καθόλου» ή «λίγο», όταν «πολύ» δηλώνει ότι συνέβη το 9,6% του δείγματος.

Πίνακας 25. Σε ποιο βαθμό ο δήμος σας παρέχει εκπαίδευση για να βοηθήσει τους υπαλλήλους του να βελτιώσουν τις γνώσεις τους σε θέματα ασφάλειας πληροφοριών;

Ερώτηση Z2	Απόλυτες Συχνότητες	Σχετικές Συχνότητες
Καθόλου	8	9,6
Λίγο	40	48,2
Μέτρια	27	32,5
Πολύ	8	9,6

Πάρα πολύ	0	0
Σύνολο	83	100,0



Διάγραμμα 24. Σε ποιο βαθμό ο δήμος σας παρέχει εκπαίδευση για να βοηθήσει τους υπαλλήλους του να βελτιώσουν τις γνώσεις τους σε θέματα ασφάλειας πληροφοριών;

Η τρίτη από αυτές διερευνούσε τον βαθμό στον οποίο το προσωπικό γνωρίζει την πολιτική ασφάλειας πληροφοριών. Με βάση τα αποτελέσματα της έρευνας, όπως αυτά παρουσιάζονται αναλυτικά στον παρακάτω πίνακα και το αντίστοιχο διάγραμμα, το 50,6% του δείγματος δηλώνει ότι αυτό συμβαίνει «καθόλου» ή «λίγο», όταν «πολύ» δηλώνει ότι συνέβη το 9,6% του δείγματος.

Πίνακας 26. Σε ποιο βαθμό το προσωπικό γνωρίζει την πολιτική ασφάλειας πληροφοριών;

Ερώτηση Z3	Απόλυτες Συχνότητες	Σχετικές Συχνότητες
Καθόλου	11	13,3
Λίγο	31	37,3
Μέτρια	33	39,8
Πολύ	8	9,6
Πάρα πολύ	0	0
Σύνολο	83	100,0



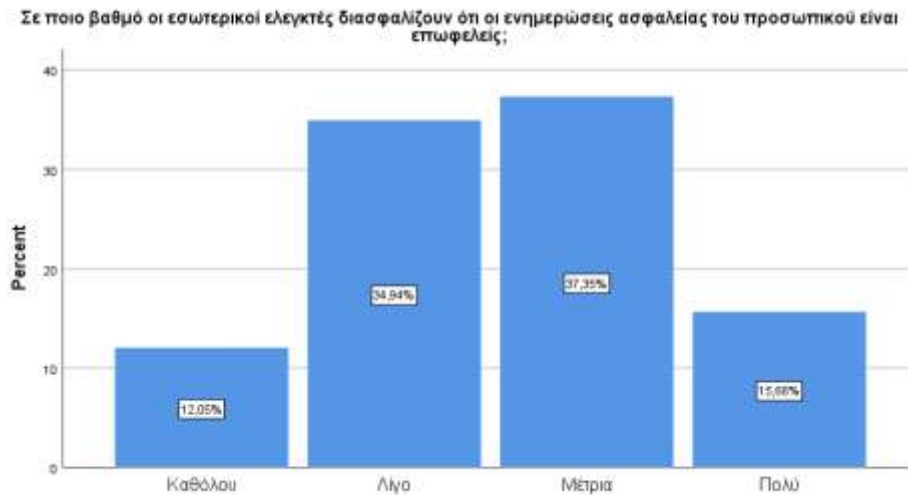


Διάγραμμα 25. Σε ποιο βαθμό το προσωπικό γνωρίζει την πολιτική ασφάλειας πληροφοριών;

Η τέταρτη και τελευταία από αυτές διερευνούσε τον βαθμό στον οποίο οι εσωτερικοί ελεγκτές διασφαλίζουν ότι οι ενημερώσεις ασφαλείας του προσωπικού είναι επωφελείς. Με βάση τα αποτελέσματα της έρευνας, όπως αυτά παρουσιάζονται αναλυτικά στον παρακάτω πίνακα και το αντίστοιχο διάγραμμα, το 46,9% του δείγματος δηλώνει ότι αυτό συμβαίνει «καθόλου» ή «λίγο», όταν «πολύ» δηλώνει ότι συνέβη το 15,7% του δείγματος.

Πίνακας 27. Σε ποιο βαθμό οι εσωτερικοί ελεγκτές διασφαλίζουν ότι οι ενημερώσεις ασφαλείας του προσωπικού είναι επωφελείς;

Ερώτηση Z4	Απόλυτες Συχνότητες	Σχετικές Συχνότητες
Καθόλου	10	12,0
Λίγο	29	34,9
Μέτρια	31	37,3
Πολύ	13	15,7
Πάρα πολύ	0	0
Σύνολο	83	100,0



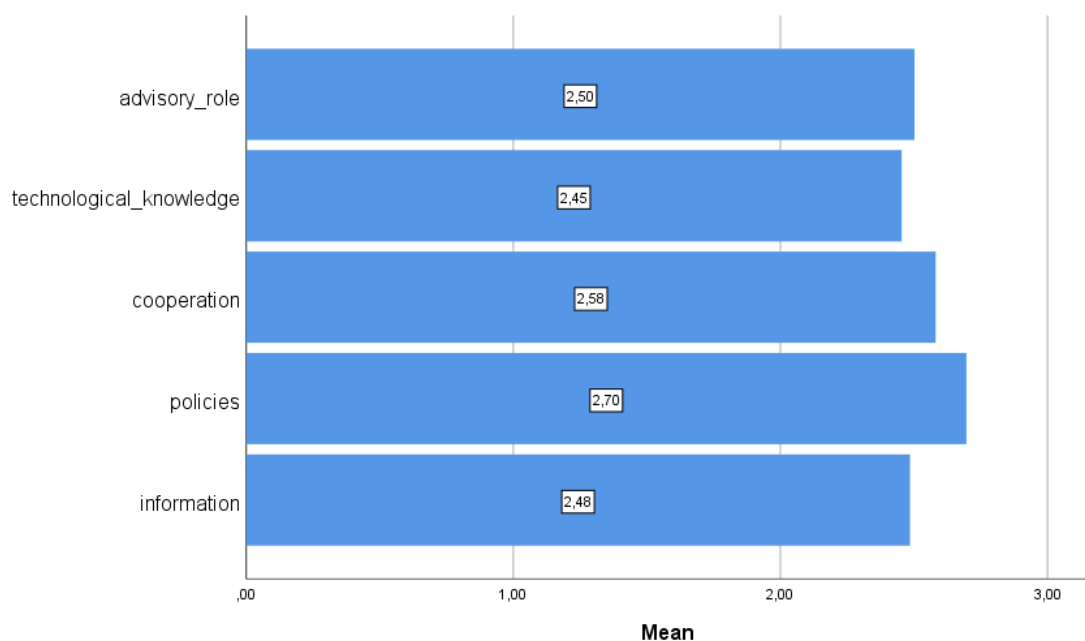
Διάγραμμα 26. Σε ποιο βαθμό οι εσωτερικοί ελεγκτές διασφαλίζουν ότι οι ενημερώσεις ασφαλείας του προσωπικού είναι επωφελείς;

#### 4.8 Οι συνολικές διαστάσεις του ερωτηματολογίου

Εξάλλου, ο επόμενος πίνακας και το αντίστοιχο διάγραμμα, παρουσιάζονται τα συνολικά αποτελέσματα για τις διαστάσεις του ερωτηματολογίου. Για την ασφάλεια, η ελάχιστη τιμή είναι 0,67, η μέγιστη τιμή είναι 3,00, η μέση τιμή είναι 1,3855 και η τυπική απόκλιση είναι 0,56665. Στην περίπτωση του συμβουλευτικού ρόλου, η ελάχιστη τιμή είναι 1,00, η μέγιστη τιμή είναι 4,00, η μέση τιμή είναι 2,5020 και η τυπική απόκλιση είναι 0,64680. Όσον αφορά τις τεχνολογικές γνώσεις, η ελάχιστη τιμή είναι 1,00, η μέγιστη τιμή είναι 3,67, η μέση τιμή είναι 2,4538 και η τυπική απόκλιση είναι 0,58104. Για τη συνεργασία, η ελάχιστη τιμή είναι 1,00, η μέγιστη τιμή είναι 4,00, η μέση τιμή είναι 2,5813 και η τυπική απόκλιση είναι 0,66386. Όσον αφορά τις πολιτικές, η ελάχιστη τιμή είναι 1,20, η μέγιστη τιμή είναι 4,20, η μέση τιμή είναι 2,6964 και η τυπική απόκλιση είναι 0,77545. Τέλος, σε σχέση με την πληροφόρηση, η ελάχιστη τιμή είναι 1,00, η μέγιστη τιμή είναι 4,00, η μέση τιμή είναι 2,4849 και η τυπική απόκλιση είναι 0,68002.

Πίνακας 28. Οι συνολικές διαστάσεις του ερωτηματολογίου

	N	Minimum	Maximum	Mean	Std. Deviation
security	83	,67	3,00	1,3855	,56665
Advisoryrole	83	1,00	4,00	2,5020	,64680
Technologicalknowledge	83	1,00	3,67	2,4538	,58104
cooperation	83	1,00	4,00	2,5813	,66386
policies	83	1,20	4,20	2,6964	,77545
information	83	1,00	4,00	2,4849	,68002



Διάγραμμα 27. Οι συνολικές διαστάσεις του ερωτηματολογίου

#### 4.9 Συσχετίσεις μεταξύ των διαστάσεων

Στην ενότητα αυτή παρουσιάζονται οι συσχετίσεις ανάμεσα στις διαστάσεις που σχετίζονται με τον εσωτερικό έλεγχο. Οι συντελεστές συσχέτισης Pearson που παρουσιάζονται στον πίνακα υποδεικνύουν τις σχέσεις μεταξύ των μεταβλητών συμβουλευτικού ρόλου, τεχνολογικής γνώσης, συνεργασίας, των πολιτικών και της πληροφόρησης. Όλες οι συσχετίσεις είναι στατιστικά σημαντικές, με τιμές  $p$

μικρότερες από 0,001, γεγονός που υποδηλώνει υψηλό επίπεδο εμπιστοσύνης σε αυτές τις σχέσεις.

Αναλυτικότερα, υπάρχει ισχυρή θετική συσχέτιση μεταξύ του συμβουλευτικού ρόλου και της τεχνολογικής γνώσης ( $r = 0,616$ ), καθώς και μεταξύ του συμβουλευτικού ρόλου και της συνεργασίας ( $r = 0,600$ ). Αυτό σημαίνει ότι όσο αυξάνεται η αξία του συμβουλευτικού ρόλου, τόσο η τεχνολογική γνώση όσο και η συνεργασία τείνουν να αυξάνονται επίσης. Υπάρχει επίσης μια μέτρια θετική συσχέτιση μεταξύ συμβουλευτικού ρόλου και πολιτικών ( $r = 0,564$ ) και μεταξύ συμβουλευτικού ρόλου και πληροφόρησης ( $r = 0,491$ ). Αυτό υποδηλώνει ότι η αύξηση του συμβουλευτικού ρόλου συνδέεται με την αύξηση των πολιτικών και των πληροφοριών. Επιπλέον, παρατηρείται μια ισχυρή θετική συσχέτιση μεταξύ της τεχνολογικής γνώσης και της συνεργασίας ( $r = 0,707$ ), που σημαίνει ότι η υψηλότερη τεχνολογική γνώση συνδέεται με μεγαλύτερη συνεργασία. Ομοίως, υπάρχει μια μέτρια θετική συσχέτιση μεταξύ της τεχνολογικής γνώσης και των πολιτικών ( $r = 0,439$ ) και μεταξύ της τεχνολογικής γνώσης και της πληροφορίας ( $r = 0,480$ ), υποδηλώνοντας ότι όσο αυξάνεται η τεχνολογική γνώση, οι πολιτικές και οι πληροφορίες τείνουν να αυξάνονται. Η σχέση μεταξύ συνεργασίας και πολιτικών είναι ισχυρή και θετική ( $r = 0,624$ ), υποδεικνύοντας ότι η αύξηση της συνεργασίας συνδέεται με αύξηση των πολιτικών. Υπάρχει επίσης ισχυρή θετική συσχέτιση μεταξύ συνεργασίας και πληροφόρησης ( $r = 0,604$ ), αποδεικνύοντας ότι η μεγαλύτερη συνεργασία συνδέεται με υψηλότερα επίπεδα πληροφόρησης. Τέλος, η ισχυρότερη συσχέτιση βρίσκεται μεταξύ πολιτικών και πληροφοριών ( $r = 0,779$ ), γεγονός που αποκαλύπτει ότι καθώς αυξάνονται οι πολιτικές, οι πληροφορίες τείνουν επίσης να αυξάνονται σημαντικά.

Πίνακας 29. Συσχετίσεις μεταξύ των χαρακτηριστικών του εσωτερικού ελέγχου

Correlations						
		advisoryr ole	technological knowledge	cooperat ion	policies	informatio n
advisoryro le	PearsonCorrel ation	1	,616**	,600**	,564**	,491**
	Sig. (2-tailed)		,000	,000	,000	,000

	N	83	83	83	83	83
technological knowledge	Pearson Correlation	,616**	1	,707**	,439**	,480**
	Sig. (2-tailed)	,000		,000	,000	,000
	N	83	83	83	83	83
cooperation	Pearson Correlation	,600**	,707**	1	,624**	,604**
	Sig. (2-tailed)	,000	,000		,000	,000
	N	83	83	83	83	83
policies	Pearson Correlation	,564**	,439**	,624**	1	,779**
	Sig. (2-tailed)	,000	,000	,000		,000
	N	83	83	83	83	83
information	Pearson Correlation	,491**	,480**	,604**	,779**	1
	Sig. (2-tailed)	,000	,000	,000	,000	
	N	83	83	83	83	83

Η συσχέτιση μεταξύ ασφάλειας και συμβουλευτικού ρόλου είναι ασθενής και όχι στατιστικά σημαντική ( $r = 0,042$ ,  $p = 0,705$ ). Αυτό σημαίνει ότι δεν υπάρχουν ισχυρά στοιχεία που να υποδηλώνουν σχέση μεταξύ ασφάλειας και συμβουλευτικού ρόλου. Ομοίως, η συσχέτιση μεταξύ ασφάλειας και τεχνολογικής γνώσης είναι επίσης ασθενής και όχι στατιστικά σημαντική ( $r = -0,060$ ,  $p = 0,587$ ), γεγονός που δείχνει ότι δεν υπάρχει ισχυρή σχέση μεταξύ ασφάλειας και τεχνολογικής γνώσης. Ωστόσο, υπάρχει μια στατιστικά μη σημαντική, ασθενής θετική συσχέτιση μεταξύ ασφάλειας και συνεργασίας ( $r = 0,180$ ,  $p = 0,103$ ). Βρίσκεται θετική συσχέτιση μεταξύ (έλλειψης) ασφάλειας και πολιτικών, η οποία είναι ασθενής και στατιστικά σημαντική ( $r = 0,281$ ,  $p = 0,010$ ). Αυτό σημαίνει ότι καθώς αυξάνεται η έλλειψη ασφάλειας, οι πολιτικές τείνουν επίσης να αυξάνονται. Τέλος, η συσχέτιση μεταξύ (έλλειψης) ασφάλειας και πληροφόρησης είναι επίσης θετική και στατιστικά σημαντική ( $r = 0,300$ ,  $p = 0,006$ ).

Πίνακας 30. Συσχετίσεις μεταξύ των χαρακτηριστικών του εσωτερικού ελέγχου και της ασφάλειας

Correlations							
		security	advisoryrole	technologicalknowledge	cooperation	policies	information
security	PearsonCorrelation	1	,042	-,060	,180	,281*	,300**
	Sig. (2-tailed)		,705	,587	,103	,010	,006
	N	83	83	83	83	83	83
advisoryrole	PearsonCorrelation	,042	1	,616**	,600**	,564**	,491**
	Sig. (2-tailed)	,705		,000	,000	,000	,000
	N	83	83	83	83	83	83
technologicalknowledge	PearsonCorrelation	-,060	,616**	1	,707**	,439**	,480**
	Sig. (2-tailed)	,587	,000		,000	,000	,000
	N	83	83	83	83	83	83
cooperation	PearsonCorrelation	,180	,600**	,707**	1	,624**	,604**
	Sig. (2-tailed)	,103	,000	,000		,000	,000
	N	83	83	83	83	83	83
policies	PearsonCorrelation	,281*	,564**	,439**	,624**	1	,779**
	Sig. (2-tailed)	,010	,000	,000	,000		,000
	N	83	83	83	83	83	83
information	PearsonCorrelation	,300**	,491**	,480**	,604**	,779**	1
	Sig. (2-tailed)	,006	,000	,000	,000	,000	
	N	83	83	83	83	83	83

#### 4.10 Η στατιστικά σημαντική επίδραση των δημογραφικών χαρακτηριστικών

Ο επόμενος πίνακας παρουσιάζει μια σύγκριση των μέσων βαθμολογιών συμβουλευτικού ρόλου μεταξύ δύο ομάδων, των ανδρών και των γυναικών. Στο δείγμα περιλαμβάνονται 31 άνδρες και 52 γυναίκες. Η μέση βαθμολογία συμβουλευτικού ρόλου για τους άνδρες είναι 2,23, με τυπική απόκλιση 0,669. Για τις γυναίκες, η μέση βαθμολογία συμβουλευτικού ρόλου είναι 2,63, με τυπική απόκλιση 0,768. Το αποτέλεσμα της τ-τεστ ( $t = -2,459$ ) υποδεικνύει μια στατιστικά σημαντική διαφορά μεταξύ των μέσων, με τιμή  $p = 0,016$ , η οποία είναι μικρότερη από το κοινό επίπεδο σημαντικότητας 0,05. Με βάση αυτά τα αποτελέσματα, μπορούμε να συμπεράνουμε ότι υπάρχει σημαντική διαφορά στη βαθμολογία συμβουλευτικού ρόλου μεταξύ ανδρών και γυναικών, με τις γυναίκες να έχουν υψηλότερη μέση βαθμολογία συμβουλευτικού ρόλου από τους άνδρες.

Πίνακας 31. Η στατιστικά σημαντική επίδραση του φύλου

Group Statistics						
	Φύλο	N	Mean	Std. Deviation	t	p-value
συμβουλευτικός ρόλος	Άντρας	31	2,23	,669		
	Γυναίκα	52	2,63	,768	-2,459	,016

#### 4.11 Η στατιστικά σημαντική επίδραση των χαρακτηριστικών των δήμων

Τέλος, ο κύκλος εργασιών των δήμων φαίνεται να επηρεάζει την ασφάλεια και τις πολιτικές σχετικά με τον εσωτερικό έλεγχο, όπως φαίνεται στον παρακάτω πίνακα.

Πίνακας 32. Η στατιστικά σημαντική επίδραση του κύκλου εργασιών των δήμων

		N	Mean	Std. Deviation	F	p-value
ασφάλεια	κάτω από 2 εκατομμύρια	8	1,63	,744		
	2-10 εκατομμύρια	22	1,77	,528		
	10-50 εκατομμύρια	42	1,26	,587		
	Πάνω από 50 εκατομμύρια	11	1,27	,467		
	Total	83	1,43	,609	4,395	,007
πολιτικές	κάτω από 2 εκατομμύρια	8	2,38	,518		
	2-10 εκατομμύρια	22	2,86	,834		
	10-50 εκατομμύρια	42	2,52	,862		
	Πάνω από 50 εκατομμύρια	11	3,27	1,009		
	Total	83	2,70	,880	2,925	,039

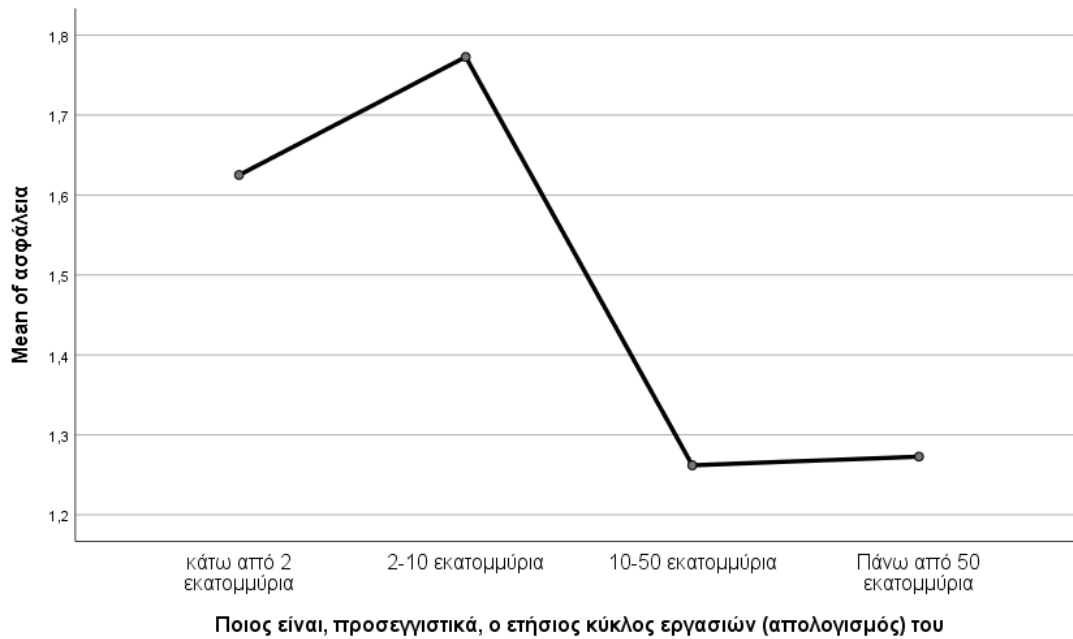
Αναλυτικότερα και σε σχέση με το post hoc test LSD, η έλλειψη ασφάλειας είναι μεγαλύτερη σε δήμους με ετήσιους κύκλους εργασιών από 2 έως 10 εκατομμύρια ευρώ σε σχέση με τους δήμους με κύκλους εργασιών από 10 έως 50 εκατομμύρια ευρώ ( $p\text{-value}= 0.001<0.05$ ) και σε σχέση με τους δήμους με κύκλους εργασιών πάνω από 50 εκατομμύρια ευρώ ( $p\text{-value}= 0.021<0.05$ ). Επιπλέον, οι πολιτικές για τον εσωτερικό έλεγχο είναι εντονότερες και συχνότερες στους δήμους με κύκλους εργασιών πάνω από 50 εκατομμύρια ευρώ σε σχέση με τους δήμους με κύκλους εργασιών από 10 έως 50 εκατομμύρια ευρώ ( $p\text{-value}= 0.011<0.05$ ) και σε σχέση με τους δήμους με κύκλους εργασιών κάτω από 2 εκατομμύρια ευρώ ( $p\text{-value}= 0.006<0.05$ ).

Πίνακας 33. Τα αποτελέσματα του posthoc test LSD

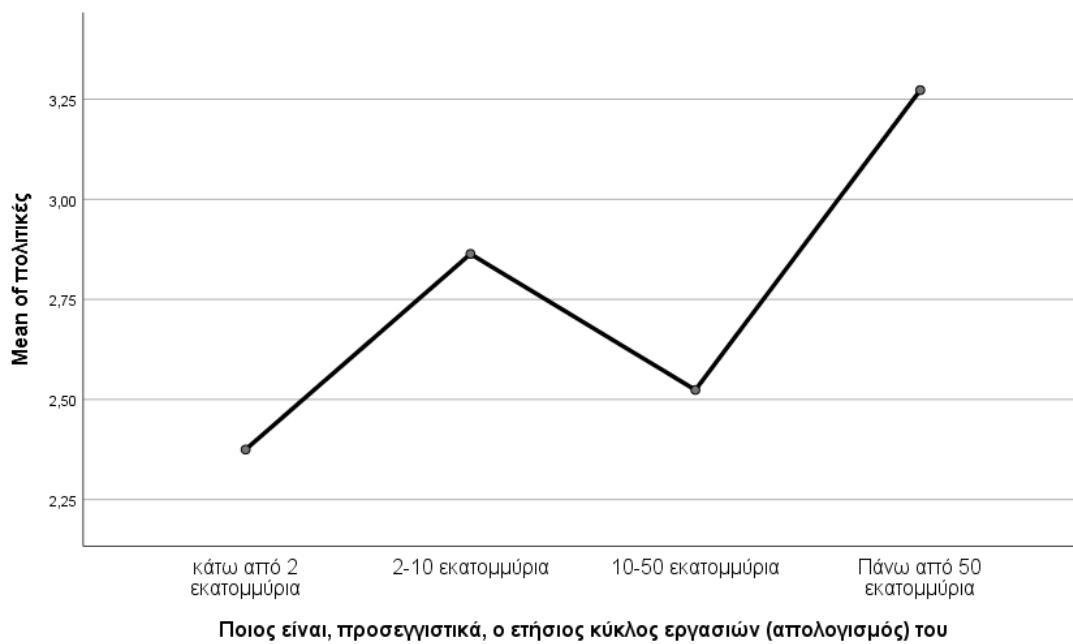
Multiple Comparisons					
LSD					
Dependent Variable	(I) Ποιος είναι, προσεγγιστικά, ο ετήσιος κύκλος εργασιών (απολογισμός) του	(J) Ποιος είναι, προσεγγιστικά, ο ετήσιος κύκλος εργασιών (απολογισμός) του	Mean Difference (I-J)	Std. Error	Sig.
ασφάλεια	κάτω από 2	2-10 εκατομμύρια	-,148	,237	,535



	εκατομμύρια	10-50 εκατομμύρια	,363	,221	,105
		Πάνω από 50 εκατομμύρια	,352	,267	,190
	2-10 εκατομμύρια	κάτω από 2 εκατομμύρια	,148	,237	,535
		10-50 εκατομμύρια	,511*	,151	,001
		Πάνω από 50 εκατομμύρια	,500*	,212	,021
	10-50 εκατομμύρια	κάτω από 2 εκατομμύρια	-,363	,221	,105
		2-10 εκατομμύρια	-,511*	,151	,001
		Πάνω από 50 εκατομμύρια	-,011	,194	,956
	Πάνω από 50 εκατομμύρια	κάτω από 2 εκατομμύρια	-,352	,267	,190
		2-10 εκατομμύρια	-,500*	,212	,021
		10-50 εκατομμύρια	,011	,194	,956
	πολιτικές	κάτω από 2 εκατομμύρια	2-10 εκατομμύρια	-,489	,351
10-50 εκατομμύρια			-,149	,328	,651
Πάνω από 50 εκατομμύρια			-,898*	,395	,026
2-10 εκατομμύρια		κάτω από 2 εκατομμύρια	,489	,351	,168
		10-50 εκατομμύρια	,340	,224	,133
		Πάνω από 50 εκατομμύρια	-,409	,314	,196
10-50 εκατομμύρια		κάτω από 2 εκατομμύρια	,149	,328	,651
		2-10 εκατομμύρια	-,340	,224	,133
		Πάνω από 50 εκατομμύρια	-,749*	,288	,011
Πάνω από 50 εκατομμύρια		κάτω από 2 εκατομμύρια	,898*	,395	,026
		2-10 εκατομμύρια	,409	,314	,196
		10-50 εκατομμύρια	,749*	,288	,011



Διάγραμμα 28. Διαγραμματική απεικόνιση της πρώτης στατιστικά σημαντικής διαφοράς του κύκλου εργασιών των δήμων



Διάγραμμα 29. Διαγραμματική απεικόνιση της πρώτης στατιστικά σημαντικής διαφοράς του κύκλου εργασιών των δήμων

## Συμπεράσματα

Ο εσωτερικός έλεγχος και η κυβερνοασφάλεια αποκτούν ολοένα και μεγαλύτερη σημασία στον δημόσιο τομέα, ιδιαίτερα για τους δήμους, καθώς προσπαθούν να προστατεύσουν ευαίσθητα δεδομένα και να διατηρήσουν την εμπιστοσύνη του κοινού. Ως κεντρικό συμπέρασμα της παρούσας εργασίας μπορεί να υπογραμμιστεί η σημασία αυτών των δύο πτυχών στο πλαίσιο των λειτουργιών της τοπικής αυτοδιοίκησης. Ο εσωτερικός έλεγχος διαδραματίζει ζωτικό ρόλο στη διασφάλιση ότι οι δήμοι διατηρούν ισχυρούς εσωτερικούς κανόνες λειτουργίας και συμμορφώνονται με τους σχετικούς κανονισμούς, πολιτικές και διαδικασίες. Αυτοί οι έλεγχοι είναι σημαντικοί για τον εντοπισμό τομέων βελτίωσης, τον εντοπισμό απάτης και την ενίσχυση της αποδοτικότητας των οργανισμών τοπικής αυτοδιοίκησης. Αξιολογώντας την αποτελεσματικότητα της διαχείρισης κινδύνου, οι εσωτερικοί ελεγκτές μπορούν να βοηθήσουν τις τοπικές κυβερνήσεις να διαφυλάξουν την οικονομική και λειτουργική τους ακεραιότητα.

Η κυβερνοασφάλεια, από την άλλη πλευρά, είναι απαραίτητο στοιχείο της σύγχρονης διακυβέρνησης του δημόσιου τομέα. Καθώς οι δήμοι βασίζονται όλο και περισσότερο στην ψηφιακή τεχνολογία για την παροχή υπηρεσιών και τη διαχείριση πληροφοριών, γίνονται πιο επιρρεπείς σε απειλές στον κυβερνοχώρο. Τα μέτρα κυβερνοασφάλειας είναι απαραίτητα για την προστασία ευαίσθητων δεδομένων, τη διασφάλιση της ιδιωτικής ζωής των πολιτών και τον μετριασμό πιθανών οικονομικών απωλειών. Για τους δήμους, η ενοποίηση του εσωτερικού ελέγχου και της ασφάλειας στον κυβερνοχώρο είναι ζωτικής σημασίας για την αντιμετώπιση του περίπλοκου και εξελισσόμενου τοπίου απειλών.

Με την ενσωμάτωση αξιολογήσεων κυβερνοασφάλειας στις διαδικασίες εσωτερικού ελέγχου, οι δήμοι μπορούν να εντοπίσουν τις ευπάθειες, να αξιολογήσουν τη στάση κινδύνου τους και να εφαρμόσουν κατάλληλες στρατηγικές μετριασμού. Αυτή η συνεργασία μεταξύ των τμημάτων εσωτερικού ελέγχου και ασφάλειας στον κυβερνοχώρο μπορεί να ενισχύσει σημαντικά τη συνολική ανθεκτικότητα και ασφάλεια των τοπικών κυβερνήσεων, προς όφελος τελικά των κοινοτήτων που εξυπηρετούν.

Εξάλλου, από την έρευνα που διεξήχθη παρατηρείται ότι οι επιθέσεις κυβερνοασφάλειας στους δήμους δεν ήταν ιδιαίτερα συχνές, αν και αυτές τείνουν να γίνονται περισσότερες τα τελευταία έτη. Το γεγονός αυτό δείχνει την αύξηση της σημασίας της κυβερνοασφάλειας στην σύγχρονη εποχή, όχι μόνο για τους ιδιώτες αλλά και για τους δημόσιους φορείς και ειδικότερα τους δήμους. Αναφορικά με το 2<sup>ο</sup> ερώτημα, οι μέσες τιμές υποδηλώνουν μια μέση κατάσταση (όλες κυμαίνονταν από το 2,45 έως το 2,69 σε μια 5βάθμια κλίμακα) γεγονός που υποδηλώνει ότι όλες είναι σε ανεκτό επίπεδο αλλά έχουν πολλές δυνατότητες περαιτέρω εξέλιξης.

Στο 3<sup>ο</sup> που εξέταζε την συσχέτιση της έλλειψης ασφάλειας (όπως μετρήθηκε αθροίζοντας τις 3 σχετικές ερωτήσεις) με τις δραστηριότητες εσωτερικού ελέγχου, η ένταση των σχέσεων ήταν μικρή γεγονός που δείχνει ότι το συμπέρασμα που προέκυψε από το ερευνητικό τμήμα της εργασίας δεν είναι ιδιαίτερα ξεκάθαρο. Σε δεύτερη ανάγνωση ωστόσο φάνηκε ότι οι ανάγκη για πληροφόρηση, εκπαίδευση και εγκαθίδρυση πολιτικών εσωτερικού ελέγχου έρχονται μάλλον ως απάντηση στον κίνδυνο έλλειψης της κυβερνοασφάλειας (αφού αυτός ενδεχομένως έχει πρώτα εκφραστεί με αύξηση των κυβερνοεπιθέσεων το τελευταίο διάστημα) και όχι προληπτικά και εξαρχής.

Αυτό, σε κάθε περίπτωση αποτελεί μια ερμηνεία των στατιστικών αποτελεσμάτων της εργασίας. Τα συμπεράσματα της έρευνας των Loiset al. (2021), στην οποία στηρίχτηκε σε μεγάλο βαθμό η παρούσα έρευνα συμφωνούν ως προς το σκέλος των πολιτικών ( το ακριβές τους συμπέρασμα είναι ότι τα πρότυπα ασφαλείας εσωτερικού ελέγχου σχετίζονται αντίστροφα με τον αριθμό των παραβιάσεων, δηλαδή σχετίζονται με την έλλειψη κυβερνοασφάλειας όπως ορίστηκε στην παρούσα εργασία). Από την άλλη πλευρά, παρόμοια σχέση οι εν λόγω ερευνητές βρήκαν για τον συμβουλευτικό ρόλο του εσωτερικού ελέγχου, ενώ η παρούσα εργασία όπως σημειώθηκε και νωρίτερα βρήκε για την πληροφόρηση και την εκπαίδευση.

Σε αυτό το σημείο είναι απαραίτητο να γίνει αναφορά και στους περιορισμούς της παρούσας εργασίας. Οι περιορισμοί αυτοί σχετίζονται αφενός με το μικρό δείγμα (γεγονός που στηρίχτηκε στην απροθυμία των δημοτικών υπαλλήλων να συμμετάσχουν στην έρευνα) και στο γεγονός ότι εξαιτίας αυτού του μικρού δείγματος αλλά και των σχετικά σθενών στατιστικά σημαντικών συσχετίσεων των διαστάσεων κξαι των προοπτικών εσωτερικού ελέγχου με την διάσταση της κυβερνοασφάλειας,

δεν έλαβε χώρα ανάλυση παλινδρόμησης όπως στην εργασία των Loiset al. (2021). Σε κάθε περίπτωση ωστόσο, η παρούσα εργασία έρχεται να συνεισφέρει στην έρευνα προς την κατεύθυνση που την όρισαν οι Loiset al. (2021), υπογραμμίζοντας με την σειρά της και αυτή, την ανάγκη των ελεγκτών ειδικά στους δημόσιους τομείς, να εμβαθύνουν τις γνώσεις τους σχετικά με την ασφάλεια στον κυβερνοχώρο προκειμένου να επιτύχουν την αποτελεσματικότητα των ελέγχων αυτών.

## Βιβλιογραφία

Alcaraz, C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection*, 8, 53-66.

Alcaraz, C., Roman, R., Najera, P., & Lopez, J. (2013). Security of industrial sensor networks: A survey. *Computer Standards & Interfaces*, 35(4), 647-657.

Alles, M. G. (2018). The role of internal audit in helping organizations navigate the cyber threat landscape. *Journal of Information Systems*, 32(3), 55-65.

Arena, M., & Azzone, G. (2009). Identifying organizational drivers of internal audit effectiveness. *International Journal of Auditing*, 13(1), 43-60.

Arens, A., Elder, R., & Beasley, M. (2014). *Auditing and Assurance Services: An Integrated Approach*. Pearson.

Barrett, P. (2007). Achieving better practice corporate governance in the public sector. *Australian Accounting Review*, 17(41), 3-11.

Behn, R. D. (2001). Performance management: Perspectives on progress. *Handbook of public administration*, 1-16.

Beresford, A., Rousseau, P., & Woin, M. (2018). The role of the internal audit function in the disclosure of material weaknesses. *The Accounting Review*, 93(1), 67-99.

Boin, A., & Rhinard, M. (2018). Managing transboundary crises: Identifying the building blocks of an effective response system. *Journal of Contingencies and Crisis Management*, 26(2), 208-218.

Carmichael, D. R. (2004). The PCAOB and the development of GAAS. *CPA Journal*, 74(5), 16-21.

Cavelty, M. D. (2018). Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. *Science and Engineering Ethics*, 24(5), 1399-1418.

Cohen, A., & Sayag, G. (2010). The effectiveness of internal auditing: An empirical examination of its determinants in Israeli organizations. *Australian Accounting Review*, 20(3), 296-307.

Cohen, J., & Knechel, W. R. (2017). Auditor independence, audit quality and the joint provision of non-audit services: A theoretical analysis. *Accounting and Business Research*, 47(3), 261-277.

Cooper, W. W., Seiford, L. M., & Zhu, J. (2006). *Handbook of data envelopment analysis*. Springer Science & Business Media.

COSO. (2013). Internal Control - Integrated Framework. Committee of Sponsoring Organizations of the Treadway Commission.

Daugherty, B., Tervo, W., & Dickins, D. (2012). The impact of PCAOB AS5 and the economic recession on client portfolio characteristics of the Big 4 audit firms. *Accounting Horizons*, 26(4), 659-678.

DeZoort, F. T., Houston, R. W., & Peters, M. F. (2012). The impact of internal audit function quality and contribution on audit delay. *Auditing: A Journal of Practice & Theory*, 31(1), 25-58.

Dye, K. M., & Stapenhurst, R. (1998). Pillars of integrity: The importance of supreme audit institutions in curbing corruption. The Economic Development Institute of the World Bank.

Egan, M. (2017). Skilling up for the fourth industrial revolution. *Journal of Cyber Policy*, 2(3), 325-334.

Eilifsen, A., & Wallage, P. (2013). The changing role of the auditor: From hindsight to insight and foresight. In *Research handbook on international financial reporting* (pp. 178-218). Edward Elgar Publishing.

Finklea, K. M., & Jaikaran, C. (2017). Cybersecurity: Legislation, hearings, and executive branch documents. Congressional Research Service.

Galanis S., Pazarskis M. (2022). Measuring Internal audit's assistance to LGOs' e-services security procedures: The Greek case. *International conference "Corporate*

*Governance: An Interdisciplinary Outlook*”, 24 November 2022, Sumy, Ukraine, Conference Proceedings, pp. 39-42.

Galanis S., Pazarskis M., Kyriakou M. (2023). Governance and internal control in LGOs: a systematic literature review. *International Journal of Business Governance and Ethics*, in press. DOI: 10.1504/IJBGE.2022.10052272

Gendron, Y., Bedard, J., & Gosselin, M. (2004). Getting inside the black box: A field study of practices in 'effective' audit committees. *Auditing: A Journal of Practice & Theory*, 23(1), 153-171.

Glover, S. M., & Prawitt, D. F. (2014). Enhancing Auditor Professional Skepticism: The Professional Skepticism Continuum. *Current Issues in Auditing*, 8(2), P1-P10.

Gómez-Aguilar, N., Humphrey, C., & Moizer, P. (2019). Shifting the audit expectation gap: The role of auditors and fraud detection. *Accounting Forum*, 43(1), 48-68.

Gordon, L. A. (2020). *The economics of cybersecurity. The Oxford Handbook of Cyber Security*, 51.

Gordon, L. A., Loeb, M. P., & Lucyshyn, W. (2015). Sharing information on computer systems security: An economic analysis. *Journal of Accounting and Public Policy*, 34(2), 142-161.

Harrison, T. M., & Guerrero, S. (2019). Cities and cybersecurity: Closing the gap. In *Cybersecurity in Cities and States* (pp. 3-26). Routledge.

Hayes, R., Dassen, R., Schilder, A., & Wallage, P. (2014). *Principles of Auditing: An Introduction to International Standards on Auditing*. Pearson.

Humphrey, C., Loft, A., & Woods, M. (2009). The global audit profession and the international financial architecture: Understanding regulatory relationships at a time of financial crisis. *Accounting, Organizations and Society*, 34(6-7), 810-825.

IAASB. (2018). *Handbook of International Quality Control, Auditing, Review, Other Assurance, and Related Services Pronouncements*. International Federation of Accountants.



IIA. (2017). International Professional Practices Framework (IPPF). The Institute of Internal Auditors.

IIA. (2021). International Professional Practices Framework (IPPF). The Institute of Internal Auditors.

INTOSAI. (2010). The International Standards of Supreme Audit Institutions (ISSAI) framework. International Organization of Supreme Audit Institutions.

Johnstone, K. M., & Bedard, J. C. (2004). Risk management in client acceptance decisions. *The Accounting Review*, 79(4), 1003-1025.

Kesan, J. P., Hayes, C. M., & Bashir, M. N. (2017). A comprehensive empirical study of data breach litigation. *Journal of Empirical Legal Studies*, 14(2), 258-299.

Knechel, W. R., Eilifsen, A., & Wallage, P. (2013). The future of risk-based auditing. *Managerial Auditing Journal*, 28(9), 728-748.

Knechel, W. R., Salterio, S. E., & Ballou, B. (2019). *Auditing: A Risk-Based Approach to Conducting a Quality Audit*. Cengage Learning.

Kshetri, N., & Voas, J. (2017). Cybersecurity for smart cities: A brief overview. *IT Professional*, 19(4), 8-12.

Mergel, I. (2016). Digital service teams in government. *Government Information Quarterly*, 33(1), 6-8.

Mihret, D. G. (2010). Antecedents and organizational performance implications of internal audit effectiveness: Some propositions and research agenda. *Pacific Accounting Review*, 22(3), 224-240.

Mihret, D. G., & Yismaw, A. W. (2007). Internal audit effectiveness: An Ethiopian public sector case study. *Managerial Auditing Journal*, 22(5), 470-484.

Mock, T. J., Stagliano, A. J., & Swartz, K. M. (2013). An integrated model of internal control reporting and financial reporting quality. *Journal of Accounting, Auditing & Finance*, 28(1), 1-29.

- Mock, T. J., Turner, J. L., & Vasarhelyi, M. A. (2013). The audit planning process. *Accounting Horizons*, 27(2), 219-234.
- Nerantzidis M., Pazarskis M., Drogalas G., Galanis S. (2022). Internal Auditing in the Public Sector: A systematic literature review and future research agenda. *Journal of Public Budgeting, Accounting and Financial Management*, 34(2), 189-209.
- Ouda, H. A. G. (2008). Toward a holistic model for government audit: The internal/external audit coordination (I/EAC) approach. *International Journal of Government Auditing*, 35(1), 9-15.
- Pazarskis M., Mitsopoulos K., Ioannidis G., Galanis S. (2020). Administrative state audit at Local Government Organizations in Greece. *Actual Problems of Economics*, 224(2), 68-91.
- Pazarskis M., Tavellaris G., Galanis S. (2022). The internal audit function in Greek Local Government Organizations: Critical factors of success. *International Journal of Critical Accounting*, 13(1), 60-74.
- Pazarskis M., Koutoupis A., Kyriakou M., Galanis S. (2023). Risk-based internal audit methodology for Greek local government organizations. *Journal of Operational Risk*, 18(1), 91-113.
- PCAOB. (2018). About the PCAOB. Retrieved from <https://pcaobus.org/About/Pages/default.aspx>
- Pickett, K. H. S. (2011). *The internal auditing handbook*. John Wiley & Sons.
- Rahaman, A. S. (2010). Critical accounting research in Africa: Whence and whither. *Critical Perspectives on Accounting*, 21(5), 420-427.
- Ramamoorti, S., Gramling, A. A., & Shenkir, W. G. (2009). A framework for establishing an internal audit function. *The CPA Journal*, 79(9), 24-30.
- Rezaee, Z. (2004). Causes, consequences, and deterrence of financial statement fraud. *Critical Perspectives on Accounting*, 15(1-2), 277-298.

- Romanosky, S., Sutherland, A., & Rudd, T. (2019). Content analysis of cyber insurance policies: How do carriers' price cyber risk? *Journal of Cybersecurity*, 5(1).
- Sarens, G., & Beelde, I. D. (2006). The relationship between internal audit and senior management: A qualitative analysis of expectations and perceptions. *International Journal of Auditing*, 10(3), 219-241.
- Savage, D., Zhang, X., Yu, X., Chou, P., & Wang, Q. (2015). An investigation of phishing awareness and education over time: When and how to best remind users. *Journal of Information Privacy and Security*, 11(2), 34-52.
- Schneider, A. (2012). The internal audit function and information quality: The effect of performance measurement systems. *Journal of Information Systems*, 26(1), 161-182.
- Shackelford, S. J. (2016). Governing the cybersecurity commons: A polycentric approach to cybersecurity and cybercrime. *Georgetown Journal of International Affairs*, 17(3), 87-96.
- Simnett, R., & Huggins, A. L. (2015). Integrated reporting and assurance: Where can research add value? *Sustainability Accounting, Management and Policy Journal*, 6(1), 29-53.
- Simnett, R., Vanstraelen, A., & Chua, W. F. (2009). Assurance on sustainability reports: An international comparison. *The Accounting Review*, 84(3), 937-967.
- Singleton, T. W., & Singleton, A. J. (2010). *Fraud Auditing and Forensic Accounting*. John Wiley & Sons.
- Singleton, T. W., Singleton, A. J., & Bologna, J. C. (2006). *Fraud auditing and forensic accounting*. John Wiley & Sons.
- Siponen, M. (2016). A critical assessment of IS security research between 1990-2015. *Journal of Information Systems Security*, 12(1), 29-56.
- Spencer, P., & Marsden, S. (2016). *Internal Audit: Efficiency Through Automation*. Wiley.

Voigt, P., & von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR)*. Cham, Switzerland: Springer International Publishing.

Weistroffer, H. R., Smith, C. A., & Narula, S. C. (2016). Assessing IT governance maturity: The case of San Marcos, Texas. *Government Information Quarterly*, 33(1), 188-199.

Wells, J. T. (2011). *Corporate fraud handbook: Prevention and detection*. John Wiley & Sons.

Ziegenfuss, D. E., & Gilsdorf, J. W. (1997). The evolution of internal auditing: A twenty-year study of the changes in the practice of internal auditing 1976-1996. *Managerial Auditing Journal*, 12(8), 399-405.

## Παράρτημα

Το ερωτηματολόγιο της έρευνας

A. Δημογραφικά χαρακτηριστικά και χαρακτηριστικά δήμου

Φύλο

Άντρας

Γυναίκα

Ηλικία

18-30

31-40

41-50

50 και άνω

Ποιος είναι, προσεγγιστικά, ο ετήσιος κύκλος εργασιών (απολογισμός) του δήμου

κάτω από 2 εκατομμύρια

2-10 εκατομμύρια

10-50 εκατομμύρια

Πάνω από 50 εκατομμύρια

Ποιος είναι, προσεγγιστικά, ο πληθυσμός του δήμου σας;

Κάτω από 10.000

10.000-40.000

40.000-70.000

Πάνω από 70.000

## B. Security of online services

Έχει δεχτεί ο οργανισμός σας επιθέσεις κυβερνο-ασφάλειας τους τελευταίους 12 μήνες;

Καμία

1-5

6-10

Πάνω από 10

Πόσα από τα παραπάνω περιστατικά εντοπίστηκαν σε σχέση με την εμφάνιση λειτουργικών προβλημάτων, οικονομικών απωλειών ή απώλειας φήμης

Κανένα

1-5

6-10

Πάνω από 10

Θεωρείτε ότι τα περιστατικά κυβερνο-επιθέσεων έχουν αυξηθεί τα τελευταία τρία χρόνια;

Καθόλου

Λίγο

Μέτρια

Πολύ

Πάρα πολύ

## Γ. Advisory role

Σε ποιο βαθμό οι εσωτερικοί ελεγκτές συμβουλεύουν διαφορετικά τμήματα (όπως το τμήμα πληροφορικής) σχετικά με την κερδοφορία τους;

Καθόλου

Λίγο

Μέτρια

Πολύ

Πάρα πολύ

Σε ποιο βαθμό οι εσωτερικοί ελεγκτές ενεργούν ως «παίκτες» μιας ομάδας και όχι ως υπηρεσίες επιβολής του νόμου;

Καθόλου

Λίγο

Μέτρια

Πολύ

Πάρα πολύ

Σε ποιο βαθμό οι εσωτερικοί ελεγκτές εμπλέκονται στην ασφάλεια των πληροφοριών και των πληροφοριακών συστημάτων;

Καθόλου

Λίγο

Μέτρια

Πολύ

Πάρα πολύ

#### Δ. Technological knowledge

Σε ποιο βαθμό συνεργάζονται οι ειδικοί σε θέματα ασφάλειας πληροφοριών με εσωτερικούς ελεγκτές για να διασφαλίσουν την ασφάλεια των συστημάτων πληροφοριών;

Καθόλου

Λίγο

Μέτρια

Πολύ

Πάρα πολύ

Σε ποιο βαθμό είναι περιορισμένη η τριβή μεταξύ εμπειρογνομόνων ασφάλειας πληροφοριών και εσωτερικών ελεγκτών;

Καθόλου

Λίγο

Μέτρια

Πολύ

Πάρα πολύ

Σε ποιο βαθμό η σχέση μεταξύ ειδικών σε θέματα ασφάλειας πληροφοριών και εσωτερικών ελεγκτών χαρακτηρίζεται ως στενή;

Καθόλου

Λίγο

Μέτρια

Πολύ

Πάρα πολύ

#### E. Cooperation

Σε ποιο βαθμό γνωρίζουν οι εσωτερικοί ελεγκτές την ασφάλεια των πληροφοριακών συστημάτων;

Καθόλου

Λίγο

Μέτρια

Πολύ

Πάρα πολύ

Σε ποιο βαθμό οι εσωτερικοί ελεγκτές έχουν εξειδικευμένη τεχνολογική γνώση των πληροφοριακών συστημάτων που χρησιμοποιούν;

Καθόλου

Λίγο

Μέτρια

Πολύ

Πάρα πολύ

Σε ποιο βαθμό υπάρχει εκπαίδευση για εσωτερικούς ελεγκτές σχετικά με την ασφάλεια των πληροφοριακών συστημάτων;

Καθόλου

Λίγο

Μέτρια

Πολύ

Πάρα πολύ



Σε ποιο βαθμό οι εσωτερικοί ελεγκτές διαθέτουν την πιστοποίηση Certified Information Systems Auditor (CISA);

Καθόλου

Λίγο

Μέτρια

Πολύ

Πάρα πολύ

ΣΤ. Policies and standards

Σε ποιο βαθμό υπάρχει καταγεγραμμένη Πολιτική Ασφάλειας Πληροφοριών;

Καθόλου

Λίγο

Μέτρια

Πολύ

Πάρα πολύ

Σε ποιο βαθμό ο δήμος σας χρησιμοποιεί κάποιο από τα πρότυπα ISO (ISO 27001, 27005, κ.λπ.);

Καθόλου

Λίγο

Μέτρια

Πολύ

Πάρα πολύ

Πόσο χρησιμοποιεί ο δήμος σας τα Πρότυπα για την Επαγγελματική Εφαρμογή του Εσωτερικού Ελέγχου;

Καθόλου

Λίγο

Μέτρια

Πολύ

Πάρα πολύ

Σε ποιο βαθμό ο δήμος σας χρησιμοποιεί συγκεκριμένα πλαίσια (όπως το Πρόγραμμα Αξιολόγησης και Βελτίωσης Ποιότητας);

Καθόλου

Λίγο

Μέτρια

Πολύ

Πάρα πολύ

Σε ποιο βαθμό οι εσωτερικοί ελεγκτές αξιολογούν τη συμμόρφωση με τις πολιτικές-και τα πρότυπα ασφαλείας;

Καθόλου

Λίγο

Μέτρια

Πολύ

Πάρα πολύ

## Z. Information and training

Σε ποιο βαθμό ο δήμος σας διαθέτει συγκεκριμένους οδηγούς που περιγράφουν τι επιτρέπεται να κάνουν οι εργαζόμενοι με τους υπολογιστές τους;

Καθόλου

Λίγο

Μέτρια

Πολύ

Πάρα πολύ

Σε ποιο βαθμό ο δήμος σας παρέχει εκπαίδευση για να βοηθήσει τους υπαλλήλους του να βελτιώσουν τις γνώσεις τους σε θέματα ασφάλειας πληροφοριών;

Καθόλου

Λίγο

Μέτρια

Πολύ

Πάρα πολύ

Σε ποιο βαθμό το προσωπικό γνωρίζει την πολιτική ασφάλειας πληροφοριών;

Καθόλου

Λίγο

Μέτρια

Πολύ

Πάρα πολύ

Σε ποιο βαθμό οι εσωτερικοί ελεγκτές διασφαλίζουν ότι οι ενημερώσεις ασφαλείας του προσωπικού είναι επωφελείς;

Καθόλου

Λίγο

Μέτρια

Πολύ

Πάρα πολύ