ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Η Επίδραση της Τεχνητής Νοημοσύνης στην Επιθεώρηση Πληροφοριακών Συστημάτων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

Πεχλιβανίδη Σπύρου

Επιβλέπουσα: Επίκουρη καθηγήτρια Διαμαντοπούλου Βασιλική

Μέλη εξεταστικής επιτροπής: Καθηγητής Κοκολάκης Σπυρίδων
Καθηγήτρια Καρύδα Μαρία

Σάμος, Ιούλιος 2025

Πρόλογος

Η παρούσα διπλωματική εργασία εκπονήθηκε στο πλαίσιο των σπουδών μου στο Τμήμα Μηχανικών Πληροφοριακών & Επικοινωνιακών Συστημάτων του Πανεπιστημίου Αιγαίου και επικεντρώνεται στην ανάλυση της επίδρασης της τεχνητής νοημοσύνης (Artificial Intelligence – AI) στον τομέα της επιθεώρησης πληροφοριακών συστημάτων (IT Audit). Η ραγδαία ανάπτυξη των τεχνολογιών τεχνητής νοημοσύνης έχει επιφέρει σημαντικές αλλαγές στον τρόπο με τον οποίο διεξάγονται οι έλεγχοι πληροφορικής, ενισχύοντας την ακρίβεια, την αποδοτικότητα και την ανίχνευση απειλών σε πραγματικό χρόνο.

Η επιλογή του θέματος συνδυάζει δύο κρίσιμους τομείς οι οποίοι σχετίζονται i) με την ασφάλεια των πληροφοριακών συστημάτων και ii) την αποδοτική λειτουργία τους στα πλαίσια ενός οργανισμού..Η εργασία αυτή στοχεύει να διερευνήσει τόσο τις ευκαιρίες όσο και τις προκλήσεις που προκύπτουν από την ενσωμάτωση της τεχνητής νοημοσύνης στις διαδικασίες επιθεώρησης πληροφοριακών συστημάτων.

Ευχαριστίες

Θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες στην επιβλέποντα καθηγήτρια μου, Διαμαντοπούλου Βασιλική , για την καθοδήγηση, την υποστήριξη και τις πολύτιμες παρατηρήσεις της καθ' όλη τη διάρκεια της εκπόνησης της εργασίας. Η καθοδήγησή της ήταν καθοριστική για την ανάπτυξη της επιστημονικής μεθοδολογίας και την επιτυχή ολοκλήρωση της μελέτης.

Τέλος, εκφράζω την ευγνωμοσύνη μου στην οικογένειά μου για την αδιάκοπη ηθική και ψυχολογική στήριξη, την υπομονή και την ενθάρρυνσή τους σε κάθε βήμα της ακαδημαϊκής μου πορείας.

ΠΕΧΛΙΒΑΝΙΔΗ ΣΠΥΡΙΔΩΝΑ

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

Πίνακας περιεχομένων

Λίστα Εικόνων

Λίστα Πινάκων

Ακρωνύμια

AI	Artificial Intelligence
AICPA	American Institute of Certified Public Accountants
CPA	Ορκωτοί Λογιστές
GDPR	Γενικός Κανονισμός Προστασίας Δεδομένων
IA	Internal Audit
IS	Information System
ISMS	Information Security Management System
IT Audit	Information Technology Audit
NLP	Natural Language Processing
SOC 1	Έκθεση ελέγχου χρηματοοικονομικών αναφορών
SOC 2	Έκθεση ελέγχου ασφάλειας ακεραιότητας διαθεσιμότητας συστήματος
TSC	Trust Services Criteria
ΠΣ	Πληροφοριακό Σύστημα

Περίληψη

Η διπλωματική αυτή εργασία εξετάζει την επίδραση της τεχνητής νοημοσύνης (Artificial Intelligence – AI) στον τομέα της επιθεώρησης Πληροφοριακών Συστημάτων (IT Audit), εστιάζοντας στις αλλαγές που επιφέρουν οι εν λόγω τεχνολογίες και εργαλεία στις διαδικασίες ελέγχου πληροφοριακών συστημάτων. Αρχικά, αναλύεται ο ρόλος και η σημασία του IT audit στο σύγχρονο επιχειρηματικό περιβάλλον, καθώς και τα παραδοσιακά εργαλεία και μέθοδοι που χρησιμοποιούνται. Στη συνέχεια, διερευνάται η ενσωμάτωση τεχνολογιών AI, όπως η μηχανική μάθηση και η ανάλυση μεγάλων δεδομένων, στην αυτοματοποίηση και βελτιστοποίηση των διαδικασιών ελέγχου.

Η μελέτη εξετάζει τις ευκαιρίες που προκύπτουν από την υιοθέτηση της τεχνητής νοημοσύνης, συμπεριλαμβανομένης της αυξημένης αποδοτικότητας, της βελτιωμένης ακρίβειας και της ενισχυμένης ανίχνευσης απειλών. Παράλληλα, επισημαίνονται οι προκλήσεις που σχετίζονται με την ασφάλεια δεδομένων, την ηθική χρήση της AI και τις ανάγκες για εξειδικευμένες δεξιότητες από τους επαγγελματίες του IT audit. Τέλος, παρουσιάζονται συμπεράσματα και προτάσεις για την αποτελεσματική αξιοποίηση της τεχνητής νοημοσύνης στον τομέα αυτό.

Abstract

This thesis examines the impact of Artificial Intelligence (AI) on the field of IT Audit, focusing on the transformative changes it brings to information systems auditing processes. Initially, the role and significance of IT audit in the modern business environment are analyzed, along with traditional tools and methods employed. Subsequently, the study investigates the integration of AI technologies, such as machine learning and big data analytics, into the automation and optimization of audit procedures.

The research highlights the opportunities arising from the adoption of AI, including increased efficiency, improved accuracy, and enhanced threat detection capabilities. At the same time, it identifies challenges related to data security, ethical considerations in AI usage, and the demand for specialized skills among IT audit professionals. The thesis concludes with key findings and recommendations for the effective utilization of AI in the IT audit sector.

1.Εισαγωγή

Στη σύγχρονη εποχή, η τεχνολογία αποτελεί αναπόσπαστο κομμάτι της καθημερινότητας, επηρεάζοντας κάθε πτυχή της προσωπικής και επαγγελματικής ζωής. Ένας από τους τομείς που έχουν υποστεί σημαντικές αλλαγές είναι αυτός της πληροφορικής και της ασφάλειας των πληροφοριακών συστημάτων. Η επιθεώρηση πληροφοριακών συστημάτων (εφεξής, IT Audit) αποτελεί μια κρίσιμη διαδικασία για την εξασφάλιση της ακεραιότητας, της ασφάλειας και της συμμόρφωσης των τεχνολογικών υποδομών των οργανισμών. Μέσα σε αυτό το πλαίσιο, η τεχνητή νοημοσύνη (AI) έχει αναδειχθεί ως μια καινοτόμος τεχνολογία που επιτρέπει την αυτοματοποίηση, την ανάλυση μεγάλων δεδομένων και τη λήψη αποφάσεων με μεγαλύτερη ακρίβεια και ταχύτητα.

Η AI προσφέρει τη δυνατότητα για σημαντική βελτίωση στις διαδικασίες του IT audit, μεταμορφώνοντας τον τρόπο με τον οποίο διεξάγονται οι έλεγχοι. Από την αυτοματοποίηση των διαδικασιών μέχρι την ανίχνευση πιθανών παρατυπιών σε πραγματικό χρόνο, η τεχνητή νοημοσύνη έχει τη δυνατότητα να ενισχύσει την αποτελεσματικότητα των ελεγκτικών διαδικασιών. Παρά τα οφέλη που προσφέρει, όμως, η υιοθέτηση της AI δημιουργεί και νέες προκλήσεις, όπως θέματα ηθικής, συμμόρφωσης με κανονισμούς και την ανάγκη αναβάθμισης των δεξιοτήτων των επαγγελματιών του IT audit.

Η επιθεώρηση πληροφοριακών συστημάτων , γνωστό και ως IT audit (Information Technology Audit), αποτελεί μια διαδικασία αξιολόγησης και ελέγχου των τεχνολογικών υποδομών ενός οργανισμού. Σκοπός του είναι να εξασφαλίσει ότι τα συστήματα πληροφορικής λειτουργούν με τρόπο ασφαλή, αξιόπιστο και σύμφωνο με τις σχετικές κανονιστικές απαιτήσεις. Οι έλεγχοι αυτοί έχουν ως κύριο στόχο τη διασφάλιση της προστασίας των πληροφοριών, την αξιολόγηση των κινδύνων, καθώς και την ανίχνευση πιθανών αδυναμιών που θα μπορούσαν να επηρεάσουν την επιχειρησιακή συνέχεια. Η τεχνητή νοημοσύνη (AI - Artificial Intelligence) αποτελεί έναν από τους πιο καινοτόμους και δυναμικούς τομείς της πληροφορικής, Η τεχνητή νοημοσύνη (AI - Artificial Intelligence) αποτελεί έναν από τους πιο καινοτόμους και δυναμικούς τομείς της πληροφορικής, καθώς εισάγει πρωτοποριακές μεθόδους μηχανικής μάθησης, αυτοματοποίησης και ανάλυσης μεγάλων δεδομένων, επηρεάζοντας σχεδόν κάθε βιομηχανία. Ο όρος τεχνητή νοημοσύνη αναφέρεται στην ικανότητα των μηχανών και των συστημάτων να μιμούνται τις ανθρώπινες γνωστικές λειτουργίες, όπως είναι η μάθηση, η επίλυση προβλημάτων, η λήψη αποφάσεων και η επεξεργασία φυσικής γλώσσας.

Η εξέλιξη της AI έχει αλλάξει δραστικά τον τρόπο με τον οποίο αντιλαμβανόμαστε και χρησιμοποιούμε την τεχνολογία, επιτρέποντας την αυτοματοποίηση διαδικασιών που παραδοσιακά απαιτούσαν ανθρώπινη παρέμβαση. Οι εφαρμογές της είναι ποικίλες, από απλά συστήματα, όπως τα bots που χρησιμοποιούνται σε πλατφόρμες εξυπηρέτησης πελατών, μέχρι προηγμένα συστήματα, όπως τα αυτόνομα οχήματα και οι πλατφόρμες ανάλυσης δεδομένων μεγάλης κλίμακας. **[1]**

Η μελέτη της επίδρασης της τεχνητής νοημοσύνης στο IT audit είναι απαραίτητη, καθώς η τεχνολογία μετασχηματίζει γρήγορα τον τρόπο με τον οποίο διεξάγονται οι έλεγχοι, επηρεάζοντας την αποτελεσματικότητα, την ασφάλεια και την αξιοπιστία των οργανισμών. Μέσω της κατανόησης και της αξιοποίησης των δυνατοτήτων της AI, οι οργανισμοί μπορούν να βελτιώσουν τις ελεγκτικές τους διαδικασίες, να διασφαλίσουν την προστασία των δεδομένων και να ανταποκριθούν στις νέες προκλήσεις της ψηφιακής εποχής.

1.1 Σκοπός της διπλωματικής εργασίας

Σκοπός της παρούσας διπλωματικής εργασίας είναι να εξετάσει την επίδραση της τεχνητής νοημοσύνης στο IT audit, αναλύοντας τόσο τα πλεονεκτήματα όσο και τις προκλήσεις που προκύπτουν από τη χρήση της. Μέσω της διερεύνησης των τεχνολογιών AI που χρησιμοποιούνται στον έλεγχο πληροφοριακών συστημάτων, καθώς και μέσω της ανάλυσης των στρατηγικών που υιοθετούνται για την ενσωμάτωσή τους, η εργασία φιλοδοξεί να συμβάλει στην κατανόηση των δυνατοτήτων αλλά και των περιορισμών της τεχνητής νοημοσύνης στον τομέα αυτόν.

Επιπλέον, στόχος είναι να αναδειχθούν οι βέλτιστες πρακτικές και οι μέθοδοι που μπορούν να ενισχύσουν την αποδοτικότητα, την ακρίβεια και τη διαφάνεια του IT audit, προτείνοντας τρόπους ενσωμάτωσης της AI στις καθημερινές λειτουργίες επιθεώρησης. Η εργασία εξετάζει, επίσης, τον ρόλο της AI στη δημιουργία νέων δυνατοτήτων για τον εντοπισμό ανωμαλιών και την προληπτική αντιμετώπιση κινδύνων.

Επιπλέον, εξετάζεται η επίδραση της AI στη διαμόρφωση των προτύπων συμμόρφωσης, στην ενίσχυση της ασφάλειας δεδομένων και στη διαχείριση περιστατικών ασφάλειας. Μέσα από τη σύνθεση θεωρητικής και πρακτικής γνώσης, η εργασία αποσκοπεί να προσφέρει μια ολοκληρωμένη προσέγγιση που θα υποστηρίξει επαγγελματίες και οργανισμούς στην ορθή εφαρμογή αυτών των τεχνολογιών.

1.2 Μεθοδολογία της εργασίας

Η μεθοδολογία που ακολουθήθηκε στην παρούσα διπλωματική εργασία βασίζεται σε μια συνδυαστική προσέγγιση, που περιλαμβάνει τη βιβλιογραφική έρευνα και την ανάλυση περιπτωσιολογικών μελετών (case studies). Αρχικά, πραγματοποιήθηκε εκτενής βιβλιογραφική ανασκόπηση, με στόχο τη συλλογή πληροφοριών σχετικά με την AI και την εφαρμογή της στο IT audit, μέσω επιστημονικών άρθρων, βιβλίων, αναφορών και διαδικτυακών πηγών. Στη συνέχεια, αναλύθηκαν παραδείγματα εφαρμογών τεχνολογιών AI σε πραγματικά σενάρια IT audit, με έμφαση στις προκλήσεις, τα πλεονεκτήματα και τα αποτελέσματά τους. Τα δεδομένα συγκεντρώθηκαν από δημοσιευμένα case studies, αναφορές οργανισμών και τεχνικές εκθέσεις. Η ανάλυση περιλαμβάνει συγκριτική αξιολόγηση μεταξύ παραδοσιακών εργαλείων IT audit και νέων τεχνολογιών AI, ενώ παράλληλα εξετάστηκαν στρατηγικές ενσωμάτωσης της AI σε οργανωσιακά περιβάλλοντα. Για την εξαγωγή συμπερασμάτων, χρησιμοποιήθηκε ποιοτική ανάλυση, με στόχο να αναδειχθούν οι

βασικοί παράγοντες επιτυχίας και οι πιθανές προκλήσεις. Η εργασία ακολουθεί συστηματική δομή, προκειμένου να εξασφαλιστεί η συνοχή και η πληρότητα της ανάλυσης.

1.3 Δομή της εργασίας

Η εργασία συνεχίζεται ως εξής: στο **Κεφάλαιο 2** που ακολουθεί, παρουσιάζεται το θεωρητικό πλαίσιο της μελέτης, όπου αναλύεται ο ορισμός και ο ρόλος του IT audit, καθώς και τα παραδοσιακά εργαλεία και μέθοδοι που χρησιμοποιούνται στον τομέα αυτό. Επιπλέον, δίνεται έμφαση στον ορισμό και τις κατηγορίες της τεχνητής νοημοσύνης, καθώς και στα βασικά χαρακτηριστικά και τις τεχνολογίες της, όπως η Μηχανική Μάθηση (Machine Learning), η Βαθιά Μάθηση (deep learning) και η Επεξεργασία Φυσικής Γλώσσας (natural language processing).

Κατόπιν, στο **Κεφάλαιο 3**, εξετάζεται η επίδραση της τεχνητής νοημοσύνης στο IT audit, με ανάλυση θεμάτων όπως η αυτοματοποίηση διαδικασιών audit μέσω AI, η ανάλυση δεδομένων και η λήψη αποφάσεων, καθώς και τα πλαίσια (frameworks) όπου χρησιμοποιείται η AI στον έλεγχο πληροφοριακών συστημάτων. Παράλληλα, παρουσιάζονται μελέτες περιπτώσεων (case studies) που αναδεικνύουν την πρακτική εφαρμογή της τεχνητής νοημοσύνης στον συγκεκριμένο τομέα.

Στο **Κεφάλαιο 4**, αναλύονται τα πλεονεκτήματα και οι προκλήσεις που σχετίζονται με την υιοθέτηση της AI στο IT audit. Εξετάζονται τα οφέλη που προσφέρει η AI, τα ηθικά διλήμματα που προκύπτουν, καθώς και ο ρόλος του ανθρώπινου παράγοντα, διερευνώντας αν η AI λειτουργεί ως συμπληρωματικό εργαλείο ή αντικαταστάτης του ανθρώπου.

Στη συνέχεια, στο **Κεφάλαιο 5**, εστιάζουμε στο νομικό και κανονιστικό πλαίσιο, με αναφορά στις νομοθεσίες και τους κανονισμούς που αφορούν την AI , καθώς και στις ηθικές προκλήσεις που προκύπτουν από την υιοθέτησή της στους ελέγχους συστημάτων.

Στο **Κεφάλαιο 6**, εξετάζεται η υιοθέτηση της AI στο IT auditing, με αναφορά στις διαθέσιμες τεχνολογίες και εργαλεία AI που μπορούν να χρησιμοποιηθούν, καθώς και στην ανάγκη επιμόρφωσης των επαγγελματιών IT audit για τη βέλτιστη αξιοποίησή τους.

Στο **Κεφάλαιο 7** εστιάζουμε στις μελλοντικές τάσεις, περιγράφοντας πιθανές εξελίξεις στον τομέα της τεχνητής νοημοσύνης και πώς αυτές αναμένεται να αλλάξουν τον τρόπο διεξαγωγής των IT audits στα επόμενα χρόνια.

Τέλος,στο **Κεφάλαιο 8** παρουσιάζονται τα βασικά ευρήματα της μελέτης σχετικά με την επίδραση της AI στο IT audit, καθώς και η γενικότερη συμβολή της AI στον τομέα αυτόν.

2.Θεωρητικό Πλαίσιο

2.1 Ορισμός και ρόλος του IT audit στα επιχειρησιακά περιβάλλοντα.

Στο συνεχώς εξελισσόμενο τοπίο της τεχνολογίας, οι οργανισμοί βασίζονται σε μεγάλο βαθμό στα συστήματα πληροφοριών και την ψηφιακή τους υποδομή για να λειτουργούν αποτελεσματικά και με ασφάλεια. Ωστόσο, με τις τεχνολογικές εξελίξεις έρχονται νέοι κίνδυνοι και τρωτά σημεία. Για να προσδιορίσουν την ακεραιότητα, τη διαθεσιμότητα και την εμπιστευτικότητα των δεδομένων, οι οργανισμοί στρέφονται σε ελέγχους IT – μια συστηματική αξιολόγηση των συστημάτων και των IT audits.

Ο έλεγχος πληροφορικής αποτελεί μια εις βάθος αξιολόγηση των συστημάτων, της υποδομής και των διαδικασιών πληροφορικής ενός οργανισμού. Ο βασικός του στόχος είναι να εκτιμήσει την αποτελεσματικότητα των εσωτερικών ελέγχων και να εντοπίσει πιθανές αδυναμίες ή ευπάθειες που μπορεί να θέσουν σε κίνδυνο την εμπιστευτικότητα, την ακεραιότητα ή τη διαθεσιμότητα των πληροφοριών του οργανισμού. Οι έλεγχοι πληροφορικής εκτείνονται σε διάφορους τομείς, όπως η ασφάλεια δεδομένων, η υποδομή δικτύου, τα στοιχεία υλικού και λογισμικού, η διακυβέρνηση πληροφορικής και η συμμόρφωση με κανονισμούς. Ο έλεγχος – είτε είναι εσωτερικός είτε από τρίτο μέρος – βοηθά τους οργανισμούς να προσδιορίσουν ότι οι δομές τους λειτουργούν όσο το δυνατόν πιο αποτελεσματικά. Ο σκοπός ενός ελέγχου πληροφορικής είναι να παρέχει αποτελεσματικότητα και ασφάλεια των συστημάτων πληροφορικής.

Ένας έλεγχος πληροφορικής περιλαμβάνει:

- **Προσδιορισμός και μετριασμός κινδύνων πληροφορικής:** Οι έλεγχοι πληροφορικής επιτρέπουν στους οργανισμούς να εντοπίζουν και να διαχειρίζονται κινδύνους όπως οι κυβερνοεπιθέσεις, οι παραβιάσεις δεδομένων και οι αστοχίες συστημάτων. Οι ελεγκτές προτείνουν μέτρα μετριασμού αυτών των κινδύνων μέσω της εφαρμογής ελέγχων ασφαλείας και της ανάπτυξης σχεδίων επιχειρησιακής συνέχειας.
- **Διασφάλιση συμμόρφωσης με νόμους και κανονισμούς:** Πολλές βιομηχανίες υπόκεινται σε συγκεκριμένους νόμους και κανονισμούς που αφορούν τα συστήματα πληροφορικής και τη διαχείριση των δεδομένων τους. Μέσω των ελέγχων πληροφορικής, οι οργανισμοί διασφαλίζουν τη συμμόρφωσή τους με αυτές τις απαιτήσεις, αποφεύγοντας πιθανές νομικές συνέπειες.

Τομέας	Κανονισμός / Νομοθεσία	Έλεγχος Πληροφορικής	Σκοπός / Όφελος
Τραπεζικός	PSD2 (EU)	Πολυπαραγοντική ταυτοποίηση (MFA)	Ασφαλείς συναλλαγές, αποτροπή

			ηλεκτρονικής απάτης
Υγειονομική Περίθαλψη	GDPR (EU), HIPAA (US)	Κρυπτογράφηση, RBAC, καταγραφή πρόσβασης	Προστασία προσωπικών δεδομένων ασθενών
Βιομηχανία / Επιχειρήσεις	SOX (US)	Audit logs, διαχωρισμός αρμοδιοτήτων, αντίγραφα ασφαλείας	Εγκυρότητα οικονομικών καταγραφών, πρόληψη απάτης
Ηλεκτρονικό Εμπόριο	PCI-DSS	Firewall, περιορισμένη πρόσβαση, τακτικοί έλεγχοι	Προστασία στοιχείων πιστωτικών καρτών πελατών

Table 1-Παραδείγματα Συμμόρφωσης με Νόμους & Κανονισμούς μέσω Ελέγχων Πληροφορικής

- **Βελτίωση της αποτελεσματικότητας των πληροφοριακών συστημάτων:** Οι έλεγχοι πληροφορικής συμβάλλουν στον εντοπισμό τομέων όπου οι λειτουργίες IT μπορούν να βελτιωθούν, όπως μέσω της αυτοματοποίησης των ροών εργασίας, οδηγώντας σε μείωση του κόστους και ενίσχυση της συνολικής επιχειρηματικής απόδοσης..
- **Προστασία εταιρικών περιουσιακών στοιχείων:** Μέσω των ελέγχων IT, οι οργανισμοί μπορούν να προστατεύσουν τα περιουσιακά τους στοιχεία από μη εξουσιοδοτημένη πρόσβαση, χρήση ή καταστροφή, εντοπίζοντας και αντιμετωπίζοντας τρωτά σημεία στα συστήματά τους.
- **Διασφάλιση της ακεραιότητας των δεδομένων:** Οι έλεγχοι πληροφορικής διασφαλίζουν ότι οι βάσεις δεδομένων του οργανισμού είναι ακριβείς, ενημερωμένες και αξιόπιστες, υποστηρίζοντας έτσι τις επιχειρηματικές αποφάσεις και τη συμμόρφωση με κανονιστικές απαιτήσεις. **[2]**

Τύποι ελέγχου πληροφορικής:

Γενικοί Έλεγχοι Πληροφορικής (General IT Controls – GITCs):

Οι γενικοί έλεγχοι πληροφορικής αφορούν τις διαδικασίες και τα συστήματα που υποστηρίζουν το σύνολο των λειτουργιών μιας εταιρείας. Οι GITCs περιλαμβάνουν:

1. **Έλεγχοι συμμόρφωσης (Compliance Audits)**

   Αξιολογούν τον βαθμό τήρησης κανονισμών, βέλτιστων πρακτικών του κλάδου και σχετικών προτύπων από έναν οργανισμό. Στην πληροφορική, σημαντικοί έλεγχοι συμμόρφωσης είναι οι **SOC 1** και **SOC 2**.

   - Ο **SOC 1** εστιάζει στους ελέγχους που σχετίζονται με την οικονομική αναφορά.

- Ο **SOC 2** αξιολογεί τον σχεδιασμό και την αποτελεσματικότητα ελέγχων που αφορούν την ασφάλεια των συστημάτων και των δεδομένων, καλύπτοντας πτυχές όπως η διαθεσιμότητα των υπηρεσιών, η ακεραιότητα της επεξεργασίας, η εμπιστευτικότητα και το απόρρητο.
  Και οι δύο τύποι ελέγχων διενεργούνται από πιστοποιημένες εταιρείες CPA [1] με εξειδίκευση στην ασφάλεια πληροφοριών και στους επιχειρηματικούς ελέγχους.

2. **Αξιολογήσεις ελέγχων (Assessment Audits)**
   Εξετάζουν κατά πόσο το σύστημα είναι διαμορφωμένο ώστε να αποτρέπει δραστηριότητες υψηλού κινδύνου. Για τη διενέργεια αυτών των αξιολογήσεων χρησιμοποιούνται διάφορα πλαίσια ελέγχου. Για παράδειγμα, αν ένας εισβολέας προσπαθήσει να παραβιάσει τα συστήματα ενός οργανισμού, η επίθεση θα αποτύχει χάρη στην ισχυρή ασφάλεια ή στον σχεδιασμό που εμποδίζει τέτοιες προσπάθειες.
3. **Έλεγχοι ασφάλειας πληροφοριών (Information Security Audits)**
   Αξιολογούν τα μέτρα που έχουν τεθεί σε εφαρμογή για την προστασία των πληροφοριών από μη εξουσιοδοτημένη πρόσβαση, τροποποίηση ή διαρροή. Περιλαμβάνουν την εξέταση της διαχείρισης κινδύνων, των πολιτικών ασφαλείας, των φυσικών μέτρων προστασίας και των πρακτικών ασφαλούς διαχείρισης δεδομένων.
4. **Έλεγχοι λειτουργικής αποδοτικότητας (Operational Efficiency Audits)**
   Εξετάζουν την αποτελεσματικότητα και την αποδοτικότητα των συστημάτων και διαδικασιών πληροφορικής, διασφαλίζοντας ότι υποστηρίζουν με τον βέλτιστο τρόπο τις επιχειρησιακές απαιτήσεις.
5. **Έλεγχοι ανάκτησης από καταστροφή και συνέχειας επιχειρήσεων (Disaster Recovery and Business Continuity Audits)**
   Αξιολογούν τα σχέδια και τις διαδικασίες που εξασφαλίζουν την ανάκαμψη από καταστροφές και τη συνέχιση της λειτουργίας του οργανισμού, διασφαλίζοντας την ανθεκτικότητα σε απρόοπτα περιστατικά.
6. **Έλεγχοι δεδομένων και απορρήτου (Data Protection and Privacy Audits)**
   Εστιάζουν στη διαχείριση, την ασφάλεια και την προστασία προσωπικών δεδομένων, καθώς και στη συμμόρφωση με κανονισμούς όπως ο GDPR.

Η υιοθέτηση των ελέγχων πληροφορικής ως αναπόσπαστο μέρος της οργανωτικής διακυβέρνησης δίνει τη δυνατότητα στις επιχειρήσεις να ευδοκιμήσουν στην ψηφιακή εποχή, όπου η τεχνολογία χρησιμεύει ως η ραχοκοκαλιά των λειτουργιών τους. Αξιοποιώντας τις

[1] Το **CPA (Certified Public Accountant)** ή ορκωτός λογιστής,είναι ο επαγγελματικός τίτλος του πιστοποιημένου δημόσιου λογιστή. Ο τίτλος απονέμεται σε λογιστές που έχουν περάσει τις απαραίτητες εξετάσεις και πληρούν συγκεκριμένες εκπαιδευτικές και επαγγελματικές απαιτήσεις. Οι CPA είναι εξειδικευμένοι σε διάφορους τομείς της λογιστικής, όπως:**Χρηματοοικονομική λογιστική**: Κατάρτιση οικονομικών καταστάσεων για επιχειρήσεις και οργανισμούς.**Φορολογία**: Παροχή συμβουλών και κατάρτιση φορολογικών δηλώσεων.**Ελεγκτικές υπηρεσίες**: Διενέργεια ελέγχων στις οικονομικές καταστάσεις για να διασφαλιστεί η ακρίβεια και η συμμόρφωση με τα πρότυπα.**Συμβουλευτικές υπηρεσίες**: Παροχή συμβουλών σε επιχειρηματικά, οικονομικά και επενδυτικά ζητήματα. **[14]**

γνώσεις που αποκτήθηκαν από τους ελέγχους πληροφορικής, οι οργανισμοί μπορούν να δημιουργήσουν μια σταθερή βάση για καινοτομία, ανάπτυξη και βιώσιμη επιτυχία. **[15]**

2.2 Παραδοσιακά εργαλεία και μέθοδοι του IT Audit

Τα **System and Organization Controls** (εφεξής **SOC**) αποτελούν ένα σύνολο ελέγχων που έχει σχεδιαστεί για να βοηθήσει τις επιχειρήσεις να διασφαλίσουν ότι τα συστήματα πληροφορικής και οι διαδικασίες τους είναι ασφαλή, αξιόπιστα και λειτουργούν όπως προβλέπεται.

Οι εκθέσεις SOC είναι ιδιαίτερα χρήσιμες για εταιρείες που παρέχουν υπηρεσίες σε άλλες επιχειρήσεις (π.χ. cloud computing, διαχείριση δεδομένων), καθώς επιτρέπουν στους πελάτες να βεβαιωθούν ότι μπορούν να εμπιστευτούν τον πάροχο για την προστασία και την ορθή διαχείριση των δεδομένων τους.

Υπάρχουν τρία κύρια είδη αναφορών SOC, και κάθε ένα εξυπηρετεί διαφορετικούς σκοπούς:

2.2.1 Είδη SOC

1. **SOC 1**:

SOC 1 (System and Organization Controls 1)

Το **SOC 1** είναι ένα πλαίσιο ελέγχου που χρησιμοποιείται για την αξιολόγηση της χρηματοοικονομικής αναφοράς και των ελέγχων που σχετίζονται με υπηρεσίες παρεχόμενες από τρίτους οργανισμούς. Ειδικότερα, επικεντρώνεται στους εσωτερικούς ελέγχους μιας εταιρείας που μπορούν να επηρεάσουν τις οικονομικές καταστάσεις των πελατών της. Αυτοί οι έλεγχοι μπορεί να περιλαμβάνουν διαδικασίες όπως η τήρηση βιβλίων, η διαχείριση πληρωμών και άλλες χρηματοοικονομικές λειτουργίες.

Υπάρχουν δύο τύποι εκθέσεων SOC 1:

- **Type I**: Αξιολογεί την καταλληλότητα του σχεδιασμού των ελέγχων σε μια συγκεκριμένη χρονική στιγμή.
- **Type II**: Αξιολογεί την αποτελεσματική λειτουργία των ελέγχων σε μια χρονική περίοδο, συνήθως 6–12 μήνες.

Απαιτήσεις SOC 1

Οι εκθέσεις SOC 1 επικεντρώνονται στην αξιολόγηση των ελέγχων που επηρεάζουν την ακεραιότητα των χρηματοοικονομικών αναφορών, ιδίως όταν η εταιρεία παρέχει υπηρεσίες που επηρεάζουν τους χρηματοοικονομικούς ελέγχους των πελατών της. Οι απαιτήσεις συνδέονται με την επάρκεια και την εφαρμογή αυτών των ελέγχων.

1. Πεδίο εφαρμογής (Scope)

- **Καθορισμός συστημάτων και διαδικασιών** που επηρεάζουν τις χρηματοοικονομικές αναφορές (π.χ. μισθοδοσία, λογιστικές διαδικασίες, επεξεργασία πληρωμών).
- **Αναγνώριση επηρεαζόμενων πελατών** και επιχειρηματικών δραστηριοτήτων που βασίζονται στις υπηρεσίες και τα δεδομένα της εταιρείας.

2. Απαιτούμενοι έλεγχοι (Required Controls)

Για τη διασφάλιση της ακεραιότητας των οικονομικών δεδομένων, η έκθεση πρέπει να περιλαμβάνει ελέγχους σε τομείς όπως:

- **Έλεγχοι πρόσβασης**: Περιορισμός πρόσβασης σε κρίσιμα συστήματα και δεδομένα μόνο σε εξουσιοδοτημένους χρήστες.
- **Επεξεργασία δεδομένων**: Διασφάλιση ακρίβειας και αξιοπιστίας στην επεξεργασία, με αποτροπή σφαλμάτων.
- **Διαχωρισμός καθηκόντων**: Κατανομή αρμοδιοτήτων ώστε να αποφεύγεται η συγκέντρωση εξουσιών (π.χ. το ίδιο άτομο να μην εγκρίνει και να καταχωρεί μια συναλλαγή).
- **Καταγραφή και εποπτεία**: Παρακολούθηση ενεργειών χρηστών για εντοπισμό παρατυπιών ή μη εξουσιοδοτημένων ενεργειών.
- **Διαχείριση αλλαγών**: Έλεγχος και έγκριση κάθε αλλαγής σε συστήματα ή δεδομένα πριν την εφαρμογή της.

3. Τύποι εκθέσεων (Types of Reports)

- **Type I**: Ελέγχει τον σχεδιασμό και την εφαρμογή των ελέγχων σε συγκεκριμένη χρονική στιγμή.
- **Type II**: Εξετάζει την αποτελεσματική λειτουργία των ελέγχων σε χρονική περίοδο (6–12 μήνες).

4. Επαλήθευση και τεκμηρίωση (Verification and Documentation)

- **Τεκμηρίωση διαδικασιών**: Αναλυτική καταγραφή όλων των ελέγχων και διαδικασιών.
- **Αποδείξεις εφαρμογής**: Διατήρηση αρχείων καταγραφής, συμφωνιών και αναφορών εποπτείας.
- **Ανεξάρτητη αξιολόγηση**: Διενέργεια του ελέγχου από ανεξάρτητο ελεγκτή, όπως ορκωτό ελεγκτή (CPA).

5. Συμμόρφωση με κανονισμούς (Regulatory Compliance)

Η έκθεση μπορεί να επηρεάζεται από νομικές ή κανονιστικές απαιτήσεις, ανάλογα με τη φύση των υπηρεσιών (π.χ. **Sarbanes–Oxley Act – SOX** για την ακρίβεια των χρηματοοικονομικών αναφορών).

6. Ευρήματα και διορθωτικές ενέργειες (Findings and Corrective Actions)

Σε περίπτωση εντοπισμού αδυναμιών, η εταιρεία πρέπει να λάβει τεκμηριωμένες διορθωτικές ενέργειες και να παρακολουθεί την αποτελεσματικότητά τους.

7. Ανάπτυξη και εφαρμογή πολιτικών (Policy Development and Implementation)

Απαραίτητη η ύπαρξη πολιτικών για:

- Διαχείριση κινδύνων
- Διασφάλιση ποιότητας δεδομένων
- Προστασία συστημάτων χρηματοοικονομικών αναφορών.

Συνοπτικά, η έκθεση SOC 1 αποδεικνύει ότι οι διαδικασίες και οι έλεγχοι ενός οργανισμού για τις χρηματοοικονομικές αναφορές είναι επαρκείς και εφαρμόζονται σωστά, εξασφαλίζοντας την ακρίβεια και την ακεραιότητα των οικονομικών δεδομένων των πελατών του. **[16]**

SOC 1 Security Controls Testing(Έλεγχοι Ασφαλείας)

Στην έκθεση **SOC 1**, οι έλεγχοι ασφαλείας επικεντρώνονται κυρίως στη διασφάλιση ότι οι εσωτερικοί έλεγχοι που σχετίζονται με τις χρηματοοικονομικές αναφορές είναι επαρκείς και σωστά σχεδιασμένοι, ώστε να αποτρέπουν και να ανιχνεύουν κινδύνους που θα μπορούσαν να επηρεάσουν την ακρίβεια των οικονομικών δεδομένων.

Σε αντίθεση με το **SOC 2**, το SOC 1 δεν δίνει έμφαση σε γενικούς ελέγχους ασφάλειας πληροφοριών (π.χ. εμπιστευτικότητα, διαθεσιμότητα), αλλά εστιάζει σε ελέγχους που σχετίζονται άμεσα με την **ακεραιότητα των οικονομικών δεδομένων**.

Κύριοι έλεγχοι ασφαλείας σε μια έκθεση SOC 1

1. **Έλεγχοι πρόσβασης (Access Controls)**

- **Πρόσβαση σε συστήματα χρηματοοικονομικών αναφορών:** Διαδικασίες που διασφαλίζουν ότι μόνο εξουσιοδοτημένο προσωπικό έχει πρόσβαση σε κρίσιμες εφαρμογές και δεδομένα.
- **Διαχείριση χρηστών:** Ελεγχόμενη διαδικασία προσθήκης και αφαίρεσης χρηστών από τα συστήματα, αποτρέποντας μη εξουσιοδοτημένη πρόσβαση.
- **Ασφάλεια κωδικών πρόσβασης:** Πολιτικές που επιβάλλουν ισχυρούς κωδικούς και τακτική αλλαγή τους, ώστε να προστατεύονται οι οικονομικές πληροφορίες.

2. **Διαδικασίες καταγραφής και εποπτείας (Logging & Monitoring Controls)**

- **Καταγραφή πρόσβασης και ενεργειών:** Μηχανισμοί που καταγράφουν δραστηριότητες χρηστών και προσβάσεις σε κρίσιμα συστήματα.
- **Εποπτεία συστημάτων:** Συνεχής παρακολούθηση και ανάλυση καταγραφών για τον εντοπισμό μη εξουσιοδοτημένων αλλαγών ή ασυνήθιστων ενεργειών.

3. **Έλεγχοι διαχείρισης αλλαγών (Change Management Controls)**

- **Αλλαγές σε συστήματα και δεδομένα:** Εξουσιοδοτημένες και ελεγχόμενες αλλαγές μετά από δοκιμή, που αφορούν νέες λειτουργίες, ενημερώσεις ή διορθώσεις.
- **Αρχειοθέτηση αλλαγών:** Καταγραφή και έλεγχος κάθε αλλαγής για αποφυγή αρνητικών επιπτώσεων στις χρηματοοικονομικές αναφορές.

4. **Έλεγχοι επεξεργασίας δεδομένων (Data Processing Controls)**

- **Ακεραιότητα επεξεργασίας:** Διασφάλιση ότι τα οικονομικά δεδομένα υποβάλλονται σε επεξεργασία με ακρίβεια και χωρίς σφάλματα.

- **Προστασία από αλλοίωση:** Διαδικασίες που αποτρέπουν τυχαία ή σκόπιμη αλλοίωση οικονομικών δεδομένων.

5. Έλεγχοι ανάκαμψης και συνέχειας (Disaster Recovery & Business Continuity Controls)

- **Σχέδιο ανάκαμψης από καταστροφές:** Διαδικασίες για την έγκαιρη επαναφορά συστημάτων και δεδομένων σε περίπτωση αστοχίας ή καταστροφής.
- **Σχέδιο συνέχειας λειτουργίας:** Διασφάλιση της συνέχισης των κρίσιμων επιχειρησιακών διαδικασιών σε περίπτωση μεγάλης διακοπής λειτουργίας.

6. Έλεγχοι αποτροπής παραποίησης δεδομένων (Fraud Prevention Controls)

- **Διαχωρισμός καθηκόντων (Segregation of Duties):** Διακριτοί ρόλοι και αρμοδιότητες ώστε να αποφεύγεται η συγκέντρωση εξουσιών.
- **Επαληθεύσεις και συμφωνίες δεδομένων:** Συνεχής συμφωνία οικονομικών δεδομένων με τα αρχικά στοιχεία και περιοδικοί έλεγχοι λογαριασμών.

7. Έλεγχοι φυσικής ασφάλειας (Physical Security Controls)

- **Προστασία φυσικής πρόσβασης:** Μέτρα περιορισμού πρόσβασης σε χώρους που στεγάζουν κρίσιμα συστήματα και δεδομένα**.**
- **Ασφάλεια εξοπλισμού:** Προστασία υποδομών από φυσικές απειλές όπως κλοπή, πυρκαγιά ή ζημιά.

Συνοπτικά, οι έλεγχοι ασφαλείας σε μια έκθεση SOC 1 επικεντρώνονται στην **προστασία των οικονομικών δεδομένων** και στην αποτροπή σφαλμάτων ή παρατυπιών που θα μπορούσαν να επηρεάσουν τις χρηματοοικονομικές αναφορές. Ο στόχος τους είναι η διασφάλιση της **ακεραιότητας, της ακρίβειας και της διαφάνειας** των οικονομικών πληροφοριών.

2. SOC 2 – Trust Services Criteria (TSC):

Το **SOC 2** επικεντρώνεται στην ασφάλεια και τη διαχείριση των δεδομένων ενός οργανισμού, διασφαλίζοντας ότι εφαρμόζονται κατάλληλα μέτρα προστασίας. Η αναφορά SOC 2 βασίζεται στα **Trust Services Criteria (TSC)** του **AICPA** (American Institute of Certified Public Accountants) και αξιολογεί πέντε βασικούς τομείς:

1. **Ασφάλεια** **(Security)**
   Προστασία των συστημάτων από μη εξουσιοδοτημένη πρόσβαση, τόσο φυσική όσο και ψηφιακή.
2. **Διαθεσιμότητα** **(Availability)**
   Εξασφάλιση ότι τα συστήματα παραμένουν λειτουργικά και προσβάσιμα σύμφωνα με τις επιχειρησιακές απαιτήσεις.

3. **Ακεραιότητα επεξεργασίας (ProcessingIntegrity)**
   Διασφάλιση ότι η επεξεργασία των δεδομένων είναι ακριβής, πλήρης και πραγματοποιείται με την κατάλληλη εξουσιοδότηση.
4. **Εμπιστευτικότητα (Confidentiality)**
   Διατήρηση και διαχείριση ευαίσθητων πληροφοριών σύμφωνα με προκαθορισμένες πολιτικές απορρήτου.
5. **Μυστικότητα / Ιδιωτικότητα (Privacy)**
   Έλεγχος της συλλογής, διαχείρισης και προστασίας των προσωπικών δεδομένων σύμφωνα με ισχύοντες κανονισμούς, όπως ο GDPR.

Τύποι εκθέσεων SOC 2

Υπάρχουν δύο τύποι εκθέσεων SOC 2, με βασική διαφορά το χρονικό πλαίσιο και την έκταση της αξιολόγησης:

- **Type 1**: Αξιολογεί τον σχεδιασμό και την καταλληλότητα των ελέγχων σε συγκεκριμένη χρονική στιγμή.
- **Type 2**: Εξετάζει την αποτελεσματικότητα των ελέγχων σε μια χρονική περίοδο (συνήθως 6–12 μήνες).

SOC 2 Type 1

Η έκθεση **SOC 2 Type 1** αξιολογεί τον σχεδιασμό και την ύπαρξη των ελέγχων σε μια συγκεκριμένη χρονική στιγμή.

- **Στόχος:** Επιβεβαιώνει ότι οι διαδικασίες και τα συστήματα είναι κατάλληλα σχεδιασμένα και εφαρμόζονται τη στιγμή του ελέγχου.
- **Πεδίο:** Εστιάζει αποκλειστικά στον σχεδιασμό των ελέγχων. Ο ανεξάρτητος ελεγκτής αξιολογεί αν οι πολιτικές, οι διαδικασίες και οι μηχανισμοί που σχετίζονται με την ασφάλεια, την εμπιστευτικότητα και την ακεραιότητα των συστημάτων είναι επαρκείς και οργανωμένοι κατά τη χρονική στιγμή της αξιολόγησης.
- **Χρονικό Πεδίο:** Η έκθεση αναφέρεται σε μια δεδομένη χρονική στιγμή (**point-in-time report**) και όχι σε μια συνεχόμενη περίοδο.
- **Πλεονέκτημα:** Προσφέρει μια άμεση επισκόπηση του κατά πόσο οι έλεγχοι έχουν εγκατασταθεί σωστά, χωρίς όμως να αξιολογεί τη μακροπρόθεσμη απόδοσή τους.

SOC 2 Type 2

Η έκθεση **SOC 2 Type 2** αξιολογεί όχι μόνο τον σχεδιασμό αλλά και τη λειτουργική αποτελεσματικότητα των ελέγχων κατά τη διάρκεια μιας συγκεκριμένης χρονικής περιόδου (συνήθως 6-12 μήνες).

- **Στόχος:** Επιβεβαιώνει ότι οι έλεγχοι είναι σωστά σχεδιασμένοι και λειτουργούν αποτελεσματικά καθ' όλη τη διάρκεια της εξεταζόμενης περιόδου.

- **Πεδίο:** Καλύπτει τόσο τον σχεδιασμό όσο και την εφαρμογή των ελέγχων στην πράξη, εξετάζοντας αν οι διαδικασίες εφαρμόζονται με συνέπεια ώστε να διατηρείται η ασφάλεια των δεδομένων και των συστημάτων.
- **Χρονικό Πεδίο:** Αξιολόγηση συνεχόμενης περιόδου (6–12 μήνες), με έλεγχο της σταθερής απόδοσης των ελέγχων σε βάθος χρόνου.
- **Πλεονέκτημα:** Παρέχει μια πιο ολοκληρωμένη εικόνα της αξιοπιστίας των ελέγχων, γεγονός ιδιαίτερα σημαντικό για πελάτες που θέλουν να διασφαλίσουν τη συνεχή και σταθερή λειτουργία των συστημάτων τους.

Κύριες Διαφορές SOC2 Type1 – Type2

Χαρακτηριστικό	**SOC 2 Type 1**	**SOC 2 Type 2**
Σκοπός:	Σχεδιασμός και ύπαρξη ελέγχων	Σχεδιασμός και λειτουργία ελέγχων
Χρονικό Πλαίσιο:	Συγκεκριμένη χρονική στιγμή	Συνεχής χρονική περίοδος (6-12 μήνες)
Βάθος Ελέγχου:	Επιβεβαίωση σχεδιασμού ελέγχων	Επιβεβαίωση σχεδιασμού και λειτουργίας ελέγχων
Κατάλληλο για:	Γρήγορη αξιολόγηση συστημάτων	Πλήρης αξιολόγηση της σταθερής λειτουργίας των συστημάτων

Table 2-Χαρακτηριστικά των SOC2

Επιλογή SOC 2 Type 1 ή Type 2;

- **Type 1:** Ιδανική για οργανισμούς που χρειάζονται μια γρήγορη αξιολόγηση των ελέγχων τους, προκειμένου να επιβεβαιώσουν ότι τα συστήματά τους είναι σωστά σχεδιασμένα. Χρησιμοποιείται κυρίως από οργανισμούς που βρίσκονται στα πρώτα στάδια ανάπτυξης των διαδικασιών τους.
- **Type 2:** Παρέχει υψηλότερο επίπεδο αξιοπιστίας, καθώς αποδεικνύει όχι μόνο ότι οι έλεγχοι είναι σχεδιασμένοι σωστά, αλλά και ότι εφαρμόζονται αποτελεσματικά με την πάροδο του χρόνου. Είναι προτιμότερη επιλογή για οργανισμούς που θέλουν να επιδείξουν συνεχή συμμόρφωση και σταθερότητα στους πελάτες και τους συνεργάτες τους.

SOC 2 Απαιτήσεις (TSC):

Ασφάλεια: Σκοπός αυτής της κατηγορίας είναι η προστασία των δεδομένων του οργανισμού και των πελατών από μη εξουσιοδοτημένη πρόσβαση, τόσο φυσική όσο και ψηφιακή.

Διαθεσιμότητα: Διασφαλίζει ότι τα δεδομένα και τα συστήματα είναι διαθέσιμα όταν απαιτείται για την προβλεπόμενη λειτουργία τους, καθώς και ότι μπορούν να ανακτηθούν σε περίπτωση τεχνικής βλάβης ή περιστατικού παραβίασης δεδομένων.

Ιδιωτικότητα: Επικεντρώνεται στην προστασία των Προσωπικών Πληροφοριών Αναγνώρισης (Personally Identifiable Information – PII) από παραβιάσεις και μη εξουσιοδοτημένη πρόσβαση, σύμφωνα με τους σχετικούς κανονισμούς και πολιτικές.
Εμπιστευτικότητα: Διασφαλίζει ότι ευαίσθητες ή επιχειρηματικά κρίσιμες πληροφορίες είναι προσβάσιμες μόνο από εξουσιοδοτημένο προσωπικό, αποτρέποντας τη διαρροή ή την κακή χρήση τους.
Ακεραιότητα διεργασίας: Εξασφαλίζει ότι η επεξεργασία των δεδομένων πραγματοποιείται με ακρίβεια, πληρότητα και συνέπεια. Τα κριτήρια ακεραιότητας επεξεργασίας καλύπτουν τις εισροές και τις εξόδους δεδομένων, την ποιότητα και εγκυρότητά τους, τα χρονοδιαγράμματα επεξεργασίας και την ακρίβεια των αναφορών που παράγονται. **[17]**

Trust Services Criterion	**Πρακτική Εφαρμογή στην CloudWorkApp**
Security (Ασφάλεια)	Η CloudWorkApp χρησιμοποιεί **firewalls**, **MFA (πολλαπλή ταυτοποίηση)** και **ανίχνευση κακόβουλης δραστηριότητας** για να αποτρέψει μη εξουσιοδοτημένη πρόσβαση στα δεδομένα των πελατών.
Availability (Διαθεσιμότητα)	Υπάρχει **σύστημα εφεδρείας (backup)**, **24/7 monitoring** και **σύμβαση SLA** που εγγυάται 99.9% uptime για τους πελάτες.
Privacy (Ιδιωτικότητα)	Η εταιρεία ζητά **ρητή συγκατάθεση** για τη συλλογή δεδομένων, εφαρμόζει **πολιτική απορρήτου** συμβατή με **GDPR**, και προσφέρει στους χρήστες τη δυνατότητα **διαγραφής των δεδομένων τους**.
Confidentiality (Εμπιστευτικότητα)	Οι πελάτες που συνεργάζονται για projects μπορούν να **ορίσουν ποιος βλέπει τι**, και τα αρχεία αποθηκεύονται με **κρυπτογράφηση** τόσο κατά τη μεταφορά όσο και στην αποθήκευση.
Processing Integrity (Ακεραιότητα Διεξεργασίας)	Οι εργασίες που καταχωρούνται στο σύστημα καταγράφονται **με ακρίβεια**, δεν "χάνονται" και αποθηκεύονται σε **λογικά χρονικά διαστήματα** χωρίς σφάλματα.

Table 3-Παράδειγμα Εταιρείας: CloudWorkApp

SOC 2 Security Controls Testing(Έλεγχοι Ασφαλείας)

Στην έκθεση **SOC 2**, οι έλεγχοι ασφαλείας σχετίζονται με την αξιολόγηση των διαδικασιών και των συστημάτων που προστατεύουν τις πληροφορίες και τα συστήματα μιας εταιρείας

από μη εξουσιοδοτημένη πρόσβαση, διαρροές και παραβιάσεις. Αποτελούν θεμέλιο για τη διατήρηση της **εμπιστευτικότητας**, της **ακεραιότητας** και της **διαθεσιμότητας** των δεδομένων.

1. **Έλεγχοι Πρόσβασης (Access Controls)**
   - **Πολιτικές Διαχείρισης Χρηστών**: Καθορισμός και εφαρμογή διαδικασιών που ορίζουν ποιος έχει πρόσβαση σε ποια συστήματα, διασφαλίζοντας ότι οι χρήστες διαθέτουν μόνο τα απαραίτητα δικαιώματα.
   - **Έλεγχος Ταυτότητας & Πολιτικές Κωδικών**: Εφαρμογή ισχυρών μηχανισμών ελέγχου ταυτότητας (π.χ. πολύπλοκοι κωδικοί, πολυπαραγοντική ταυτοποίηση – MFA).
   - **Αφαίρεση Πρόσβασης**: Διασφάλιση της έγκαιρης αφαίρεσης δικαιωμάτων όταν ένας εργαζόμενος αποχωρεί ή αλλάζει ρόλο.
2. **Έλεγχοι Επίβλεψης & Καταγραφής Δραστηριότητας (Monitoring & Logging Controls)**
   - **Καταγραφή Συμβάντων**: Συστηματική καταγραφή δραστηριοτήτων χρηστών (logging) για τον εντοπισμό ύποπτης ή ασυνήθιστης δραστηριότητας.
   - **Ανάλυση Συμβάντων**: Διερεύνηση των καταγεγραμμένων περιστατικών για εντοπισμό πιθανών παραβιάσεων.
   - **Ανίχνευση Απειλών**: Χρήση συστημάτων έγκαιρης προειδοποίησης για ανίχνευση απειλών σε πραγματικό χρόνο.
3. **Έλεγχοι Ασφάλειας Δικτύου (Network Security Controls)**
   - **Firewalls & IDS**: Χρήση τειχών προστασίας και συστημάτων ανίχνευσης εισβολών για την αποτροπή μη εξουσιοδοτημένων προσβάσεων.
   - **Κρυπτογράφηση**: Εφαρμογή ισχυρής κρυπτογράφησης κατά τη μεταφορά και την αποθήκευση δεδομένων.
   - **Ασφαλείς Διασυνδέσεις**: Διασφάλιση επικοινωνίας μέσω ασφαλών πρωτοκόλλων (π.χ. TLS, VPN).
4. **Διαχείριση Αλλαγών (Change Management Controls)**
   - **Έγκριση & Τεκμηρίωση Αλλαγών**: Διαδικασίες για τον έλεγχο και την καταγραφή αλλαγών σε συστήματα και λογισμικό.
   - **Δοκιμές σε Ασφαλές Περιβάλλον**: Έλεγχος αλλαγών σε δοκιμαστικό περιβάλλον πριν την υλοποίηση.
5. **Έλεγχοι Ετοιμότητας για Ανάκτηση (Disaster Recovery & Incident Response Controls)**
   - **Σχέδια Ανάκαμψης**: Ανάπτυξη και εφαρμογή σχεδίων αποκατάστασης μετά από περιστατικά ή καταστροφές.
   - **Τακτικές Δοκιμές**: Προγραμματισμένες ασκήσεις ανάκτησης για έλεγχο της ετοιμότητας της ομάδας IT.
6. **Φυσική Ασφάλεια (Physical Security Controls)**
   - **Έλεγχος Πρόσβασης σε Εγκαταστάσεις**: Μηχανισμοί όπως κάρτες πρόσβασης, συστήματα CCTV και φύλακες ασφαλείας.
   - **Προστασία Εξοπλισμού**: Διασφάλιση ότι οι υποδομές προστατεύονται από κλοπή, βλάβες ή φυσικές καταστροφές.
7. **Εκπαίδευση & Ευαισθητοποίηση Προσωπικού (Employee Training & Awareness Controls)**

- **Εκπαίδευση Ασφάλειας**: Τακτικά προγράμματα κατάρτισης για κυβερνοαπειλές και πολιτικές ασφαλείας.
- **Ενημερωτικές Καμπάνιες**: Προγράμματα ευαισθητοποίησης για την αναγνώριση και αποφυγή κινδύνων, όπως το phishing.

3. SOC 3:

Αυτός ο τύπος αναφοράς είναι παρόμοιος με το **SOC 2**, αλλά είναι πιο απλοποιημένος. Έχει σχεδιαστεί για να κοινοποιείται στο ευρύ κοινό, χωρίς να περιλαμβάνει όλες τις λεπτομέρειες των ελέγχων. Μπορεί να χρησιμοποιηθεί από εταιρείες ως μέσο δημόσιας απόδειξης ότι τηρούν τα απαραίτητα πρότυπα ασφαλείας, χωρίς να αποκαλύπτονται τεχνικές λεπτομέρειες.
Οι βασικές αρχές που καλύπτει είναι: **Ασφάλεια**, **Διαθεσιμότητα**, **Μυστικότητα**, **Εμπιστευτικότητα** και **Ακεραιότητα Επεξεργασίας**

Προσδιορισμός του πεδίου εφαρμογής:

Αρχικά, εξετάζονται τα **Trust Services Criteria (TSC)** που ορίζονται από την AICPA. Τα κριτήρια αυτά αποτελούν τη βάση για την αξιολόγηση των συστημάτων και διαδικασιών της επιχείρησης. Δεν είναι απαραίτητο όλες οι αξιολογήσεις SOC 2 να καλύπτουν και τις πέντε κατηγορίες κριτηρίων. Είναι σημαντικό να προσδιοριστούν ποια συστήματα, πολιτικές και διαδικασίες σχετίζονται με τις ισχύουσες αρχές.

Για παράδειγμα, αν οι υπηρεσίες της εταιρείας επικεντρώνονται κυρίως στην **ασφάλεια** και τη **διαθεσιμότητα** των δεδομένων, τότε η οριοθέτηση του πεδίου εφαρμογής περιλαμβάνει τον εντοπισμό των σχετικών συστημάτων, πολιτικών και διαδικασιών που συνδέονται με αυτές τις αρχές.
Αυτή η διαδικασία οριοθέτησης εξασφαλίζει ότι ο έλεγχος επικεντρώνεται στους πιο σχετικούς τομείς και παρέχει σαφές πλαίσιο αξιολόγησης.

Καθ' όλη τη διάρκεια του ελέγχου, ο ελεγκτής εξετάζει τόσο την τεκμηρίωση του οργανισμού όσο και τα ίδια τα συστήματα, προκειμένου να εκτιμήσει την αποτελεσματικότητά τους.
Η τεκμηρίωση που μπορεί να ζητηθεί περιλαμβάνει, μεταξύ άλλων:

- Λίστες με τα περιουσιακά στοιχεία
- Λεπτομέρειες και διαδικασίες διαχείρισης αλλαγών
- Αρχεία συντήρησης εξοπλισμού
- Αρχεία καταγραφής για αντίγραφα ασφαλείας συστημάτων
- Κώδικα δεοντολογίας και πολιτικές ηθικής
- Σχέδια επιχειρηματικής συνέχειας και αντιμετώπισης περιστατικών

Επιλογή τύπου αναφοράς

Το πρώτο βήμα στη διαδικασία είναι ο καθορισμός του κατάλληλου τύπου αναφοράς **SOC 2** για τον οργανισμό παροχής υπηρεσιών.

- **SOC 2 Τύπος I**: Αξιολογεί εάν τα συστήματα έχουν σχεδιαστεί σε συμφωνία με τα **Trust Services Criteria (TSC)**. Εξετάζεται η ύπαρξη και η καταλληλότητα του σχεδιασμού των ελέγχων σε μια συγκεκριμένη χρονική στιγμή.
- **SOC 2 Τύπος II**: Αξιολογεί όχι μόνο τον σχεδιασμό των συστημάτων αλλά και την **λειτουργική τους αποτελεσματικότητα** σε βάθος χρόνου. Περιλαμβάνει την αξιολόγηση της συνέπειας και της ορθής εφαρμογής των ελέγχων στην πράξη.

Διεξαγωγή εκτίμησης κινδύνου

- Η εκτίμηση κινδύνου αποτελεί κρίσιμο βήμα για την προστασία των περιουσιακών στοιχείων μιας εταιρείας, καθώς επιτρέπει τον εντοπισμό πιθανών απειλών και την εφαρμογή κατάλληλων μέτρων προστασίας.
- Συνδράμει στην κατανόηση των κινδύνων που απειλούν τα δεδομένα και τα συστήματα. Για παράδειγμα, μπορεί να εντοπιστεί κίνδυνος μη εξουσιοδοτημένης πρόσβασης στη βάση δεδομένων πελατών.

Χαρτογράφηση ελέγχου και ανάλυση χάσματος

- Διεξαγωγή ανάλυσης κενών και χαρτογράφησης ελέγχου για να αξιολογηθεί η ευθυγράμμιση του εσωτερικού ελέγχου με τα Trust Service Criteria (TSC).
- Αυτή η διαδικασία εντοπίζει ελλείψεις στη συμμόρφωση και επιτρέπει την εφαρμογή προληπτικών μέτρων πριν τον επίσημο έλεγχο.
- Για παράδειγμα, αν το πλαίσιο απαιτεί καταγραφή δραστηριοτήτων του συστήματος, η ανάλυση κενού θα αξιολογήσει αν οι υφιστάμενοι έλεγχοι ανταποκρίνονται σε αυτή την ανάγκη.

Διεξαγωγή εσωτερικού ελέγχου

- Ο εσωτερικός έλεγχος αποτελεί κρίσιμο βήμα στην προετοιμασία για το SOC 2, διασφαλίζοντας την ασφάλεια των δεδομένων και την προστασία των περιουσιακών στοιχείων της εταιρείας.
- Για παράδειγμα, αν η εταιρεία αποθηκεύει ευαίσθητα δεδομένα πελατών, ένας εσωτερικός έλεγχος βοηθά στον εντοπισμό πιθανών κινδύνων, όπως η μη εξουσιοδοτημένη πρόσβαση.
- Επιπλέον, ο εσωτερικός έλεγχος επιτρέπει στην ομάδα διαχείρισης να εντοπίσει αδυναμίες πριν τον τελικό έλεγχο SOC 2.

Επιλογή Εξωτερικού Ελεγκτή

- Για την ολοκλήρωση της διαδικασίας SOC 2, η εταιρεία πρέπει να επιλέξει έναν ανεξάρτητο ελεγκτή, όπως έναν Ορκωτό Ελεγκτή Λογιστή ή έναν εξειδικευμένο φορέα συμμόρφωσης τρίτων.

- Όταν η εταιρεία είναι έτοιμη, οι εξωτερικοί ελεγκτές πραγματοποιούν ανεξάρτητες δοκιμές και αξιολογήσεις, παρέχοντας αμερόληπτη γνωμοδότηση σχετικά με την επάρκεια και την αποτελεσματικότητα των ελέγχων σε σχέση με τα TSC. **[5]**

Συμβουλές για έναν επιτυχημένο έλεγχο SOC 2

Ορισμένες συμβουλές για την επιτυχή ολοκλήρωση ενός ελέγχου SOC 2.

Διεξαγωγή εσωτερικών αξιολογήσεων

Πριν από τον έλεγχο SOC 2, η εκτέλεση εσωτερικών αξιολογήσεων μπορεί να βοηθήσει στον εντοπισμό τυχόν κενών ή αδυναμιών στους ελέγχους ασφαλείας. Με αυτό το βήμα, μπορούν να αντιμετωπιστούν τυχόν προβλήματα ώστε να υπάρχει βεβαιότητα για τον έλεγχο.

Εφαρμογή εκπαίδευσης ευαισθητοποίησης για την ασφάλεια

Η εκπαίδευση του προσωπικού στις βέλτιστες πρακτικές και στις ευθύνες που αφορούν την ασφάλεια είναι κρίσιμη. Η τακτική διοργάνωση σεμιναρίων και εκπαιδευτικών συνεδριών συμβάλλει στην κατανόηση του ρόλου κάθε εργαζομένου στη διατήρηση της συμμόρφωσης και ενός ασφαλούς περιβάλλοντος.

Τακτική παρακολούθηση και επανεξέταση των ελέγχων

Η συνεχής παρακολούθηση και τακτική επανεξέταση των ελέγχων ασφαλείας διασφαλίζουν τη συνεχή συμμόρφωση. Η εγκατάσταση μηχανισμών για την ανίχνευση αποκλίσεων ή περιστατικών ασφαλείας ενισχύει την αποτελεσματικότητα των μέτρων προστασίας.

Εκτέλεση αξιολογήσεων τρωτότητας και δοκιμές διείσδυσης

Η τακτική αξιολόγηση ευπαθειών και οι δοκιμές διείσδυσης εντοπίζουν και διορθώνουν αδύναμα σημεία στα συστήματα. Η πρακτική αυτή μειώνει τον κίνδυνο παραβίασης και διασφαλίζει την ευθυγράμμιση με τις βέλτιστες πρακτικές του κλάδου.

Διαδικασίες διαχείρισης αλλαγών εγγράφων

Η σωστή τεκμηρίωση των διαδικασιών διαχείρισης αλλαγών αποδεικνύει ότι οι τροποποιήσεις στα συστήματα σχεδιάζονται, δοκιμάζονται και εγκρίνονται μεθοδικά. Η τεκμηρίωση πρέπει να περιλαμβάνει αιτήματα αλλαγών, εγκρίσεις, λεπτομέρειες υλοποίησης και ελέγχους μετά την εφαρμογή.

Διατήρηση σχεδίων αντιμετώπισης περιστατικών και αποκατάστασης

Η ύπαρξη πλήρως καθορισμένων σχεδίων διαχείρισης συμβάντων και αποκατάστασης επιτρέπει την άμεση αντίδραση σε παραβιάσεις ασφάλειας. Τα σχέδια πρέπει να περιγράφουν αναλυτικά τα βήματα περιορισμού, έρευνας, αποκατάστασης και επικοινωνίας κατά τη διάρκεια και μετά από ένα περιστατικό.

Τι περιλαμβάνει ένα SOC Report:

Ένα **SOC 2 Report** αποτελεί πλούσια πηγή πληροφοριών για τον ελεγχόμενο οργανισμό. Περιλαμβάνει, μεταξύ άλλων, γενικές πληροφορίες για την εταιρεία, τη γνώμη του ελεγκτή σχετικά με τη συμμόρφωση των ελέγχων, καθώς και την περιγραφή των σχετικών δοκιμών που πραγματοποιήθηκαν. Όπου κρίνεται απαραίτητο, περιέχει επίσης συστάσεις για τη βελτίωση των πρωτοκόλλων ασφαλείας.

Ακολουθεί μια μικρή περιγραφή για κάθε ενότητα και τι περιέχει:

Ενότητα 1: Ισχυρισμός Διοίκησης

Η πρώτη ενότητα περιλαμβάνει δηλώσεις, ισχυρισμούς και πραγματικά στοιχεία που παρέχονται από τον ίδιο τον ελεγχόμενο οργανισμό. Αφορά τα συστήματα που βρίσκονται υπό έλεγχο και συντάσσεται εξ ολοκλήρου από τη διοίκηση, η οποία αναγνωρίζει ότι οι πληροφορίες είναι ακριβείς και σχετικές.

Η ενότητα αυτή συνοψίζει τις υπηρεσίες, τα προϊόντα, τη δομή, τα συστήματα και τους ελέγχους του οργανισμού, χωρίς να εισέρχεται σε τεχνικές λεπτομέρειες.

Τυπικό περιεχόμενο Ενότητας 1:

1. **Παρεχόμενες υπηρεσίες** – Περιγραφή των βασικών υπηρεσιών που προσφέρει ο οργανισμός.
2. **Στοιχεία συστήματος** – Αναφορά σε υποδομή, λογισμικό συστημάτων, ανθρώπινο δυναμικό, διαδικασίες και δεδομένα.
3. **Όψεις συστήματος** – Χαρακτηριστικά και λειτουργίες των συστημάτων.
4. **Καταγραφή και διαχείριση σημαντικών γεγονότων** – Τρόπος με τον οποίο τα συστήματα εντοπίζουν, καταγράφουν και αντιμετωπίζουν κρίσιμα περιστατικά ή συνθήκες.
5. **Διαδικασίες αναφοράς** – Μέθοδοι προετοιμασίας και παράδοσης αναφορών προς πελάτες ή ενδιαφερόμενα μέρη.
6. **Μη πληρούμενα Κριτήρια Υπηρεσιών Εμπιστοσύνης (TSC)** – Σημεία στα οποία οι έλεγχοι δεν ανταποκρίνονται πλήρως στα TSC, συνοδευόμενα από αιτιολόγηση.

Ενότητα 2: Έκθεση Ανεξάρτητου Ελεγκτή Υπηρεσίας

Αυτή η ενότητα αποτυπώνει τη βαθμολογία του ελεγκτή σχετικά με τη συμμόρφωσή. Δείχνει αν περάσατε ή όχι την αξιολόγηση. Είναι, επομένως, ένα από τα πιο σημαντικά τμήματα της έκθεσης.

Σε αυτήν την ενότητα, ο ελεγκτής μοιράζεται τη γνώμη του σχετικά με την ετοιμότητα ελέγχου SOC 2. Περιλαμβάνει επίσης μια περιγραφή του εύρους του ελέγχου, των ευθυνών του οργανισμού, της ευθύνης του ελεγκτή και εγγενών περιορισμών στην αξιολόγηση, όπως το ανθρώπινο λάθος και η παράκαμψη των ελέγχων, για να αναφέρουμε μερικά. Ακολουθούν οι τέσσερις τύποι απόψεων ελεγκτών και τι σημαίνουν:

- **Unqualified** – Εξαιρετικά αποτελέσματα!
- **Πιστοποιημένο** – Ικανοποιητικά.
- **Ανεπιθύμητη** – Αποτυχία.
- **Αποποίηση γνώμης** – Κανένα σχόλιο!

Ακολουθεί ένα **παράδειγμα έκθεσης ελέγχου SOC 2** που υπογραμμίζει τη γνώμη του ελεγκτή.

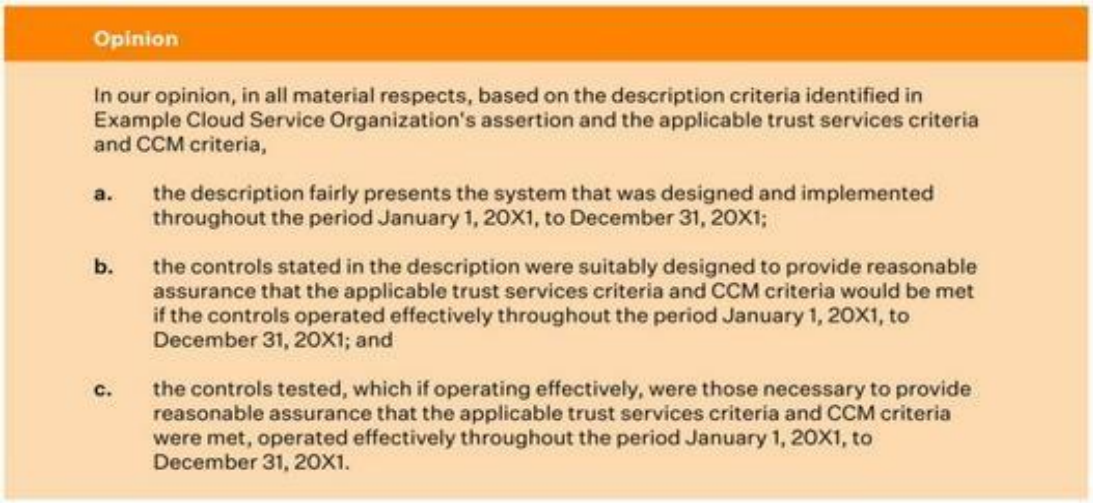


Figure 1-Ενδεικτική Αναφορά SOC 2 τύπου 2 της AICPA με τα κριτήρια στο Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM)

Με βάση την παραπάνω εικόνα: η περιγραφή του συστήματος που σχεδιάστηκε και υλοποιήθηκε κατά την περίοδο από 1 Ιανουαρίου 20X1 έως 31 Δεκεμβρίου 20X1 ανταποκρίνεται με ακρίβεια στις απαιτήσεις που ορίστηκαν. Επιπλέον, οι έλεγχοι που περιγράφονται είναι κατάλληλα σχεδιασμένοι ώστε να παρέχουν εύλογη διασφάλιση ότι πληρούνται τα κριτήρια εμπιστοσύνης και τα κριτήρια του Cloud Control Matrix (CCM), υπό την προϋπόθεση ότι οι έλεγχοι αυτοί λειτουργούν αποτελεσματικά καθ' όλη τη διάρκεια της εν λόγω περιόδου. Οι έλεγχοι που δοκιμάστηκαν, οι οποίοι είναι απαραίτητοι για την παροχή εύλογης διασφάλισης, λειτούργησαν επίσης αποτελεσματικά κατά την ίδια περίοδο.

Ενότητα 3: Περιγραφή συστήματος

Εάν ο ισχυρισμός της διοίκησης ήταν μια σύντομη επισκόπηση της περιγραφής του συστήματος του οργανισμού, αυτή η ενότητα είναι μια λεπτομερής βαθιά κατάδυση. Είναι μια ενότητα που πρέπει να διαβαστεί και καλύπτει τα συστήματα, το εύρος και τις απαιτήσεις, τα στοιχεία, τα στοιχεία ελέγχου, τους οργανισμούς υπο-υπηρεσιών και άλλες πληροφορίες συστημάτων.

Περιλαμβάνει λεπτομέρειες για τους ανθρώπινους πόρους, τους ρόλους και τις αρμοδιότητες και περιλαμβάνει επίσης τη λίστα των στοιχείων του συστήματος και των ελέγχων που ομαδοποιούνται με τα σχετικά κοινά κριτήρια.

Αυτή η ενότητα καλύπτει λεπτομερή περιγραφή του περιβάλλοντος ελέγχου, τις δραστηριότητες ελέγχου (πολιτικές και διαδικασίες), το σύστημα πληροφοριών και επικοινωνίας, την παρακολούθηση (για την αξιολόγηση της ποιότητας της απόδοσης εσωτερικού ελέγχου μέσω δοκιμών διείσδυσης και σαρώσεων ευπάθειας) και την αξιολόγηση κινδύνου.

Στοιχεία που συνήθως περιλαμβάνει η Περιγραφή Συστήματος:

Επισκόπηση των παρεχόμενων υπηρεσιών*:* Σύντομη παρουσίαση των υπηρεσιών που προσφέρει ο οργανισμός. Περιλαμβάνονται οι δεσμεύσεις υπηρεσιών και οι απαιτήσεις του συστήματος. Εδώ,

ο πελάτης μπορεί να επιβεβαιώσει ότι οι υπηρεσίες που τον ενδιαφέρουν εμπίπτουν στο πεδίο συμμόρφωσης.

Στοιχεία συστήματος*:* Τεχνικές λεπτομέρειες για την υποδομή, το λογισμικό, το ανθρώπινο δυναμικό, τις διαδικασίες και τα δεδομένα που χρησιμοποιούνται. Επίσης, περιλαμβάνονται πληροφορίες για την τοποθεσία φιλοξενίας (π.χ. AWS), τις ρυθμίσεις ασφαλείας, τα εργαλεία που χρησιμοποιούνται και τους μηχανισμούς ελέγχου πρόσβασης.

Δραστηριότητες ελέγχου*:* Αναλυτική περιγραφή των πολιτικών και διαδικασιών ελέγχου. Περιλαμβάνονται θέματα όπως η διαδικασία ένταξης νέων υπαλλήλων, η προστασία δεδομένων (κρυπτογράφηση, έλεγχος πρόσβασης, προστασία βάσεων δεδομένων) και η εφαρμογή τεχνικών μέτρων ασφαλείας.

Αποκάλυψη περιστατικών: Αναφορές για τυχόν παραβιάσεις ή περιστατικά που έχουν επηρεάσει τις δεσμεύσεις του πελάτη.

Μη ισχύοντα κριτήρια υπηρεσιών εμπιστοσύνης *:* Αναφορά κριτηρίων που δεν εφαρμόζονται για τον συγκεκριμένο οργανισμό, συνοδευόμενη από αιτιολόγηση.

Συμπληρωματικοί έλεγχοι οντοτήτων χρήστη (CUEC) και **συμπληρωματικοί έλεγχοι οργανισμών δευτερεύουσας υπηρεσίας** (CSOC) περιλαμβάνονται επίσης εδώ. Οποιεσδήποτε σημαντικές αλλαγές στο σύστημα κατά τη διάρκεια της περιόδου (μόνο αναφορές τύπου 2) περιγράφονται επίσης εδώ. *Για παράδειγμα* , μια νέα απόκτηση ή μια αλλαγή στον πάροχο υπηρεσιών cloud, για να αναφέρουμε μερικά. Αυτή η ενότητα θα περιέχει επίσης συμβάντα συστήματος εάν ο οργανισμός δεν τηρήσει τις δεσμεύσεις του.

Ενότητα 4: Ισχύοντα κριτήρια υπηρεσιών εμπιστοσύνης και συναφή στοιχεία ελέγχου, δοκιμές στοιχείων ελέγχου και αποτελέσματα δοκιμών

Αυτή η ενότητα περιγράφει λεπτομερώς όλες τις δοκιμές (και τα αποτελέσματά τους) που πραγματοποιήθηκαν κατά τη διάρκεια του ελέγχου και ως εκ τούτου αποτελεί ένα κρίσιμο τμήμα της έκθεσης. Παρέχει τις πληροφορίες που εξηγούν τη γνώμη του ελεγκτή λεπτομερώς στην ενότητα 2.

- **Αναφορά κριτηρίων**: Τα κριτήρια των υπηρεσιών εμπιστοσύνης **(TSC)** που αντιστοιχίζονται στο στοιχείο ελέγχου.
- **Αριθμός ελέγχου**: Ο αριθμός αναφοράς για το στοιχείο ελέγχου εντός των κριτηρίων υπηρεσιών εμπιστοσύνης.
- **Δραστηριότητα ελέγχου**: Μια περιγραφή του τι κάνει το στοιχείο ελέγχου.
- **Κάτοχος ελέγχου**: Το άτομο στον οργανισμό σας που είναι υπεύθυνο για την εφαρμογή και τη διατήρηση του ελέγχου.
- **Επίπεδο κινδύνου**: Η πιθανότητα να αποτύχει ένας έλεγχος και ο αντίκτυπος που θα έχει εάν αποτύχει, δηλωμένο ως χαμηλό, μέτριο ή υψηλό.

CCM ID	CCM Criteria[4]	Description of Example Cloud Service Organization's Controls	Tests of Controls	Results of Tests
IS-03	Management shall approve a formal Information Security Policy document which shall be communicated and published to employees, contractors and other relevant external parties. The Information Security Policy shall establish the direction of the organization and align to best practices, regulatory, federal/state and international laws where applicable. The Information Security Policy shall be supported by a strategic plan and a security program with well-defined roles and responsibilities for leadership and officer roles.	**Content** The Information Security Policy is reviewed by xxx to ensure it includes • strategic plan considerations, • applicable laws for the respective territories, and • roles and responsibilities for leadership and officers. **Updates** Responsibility for and maintenance of the Information Security Policy is assigned to the director of information security under the direction of the chief technology officer (CTO). The Information Security Policy is updated at least annually. **Communication** Example Cloud Service Organization publishes and communicates the Information Security Policy to employees, contractors, and external parties at least annually.	Inspected the Information Security Policy dated and noted that it included • strategic plan considerations, • applicable laws for the respective territories, • roles and responsibilities for leadership and officers, and • evidence of review of the update which occurred within the last year. Obtained evidence of the Information Security Policy being communicated to all employees, contractors and vendors via annual written communications and confirmation with each respective party	No exceptions noted.

Figure 2-AICPA's Illustrative Type 2 SOC 2 Report with the Criteria in the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM)

Η αναφορά σχετικά με τον έλεγχο του CCM ID IS-03 καταδεικνύει ότι η Example Cloud Service Organization έχει υλοποιήσει μια συνεπή και οργανωμένη πολιτική ασφάλειας πληροφοριών. Η πολιτική αυτή περιέχει:

1. **Έγκριση και Διάθεση**: Έχει εγκριθεί από την κατάλληλη διεύθυνση και δημοσιοποιείται ετησίως σε υπαλλήλους, εργολάβους και άλλους εξωτερικούς συνεργάτες, διασφαλίζοντας ότι όλοι οι σχετικοί φορείς είναι ενήμεροι.
2. **Στρατηγική Κατεύθυνση**: Η πολιτική ευθυγραμμίζεται με τις βέλτιστες πρακτικές και τις εφαρμοστέες νομικές απαιτήσεις, υποστηριζόμενη από έναν στρατηγικό σχεδιασμό που περιλαμβάνει καθορισμένους ρόλους και ευθύνες για τους ηγέτες και τους υπεύθυνους.
3. **Τακτική Ενημέρωση**: Η πολιτική αναθεωρείται τουλάχιστον ετησίως, με υπευθυνότητα και συντήρηση από τον διευθυντή ασφάλειας πληροφοριών υπό την καθοδήγηση του CTO.
4. **Αποτελεσματικότητα Ελέγχων**: Οι έλεγχοι επιβεβαίωσαν ότι η πολιτική περιλαμβάνει στρατηγικά σχέδια και τους εφαρμοστέους νόμους για τις αντίστοιχες περιοχές, καθώς και ρόλους και ευθύνες. Επίσης, οι ετήσιες γραπτές επικοινωνίες διασφαλίζουν ότι η πολιτική έχει κοινοποιηθεί σε όλους τους εμπλεκόμενους φορείς, χωρίς να σημειωθούν εξαιρέσεις.

Συνολικά, οι έλεγχοι που διενεργήθηκαν αποδεικνύουν ότι η Example Cloud Service Organization διαθέτει μια καλά δομημένη και αποτελεσματική πολιτική ασφάλειας πληροφοριών που πληροί τα κριτήρια του CCM ID IS-03.

Ενότητα 5: Άλλες πληροφορίες που παρέχονται από τη Διοίκηση

Αυτή η ενότητα είναι προαιρετική και περιγράφει λεπτομερώς την απάντηση της διοίκησης σε τυχόν αποκλίσεις ή εξαιρέσεις που επισημαίνονται από τον ελεγκτή στην Ενότητα 4, παρέχοντας περισσότερο πλαίσιο και πληροφορίες σχετικά με τις εξαιρέσεις.

Αναγνώριση Εξαιρέσεων: Καταγραφή των εξαιρέσεων που επισήμανε ο ελεγκτής, συνοδευόμενη από παραδοχή ή διευκρίνιση από τη διοίκηση.

Αιτιολόγηση ή Επεξηγήσεις : Παροχή πληροφοριών για τους παράγοντες που συνέβαλαν στο εύρημα, με στόχο να αποσαφηνιστεί η φύση και η σοβαρότητά του.

Προληπτικές Ενέργειες: Περιγραφή των διαδικασιών που θα εφαρμοστούν ώστε να αποφευχθούν παρόμοια ζητήματα στο μέλλον.

Μελλοντικά Σχέδια και Εξελίξεις: Παρουσίαση στρατηγικών ή τεχνολογικών αλλαγών που ενδέχεται να επηρεάσουν το περιβάλλον ελέγχου, την υποδομή ή τα συστήματα του οργανισμού. **[4]**

Πρόσθετη τεκμηρίωση συμμόρφωσης με το SOC 2

Εκτός από τα βασικά έγγραφα, ο ελεγκτής μπορεί να ζητήσει πρόσθετα έγγραφα κατά τη διάρκεια του ελέγχου SOC 2.Αυτά τα έγγραφα πρέπει είτε να είναι διαθέσιμα είτε να δημιουργηθούν εφόσον δεν υπάρχουν ήδη. Οι απαιτήσεις διαφέρουν ανάλογα με τα κριτήρια και τους ελέγχους που σχετίζονται με τον οργανισμό, καθώς και με τον τύπο της αναφοράς SOC 2 που απαιτείται

Μερικά από αυτά τα πρόσθετα έγγραφα περιλαμβάνουν:

System security

Anti-virus software: εγκατεστημένο και ενεργό σε όλες τις συσκευές, τακτικά ενημερωμένο.

Τοίχος προστασίας δικτύου(network firewall): εγκατεστημένο και ενεργό σε όλες τις συσκευές, τακτικά ενημερωμένο, περιλαμβάνει συστήματα ανίχνευσης και πρόληψης εισβολών(IDS/IPS[2]).

Hardware: όλες οι συσκευες διαθέτουν κλείδωμα οθόνης και κωδικό πρόσβασης, πληρούν τις ελάχιστες απαιτήσεις για εκτέλεση προγραμμάτων ασφαλείας, καταγράφονται οι κινήσεις κάθε χρηστη στην συσκευή.

[2] *Το IPS (Intrusion Prevention System) είναι ένα σύστημα πρόληψης εισβολών που έχει ως κύριο στόχο την ανίχνευση και την αποτροπή κακόβουλων δραστηριοτήτων ή επιθέσεων σε δίκτυα και συστήματα πληροφορικής. Σε αντίθεση με το IDS (Intrusion Detection System), το οποίο απλώς ανιχνεύει και ειδοποιεί για πιθανές απειλές, το IPS μπορεί να αναλάβει αυτόματα δράση για να αποτρέψει ή να περιορίσει μια επίθεση σε πραγματικό χρόνο.*

Κωδικοί: όλοι οι κωδικοί είναι κρυπτογραφημένοι, απαιτούν κριτήρια αλφαριθμητικών και συμβόλων, αλλάζουν ανά τακτά χρονικά διαστήματα, κλείδωμα λογαριασμού μετά από 3 λανθασμένες προσπάθειες.

Λογαριασμοί: οι αδρανείς λογαριασμοί καταργούνται, μετάδοση πληροφοριών λογαριασμού μόνο μέσω κρυπτογράφησης, ανάθεση δικαιωμάτων ανάλογα με το είδος χρήστη.

Φυσική ασφάλεια: όλες οι κτιριακές εγκαταστάσεις έχουν κλειδαριές σε πόρτες και παράθυρα, κάμερες ασφαλείας ,φορητές συσκευές έχουν εγκατεστημένα προγράμματα για απομακρυσμένη διαγραφή ,υπάλληλοι που δουλεύουν εξ' αποστάσεως πληρούν τις ελάχιστες απαιτήσεις ασφαλείας.

Ειδοποιήσεις: μη εξουσιοδοτημένη πρόσβαση συστήματος, προγραμματισμένες τροποποιήσεις συστήματος, εισβολής στις κτιριακές εγκαταστάσεις ή στα Π.Σ.

Standards and procedures

1. **Απαιτήσεις Εργαζομένων**
   - **Έλεγχοι ιστορικού:** Όλοι οι νέοι εργαζόμενοι υπόκεινται σε διαδικασία επαλήθευσης ιστορικού πριν από την πρόσβαση σε συστήματα ή δεδομένα του οργανισμού.
   - **Συμφωνίες πολιτικής ασφαλείας:** Το σύνολο του προσωπικού έχει υπογράψει συμφωνία συμμόρφωσης με την πολιτική ασφάλειας πληροφοριών του οργανισμού.
   - **Εκπαίδευση ασφάλειας:** Όλοι οι εργαζόμενοι συμμετέχουν σε υποχρεωτικά προγράμματα εκπαίδευσης που καλύπτουν τις αρχές ασφάλειας, την αναγνώριση κινδύνων και τις βέλτιστες πρακτικές.
2. **Ανάκτηση Καταστροφών και Απόκριση σε Περιστατικά**
   - **Σχέδιο έκτακτης ανάγκης:** Υπάρχει τεκμηριωμένο και τακτικά επικαιροποιημένο σχέδιο επιχειρησιακής συνέχειας και αποκατάστασης λειτουργιών.
   - **Καθορισμένοι ρόλοι:** Οι ρόλοι και οι ευθύνες για καταστάσεις έκτακτης ανάγκης είναι σαφώς καθορισμένοι και γνωστοποιημένοι σε όλο το προσωπικό.
   - **Εκπαίδευση προσωπικού:** Διεξάγονται τακτικές εκπαιδεύσεις και ασκήσεις για την ετοιμότητα αντιμετώπισης περιστατικών και καταστροφών.
3. **Διαχείριση και Διάθεση Εγγράφων**
   - **Καταστροφή φυσικών εγγράφων:** Ευαίσθητα έγγραφα σε έντυπη μορφή καταστρέφονται με ασφαλή τρόπο όταν παύουν να είναι απαραίτητα.
   - **Επαναφορά συσκευών:** Όλες οι συσκευές (υπολογιστές, κινητά, αποθηκευτικά μέσα) επαναφέρονται στις εργοστασιακές ρυθμίσεις πριν δοθούν σε άλλο χρήστη ή αποσυρθούν.
4. **Διαχείριση Αντιγράφων Ασφαλείας**
   - **Συχνότητα δημιουργίας:** Δημιουργούνται καθημερινά αντίγραφα ασφαλείας κρίσιμων δεδομένων.
   - **Έλεγχος ακεραιότητας:** Τα αντίγραφα ασφαλείας ελέγχονται τακτικά για να διασφαλιστεί η δυνατότητα ανάκτησης.

- **Πολλαπλά σημεία αποθήκευσης:** Τα αντίγραφα ασφαλείας τηρούνται σε τουλάχιστον δύο διαφορετικές τοποθεσίες ή μέσα αποθήκευσης για μείωση του κινδύνου απώλειας.

Documentation and Reporting

1. **Πρωτόκολλα Ασφαλείας**
   - **Τεκμηρίωση:** Όλα τα πρωτόκολλα ασφάλειας είναι επίσημα καταγεγραμμένα και διατηρούνται σε ελεγχόμενο αποθετήριο εγγράφων.
   - **Ενημέρωση:** Τα πρωτόκολλα αναθεωρούνται και επικαιροποιούνται μετά από κάθε τροποποίηση συστήματος ή μετά από περιστατικό ασφάλειας, ώστε να αντανακλούν τις τρέχουσες πρακτικές και απαιτήσεις.
2. **Αρχεία Καταγραφής (Logs)**
   - **Πρόσβαση:** Η πρόσβαση στα αρχεία καταγραφής είναι αυστηρά ελεγχόμενη και περιορίζεται σε εξουσιοδοτημένο προσωπικό.
   - **Επανεξέταση:** Τα logs ελέγχονται τουλάχιστον μία φορά την εβδομάδα για εντοπισμό ανωμαλιών ή ενδείξεων παραβίασης.
   - **Διατήρηση:** Τα αρχεία καταγραφής τηρούνται για ελάχιστο διάστημα έξι (6) μηνών, σε ασφαλές αποθηκευτικό μέσο.
3. **Αναφορές Περιστατικών**
   - **Περιεχόμενο**: Κάθε αναφορά περιλαμβάνει περιγραφή του περιστατικού, ανάλυση αιτιών, ενέργειες απόκρισης και υλοποιημένες λύσεις.
   - **Αρχειοθέτηση:** Οι αναφορές τηρούνται για σκοπούς συμμόρφωσης, ανάλυσης τάσεων και βελτίωσης διαδικασιών.
4. **Διακοπές Λειτουργίας (Outages)**
   - **Στατιστικά**: Παρακολουθείται η συχνότητα τόσο των προγραμματισμένων όσο και των μη προγραμματισμένων διακοπών λειτουργίας.
   - **Δείκτες**: Καταγράφεται ο μέσος χρόνος επίλυσης (Mean Time to Repair – MTTR), ο μέσος χρόνος μεταξύ αποτυχιών (Mean Time Between Failures – MTBF) και ο συνολικός χρόνος διακοπής του συστήματος.
5. **Αποθήκευση Δεδομένων**
   - **Πόροι:** *Παρακολουθείται η χρήση και διαθεσιμότητα αποθηκευτικών πόρων, συμπεριλαμβανομένων φυσικών μέσων (σκληροί δίσκοι) και cloud υποδομών*.
6. **Απόδοση Δικτύου**
   - **Δείκτες:** Μετρούνται ταχύτητες λήψης και μεταφόρτωσης, καθώς και ποσοστά απώλειας πακέτων (packet loss).
7. **Κόστη Πληροφοριακών Συστημάτων**
   - **Συνολικά έξοδα**: Καταγράφεται το συνολικό κόστος λειτουργίας των πληροφοριακών συστημάτων.

- **Δείκτες κόστους:**
    - Δαπάνες πληροφορικής ανά εργαζόμενο.
    - Κόστος ανά χρήστη.
    - Κόστος ανά μονάδα στοιχείου (π.χ. ανά GB αποθήκευσης).

Systems development

8. **Ανάπτυξη και Σχεδιασμός Συστημάτων**
    - **Αναθεώρηση Αναγκών:** Οι ανάγκες των συστημάτων αξιολογούνται τακτικά, ώστε να εξασφαλίζεται η ευθυγράμμισή τους με τις επιχειρησιακές και τεχνικές απαιτήσεις.
    - **Τεκμηρίωση Διαδικασιών:** Όλες οι διαδικασίες σχεδιασμού είναι πλήρως τεκμηριωμένες και ακολουθούνται συστηματικά.
    - **Διαχείριση Εγκρίσεων:** Απαιτούνται εγκρίσεις σε όλα τα κρίσιμα στάδια ανάπτυξης, με σαφή καθορισμό αρμοδιοτήτων.
    - **Ακρίβεια Εισαγωγής Δεδομένων:** Τα έγγραφα και οι διαδικασίες εισαγωγής δεδομένων ελέγχονται για ακρίβεια και πληρότητα.
9. **Δοκιμές**
    - **Αυστηρότητα Ελέγχων:** Οι δοκιμές εκτελούνται με αυστηρά καθορισμένα πρωτόκολλα, τα οποία περιλαμβάνουν σενάρια λειτουργίας, δοκιμές ασφαλείας και δοκιμές απόδοσης.
    - **Ορθή Υλοποίηση**: Τα αποτελέσματα των δοκιμών καταγράφονται και αξιολογούνται, διασφαλίζοντας ότι τα συστήματα πληρούν τις απαιτήσεις πριν από την παραγωγική λειτουργία.
10. **Εκτέλεση και Υλοποίηση**
    - **Επανεξέταση Διαδικασιών:** Οι διαδικασίες υλοποίησης ελέγχονται και επικαιροποιούνται τακτικά.
    - **Έγκριση Αλλαγών:** Κάθε αλλαγή περνά από τυπική διαδικασία έγκρισης πριν την εφαρμογή.
    - **Έλεγχοι Ασφάλειας:** Υπάρχουν επαρκείς μηχανισμοί ελέγχου για τη διασφάλιση της ακεραιότητας και της ασφάλειας κατά τη διάρκεια αλλαγών.
    - **Τελική Αναθεώρηση:** Πραγματοποιείται συνολικός έλεγχος ασφαλείας και συμμόρφωσης με τα πρότυπα, πριν την παράδοση σε λειτουργία. **[6]**

Ποιος διενεργεί έλεγχο SOC 2;

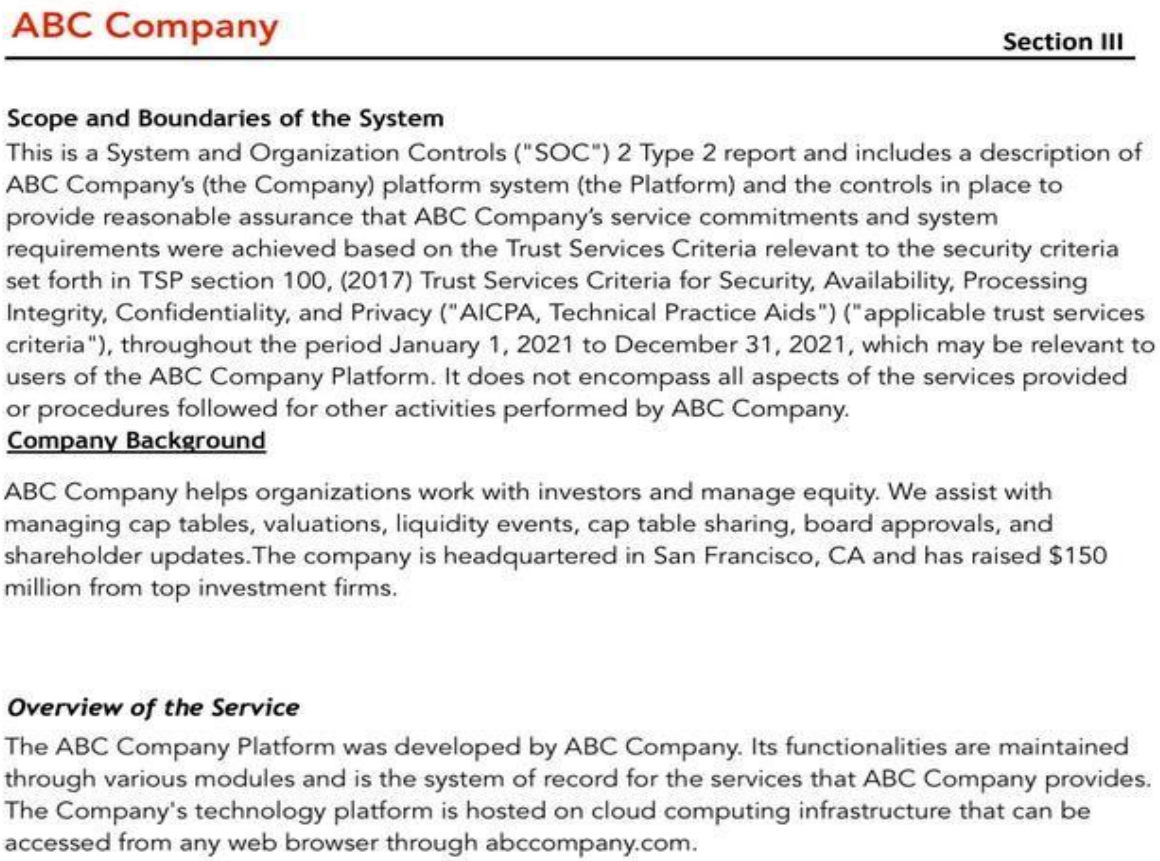
Οι έλεγχοι SOC 2 διενεργούνται συνήθως από πιστοποιημένες δημόσιες λογιστικές εταιρείες (CPA). Αυτές οι εταιρείες ειδικεύονται στη διεξαγωγή ελέγχων και διαθέτουν επαγγελματίες εκπαιδευμένους για τον έλεγχο ενός οργανισμού και τη συμμόρφωση με τις απαιτήσεις του SOC 2.

Παράδειγμα αναφοράς SOC 2

Ακολουθούν αποσπάσματα του άρθρου <<A Real-World SOC 2 Report Example>> της SecureFrame

Η επιχείρηση της ABC Company βασίζεται στη διατήρηση των δεδομένων των πελατών της ασφαλή. Η έκθεσή τους SOC 2, που περιγράφεται παρακάτω, δείχνει πώς το κάνουν αυτό μέσω του προτύπου που ορίζεται από τα Κριτήρια Υπηρεσιών Εμπιστοσύνης της AICPA.
Ενώ πολλές αναφορές SOC 2 έχουν πάνω από 100 σελίδες τεκμηρίωσης, θα επικεντρωθούμε στην επισήμανση ορισμένων από τις πιο αξιόλογες περιοχές.

Έκθεση του ελεγκτή



ABC Company

Section III

Scope and Boundaries of the System

This is a System and Organization Controls ("SOC") 2 Type 2 report and includes a description of ABC Company's (the Company) platform system (the Platform) and the controls in place to provide reasonable assurance that ABC Company's service commitments and system requirements were achieved based on the Trust Services Criteria relevant to the security criteria set forth in TSP section 100, (2017) Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy ("AICPA, Technical Practice Aids") ("applicable trust services criteria"), throughout the period January 1, 2021 to December 31, 2021, which may be relevant to users of the ABC Company Platform. It does not encompass all aspects of the services provided or procedures followed for other activities performed by ABC Company.

Company Background

ABC Company helps organizations work with investors and manage equity. We assist with managing cap tables, valuations, liquidity events, cap table sharing, board approvals, and shareholder updates.The company is headquartered in San Francisco, CA and has raised $150 million from top investment firms.

Overview of the Service

The ABC Company Platform was developed by ABC Company. Its functionalities are maintained through various modules and is the system of record for the services that ABC Company provides. The Company's technology platform is hosted on cloud computing infrastructure that can be accessed from any web browser through abccompany.com.

Figure 3-Έκθεση του ελεγκτή

Κύρια Σημεία:

1. **Πεδίο Εφαρμογής:** Η αναφορά καλύπτει την περίοδο από 1 Ιανουαρίου 2021 έως 31 Δεκεμβρίου 2021 και αναφέρεται αποκλειστικά στους ελέγχους που αφορούν την Πλατφόρμα της ABC Company. Δεν περιλαμβάνει άλλες υπηρεσίες ή διαδικασίες που ακολουθούνται από την εταιρεία.
2. **Ιστορικό Εταιρείας:** Η ABC Company παρέχει υποστήριξη σε οργανισμούς για τη διαχείριση επενδύσεων και κεφαλαίων, συμπεριλαμβανομένων διαδικασιών όπως η διαχείριση των cap tables, εκτιμήσεις, και ενημερώσεις μετόχων. Η εταιρεία έχει την έδρα της στο Σαν Φρανσίσκο και έχει αντλήσει 150 εκατομμύρια δολάρια από κορυφαίες επενδυτικές εταιρείες.

3. **Περιγραφή Υπηρεσίας:** Η Πλατφόρμα αναπτύχθηκε και διατηρείται από την ABC Company, παρέχοντας λειτουργίες μέσω διαφόρων modules. Η τεχνολογική υποδομή φιλοξενείται σε υπολογιστικό νέφος, επιτρέποντας την πρόσβαση μέσω οποιουδήποτε web browser.

Συνολικά, η αναφορά αναδεικνύει τη δέσμευση της ABC Company για την ασφάλεια και την αποτελεσματικότητα των υπηρεσιών της, παρέχοντας τη διασφάλιση ότι πληρούνται τα κριτήρια εμπιστοσύνης κατά τη διάρκεια της εν λόγω περιόδου.

Δοκιμή

ABC Company

Section IV

Trust Services Category, Criteria, Related Controls, Test of Controls and Results of Tests
Criteria Related to the Security (Common Criteria) Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by ABC Company	Tests of Controls Performed by Auditor Firm	Results of Tests
	Common Criteria Related to Control Environment				
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	1.1a	ABC Company Human Resourcesand Information Technolog y teams review and update the organizational structure, reporting lines, and responsibilities on a quarterly basis.	Interviewed ABC Company personnel and confirmed the control procedure described. Inspected Organizational Chart and determined that the structure, reporting lines, and responsibilities are documented. Inspected quarterly review meeting minutes and found that meeting minutes document Humans Resources and Information Technology teams review and update the organizational structure and responsibilities.	No exceptions noted.
		1.1b	ABC Company has a formal Information Security Policy that addresses internal and external security issues relevant to the Platform and its users. The Policy establishes roles, responsibilities, and rules for achieving ABC Company's information security goals. All new hires are required to read and accept this Policy during onboarding.	Interviewed ABC Company personnel and confirmed the control procedure described. Reviewed the Information Security Policy and confirmed that ABC Company has established a formal Policy. Examined the onboarding process for a selection of new hires to determine whether they received and accepted the Policy during onboarding.	Exception noted. For 1 of 45 new hires selected, Policy acknowledgement was not documented. For another 2 of 45 new hires selected, acknowledgements were dated several months after the hire date.

Figure 4-Δοκιμή συστήματος Από το απόσπασμα του ελέγχου SOC 2 της ABC Company που παρουσιάζεις, φαίνεται πως οι ελεγκτές εξετάζουν τη συμμόρφωση της εταιρείας με κριτήρια που σχετίζονται με την ακεραιότητα και τις ηθικές αξίες του ελέγχου του περιβάλλοντος.

Αναλυτικότερα:

CC1.1 (Κριτήριο 1.1α):

Περιγραφή: Η εταιρεία επιβεβαιώνει ότι η ομάδα Ανθρώπινου Δυναμικού και η ομάδα Πληροφορικής αναθεωρούν και ενημερώνουν την οργανωτική δομή και τα καθήκοντα σε τριμηνιαία βάση.

- **Αποτελέσματα του ελέγχου:** Δεν σημειώθηκαν εξαιρέσεις (No exceptions noted).
  Οι ελεγκτές επιβεβαίωσαν ότι η διαδικασία αυτή εφαρμόζεται σωστά και τα σχετικά στοιχεία τεκμηριώνονται.

CC1.1 (Κριτήριο 1.1β):

Περιγραφή: Η εταιρεία έχει επίσημη πολιτική ασφάλειας πληροφοριών που ασχολείται με ζητήματα ασφαλείας, εσωτερικά και εξωτερικά. Όλοι οι νέοι υπάλληλοι είναι υποχρεωμένοι να

αναγνωρίσουν και να αποδεχθούν την πολιτική κατά τη διαδικασία εισαγωγής τους. **Αποτελέσματα του ελέγχου:** Σημειώθηκε μία εξαίρεση (Exception noted). Από τους 45 νέους υπαλλήλους που επιλέχθηκαν για έλεγχο, σε έναν η αναγνώριση της πολιτικής δεν τεκμηριώθηκε, ενώ για δύο άλλους η αναγνώριση έγινε αρκετό καιρό μετά την πρόσληψή τους.

Γενικά σχόλια:

Η εταιρεία φαίνεται να έχει καλές διαδικασίες για την ακεραιότητα και τη συμμόρφωση με τα κριτήρια του SOC 2, ειδικά όσον αφορά την ενημέρωση της οργανωτικής δομής. Ωστόσο, υπάρχουν μικρές αστοχίες στις διαδικασίες onboarding, ειδικά σε ό,τι αφορά την επιβεβαίωση της αναγνώρισης της πολιτικής ασφάλειας από νέους υπαλλήλους. Αυτή η εξαίρεση μπορεί να οδηγήσει σε συστάσεις για βελτίωση των εσωτερικών διαδικασιών παρακολούθησης και επιβεβαίωσης.

Απάντηση της διοίκησης στις εξαιρέσεις που εντοπίστηκαν στον έλεγχο

ABC Company

Section V

Management's Responses to Exceptions Noted

Criteria Number	Criteria Details	Controls Specified by ABC Company	Results of Tests Performed	Management Response
1.1	The entity demonstrates a commitment to integrity and ethical values.	ABC Company has a formal Information Security Policy that addresses internal and external security Issues relevant to the Platform and its users. The Policy establishes roles. responsibilities, and rules for achieving ABC Company's information security goals. All new hires are required to read and accept this Policy during onboarding	Exception noted. For 1 of 45 new hires selected, Policy acknowledgement was not documented. For another 2 of 45 new hires selected, acknowledgements were dated several months after the hire date.	ABC Company will perform more frequent reviews of policy acknowledgements for new hires in the future.
1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			

Figure 5-Απάντηση της διοίκησης

Κριτήρια και Εξαιρέσεις

1. Κριτήριο 1.1 (Δέσμευση στην ακεραιότητα και τις ηθικές αξίες):
    - Εξαίρεση: Σε 1 από τους 45 νέους υπαλλήλους που επιλέχθηκαν, δεν τεκμηριώθηκε η αναγνώριση της πολιτικής ασφάλειας. Σε 2 άλλες περιπτώσεις, η αναγνώριση έγινε μήνες μετά την ημερομηνία πρόσληψης.
    - Αντίδραση της Διοίκησης: Η εταιρεία δεσμεύεται να διενεργεί πιο συχνές αναθεωρήσεις της επιβεβαίωσης αποδοχής πολιτικών για τους νέους υπαλλήλους.

2. Κριτήρια 1.3, 1.4, 5.3:
    - Εδώ περιγράφονται τα συστήματα και οι διαδικασίες που θέτει η διοίκηση για την ανάπτυξη αρμοδιοτήτων και τη διασφάλιση ότι οι πολιτικές της εταιρείας εφαρμόζονται. Αν και δεν υπάρχουν συγκεκριμένες εξαιρέσεις που να σχετίζονται με αυτά τα κριτήρια, ο πίνακας τονίζει τη σημασία των πολιτικών για την ασφάλεια πληροφοριών και το onboarding των υπαλλήλων.

Γενικά Σχόλια:

- Το μεγαλύτερο ζήτημα είναι η έλλειψη τεκμηρίωσης ή οι καθυστερήσεις στην επιβεβαίωση ότι οι νέοι υπάλληλοι αναγνωρίζουν την πολιτική ασφάλειας πληροφοριών κατά τη διαδικασία onboarding.
- Η απάντηση της διοίκησης δείχνει ότι η ABC Company αναγνωρίζει το πρόβλημα και δεσμεύεται να το διορθώσει μέσω συχνότερων ελέγχων στο μέλλον.

2.2.2 Πλάισια Διακυβέρνησης & Ελέγχου

Δύο από τα πιο σημαντικά πλαίσια διακυβέρνησης και ελέγχου που χρησιμοποιούνται για την διασφάλιση της αποτελεσματικότητας των Πληροφοριακών συστημάτων:

COBIT

Το **COBIT** (Control Objectives for Information and Related Technologies) είναι ένα πλαίσιο που αναπτύχθηκε από το **ISACA** για την αποτελεσματική διαχείριση και τον έλεγχο των πληροφοριακών πόρων ενός οργανισμού. Στόχος του είναι να ευθυγραμμίζει τη λειτουργία της Πληροφορικής (**IT**) με τους επιχειρηματικούς στόχους, να υποστηρίζει την αξιολόγηση κινδύνων και να προάγει την εφαρμογή κατάλληλων ελέγχων για την ασφάλεια και την αποδοτική διαχείριση των συστημάτων.

Στοιχεία του COBIT:

- **Διακυβέρνηση IT (IT Governance):** Εστιάζει στη διασφάλιση ότι η IT υποστηρίζει τους επιχειρηματικούς στόχους, διαχειρίζεται αποτελεσματικά τους κινδύνους και μεγιστοποιεί την αξία που προσφέρει στην επιχείρηση.
- **Διαχείριση IT (IT Management):** Περιλαμβάνει διαδικασίες για την αποτελεσματική λειτουργία και διαχείριση της IT υποδομής.
- **Έλεγχοι και Συμμόρφωση:** Εξασφαλίζει ότι εφαρμόζονται σωστοί έλεγχοι και οι οργανισμοί συμμορφώνονται με κανονιστικά πλαίσια.

Σύνδεση του COBIT με το SOC 2:

Το **SOC 2** (Service Organization Control 2) είναι ένα πρότυπο ελέγχου που αξιολογεί την **ασφάλεια**, **διαθεσιμότητα**, **ακεραιότητα** και **εμπιστευτικότητα** και **ιδιωτικότητα** των συστημάτων σε παρόχους υπηρεσιών, κυρίως σε οργανισμούς που χειρίζονται δεδομένα πελατών μέσω cloud ή άλλων υπηρεσιών. `

Η σύνδεση του COBIT με το SOC 2 είναι σημαντική καθώς και τα δύο πλαίσια:

Ασχολούνται με την ασφάλεια των πληροφοριών: Το SOC 2 αξιολογεί συγκεκριμένες αρχές (ασφάλεια, διαθεσιμότητα, εμπιστευτικότητα), ενώ το COBIT παρέχει έναν γενικότερο οδηγό για τη διαχείριση της πληροφορικής, συμπεριλαμβανομένης της ασφάλειας.

Παρέχουν δομές για συμμόρφωση: Το COBIT βοηθά στον σχεδιασμό και την υλοποίηση συστημάτων και διαδικασιών που συμμορφώνονται με πρότυπα όπως το SOC 2.

Εστιάζουν στους ελέγχους και στη διαχείριση κινδύνων: Και τα δύο πλαίσια προωθούν την εφαρμογή κατάλληλων ελέγχων για τη διαχείριση των IT κινδύνων και την προστασία των δεδομένων.

Με τη χρήση του COBIT, οι οργανισμοί μπορούν να εξασφαλίσουν ότι οι έλεγχοι τους καλύπτουν τους στόχους του SOC 2, διευκολύνοντας τη συμμόρφωση και βελτιώνοντας την ποιότητα των εσωτερικών ελέγχων ασφαλείας και πληροφορικής.

Use Case Study:

Το άρθρο περιγράφει πώς ο διευθυντής πληροφορικής του Ευρωπαικού Δικτύου Διαχειριστών Συστημάτων Μεταφοράς Ηλεκτρικής Ενέργειας(**ENTSO-E)** υιοθέτησε το **COBIT 5** για να βελτιώσει τη διακυβέρνηση της πληροφορικής. Με στόχο να ευθυγραμμιστεί με τους επιχειρηματικούς στόχους, χρησιμοποίησε τη μεθοδολογία **Goals Cascade** του COBIT 5 για να δώσει προτεραιότητα στις IT διαδικασίες. Η υιοθέτηση περιλάμβανε τη βελτίωση της διαχείρισης IT, ασφάλειας πληροφοριών και δεδομένων, καθώς και την εφαρμογή βέλτιστων πρακτικών και προτύπων.

COSO

Το **COSO (Committee of Sponsoring Organizations)** είναι ένα ευρέως αναγνωρισμένο πλαίσιο για τη διαχείριση κινδύνων και την εσωτερική διακυβέρνηση. Αρχικά δημιουργήθηκε για να βοηθήσει τις εταιρείες να διαχειρίζονται και να βελτιώνουν τους εσωτερικούς ελέγχους τους, με έμφαση στην ενίσχυση της διαφάνειας, της αξιοπιστίας των οικονομικών αναφορών και τη διαχείριση των κινδύνων.

Το πλαίσιο **COSO** βασίζεται σε πέντε βασικά συστατικά στοιχεία:

- **Περιβάλλον ελέγχου (Control Environment):** Θέτει τα θεμέλια για τον εσωτερικό έλεγχο, καθορίζοντας την κουλτούρα, τη δεοντολογία και τις αρχές διακυβέρνησης**. Αξιολόγηση κινδύνων (Risk Assessment):** Εντοπίζει και αναλύει τους κινδύνους που μπορούν να επηρεάσουν την επίτευξη των στόχων της επιχείρησης.
- **Δραστηριότητες ελέγχου (Control Activities):** Πρόκειται για πολιτικές και διαδικασίες που διασφαλίζουν ότι οι ενέργειες της επιχείρησης ακολουθούνται σωστά και ελέγχονται**. Πληροφορίες και επικοινωνία (Information and Communication):** Περιλαμβάνει τη συλλογή και την ανταλλαγή πληροφοριών απαραίτητων για τη λήψη αποφάσεων. **Παρακολούθηση (Monitoring):** Οι διαδικασίες παρακολουθούνται τακτικά για να διασφαλίζεται ότι λειτουργούν αποτελεσματικά.

Σύνδεση του COSO με το SOC 2:

Το SOC 2 εστιάζει στην προστασία των πληροφοριών και των δεδομένων που διαχειρίζονται οι οργανισμοί, κυρίως μέσω cloud υπηρεσιών. Το SOC 2 περιλαμβάνει τις πέντε κατηγορίες αρχών εμπιστοσύνης (Trust Service Criteria).

Η σύνδεση του COSO με το SOC 2 προκύπτει από το γεγονός ότι και τα δύο πλαίσια επιδιώκουν τη διαχείριση κινδύνων και τη διασφάλιση της εφαρμογής κατάλληλων ελέγχων. Το COSO είναι χρήσιμο για την ανάπτυξη του συνολικού περιβάλλοντος ελέγχου και διακυβέρνησης μιας επιχείρησης, το οποίο είναι απαραίτητο για τη συμμόρφωση με τα κριτήρια του SOC 2.

Πιο συγκεκριμένα:

- Το COSO βοηθά στη δομή και οργάνωση της διακυβέρνησης και των ελέγχων σε ολόκληρο τον οργανισμό, κάτι που είναι κρίσιμο για την εφαρμογή των αρχών SOC 2, όπως η ασφάλεια και η διαθεσιμότητα των συστημάτων.
- Στο πλαίσιο του SOC 2, το COSO βοηθά να δημιουργηθεί ένα **συνεπές και διαφανές περιβάλλον ελέγχου**, το οποίο απαιτείται για την επίτευξη των απαιτούμενων **Trust Service Criteria** (ασφάλεια, διαθεσιμότητα, ακεραιότητα επεξεργασιών, απόρρητο, και προστασία προσωπικών δεδομένων).
- Το SOC 2 εστιάζει σε πιο τεχνικές λεπτομέρειες, αλλά το COSO παρέχει ένα γενικότερο πλαίσιο που μπορεί να βοηθήσει στην ανάπτυξη ελέγχων και διαδικασιών που να πληρούν τις απαιτήσεις του SOC 2.

Συνολικά, το COSO μπορεί να χρησιμοποιηθεί ως εργαλείο για να διασφαλιστεί ότι οι εσωτερικές διαδικασίες και οι έλεγχοι συμμορφώνονται με τα κριτήρια του SOC 2, ειδικά στην αντιμετώπιση των κινδύνων και τη διαχείριση της ασφάλειας πληροφοριών.

Σημαντικότητα του COBIT FRAMEWORK και COSO FRAMEWORK στο SOC 2:

Το **SOC 2** είναι ένας έλεγχος που στοχεύει στην αξιολόγηση της εσωτερικής ασφάλειας, της διαχείρισης κινδύνων και της εμπιστοσύνης δεδομένων για οργανισμούς που παρέχουν cloud και IT υπηρεσίες. Το **COSO** και το **COBIT** υποστηρίζουν αυτή τη διαδικασία ως εξής:

- **COSO**: Βοηθά στην εστίαση στους εσωτερικούς ελέγχους και την αντιμετώπιση κινδύνων σε σχέση με την ασφάλεια πληροφοριών.
- **COBIT**: Παρέχει μια δομημένη προσέγγιση για τη διακυβέρνηση IT, εξασφαλίζοντας ότι οι διαδικασίες πληροφορικής είναι ασφαλείς και ευθυγραμμισμένες με τους επιχειρηματικούς στόχους.

Συνολικά, και τα δύο πλαίσια αποτελούν θεμέλια για την επιτυχή προετοιμασία και διενέργεια ενός **SOC 2** ελέγχου, διασφαλίζοντας ότι οι διαδικασίες IT ελέγχονται σωστά και οι κίνδυνοι ελαχιστοποιούνται.

2.2.3 ISO 27001

Το **ISO/IEC 27001** είναι ένα διεθνές πρότυπο για τη διαχείριση της ασφάλειας πληροφοριών.Το πρότυπο δημοσιεύθηκε αρχικά από κοινού από τον **Διεθνή Οργανισμό Τυποποίησης (ISO)** και τη **Διεθνή Ηλεκτροτεχνική Επιτροπή (IEC)** το 2005,αναθεωρήθηκε το 2013, και πάλι πιο πρόσφατα το 2022. Στόχος του είναι να βοηθήσει τους οργανισμούς να κάνουν τα στοιχεία πληροφοριών που διαθέτουν πιο ασφαλή. **[8]**

Τι είναι το ISO 27001:2022

Η νέα έκδοση, με πλήρη τίτλο *«Ασφάλεια πληροφοριών, κυβερνοασφάλεια και προστασία της ιδιωτικότητας – Συστήματα διαχείρισης ασφάλειας πληροφοριών – Απαιτήσεις»*, αντικαθιστά την προηγούμενη του 2013 και ενσωματώνει εξελίξεις σε θέματα κυβερνοασφάλειας και προστασίας ιδιωτικότητας.

Πλεονεκτήματα από την εφαρμογή του ISO 27001:2022

Η εφαρμογή του ISO 27001:2022 προσφέρει πολλά πλεονεκτήματα για μια επιχείρηση ή οργανισμό. Ανάμεσα στα κύρια πλεονεκτήματα περιλαμβάνονται:

1. **Βελτίωση της Ασφάλειας Πληροφοριών:** Το ISO 27001:2022 παρέχει ένα ολοκληρωμένο πλαίσιο για την ανάπτυξη, εφαρμογή και διατήρηση ενός συστήματος διαχείρισης ασφάλειας πληροφοριών (ISMS), το οποίο ενισχύει την αντίληψη και τη διαχείριση των ασφαλειών πληροφοριών σε μια επιχείρηση.
2. **Προστασία των Δεδομένων:** Μέσω του ISO 27001:2022, οι επιχειρήσεις μπορούν να ενισχύσουν την προστασία των δεδομένων τους, συμπεριλαμβανομένων των προσωπικών δεδομένων, και να μειώσουν τους κινδύνους διαρροής ή απώλειας δεδομένων.
3. **Συμμόρφωση με Νομικές Απαιτήσεις:** Η υλοποίηση του ISO 27001:2022 βοηθά τις επιχειρήσεις να επιτύχουν συμμόρφωση με τις νομικές απαιτήσεις περί ασφάλειας πληροφοριών και προστασίας δεδομένων, όπως το GDPR.
4. **Ενίσχυση Εμπιστοσύνης:** Η πιστοποίηση στο ISO 27001:2022 δείχνει στους πελάτες, τους εταίρους και τους ενδιαφερόμενους ότι η επιχείρηση λαμβάνει σοβαρά μέτρα για την προστασία των πληροφοριών τους.
5. **Βελτίωση Διαδικασιών:** Η υλοποίηση του ISO 27001:2022 προωθεί τη βελτίωση των διαδικασιών και των πρακτικών διαχείρισης ασφάλειας πληροφοριών μέσα στην επιχείρηση, βοηθώντας την να λειτουργεί αποτελεσματικότερα και πιο ασφαλώς. 6. Μείωση Κινδύνων: Με την αναγνώριση και τη διαχείριση των κινδύνων ασφάλειας πληροφοριών, οι επιχειρήσεις μειώνουν τον κίνδυνο παραβιάσεων και πιθανών αρνητικών επιπτώσεων.

Πώς λειτουργεί το πρότυπο

- Εξετάζει συστηματικά τους κινδύνους για την ασφάλεια των πληροφοριών του οργανισμού, λαμβάνοντας υπόψη τις απειλές, τα τρωτά σημεία και τις επιπτώσεις.
- Σχεδιάστε και εφαρμόστε μια συνεκτική και ολοκληρωμένη σειρά ελέγχων ασφάλειας πληροφοριών ή/και άλλων μορφών αντιμετώπισης κινδύνων (όπως η αποφυγή ή η μεταφορά κινδύνου) για την αντιμετώπιση των κινδύνων που κρίνονται απαράδεκτοι. και
- Υιοθετήστε μια γενική διαδικασία διαχείρισης για να διασφαλίσετε ότι οι έλεγχοι ασφάλειας πληροφοριών συνεχίζουν να καλύπτουν τις ανάγκες ασφάλειας πληροφοριών του οργανισμού σε συνεχή βάση.

Το ποιοι έλεγχοι θα δοκιμαστούν ως μέρος της πιστοποίησης κατά ISO/IEC 27001 εξαρτώνται από τον ελεγκτή πιστοποίησης. Αυτό μπορεί να περιλαμβάνει οποιουσδήποτε ελέγχους που ο οργανισμός θεωρεί ότι εμπίπτουν στο πεδίο εφαρμογής του ISMS και αυτός ο έλεγχος μπορεί να είναι σε οποιοδήποτε βάθος ή έκταση όπως εκτιμάται από τον ελεγκτή όπως απαιτείται για να ελεγχθεί ότι ο έλεγχος έχει εφαρμοστεί και λειτουργεί αποτελεσματικά. Η διοίκηση καθορίζει το εύρος του ISMS για σκοπούς πιστοποίησης και μπορεί να το περιορίσει, για παράδειγμα, σε μια μεμονωμένη επιχειρηματική μονάδα ή τοποθεσία. Το πιστοποιητικό ISO/IEC 27001 δεν σημαίνει απαραίτητα ότι το υπόλοιπο του οργανισμού, εκτός του πεδίου εφαρμογής, έχει επαρκή προσέγγιση στη διαχείριση της ασφάλειας πληροφοριών.

Γενικός Κανονισμός Προοστασίας Δεδομένων και ISO 27001:2022

Ο Γενικός Κανονισμός Προστασίας Δεδομένων – ΓΚΠΔ, (εφεξής GDPR) και το ISO 27001:2022 συσχετίζονται καθώς αφορούν και τα δύο την προστασία των προσωπικών δεδομένων και την ασφάλεια των πληροφοριών:

- **Προστασία Προσωπικών Δεδομένων:** Ο GDPR και το ISO 27001:2022 έχουν ως στόχο την προστασία των προσωπικών δεδομένων. Ο GDPR καθορίζει τις νομικές απαιτήσεις που πρέπει να τηρούν οι επιχειρήσεις για την επεξεργασία των προσωπικών δεδομένων, ενώ το ISO 27001:2022 παρέχει ένα πλαίσιο διαχείρισης ασφάλειας πληροφοριών που μπορεί να εφαρμοστεί για την προστασία αυτών των δεδομένων.
- **Συμμόρφωση και Διαχείριση Κινδύνων:** Ο GDPR και το ISO 27001:2022 απαιτούν από τις επιχειρήσεις να αναγνωρίζουν και να διαχειρίζονται τους κινδύνους που σχετίζονται με την επεξεργασία των προσωπικών δεδομένων και την ασφάλεια των πληροφοριών.
- **Εσωτερικός Έλεγχος και Παρακολούθηση:** Ο GDPR και το ISO 27001:2022 προωθούν την υλοποίηση ενός συστήματος εσωτερικού ελέγχου και παρακολούθησης για τη διασφάλιση της συμμόρφωσης και της αποτελεσματικής λειτουργίας των διαδικασιών ασφάλειας και προστασίας δεδομένων.

Επομένως, η συμμόρφωση με το ISO 27001:2022 μπορεί να βοηθήσει τις επιχειρήσεις να επιτύχουν συμμόρφωση με τον GDPR, παρέχοντας ένα ολοκληρωμένο πλαίσιο για την προστασία των προσωπικών δεδομένων και την ασφάλεια των πληροφοριών. **[7]**

Κοινά μεταξύ SOC2 και ISO27001

Το SOC 2 (System and Organization Controls 2) και το ISO 27001 είναι πρότυπα που σχετίζονται με τη διαχείριση της ασφάλειας πληροφοριών και την προστασία των δεδομένων. Παρόλο που προέρχονται από διαφορετικά νομικά και κανονιστικά πλαίσια (SOC 2 είναι πιο διαδεδομένο στις ΗΠΑ, ενώ το ISO 27001 είναι διεθνές πρότυπο), έχουν πολλά κοινά σημεία:

- **Ασφάλεια Πληροφοριών:** Και τα δύο πρότυπα επικεντρώνονται στη διασφάλιση ότι οι οργανισμοί εφαρμόζουν κατάλληλα μέτρα για την προστασία των πληροφοριών από παραβιάσεις, μη εξουσιοδοτημένη πρόσβαση, και διαρροές.
- **Προσέγγιση βασισμένη σε διαδικασίες:** Και το SOC 2 και το ISO 27001 επικεντρώνονται σε διαδικασίες και ελέγχους που εξασφαλίζουν ότι οι οργανισμοί παρακολουθούν και ελέγχουν τις λειτουργίες τους για να προστατεύσουν τα δεδομένα. **Διαχείριση Κινδύνου:** Και τα δύο πρότυπα απαιτούν από τους οργανισμούς να αναγνωρίσουν, να αναλύσουν και να διαχειριστούν τους κινδύνους που σχετίζονται με την ασφάλεια των πληροφοριών.
- **Συνεχής Βελτίωση:** Και τα δύο πρότυπα υποστηρίζουν τη συνεχή βελτίωση των διαδικασιών και των μέτρων ασφαλείας, ώστε να ανταποκρίνονται στις εξελισσόμενες απειλές και απαιτήσεις.
- **Πολιτικές και Διαδικασίες:** Απαιτούν από τους οργανισμούς να έχουν καθορισμένες πολιτικές και διαδικασίες ασφάλειας πληροφοριών που να είναι τεκμηριωμένες και να ακολουθούνται από το προσωπικό.
- **Εξωτερικοί Έλεγχοι:** Και τα δύο πρότυπα απαιτούν από τους οργανισμούς να υπόκεινται σε εξωτερικούς ελέγχους (audit), για να επιβεβαιωθεί η συμμόρφωση με τα πρότυπα.

Αν και το SOC 2 επικεντρώνεται περισσότερο σε ελέγχους και ασφάλεια για υπηρεσίες παρόχων και το ISO 27001 επικεντρώνεται στη διαχείριση ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ISMS), οι στόχοι και τα θέματα που καλύπτουν είναι παρόμοια όσον αφορά την προστασία των πληροφοριών. **[18]**

Βασικές διαφορές μεταξύ SOC2 και ISO27001

Ελεγκτικό πλαίσιο:

- **SOC 2:** Επικεντρώνεται σε πέντε κατηγορίες ελέγχων (Trust Service Criteria): ασφάλεια, διαθεσιμότητα, ακεραιότητα επεξεργασίας, εμπιστευτικότητα και ιδιωτικότητα. Ο οργανισμός μπορεί να επιλέξει ποια από τα κριτήρια αυτά θα συμπεριλάβει στον έλεγχο του SOC 2.
- ISO 27001: Απαιτεί από τον οργανισμό να υιοθετήσει ένα πλήρες σύστημα διαχείρισης της ασφάλειας πληροφοριών, με βάση τις απαιτήσεις του προτύπου. Οι έλεγχοι είναι προκαθορισμένοι και περιλαμβάνονται στο Annex A του ISO 27001.

Πιστοποίηση vs. Έλεγχος:

- **SOC 2**: Δεν οδηγεί σε "πιστοποίηση", αλλά σε αναφορά (report) από έναν ανεξάρτητο ελεγκτή (auditor), η οποία περιγράφει αν ο οργανισμός τηρεί τις καθορισμένες απαιτήσεις ασφαλείας.
- ISO 27001: Οδηγεί σε πιστοποίηση, η οποία παρέχεται από έναν αναγνωρισμένο φορέα πιστοποίησης εφόσον ο οργανισμός περάσει έναν αυστηρό έλεγχο των διαδικασιών του.

Διάρκεια Ελέγχου:

- **SOC 2:** Συνήθως καλύπτει μια περίοδο 6-12 μηνών και απαιτεί τακτικούς επαναληπτικούς ελέγχους για να διατηρήσει τη συμμόρφωση.
- **ISO 27001:** Η πιστοποίηση ισχύει για τρία χρόνια, με ετήσιους επιτόπιους ελέγχους για να διασφαλιστεί ότι διατηρούνται τα πρότυπα.

Συνολικά, το SOC 2 είναι πιο εξειδικευμένο για οργανισμούς παροχής υπηρεσιών, ενώ το ISO 27001 αφορά τη γενική ασφάλεια πληροφοριών ενός οργανισμού σε κάθε επίπεδο.

2.2.4 ISO 27007

Το ISO/IEC 27007 είναι ένα διεθνές πρότυπο που παρέχει κατευθυντήριες οδηγίες για την ανασκόπηση και τον έλεγχο των συστημάτων διαχείρισης ασφάλειας πληροφοριών (Information Security Management Systems, ISMS) σύμφωνα με το πρότυπο ISO/IEC 27001.

Το ISO/IEC 27007 βοηθά τους οργανισμούς να κατανοήσουν τις διαδικασίες ελέγχου που απαιτούνται για την αξιολόγηση του ISMS και παρέχει οδηγίες για τη διαδικασία του εσωτερικού ελέγχου της ασφάλειας των πληροφοριών. Ειδικότερα, καλύπτει τα εξής θέματα:

1. Ανασκόπηση και αξιολόγηση του ISMS: Καθορίζει την έννοια της ανασκόπησης του ISMS, που περιλαμβάνει την αξιολόγηση της συμμόρφωσης και της αποτελεσματικότητάς του.
2. Αξιολόγηση κινδύνου: Ορίζει τις διαδικασίες που πρέπει να ακολουθηθούν για την εκτίμηση των κινδύνων που σχετίζονται με την ασφάλεια των πληροφοριών και την επίδραση που μπορεί να έχουν στην οργάνωση.
3. Βελτίωση και ενίσχυση: Παρέχει οδηγίες για την αναγνώριση περιοχών που χρήζουν βελτίωσης και την εφαρμογή ενεργειών για την ενίσχυση του συστήματος.

Κοινά μεταξύ SOC2 και ISO27007

Τα **SOC 2** και **ISO/IEC 27007** αναφέρονται και τα δύο στη διαχείριση της ασφάλειας των πληροφοριών, αλλά επικεντρώνονται σε διαφορετικές πτυχές αυτής της διαχείρισης. Παρά τις διαφορές τους, υπάρχουν και κοινά σημεία μεταξύ τους:

- **Ασφάλεια των Πληροφοριών:** Και τα δύο πρότυπα επικεντρώνονται στη διασφάλιση της προστασίας των πληροφοριών, είτε αφορά την προστασία των δεδομένων του πελάτη (SOC 2) είτε την προστασία της συνολικής υποδομής ασφάλειας πληροφοριών ενός οργανισμού (ISO/IEC 27007).
- **Διαχείριση Ρίσκου:** Και τα δύο πρότυπα απαιτούν από τους οργανισμούς να κατανοήσουν και να διαχειριστούν τους κινδύνους που σχετίζονται με την ασφάλεια των πληροφοριών. Στο SOC

2, αυτό επικεντρώνεται στη διαχείριση των κινδύνων που ενδέχεται να επηρεάσουν την προστασία των δεδομένων του πελάτη, ενώ στο ISO 27007 ενσωματώνεται στο ευρύτερο πλαίσιο του **ISO/IEC 27001**, το οποίο εστιάζει στη διαχείριση όλων των κινδύνων ασφάλειας πληροφοριών.

- **Έλεγχος και Αξιολόγηση:** Και τα δύο πρότυπα περιλαμβάνουν διαδικασίες ελέγχου και αξιολόγησης της ασφάλειας των πληροφοριών:

SOC 2: Αξιολογεί τις διαδικασίες και τους ελέγχους που σχετίζονται με τις πέντε αρχές του Trust Services Criteria: Ασφάλεια, Διαθεσιμότητα, Εμπιστευτικότητα, Διαχείριση Απορρήτου και Ικανότητα Επεξεργασίας.

ISO 27007: Παρέχει οδηγίες για την αξιολόγηση και την ανασκόπηση του ISMS, περιλαμβάνοντας τον έλεγχο της συμμόρφωσης και της αποτελεσματικότητάς του.

- **Συμμόρφωση με Διεθνή Πρότυπα:** Και τα δύο είναι διεθνή πρότυπα (ή πλαίσια ελέγχου), και αν και το SOC 2 είναι πιο επικεντρωμένο στις υπηρεσίες, το ISO/IEC 27007 συνδέεται με το ISO 27001, που είναι παγκόσμια αναγνωρισμένο πρότυπο για τα Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών (ISMS).
- **Βελτίωση Συνεχούς Διαδικασίας:** Και τα δύο πρότυπα τονίζουν τη συνεχιζόμενη βελτίωση και εξέλιξη των διαδικασιών ασφάλειας. Το SOC 2 απαιτεί από τους οργανισμούς να διασφαλίσουν ότι οι ελέγχοι συνεχώς παρακολουθούνται και προσαρμόζονται για την επίτευξη των επιθυμητών αποτελεσμάτων, ενώ το ISO/IEC 27007 περιλαμβάνει διαδικασίες συνεχούς βελτίωσης του ISMS.

Αν και το SOC 2 εστιάζει σε συγκεκριμένα κρίσιμα σημεία σχετικά με την ασφάλεια και την ιδιωτικότητα για τις επιχειρήσεις που παρέχουν υπηρεσίες σε τρίτους, το ISO 27007 επικεντρώνεται στο σύνολο της διαδικασίας διαχείρισης ασφάλειας πληροφοριών και είναι μέρος ενός μεγαλύτερου συστήματος διαχείρισης.

Βασικές διαφορές μεταξύ SOC2 και ISO27001

Σκοπός και Αντικείμενο:

SOC 2: Αφορά την αξιολόγηση των εσωτερικών ελέγχων και διαδικασιών ασφάλειας των πληροφοριών που σχετίζονται με τις υπηρεσίες που παρέχονται από τρίτους οργανισμούς, κυρίως σε επιχειρήσεις που παρέχουν υπηρεσίες μέσω του cloud ή άλλων τεχνολογιών. Στοχεύει να διασφαλίσει ότι οι υπηρεσίες που παρέχονται πληρούν αυστηρές απαιτήσεις για την προστασία της ασφάλειας, της διαθεσιμότητας, της εμπιστευτικότητας, της επεξεργασίας δεδομένων και του απορρήτου.

ISO/IEC 27007: Το ISO 27007 επικεντρώνεται στη διαδικασία εσωτερικής αξιολόγησης και βελτίωσης του συστήματος διαχείρισης ασφάλειας πληροφοριών ενός οργανισμού σε γενικό επίπεδο.

Σχέση με Άλλα Πρότυπα:

SOC 2: Αν και το SOC 2 έχει κάποια σχέση με άλλες κατευθυντήριες οδηγίες ασφάλειας, όπως το ISO 27001, λειτουργεί περισσότερο ως ανεξάρτητη αναφορά για τις διαδικασίες και ελέγχους ασφάλειας που εφαρμόζονται σε οργανισμούς που παρέχουν υπηρεσίες σε τρίτους.

ISO/IEC 27007: Είναι κατευθυντήριες οδηγίες για την αξιολόγηση των συστημάτων διαχείρισης ασφάλειας πληροφοριών (ISMS) που έχει υιοθετήσει ένας οργανισμός σύμφωνα με το πρότυπο ISO/IEC 27001. Επομένως, η εφαρμογή του είναι περισσότερο συνδεδεμένη με την ύπαρξη ενός επίσημου ISMS και την κατευθυντήρια γραμμή για τη συνεχιζόμενη βελτίωση αυτού του συστήματος.

Εφαρμογή και Πεδίο Εφαρμογής:

SOC 2: Είναι σχεδιασμένο για οργανισμούς που παρέχουν υπηρεσίες σε πελάτες (κυρίως σε cloud-based ή SaaS πλατφόρμες) και επιθυμούν να επιδείξουν την ικανότητά τους να προστατεύουν τα δεδομένα και τις πληροφορίες των πελατών. Η εφαρμογή του είναι περισσότερο προσανατολισμένη σε εξωτερικούς ελέγχους και αναφορά στους πελάτες.

ISO/IEC 27007: Εφαρμόζεται σε οργανισμούς που θέλουν να δημιουργήσουν και να βελτιώσουν ένα ολοκληρωμένο σύστημα διαχείρισης ασφάλειας πληροφοριών (ISMS), το οποίο διασφαλίζει την προστασία των πληροφοριών σε επίπεδο οργανισμού. Η εφαρμογή του είναι περισσότερο εσωτερική και επικεντρωμένη στη βελτίωση του συστήματος.

Είδη Ελέγχου:

SOC 2: Η αξιολόγηση και η αναφορά διαφέρουν ανάλογα με τους 5 δείκτες εμπιστοσύνης (Trust Service Criteria): Ασφάλεια, Διαθεσιμότητα, Εμπιστευτικότητα, Διαχείριση
Απορρήτου και Ικανότητα Επεξεργασίας. Οι έλεγχοι είναι έξωθεν και επαληθεύονται από εξωτερικούς ελεγκτές (συνήθως ανεξάρτητους λογιστές ή άλλους ειδικούς).

ISO/IEC 27007: Παρέχει οδηγίες για τη συνεχιζόμενη παρακολούθηση, αξιολόγηση και ανασκόπηση του ISMS, κυρίως σε σχέση με το ISO 27001. Οι εσωτερικοί ή εξωτερικοί ελεγκτές πρέπει να ελέγξουν εάν το ISMS συμμορφώνεται με τα απαιτούμενα πρότυπα και κατευθυντήριες οδηγίες του ISO.

Διαδικασία Έγκρισης:

SOC 2: Ένας οργανισμός χρειάζεται να περάσει από εξωτερικούς ελέγχους για να πιστοποιηθεί, και η αναφορά παρέχεται στους πελάτες ή στο κοινό, επιδεικνύοντας την συμμόρφωση με τις προδιαγραφές ασφάλειας που καθορίζονται από το SOC 2.

ISO/IEC 27007: Δεν εκδίδεται πιστοποίηση, αλλά παρέχονται οδηγίες για τη βελτίωση του συστήματος διαχείρισης ασφάλειας πληροφοριών. Η εφαρμογή του μπορεί να οδηγήσει σε πιστοποίηση ISO/IEC 27001 (αν το ISMS συμμορφώνεται με το πρότυπο αυτό).

Συνοπτικά:

Το **SOC 2** επικεντρώνεται στην αξιολόγηση των διαδικασιών ασφάλειας και της προστασίας των πληροφοριών που παρέχονται σε πελάτες, και χρησιμοποιείται κυρίως από οργανισμούς υπηρεσιών.

Το **ISO/IEC 27007** παρέχει οδηγίες για την ανασκόπηση και την συνεχιζόμενη βελτίωση των συστημάτων διαχείρισης ασφάλειας πληροφοριών, κυρίως για οργανισμούς που θέλουν να διασφαλίσουν τη συνολική ασφάλεια των πληροφοριών τους και να συμμορφωθούν με το ISO/IEC 27001.

2.3 Ορισμός και κατηγορίες της τεχνητής νοημοσύνης.

Ο όρος τεχνητή νοημοσύνη αναφέρεται στον κλάδο της πληροφορικής ο οποίος ασχολείται με τη σχεδίαση και την υλοποίηση υπολογιστικών συστημάτων που μιμούνται στοιχεία της ανθρώπινης συμπεριφοράς τα οποία υπονοούν έστω και στοιχειώδη ευφυΐα: μάθηση, προσαρμοστικότητα, εξαγωγή συμπερασμάτων, κατανόηση από συμφραζόμενα, επίλυση προβλημάτων κλπ. Ουσιαστικά, η τεχνητή νοημοσύνη προσπαθεί να "διδάξει" τις μηχανές να **σκέφτονται και να ενεργούν** με έξυπνο τρόπο, με σκοπό να μιμηθούν τις γνωστικές λειτουργίες του ανθρώπου.

Κύριες Κατηγορίες Τεχνητής Νοημοσύνης:

- **Στενή (Weak AI):** Ένα σύστημα AI σχεδιασμένο για να εκτελεί μια συγκεκριμένη εργασία ή ένα σύνολο εργασιών. Αυτός είναι ο τύπος AI που χρησιμοποιείται στις τρέχουσες εφαρμογές. Ονομάζεται αδύναμο όχι επειδή στερείται δύναμης ή ικανότητας, αλλά επειδή απέχει πολύ από το να έχουμε την ανθρώπινη κατανόηση ή συνείδηση που συσχετίζουμε με την αληθινή νοημοσύνη. Αυτά τα συστήματα είναι περιορισμένα στο πεδίο εφαρμογής τους και δεν έχουν τη δυνατότητα να εκτελούν εργασίες εκτός του συγκεκριμένου τομέα τους. Παραδείγματα στενής τεχνητής νοημοσύνης είναι οι βοηθοί φωνής, η αναγνώριση προσώπου και ομιλίας και τα αυτοοδηγούμενα αυτοκίνητα.
- **Γενική (Strong AI):** Η γενική τεχνητή νοημοσύνη, σε θεωρητικό επίπεδο, θα μπορούσε να εκτελεί οποιαδήποτε διανοητική εργασία που μπορεί να επιτελέσει ένας άνθρωπος — ενδεχομένως και καλύτερα.

  Χαρακτηριστικά: Ικανότητα μάθησης από την εμπειρία, πρόβλεψη προτύπων και γενίκευση γνώσης σε ποικίλες καταστάσεις.

  Δυνατότητες: Προσαρμογή σε νέες εργασίες που δεν καλύπτονται από προηγούμενα δεδομένα ή αλγορίθμους.

  Κατάσταση ανάπτυξης: Δεν έχει επιτευχθεί ακόμη, αλλά η έρευνα και η ανάπτυξη στον τομέα προχωρούν με ενθαρρυντικά αποτελέσματα.
- **Υπερευφυές (Superintelligence):** Η υπερευφυής τεχνητή νοημοσύνη είναι μια υποθετική μορφή AI που θα ξεπερνούσε τη νοημοσύνη και τις ικανότητες του ανθρώπου σε όλα τα επίπεδα.

  Χαρακτηριστικά: Πλήρης αυτογνωσία, ικανότητα αυτοβελτίωσης, λήψη αποφάσεων με ανώτερο επίπεδο κατανόησης.

Δυνατότητες: Ανάλυση και κατανόηση της ανθρώπινης σκέψης σε θεμελιώδες επίπεδο, αξιοποίηση τεράστιας υπολογιστικής ισχύος.

Κατάσταση ανάπτυξης: Παραμένει στη σφαίρα της επιστημονικής φαντασίας, χωρίς γνωστή μέθοδο δημιουργίας της, αλλά με σημαντικές θεωρητικές και ηθικές προεκτάσεις.

2.4 Βασικά χαρακτηριστικά και τεχνολογίες της AI (machine learning, deep learning, neural networks, natural language processing).

Η **Τεχνητή Νοημοσύνη (AI)** περιλαμβάνει διάφορες τεχνολογίες και μεθόδους που αποσκοπούν στη δημιουργία συστημάτων ικανών να εκτελούν καθήκοντα που απαιτούν ανθρώπινη νοημοσύνη. Τα βασικά χαρακτηριστικά της περιλαμβάνουν τα εξής:

1. **Αυτόματη Μάθηση (Machine Learning):** Η ικανότητα ενός συστήματος να μαθαίνει από δεδομένα και να βελτιώνει την απόδοσή του με την εμπειρία, χωρίς να χρειάζεται να προγραμματιστεί εκ νέου. Κύριες τεχνικές:

- **Επιβλεπόμενη Μάθηση** (Supervised Learning): Χρήση ετικετοποιημένων δεδομένων για να "μάθει" το σύστημα να προβλέπει αποτελέσματα.
- **Μη Επιβλεπόμενη Μάθηση** (Unsupervised Learning): Ανάλυση δεδομένων χωρίς προκαθορισμένες ετικέτες για την ανακάλυψη μοτίβων.
- **Ενισχυτική Μάθηση** (Reinforcement Learning): Το σύστημα μαθαίνει μέσω επιβράβευσης και τιμωρίας, βελτιστοποιώντας τη συμπεριφορά του.

2. **Προσαρμοστικότητα :**Η ικανότητα ενός συστήματος AI να προσαρμόζεται σε νέες καταστάσεις, δεδομένα και προβλήματα. Αυτό σημαίνει ότι το σύστημα μπορεί να αναγνωρίσει μοτίβα και να προσαρμόσει τη λειτουργία του σε νέα περιβάλλοντα χωρίς ανθρώπινη παρέμβαση.
3. **Αυτοματοποίηση:** Τα συστήματα AI μπορούν να αυτοματοποιήσουν εργασίες που απαιτούν νοημοσύνη, όπως η ανάλυση δεδομένων, η επεξεργασία φυσικής γλώσσας και η αναγνώριση εικόνας. Αυτή η ικανότητα βελτιώνει την αποδοτικότητα και την ακρίβεια σε πολλούς τομείς.
4. **Γνωστική Υπολογιστική Ικανότητα :** Τα AI συστήματα μπορούν να μιμηθούν ανθρώπινες γνωστικές λειτουργίες, όπως η συλλογιστική, η λήψη αποφάσεων, η πρόβλεψη και η επίλυση προβλημάτων. Αυτό τους επιτρέπει να εκτελούν πολύπλοκα έργα όπως ο σχεδιασμός στρατηγικής, η διάγνωση ασθενειών ή η αυτόματη αναγνώριση προσώπων.
5. **Επεξεργασία Μεγάλων Ποσοτήτων Δεδομένων:** Η AI μπορεί να επεξεργαστεί και να αναλύσει τεράστιες ποσότητες δεδομένων με ταχύτητα και ακρίβεια, εξάγοντας χρήσιμα συμπεράσματα και δημιουργώντας προβλέψεις με βάση τα δεδομένα.
6. **Εξαγωγή Γνώσης:** Η AI μπορεί να εξάγει πολύτιμες πληροφορίες από δομημένα και μη δομημένα δεδομένα (π.χ. κείμενα, εικόνες, βίντεο), κάνοντας αναγνώριση μοτίβων, ανάλυση συναισθήματος και ανακάλυψη νέων γνώσεων.
7. **Δημιουργία Περιεχομένου:** Τα AI συστήματα μπορούν να δημιουργήσουν περιεχόμενο (π.χ. κείμενο, εικόνες, μουσική) βασισμένο σε πρότυπα και συνδυασμούς δεδομένων. Για

παράδειγμα, ένα AI μπορεί να γράψει άρθρα ή να δημιουργήσει οπτικές εικόνες χρησιμοποιώντας κατάλληλους αλγορίθμους.

8. **Αντίληψη και Αίσθηση:** Η AI μπορεί να «αντιληφθεί» και να αναλύσει το φυσικό περιβάλλον μέσω τεχνολογιών όπως η όραση υπολογιστών (computer vision) και η αναγνώριση φωνής. Αυτή η ικανότητα επιτρέπει στα ρομπότ ή στα αυτόνομα οχήματα να αντιλαμβάνονται και να αλληλεπιδρούν με το περιβάλλον τους.
9. **Ανάλυση Φυσικής Γλώσσας (Natural Language Processing - NLP):** Τα συστήματα AI είναι σε θέση να κατανοήσουν και να παράγουν φυσική γλώσσα, καθιστώντας δυνατή την αλληλεπίδραση μεταξύ ανθρώπων και μηχανών μέσω λόγου ή γραπτού κειμένου.
10. **Λήψη Αποφάσεων:** Οι αλγόριθμοι AI μπορούν να λαμβάνουν αποφάσεις βασισμένες σε μεγάλα σύνολα δεδομένων και να προβλέπουν αποτελέσματα με ακρίβεια, κάτι που χρησιμοποιείται ευρέως σε τομείς όπως τα οικονομικά, η ιατρική και η βιομηχανία.
11. **Αυτοβελτίωση:** Τα προηγμένα συστήματα AI είναι σε θέση να μαθαίνουν από τα λάθη τους και να βελτιώνουν τη λειτουργικότητά τους με την πάροδο του χρόνου, κάτι που τους επιτρέπει να γίνονται πιο αποτελεσματικά. **[10]**

Πέρα από τις κύριες ταξινομήσεις της στενής, γενικής και υπερευφυούς τεχνητής νοημοσύνης, υπάρχουν αρκετά πιο διαφορετικά και αλληλένδετα επίπεδα τεχνητής νοημοσύνης.

Η μηχανική μάθηση (Machine Learning) είναι ένα υποσύνολο της τεχνητής νοημοσύνης που επιτρέπει στα συστήματα υπολογιστών να μαθαίνουν και να βελτιώνονται από την εμπειρία ή τα δεδομένα, και ενσωματώνει στοιχεία από τομείς όπως η επιστήμη των υπολογιστών, η στατιστική, η ψυχολογία, η νευροεπιστήμη και η οικονομία. Εφαρμόζοντας αλγορίθμους σε διαφορετικούς τύπους μεθόδων μάθησης και τεχνικών ανάλυσης, η ML μπορεί αυτόματα να μάθει και να βελτιωθεί από τα δεδομένα και την εμπειρία χωρίς να έχει προγραμματιστεί ρητά να το κάνει. Για τις επιχειρήσεις, η μηχανική μάθηση μπορεί να χρησιμοποιηθεί για την πρόβλεψη αποτελεσμάτων με βάση την ανάλυση μεγάλων, σύνθετων συνόλων δεδομένων.

Τα νευρωνικά δίκτυα(Neural Networks) είναι ένα θεμελιώδες συστατικό της τεχνητής νοημοσύνης, εμπνευσμένο από τη δομή και τη λειτουργία του ανθρώπινου εγκεφάλου. Αυτά τα πολυεπίπεδα υπολογιστικά μοντέλα έχουν κόμβους συγκεντρωμένους μαζί όπως οι νευρώνες σε έναν βιολογικό εγκέφαλο. Κάθε τεχνητός νευρώνας λαμβάνει είσοδο, εκτελεί μαθηματικές πράξεις σε αυτό και παράγει ένα αποτέλεσμα που στη συνέχεια περνά σε επόμενα στρώματα νευρώνων μέσω γρήγορης, παράλληλης επεξεργασίας. Κατά τη διάρκεια της εκπαίδευσης, τα νευρωνικά δίκτυα προσαρμόζουν τη δύναμη των συνδέσεων μεταξύ των νευρώνων με βάση παραδείγματα στα δεδομένα, επιτρέποντάς τους να αναγνωρίζουν μοτίβα, να κάνουν προβλέψεις και να επιλύουν προβλήματα. Χρησιμοποιούν μια ποικιλία μεθόδων για να μάθουν από τα δεδομένα ανάλογα με την εργασία και τον τύπο των δεδομένων. Τα νευρωνικά δίκτυα έχουν βρει εφαρμογές σε διάφορους τομείς όπως η αναγνώριση εικόνας και ομιλίας, η επεξεργασία φυσικής γλώσσας, η μοντελοποίηση, τα αυτόνομα οχήματα και πολλά άλλα.

Η βαθιά μάθηση (Deep Learning) είναι ένα υπολογιστικό υποσύνολο της μηχανικής μάθησης που χρησιμοποιεί νευρωνικά δίκτυα με πολλαπλά (βαθιά) επίπεδα για να μάθει και να εξαγάγει χαρακτηριστικά από τεράστιες ποσότητες δεδομένων. Αυτά τα βαθιά νευρωνικά δίκτυα μπορούν αυτόματα να ανακαλύψουν περίπλοκα πρότυπα και σχέσεις στα δεδομένα που μπορεί να μην είναι άμεσα προφανή στους ανθρώπους, επιτρέποντας πιο ακριβείς προβλέψεις και αποφάσεις. Η βαθιά μάθηση υπερέχει σε εργασίες όπως η αναγνώριση εικόνας και ομιλίας, η επεξεργασία φυσικής γλώσσας και η ανάλυση δεδομένων. Αξιοποιώντας την ιεραρχική δομή των βαθιά νευρωνικών δικτύων, η βαθιά μάθηση έχει φέρει επανάσταση σε πολλούς τομείς, συμπεριλαμβανομένης της υγειονομικής περίθαλψης, των οικονομικών και των αυτόνομων συστημάτων.

Επεξεργασία Φυσικής Γλώσσας (Natural Language Processing) είναι ένας τομέας της Τεχνητής Νοημοσύνης που ασχολείται με την αλληλεπίδραση μεταξύ υπολογιστών και ανθρώπινης γλώσσας. Στόχος του NLP είναι να δώσει στους υπολογιστές τη δυνατότητα να κατανοούν, να αναλύουν και να απαντούν σε φυσική γλώσσα — δηλαδή στη γλώσσα που χρησιμοποιούν οι άνθρωποι για να επικοινωνούν.Κύριες πτυχές του NLP: Κατανόηση Φυσικής Γλώσσας, Παραγωγή Φυσικής Γλώσσας(ικανότητα των συστημάτων να παράγουν φυσική γλώσσα από δεδομένα ή πληροφορίες,όπου ακούγεται φυσικό και λογικό), Εξαγωγή
Πληροφοριών(διαδικασία κατά την οποία το σύστημα συλλέγει και εξάγει χρήσιμες πληροφορίες από κείμενα π.χ. αναγνώριση ονομάτων, ημερομηνιών, τοποθεσιών κ.λπ.), Ανάλυση
Συναισθήματος (Sentiment Analysis**)**: Ένα κοινό υποσύνολο του NLP που αναλύει κείμενα (όπως σχόλια χρηστών ή δημοσιεύσεις στα social media) για να κατανοήσει αν το συναίσθημα πίσω από το κείμενο είναι θετικό, αρνητικό ή ουδέτερο, Μετάφραση Μηχανής**(** αυτόματη μετάφραση κειμένων από μία γλώσσα σε μία άλλη, όπως το Google Translate). [11]

3. Η επίδραση της AI στο IT Audit

Ανατρεπτικές τεχνολογίες αυτοματισμού

Το «φάσμα αυτοματισμού», όπως το ορίζουμε, περιλαμβάνει ένα ευρύ φάσμα ψηφιακών τεχνολογιών. Στο ένα άκρο υπάρχουν μοντέλα πρόβλεψης και εργαλεία για την ολοκλήρωση και οπτικοποίηση δεδομένων και στο άλλο άκρο είναι προηγμένες τεχνολογίες με γνωστικά στοιχεία που μιμούνται την ανθρώπινη συμπεριφορά.

Πολλοί οργανισμοί ΙΑ είναι εξοικειωμένοι με το πρώτο μέρος του φάσματος αυτοματισμού, έχοντας ήδη δημιουργήσει θεμελιώδη προγράμματα ενοποίησης δεδομένων και ανάλυσης για την ενίσχυση των διαδικασιών αξιολόγησης κινδύνου, ελέγχου πεδίου και αναφοράς. Καθώς αυτοί οι οργανισμοί εργάζονται σε αυτό το συνεχές, ορισμένοι έχουν αρχίσει να υιοθετούν το RPA(Robotic process automation) σε συνδυασμό με ορισμένα εργαλεία CI(Continuous integration), συλλογικά γνωστό ως RPA&CI, για να συμβάλει στην αύξηση της αποδοτικότητας και της αποτελεσματικότητας, να επεκτείνει την ικανότητα, να ενισχύσει την ποιότητα και να επιτρέψει μεγαλύτερη κάλυψη ελέγχου. Η μηχανική μάθηση και η τεχνητή νοημοσύνη βρίσκονται στο άκρο αυτού του εύρους, με λιγότερους οργανισμούς να έχουν φτάσει σε αυτό το επίπεδο ψηφιακής ωριμότητας. Ωστόσο, αυτή η κατάσταση αλλάζει γρήγορα. Οι γνωστικές τεχνολογίες αναμένεται να γίνουν πιο διαδεδομένες στο εγγύς μέλλον, καθώς οι πρώτοι υιοθετητές αποδεικνύουν την ικανότητά τους να ενισχύουν την πρόταση αξίας της ελεγκτικής λειτουργίας. Για παράδειγμα, ορισμένοι οργανισμοί εκτίμησης επιπτώσεων έχουν εφαρμόσει αποτελεσματικά τη χρήση της τεχνητής νοημοσύνης για τον προληπτικό εντοπισμό αναδυόμενων κινδύνων για εκτιμήσεις κινδύνου.

Οι βασικές κατηγορίες τεχνολογιών που σχετίζονται με την επεξεργασία και την ανάλυση δεδομένων, καθώς και την αυτοματοποίηση επιχειρησιακών διαδικασιών είναι οι εξής:

- **Ίδρυμα:** Εστιάζει στην **ενοποίηση δεδομένων**, δηλαδή στη συγκέντρωση και ενοποίηση πληροφοριών από διαφορετικές πηγές, ώστε να παρέχεται μια συνεπής και αξιόπιστη βάση δεδομένων.
- **Ανάλυση:** Περιλαμβάνει την **προγνωστική ανάλυση**, η οποία χρησιμοποιεί μαθηματικά μοντέλα για την πρόβλεψη κινδύνων και τάσεων, καθώς και την **οπτικοποίηση δεδομένων**, που βοηθά στην παρουσίαση πολύπλοκων δεδομένων μέσω γραφημάτων και διαδραστικών πινάκων εργαλείων.
- **Ρομποτική:** Αναφέρεται στη **ρομποτική αυτοματοποίηση διεργασιών (RPA)**, μια τεχνολογία που επιτρέπει την αυτοματοποίηση επαναλαμβανόμενων εργασιών, μιμούμενη την ανθρώπινη αλληλεπίδραση με τα συστήματα πληροφορικής.
- **Γνωστική Νοημοσύνη:** Συμπεριλαμβάνει προηγμένες τεχνολογίες όπως η **παραγωγή και επεξεργασία φυσικής γλώσσας (NLP)**, η **μηχανική μάθηση (Machine Learning)** για την ανάπτυξη αλγορίθμων που βελτιώνονται μέσω εμπειρίας, και η **ταυτοποίηση γλώσσας**, που επιτρέπει την κατανόηση και μετάφραση μεταξύ διαφορετικών γλωσσών, προσομοιώνοντας ανθρώπινες νοητικές λειτουργίες.

Αυτές οι τεχνολογίες αποτελούν βασικά εργαλεία για τον ψηφιακό μετασχηματισμό οργανισμών, βελτιώνοντας την αποδοτικότητα, την ασφάλεια και την ακρίβεια στη διαχείριση δεδομένων και επιχειρησιακών διαδικασιών.

Τα οφέλη της ενσωμάτωσης αυτοματισμού

Υπάρχουν πολλοί τρόποι με τους οποίους η εκτίμηση επιπτώσεων μπορεί να αξιοποιήσει τις δυνατότητες αυτοματοποίησης καθ' όλη τη διάρκεια του κύκλου ζωής του ελέγχου, συμπεριλαμβανομένων των εκτιμήσεων κινδύνου, του σχεδιασμού ελέγχου, της επιτόπιας εργασίας και της υποβολής εκθέσεων

Απόδοση υψηλότερης ποιότητας. Το RPA&CI επιτρέπει την εκτέλεση των εργασιών πιο ομοιόμορφα και αποτελεσματικά. Επιπλέον, τα αποτελέσματα είναι εξαιρετικά ανιχνεύσιμα και ελέγξιμα. Με την εγγενή τυποποίηση της διαδικασίας, είναι πιθανό να προκύψουν λιγότερα χειροκίνητα σφάλματα, γεγονός που βελτιώνει την ακρίβεια και την ποιότητα των ελέγχων.

Αυξημένη αποδοτικότητα και μειωμένο κόστος. Το RPA&CI μπορεί να λειτουργεί και να εκτελεί εργασίες ελέγχου όλο το εικοσιτετράωρο με επιταχυνόμενο ρυθμό (σε πολλές περιπτώσεις, περισσότερο από 90% ταχύτερα από τις χειροκίνητες διαδικασίες). Μειώνοντας τις χρονοβόρες χειρωνακτικές δραστηριότητες, η αυτοματοποίηση μπορεί να οδηγήσει σε σημαντική εξοικονόμηση κόστους.

Καλύτερη χρήση πόρων.Αντικαθιστώντας τις μη αυτόματες δραστηριότητες, η αυτοματοποίηση μπορεί να απελευθερώσει ανθρώπινο δυναμικό,επιτρέποντας στο προσωπικό να επικεντρωθεί σε δραστηριότητες υψηλότερης αξίας,όπως αναθεωρήσεις διασφάλισης ποιότητας,διαχείριση εξαιρέσεων, βελτίωση διαδικασιών και διαπροσωπικών αλληλεπιδράσεων. **[12]**

3.2 Αυτοματοποίηση διαδικασιών Audit μέσω AI.

Η ενσωμάτωση της τεχνητής νοημοσύνης (AI) στην επιθεώρηση πληροφοριακών συστημάτων μετασχηματίζει ριζικά τις παραδοσιακές ελεγκτικές διαδικασίες. Πέρα από τη γενική αυτοματοποίηση και την αναγνώριση μοτίβων, η AI εφαρμόζεται σε συγκεκριμένες λειτουργίες που ενισχύουν την ακρίβεια, την αποδοτικότητα και την εμβάθυνση της ανάλυσης.

Ανίχνευση απάτης μέσω Machine Learning:
Μία από τις πιο διαδεδομένες χρήσεις της AI στο audit είναι η ανίχνευση απάτης μέσω αλγορίθμων μηχανικής μάθησης (Machine Learning). Χρησιμοποιούνται τόσο supervised όσο και unsupervised τεχνικές, όπως δέντρα αποφάσεων (decision trees), τυχαία δάση (random forests) και μοντέλα clustering. Τα εργαλεία αυτά επιτρέπουν την κατάρτιση προγνωστικών μοντέλων με βάση ιστορικά δεδομένα, εντοπίζοντας ασυνήθιστα μοτίβα συναλλαγών ή αποκλίσεις από καθιερωμένους κανόνες. Για παράδειγμα, η AI μπορεί να ανιχνεύσει πολλαπλές συναλλαγές που διαιρούνται τεχνητά ώστε να παρακάμπτουν ένα όριο έγκρισης.

Ανάλυση εγγράφων με Natural Language Processing (NLP):
Μέσω τεχνικών φυσικής γλώσσας (Natural Language Processing - NLP), τα συστήματα AI μπορούν να αναλύσουν έγγραφα, συμβόλαια και τιμολόγια. Ένα παράδειγμα είναι η αυτόματη

εξαγωγή όρων πληρωμής από PDF τιμολόγια ή ο εντοπισμός αναφορών κινδύνου σε εταιρικά emails. Έτσι, η AI καθιστά δυνατή την ποσοτικοποίηση και αξιολόγηση ποιοτικών στοιχείων.

Ρομποτική Αυτοματοποίηση Διαδικασιών (RPA): Η RPA συμπληρώνει τη λειτουργικότητα της AI, εκτελώντας επαναλαμβανόμενες ενέργειες όπως η αντιγραφή δεδομένων μεταξύ ERP συστημάτων και λογιστικών φύλλων. Μπορεί να εφαρμοστεί για τη μαζική σύγκριση εγγραφών, την επιβεβαίωση πληρωμών ή την αυτόματη δημιουργία reports συμμόρφωσης.

Continuous Auditing και Real-time Monitoring:

Η AI επιτρέπει την υλοποίηση συνεχούς ελέγχου (continuous auditing), όπου το σύστημα επεξεργάζεται το 100% των συναλλαγών σε πραγματικό χρόνο, αντί για την παραδοσιακή δειγματοληψία. Μέσω διασύνδεσης με βάσεις δεδομένων ή ERP συστήματα (όπως SAP), η AI παρακολουθεί μεταβολές και ενεργοποιεί ειδοποιήσεις (alerts) για εντοπισμένες αποκλίσεις από πολιτικές κανονιστικής συμμόρφωσης.

Ανάλυση Μεγάλων Όγκων Δεδομένων: Η ανάλυση μεγάλων όγκων δεδομένων (Big Data Analytics) μέσω της τεχνητής νοημοσύνης (AI) αποτελεί μία από τις πιο ισχυρές και σύγχρονες μεθόδους για τον αυτοματοποιημένο έλεγχο (audit). Δεδομένου ότι οι οργανισμοί παράγουν τεράστιες ποσότητες δεδομένων, τα παραδοσιακά εργαλεία ανάλυσης δεν επαρκούν πλέον για την αποτελεσματική διερεύνηση και αξιολόγηση. Η AI επιτρέπει την ανάλυση αυτών των δεδομένων με μεγαλύτερη ακρίβεια και ταχύτητα.

Τρόποι Ανάλυσης Μεγάλων Όγκων Δεδομένων με AI στο Audit :

- **Επεξεργασία και Δομημένη Ανάλυση Μη Δομημένων Δεδομένων:** Στο πλαίσιο ενός audit, οι ελεγκτές συχνά πρέπει να αναλύσουν μη δομημένα δεδομένα όπως emails, λογιστικά αρχεία, έγγραφα και μηνύματα. Με τη χρήση αλγορίθμων μηχανικής μάθησης (machine learning), η AI μπορεί να ταξινομήσει και να κατηγοριοποιήσει τα δεδομένα αυτά, επιτρέποντας την εύκολη ανάλυση μεγάλων αρχείων χωρίς τη χειροκίνητη επέμβαση.
- **Ανίχνευση Ανωμαλιών:** Η AI είναι εξαιρετικά αποτελεσματική στον εντοπισμό ανωμαλιών σε μεγάλα datasets, χρησιμοποιώντας τεχνικές όπως η ανίχνευση outliers (δεδομένων που αποκλίνουν από το αναμενόμενο μοτίβο). Αυτό είναι εξαιρετικά χρήσιμο στον έλεγχο, καθώς μπορεί να αποκαλύψει παρατυπίες ή ύποπτες συναλλαγές που χρειάζονται περαιτέρω διερεύνηση.
- **Προγνωστική Ανάλυση (Predictive Analytics):** Με τη χρήση μηχανικής μάθησης, η AI μπορεί να χρησιμοποιήσει ιστορικά δεδομένα για να προβλέψει μελλοντικά γεγονότα ή συμπεριφορές. Αυτό επιτρέπει στους ελεγκτές να εντοπίζουν περιοχές που μπορεί να διατρέχουν κίνδυνο ή να ανακαλύψουν πιθανά σενάρια απάτης πριν αυτά συμβούν. • **Αυτοματοποιημένη Ομαδοποίηση Δεδομένων:** Η AI μπορεί να ταξινομεί τα δεδομένα σε ομάδες βάσει ομοιοτήτων (clustering), χωρίς την ανάγκη προκαθορισμένων κανόνων. Αυτό βοηθά στην αναγνώριση μοτίβων και ομάδων συναλλαγών ή δραστηριοτήτων που μπορούν να ενισχύσουν την κατανόηση του πώς λειτουργεί ένας οργανισμός και να βελτιώσουν τον έλεγχο.

- **Αλγόριθμοι Μηχανικής Μάθησης για Βελτίωση Ακρίβειας:** Οι αλγόριθμοι μηχανικής μάθησης προσαρμόζονται με την πάροδο του χρόνου, βελτιώνοντας την ακρίβειά τους όσο αυξάνεται η ποσότητα και η ποικιλία των δεδομένων. Αυτό σημαίνει ότι όσο περισσότερα δεδομένα επεξεργάζεται ένας αλγόριθμος, τόσο πιο ακριβή και αποτελεσματικά γίνονται τα αποτελέσματα των ελέγχων.
- **Γλωσσική Ανάλυση (Natural Language Processing – NLP):** Η NLP χρησιμοποιείται για την ανάλυση γραπτών κειμένων και την εξαγωγή σημαντικών πληροφοριών από μη δομημένα δεδομένα, όπως email και έγγραφα. Αυτό επιτρέπει στους ελεγκτές να εντοπίζουν κινδύνους ή αποκλίσεις σε κείμενα, χωρίς να χρειάζεται να τα αναλύσουν χειροκίνητα.

Προγνωστικά μοντέλα Machine Learning στο Audit:

Τα **προγνωστικά μοντέλα (predictive models)** μαθαίνουν από ιστορικά δεδομένα για να προβλέπουν μελλοντικές ή ασυνήθιστες καταστάσεις, π.χ. αν μια συναλλαγή είναι ύποπτη. Χωρίζονται κυρίως σε δύο τύπους:

◇ **Supervised Learning Models (Μοντέλα με ετικέτες/labels)**

Σε αυτά τα μοντέλα η μηχανή μαθαίνει από ένα σύνολο δεδομένων όπου τα αποτελέσματα είναι ήδη γνωστά (π.χ. αν μια συναλλαγή είναι «απάτη» ή «όχι απάτη»). Ο στόχος είναι να μάθει να προβλέπει σωστά το αποτέλεσμα σε νέες, άγνωστες συναλλαγές.

1. **Decision Trees (Δέντρα Αποφάσεων)**
   Χωρίζουν τα δεδομένα σε κόμβους με βάση συγκεκριμένα χαρακτηριστικά (π.χ. ποσό συναλλαγής, χώρα προέλευσης). Στο τέλος παράγεται μια «διαδρομή απόφασης», εύκολα κατανοητή ακόμα και από μη τεχνικούς, γι' αυτό και χρησιμοποιούνται συχνά σε audit reports.
2. **Random Forests**
   Αντί να βασίζεται μόνο σε ένα decision tree, δημιουργεί πολλά διαφορετικά δέντρα και «ψηφίζει» ποιο είναι το πιο σωστό αποτέλεσμα. Έτσι μειώνει τα λάθη και αποφεύγει το overfitting, δηλαδή το να «μάθει απ' έξω» τα δεδομένα χωρίς να γενικεύει σωστά.
3. **Logistic Regression**
   Απλό αλλά αξιόπιστο μοντέλο που χρησιμοποιείται κυρίως για δυαδικές αποφάσεις (ναι/όχι, σωστό/λάθος). Παρά την απλότητά του, είναι χρήσιμο σε audit περιβάλλοντα όπου χρειάζεται γρήγορη και ξεκάθαρη ταξινόμηση συναλλαγών.
4. **Gradient Boosting Machines (π.χ. XGBoost, LightGBM)**
   Κατασκευάζουν μια σειρά από απλά decision trees, όπου κάθε επόμενο δέντρο προσπαθεί να διορθώσει τα λάθη του προηγούμενου. Έτσι το μοντέλο γίνεται πιο «έξυπνο» βήμα-βήμα. Είναι από τις πιο ισχυρές μεθόδους για μεγάλα σύνολα δεδομένων, όπως αυτά που συναντάμε σε ελέγχους τραπεζικών συναλλαγών.

◇ **Unsupervised Learning Models (Μοντέλα χωρίς ετικέτες)**

Αυτά τα μοντέλα είναι χρήσιμα όταν δεν έχουμε προκαθορισμένες κατηγορίες (π.χ. δεν ξέρουμε

ποιες συναλλαγές είναι απάτη και ποιες όχι). Αντί να προβλέπουν, προσπαθούν να βρουν μοτίβα και ασυνήθιστες συμπεριφορές.

1. **Clustering (π.χ. K-means)**

   Ομαδοποιεί συναλλαγές που μοιάζουν μεταξύ τους. Για παράδειγμα, αν οι περισσότερες συναλλαγές ενός πελάτη είναι μικρού ποσού και ξαφνικά εμφανιστεί μία πολύ μεγάλη, αυτή ξεχωρίζει ως «ανωμαλία».

2. **Autoencoders (Νευρωνικά Δίκτυα)**

   Μαθαίνουν να αναπαριστούν «φυσιολογικές» συναλλαγές με τη βοήθεια τεχνητών νευρωνικών δικτύων. Όταν μια συναλλαγή διαφέρει πολύ από το συνηθισμένο μοτίβο, το μοντέλο αποτυγχάνει να την αναπαραστήσει σωστά και τη σημαίνει ως ύποπτη.

3. **Isolation Forests**

   Εξειδικευμένα για ανίχνευση outliers. Αν μια συναλλαγή απομονώνεται πολύ εύκολα από τις υπόλοιπες (δηλαδή ξεχωρίζει χωρίς μεγάλη προσπάθεια), τότε θεωρείται πιθανόν ύποπτη.

4. **One-Class SVM**

   Δημιουργεί ένα μαθηματικό όριο γύρω από τις «κανονικές» συναλλαγές. Ό,τι βρίσκεται έξω από αυτό το όριο θεωρείται εκτός προτύπου και άρα ύποπτο.

Πώς επιλέγεται το κατάλληλο μοντέλο στο Audit;

- Αν υπάρχουν **ιστορικά ετικετοποιημένα δεδομένα απάτης**, χρησιμοποιούνται supervised μοντέλα.
- Αν υπάρχουν **μόνο τρέχοντα δεδομένα χωρίς labels**, εφαρμόζονται unsupervised ή hybrid προσέγγιση.
- Συχνά, γίνεται χρήση **ensemble models** ή **hybrid pipelines** (π.χ. πρώτα clustering, μετά supervised classification).

Κατά την επιλογή του κατάλληλου προγνωστικού μοντέλου στο audit, είναι κρίσιμο να συνεκτιμηθούν παράγοντες όπως η ποιότητα των διαθέσιμων δεδομένων, ο συγκεκριμένος σκοπός του ελέγχου (π.χ. ανίχνευση απάτης ή πρόβλεψη κινδύνου), η υπολογιστική πολυπλοκότητα, καθώς και η ερμηνευσιμότητα των αποτελεσμάτων. Ιδιαίτερη σημασία έχει το κατά πόσο το μοντέλο μπορεί να τεκμηριώσει τις προβλέψεις του, δεδομένου ότι οι ελεγκτές χρειάζονται σαφήνεια για να υποστηρίξουν τα ευρήματά τους. Επιπλέον, τα προγνωστικά μοντέλα πρέπει να πληρούν κανονιστικές απαιτήσεις (όπως GDPR και EU AI Act) και να αποφεύγουν φαινόμενα μεροληψίας. Τέλος, η επιλογή οριστικοποιείται με βάση πειραματική αξιολόγηση (π.χ. ROC curve, confusion matrix) και τη βέλτιστη ισορροπία μεταξύ ακρίβειας, κόστους και χρησιμότητας στο audit.

Παραδείγματα εφαρμογών που χρησιμοποιούν Τεχνητή Νοημοσύνη για την αυτοματοποίηση ανάλυσης μεγάλων όγκων στο Audit:

Στον χώρο του ελέγχου (audit), η τεχνητή νοημοσύνη έχει βρει ιδιαίτερα χρήσιμες εφαρμογές στην αυτοματοποίηση της ανάλυσης μεγάλων όγκων δεδομένων. Το **CaseWare IDEA** αποτελεί

χαρακτηριστικό παράδειγμα, προσφέροντας δυνατότητες αποτελεσματικής ανάλυσης εκτεταμένων συνόλων δεδομένων, δημιουργίας προσαρμοσμένων αναφορών και οπτικοποιήσεων, καθώς και εντοπισμού ανωμαλιών και πρόβλεψης κινδύνων.

Αντίστοιχα, το **ACL Robotics** (Galvanize) επιτρέπει την υλοποίηση αυτοματοποιημένων ελέγχων δεδομένων σε πραγματικό χρόνο, ενσωματώνοντας ισχυρές δυνατότητες ανάλυσης και εντοπισμού αποκλίσεων. Παράλληλα, προσφέρει προσαρμοσμένες αναφορές και δυναμικούς πίνακες ελέγχου (dashboards), διευκολύνοντας τη λήψη τεκμηριωμένων αποφάσεων.

Σημαντική θέση κατέχει και το **IBM Watson for Audit**, το οποίο ειδικεύεται στην ανάλυση μη δομημένων δεδομένων, αξιοποιώντας την τεχνολογία επεξεργασίας φυσικής γλώσσας (NLP) για την επεξεργασία και ερμηνεία εγγράφων. Με αυτόν τον τρόπο, συμβάλλει στον εντοπισμό προβλημάτων συμμόρφωσης και αποκλίσεων, προσφέροντας ένα επιπλέον επίπεδο ελέγχου και ακρίβειας στη διαδικασία αξιολόγησης.

Ανίχνευση και Πρόληψη απατών

Η AI μπορεί να ανιχνεύει και να προλαμβάνει απάτες πολύ πιο αποτελεσματικά από τις παραδοσιακές μεθόδους, αναλύοντας μοτίβα, συμπεριφορές και μεγάλους όγκους δεδομένων σε πραγματικό χρόνο:

- **Ανάλυση Πρότυπων Συμπεριφορών:** Η AI χρησιμοποιεί τεχνικές μηχανικής μάθησης (machine learning) για να αναλύει ιστορικά δεδομένα και να μαθαίνει πρότυπα φυσιολογικής συμπεριφοράς για έναν οργανισμό ή άτομα. Όταν ανιχνεύονται αποκλίσεις από αυτά τα πρότυπα, μπορεί να ειδοποιήσει τους ελεγκτές για πιθανές περιπτώσεις απάτης.

Τεχνικές ML για Ανάλυση Πρότυπων Συμπεριφορών

Κατηγορία Τεχνικής	Τεχνική / Μέθοδος	Περιγραφή	Χρήση στην Ανίχνευση Απάτης
Unsupervised Learning	Isolation Forest	"Απομονώνει" σημεία δεδομένων που είναι διαφορετικά από τα υπόλοιπα.	Εντοπισμός ακραίων συναλλαγών ή συμπεριφορών.
	One-Class SVM	Μαθαίνει μόνο από "κανονικά" δεδομένα και εντοπίζει τις αποκλίσεις.	Ιδανικό όταν δεν έχουμε ετικέτες "απάτης".
Supervised Learning	Random Forest / XGBoost	Χρησιμοποιεί ιστορικά δεδομένα με ετικέτες (fraud /	Εντοπισμός απάτης όταν υπάρχει παρελθοντική γνώση.

		no fraud) για εκπαίδευση.	
Statistical Methods	Z-score, IQR, Mahalanobis Distance	Ανιχνεύουν στατιστικά ακραίες τιμές.	Εφαρμόζονται σε αριθμητικά χαρακτηριστικά (π.χ. ποσά).
Sequence Models	LSTM / RNN	Μαθαίνουν χρονικά μοτίβα (patterns) από data.	Ανάλυση χρονικών αποκλίσεων σε χρήστες/συναλλαγές.

Table 4-Τεχνικές ML για Ανάλυση Πρότυπων Συμπεριφορών

Εργαλεία για Ανάλυση Πρότυπων Συμπεριφορών & Ανίχνευση Απάτης

Εργαλείο	Τεχνική ή Μέθοδος	Περιγραφή& Χρήση	Καλές Περιπτώσεις Χρήσης
RapidMiner	Data Science, Anomaly Detection	Πλατφόρμα για ανάλυση δεδομένων με drag-and-drop interface.	Δημιουργία μοντέλων ανίχνευσης απάτης χωρίς ανάγκη κώδικα.
Amazon SageMaker	Supervised / Unsupervised Learning	Υπηρεσία από το AWS για εκπαίδευση και ανάλυση μοντέλων machine learning.	Ανίχνευση ανωμαλιών σε cloud-based εφαρμογές και υπηρεσίες.
IBM Watson Studio	AutoAI, Machine Learning	Υπηρεσία της IBM για εκπαίδευση μοντέλων AI και ανίχνευση ανωμαλιών.	Ανίχνευση απάτης και δημιουργία στρατηγικών ασφάλειας μέσω AI.
Splunk	SIEM (Security Information and Event Management)	Εργαλείο για ανάλυση δεδομένων και logs σε πραγματικό χρόνο.	Ανίχνευση ανωμαλιών και παραβάσεων σε οργανωτικά συστήματα.
TensorFlow / Keras	LSTM, Autoencoders	Deep learning για ανάλυση	Ανίχνευση απάτης σε πραγματικό

		χρονοσειρών και ανωμαλιών.	χρόνο (π.χ. σε συναλλαγές).

Table 5-Εργαλεία για Ανάλυση Πρότυπων Συμπεριφορών & Ανίχνευση Απάτης

- **Επεξεργασία Φυσικής Γλώσσας (Natural Language Processing - NLP):** Η NLP μπορεί να αναλύσει μη δομημένα δεδομένα, όπως emails, έγγραφα και άλλα κείμενα, για να εντοπίσει ύποπτη γλώσσα ή αλληλογραφίες που μπορεί να σχετίζονται με απάτη. Αυτό είναι χρήσιμο ειδικά όταν υπάρχει μεγάλη ποσότητα επικοινωνιών που πρέπει να αναλυθεί.

  Παραδείγματα NLP για Ανίχνευση Απάτης

Περιοχή Εφαρμογής	**Περιγραφή NLP Χρήσης**	**Τι ανιχνεύει**
Emails υπαλλήλων σε μια επιχείρηση	**μια επιχείρηση** NLP εργαλείο σαρώνει αυτόματα χιλιάδες email για λέξεις/φράσεις όπως "επείγουσα πληρωμή", "μην το πεις σε κανέναν", "παράκαμψη έγκρισης".	Εντοπισμός **phishing** ή **insider threats** (απάτη εκ των έσω).
Συνομιλίες σε εφαρμογές μηνυμάτων (Slack, Teams)	Ανάλυση συναισθήματος (sentiment analysis) και εντοπισμός ύποπτων μοτίβων επικοινωνίας.	Αναγνώριση **ύποπτης συμπεριφοράς** πριν εξελιχθεί σε απάτη.
Έγγραφα τιμολόγησης / λογιστικά αρχεία	Ανάλυση περιεχομένου PDF/Word για ανακολουθίες στη γλώσσα ή δομή, όπως διπλότυπες εγγραφές ή ασυνήθιστες περιγραφές.	Εντοπισμός **πλαστών ή τροποποιημένων εγγράφων**.
Κλήσεις υποστήριξης πελατών (μετατροπή φωνής σε κείμενο)	NLP μετατρέπει ηχητικά σε κείμενο και αναλύει μοτίβα απάτης (π.χ. επαναλαμβανόμενες καταγγελίες για το ίδιο άτομο ή λογαριασμό).	Προστασία από **απάτες με επιστροφές/αποζημιώσεις**.

Αυτόματη μετάφραση email από ξένες γλώσσες	NLP μεταφράζει μηνύματα σε πραγματικό χρόνο για ανάλυση και αναζήτηση "red flag" εκφράσεων.	Εντοπισμός **διασυνοριακής απάτης ή κοινωνικής μηχανικής**.

Table 6-Παραδείγματα NLP για Ανίχνευση Απάτης

Εργαλεία και Τεχνολογίες NLP για Ανίχνευση Απάτης

Κατηγορία	**Εργαλείο / Πλατφόρμα**	**Περιγραφή**
Γλώσσες Προγραμματισμού	Python, R	Οι πιο δημοφιλείς για NLP και data analysis.
Βιβλιοθήκες NLP	spaCy, NLTK, TextBlob, Stanza	Χρησιμοποιούνται για tokenization, POS tagging, named entity recognition, parsing, κ.ά.
Deep Learning / NLP μοντέλα	Transformers της Hugging Face(π.χ.BERT, RoBERTa)	Για πιο εξελιγμένη κατανόηση φυσικής γλώσσας, ιδανικά για emails και έγγραφα.
Ανάλυση Συναισθήματος (Sentiment Analysis)	VADER, TextBlob, BERT Sentiment Models	Για εντοπισμό ύποπτης γλώσσας ή συναισθηματικών αλλαγών.
Speech to Text	Google Speech-to-Text, IBM Watson, Azure Speech	Μετατροπή ομιλίας σε κείμενο για ανάλυση κλήσεων/συνομιλιών.

Table 7-Εργαλεία και Τεχνολογίες NLP για Ανίχνευση Απάτης

- **Προγνωστική Ανάλυση (Predictive Analytics):** Η προγνωστική ανάλυση χρησιμοποιεί δεδομένα από προηγούμενες περιπτώσεις απάτης για να αναγνωρίσει μοτίβα και τάσεις που μπορεί να υποδεικνύουν μελλοντικές απάτες. Με βάση τις ιστορικές συμπεριφορές, η AI μπορεί να εντοπίσει συναλλαγές ή ενέργειες που παρουσιάζουν υψηλό κίνδυνο απάτης.
- **Μηχανική Μάθηση (Machine Learning) και Βαθιά Μάθηση (Deep Learning):** Η AI μπορεί να χρησιμοποιεί αλγόριθμους μηχανικής μάθησης και βαθιάς μάθησης για να αναγνωρίζει μοτίβα που είναι δύσκολο να ανιχνευθούν με τα παραδοσιακά εργαλεία. Οι αλγόριθμοι αυτοί βελτιώνονται με τον χρόνο, μαθαίνοντας από νέα δεδομένα, και μπορούν να εντοπίζουν ολοένα και πιο σύνθετες μορφές απάτης.

Παραδείγματα Εργαλείων AI για Ανίχνευση Απάτης:

Darktrace: Το Darktrace είναι μια πλατφόρμα που χρησιμοποιεί AI για την ανίχνευση ανωμαλιών σε δίκτυα και την πρόληψη απάτης σε συστήματα πληροφοριών.Η πλατφόρμα χρησιμοποιεί "ανοσοποιητικό σύστημα" τεχνολογία, η οποία ανιχνεύει περίεργη συμπεριφορά σε πραγματικό χρόνο και προσαρμόζεται συνεχώς στις νέες απειλές. **SAS Fraud Management:** Το SAS χρησιμοποιεί αλγόριθμους AI για τον εντοπισμό και την πρόληψη οικονομικής απάτης.Η πλατφόρμα του παρέχει συνεχή ανάλυση σε πραγματικό χρόνο και ειδοποιήσεις για ύποπτες συναλλαγές, μειώνοντας τους χρόνους αντίδρασης και βελτιώνοντας τη λήψη αποφάσεων.

Συνεχής Παρακολούθηση (Continuous Monitoring)

Η Συνεχής Παρακολούθηση αναφέρεται στη δυνατότητα συνεχούς συλλογής, ανάλυσης και αξιολόγησης δεδομένων και διαδικασιών, με στόχο τον εντοπισμό παρατυπιών, σφαλμάτων, απάτης ή κινδύνων.Η AI ενισχύει αυτή τη διαδικασία με αυτοματοποιημένα συστήματα που επεξεργάζονται μεγάλα σύνολα δεδομένων σε πραγματικό χρόνο, ανιχνεύουν ανωμαλίες και δημιουργούν προγνωστικές αναλύσεις για πιθανούς κινδύνους.

Ανίχνευση και Ειδοποίηση για Ανωμαλίες σε Πραγματικό Χρόνο: Η AI μπορεί να παρακολουθεί διαρκώς τα συστήματα IT για να εντοπίζει ανωμαλίες ή ύποπτες δραστηριότητες, όπως παραβιάσεις ασφαλείας, απροσδόκητες αλλαγές στα δεδομένα ή ασυνήθιστη συμπεριφορά συστημάτων. Όταν εντοπιστούν αποκλίσεις, το σύστημα ειδοποιεί αμέσως τους ελεγκτές για να ερευνήσουν περαιτέρω.

Τεχνολογίες που Χρησιμοποιούνται:

Alerting Systems: Χρησιμοποιούνται **webhooks**, **email triggers**, ή **SMS ειδοποιήσεις** για να ειδοποιούν το προσωπικό όταν ανιχνευθεί ανωμαλία.

SIEM (Security Information and Event Management): π.χ. **Splunk**, **IBM QRadar**, **Elastic SIEM** για real-time συλλογή και ανάλυση logs.

Παράδειγμα Ανίχνευσης Ανωμαλιών:

1. **Συλλογή δεδομένων**: Το σύστημα παρακολουθεί το δίκτυο της εταιρείας, τα logs των συστημάτων, τις συναλλαγές των χρηστών, κ.λπ.
2. **Μοντέλο μηχανικής μάθησης**: Χρησιμοποιεί το **Isolation Forest** για να μάθει τις φυσιολογικές συμπεριφορές χρηστών και να ανιχνεύει απόκλιση.
3. **Ανίχνευση ανωμαλίας**: Ο χρήστης προσπαθεί να αποκτήσει πρόσβαση σε ευαίσθητα δεδομένα σε μη φυσιολογική ώρα ή από ασυνήθιστη τοποθεσία.
4. **Ειδοποίηση**: Το σύστημα στέλνει ειδοποίηση στον υπεύθυνο ασφαλείας για να ερευνήσει το περιστατικό.
5. **Αντίδραση**: Ο υπεύθυνος αποφασίζει αν πρέπει να διακόψει την πρόσβαση ή να ενεργοποιήσει περαιτέρω μέτρα ασφαλείας.

Η **Συνεχής Συμμόρφωση (Compliance Monitoring)** αποτελεί μια τεχνολογική προσέγγιση που αυτοματοποιεί την παρακολούθηση των διαδικασιών συμμόρφωσης, βελτιώνοντας τη διαχείριση κινδύνων και μειώνοντας την πιθανότητα μη συμμόρφωσης με **κανονιστικά πλαίσια**, όπως το **GDPR**, το **PCI DSS**, το **ISO 27001** και άλλα. Η τεχνητή νοημοσύνη παρακολουθεί αυτόματα κατά πόσο οι διαδικασίες ευθυγραμμίζονται με τις πολιτικές, τους κανονισμούς και τα πρότυπα ασφαλείας, εντοπίζοντας πιθανές παραβιάσεις πριν αυτές εξελιχθούν σε σοβαρότερα προβλήματα. Παράλληλα, η AI μπορεί να παρακολουθεί και να καταγράφει αλλαγές που πραγματοποιούνται σε κρίσιμα συστήματα, όπως τροποποιήσεις σε αρχεία ή λογισμικό. Ο έγκαιρος εντοπισμός μη εξουσιοδοτημένων αλλαγών ή παρεμβάσεων συμβάλλει στην πρόληψη παραβιάσεων ασφαλείας και στη μείωση κινδύνων που ενδέχεται να επηρεάσουν την ακεραιότητα των δεδομένων και την ομαλή λειτουργία των συστημάτων.

Παραδείγματα Εργαλείων AI για Συνεχή Παρακολούθηση στο IT Audit:

Control Case Continuous Compliance Monitoring: το ControlCase είναι ένα εργαλείο που επιτρέπει τη συνεχή παρακολούθηση της συμμόρφωσης σε κανονιστικά πλαίσια όπως το GDPR, το PCI DSS και άλλα πρότυπα ασφαλείας. Η AI βοηθά στη διαχείριση των δεδομένων και τον έλεγχο συμμόρφωσης σε πραγματικό χρόνο, μειώνοντας το ρίσκο παραβιάσεων.

Vanta: Το Vanta χρησιμοποιεί AI για να αυτοματοποιήσει τις διαδικασίες συμμόρφωσης για πρότυπα όπως το SOC 2, ISO 27001, και GDPR. Παρακολουθεί συνεχώς τα δεδομένα από τα IT συστήματα ενός οργανισμού και ειδοποιεί όταν υπάρχει παραβίαση ή μη συμμόρφωση, ενώ παράγει και αυτόματες αναφορές.

Αυτοματοποιημένη Τεκμηρίωση και Αναφορές

Η **αυτοματοποιημένη τεκμηρίωση και οι αναφορές μέσω AI στο IT audit** είναι μία από τις πιο χρήσιμες εφαρμογές της τεχνητής νοημοσύνης, καθώς επιτρέπει στους οργανισμούς να εξοικονομούν χρόνο και πόρους κατά τη διάρκεια του ελέγχου, παρέχοντας παράλληλα ακριβείς και λεπτομερείς αναφορές. Αυτή η διαδικασία συνδυάζει την αυτοματοποίηση της συλλογής δεδομένων, την ανάλυση πληροφοριών, και την παραγωγή αναφορών, δίνοντας στους ελεγκτές πιο αποδοτικά εργαλεία για τη δημιουργία των εγγράφων τεκμηρίωσης και την υποβολή των αναγκαίων εκθέσεων.

Πώς η AI Βοηθάει στην Αυτοματοποιημένη Τεκμηρίωση και Παραγωγή Αναφορών:

1. **Αυτόματη Συλλογή Δεδομένων:** Η AI μπορεί να συλλέγει δεδομένα από πολλαπλές πηγές συστημάτων, εφαρμογών, και αρχεία καταγραφής (logs) του οργανισμού, διευκολύνοντας τη διαδικασία τεκμηρίωσης. Η αυτοματοποίηση της διαδικασίας εξαλείφει την ανάγκη για χειροκίνητη συλλογή δεδομένων και διασφαλίζει ότι όλα τα απαραίτητα δεδομένα έχουν ληφθεί και καταγραφεί.

2. **Οργάνωση και Κατηγοριοποίηση Δεδομένων:** Οι τεχνολογίες AI μπορούν να οργανώσουν αυτόματα τα δεδομένα, να τα κατηγοριοποιήσουν και να τα ευθυγραμμίσουν με τις σχετικές απαιτήσεις του audit. Αυτό περιλαμβάνει την κατάλληλη μορφοποίηση των δεδομένων και την αποθήκευση τους με τρόπο που να ανταποκρίνεται στις απαιτήσεις του ελέγχου.
3. **Δημιουργία Αυτοματοποιημένων Αναφορών:** Η AI δημιουργεί αναφορές βασισμένες στα δεδομένα που συλλέγονται, ακολουθώντας συγκεκριμένα πρότυπα που απαιτούνται από τα ρυθμιστικά πλαίσια ή τις εσωτερικές πολιτικές του οργανισμού. Οι αναφορές μπορεί να περιλαμβάνουν:
4. **Εκθέσεις συμμόρφωσης**: Παραγωγή λεπτομερών αναφορών σχετικά με τη συμμόρφωση του οργανισμού με πρότυπα όπως το GDPR, το PCI DSS, το ISO 27001 κ.λπ.
5. **Εκθέσεις διαχείρισης κινδύνων**: Τεκμηρίωση κινδύνων που εντοπίστηκαν κατά τη διάρκεια του audit και προτάσεις για βελτιώσεις.
6. **Εκθέσεις απόδοσης IT**: Παρακολούθηση της απόδοσης συστημάτων και υπηρεσιών και ανάλυση αποκλίσεων από τις προκαθορισμένες διαδικασίες.

Τεχνολογίες AI που Χρησιμοποιούνται:

1. **Natural Language Generation (NLG):** Η επεξεργασία φυσικής γλώσσας (NLG) επιτρέπει την αυτόματη δημιουργία κειμένων για αναφορές και τεκμηρίωση. Με τη βοήθεια των NLG αλγορίθμων, η AI μπορεί να παράγει κατανοητά και συνεκτικά κείμενα που μεταφράζουν δεδομένα σε εκθέσεις, αποφεύγοντας την ανάγκη για χειροκίνητη συγγραφή.
2. **Data Mining και Machine Learning:** Η AI χρησιμοποιεί τεχνικές data mining για την εξαγωγή πληροφοριών από τα δεδομένα και τη δημιουργία αναφορών με βάση μοτίβα, τάσεις, και αποκλίσεις. Η μηχανική μάθηση επιτρέπει στην AI να μαθαίνει από τις προηγούμενες αναφορές και να προσαρμόζει τις επόμενες με μεγαλύτερη ακρίβεια.
3. **Robotic Process Automation (RPA):** Οι RPA λύσεις βοηθούν στην αυτοματοποίηση των διαδικασιών συλλογής, ανάλυσης, και διανομής δεδομένων. Αυτές οι λύσεις συνεργάζονται με AI εργαλεία για να εξασφαλίσουν ότι όλες οι διαδικασίες ελέγχου εκτελούνται με ταχύτητα και ακρίβεια.

Παραδείγματα Εφαρμογών AI για Αυτοματοποιημένη Τεκμηρίωση και Αναφορές:

1. **TruNarrative:** Το TruNarrative προσφέρει δυνατότητες αυτοματοποίησης για την ανίχνευση κινδύνων και τη δημιουργία προσαρμοσμένων αναφορών. Με τη χρήση AI, η πλατφόρμα παράγει αναφορές συμμόρφωσης σε πραγματικό χρόνο με βάση τα δεδομένα που συλλέγονται από τα συστήματα του οργανισμού.
2. **Alteryx:** Το Alteryx προσφέρει λύσεις ανάλυσης δεδομένων που χρησιμοποιούν AI για την αυτοματοποίηση της δημιουργίας αναφορών, ειδικά για επιχειρησιακή ανάλυση και συμμόρφωση. Βοηθά τους auditors να μετατρέπουν ακατέργαστα δεδομένα σε τεκμηριωμένες αναφορές.

Ανάλυση Κινδύνου (Risk Assessment)

Η ανάλυση κινδύνου με τη χρήση της τεχνητής νοημοσύνης (AI) στο IT audit αποτελεί ένα ισχυρό εργαλείο για τον εντοπισμό, την αξιολόγηση και τη διαχείριση των κινδύνων που απειλούν τα πληροφοριακά συστήματα και τις υποδομές μιας επιχείρησης. Η AI ενισχύει την παραδοσιακή ανάλυση κινδύνου μέσω αυτοματοποιημένων διαδικασιών, βαθιάς ανάλυσης δεδομένων, και προηγμένων τεχνικών πρόβλεψης, καθιστώντας τις επιχειρήσεις πιο ανθεκτικές σε απειλές και πιο αποτελεσματικές στην πρόληψη παραβιάσεων ασφαλείας.

Πώς η AI Βελτιώνει την Ανάλυση Κινδύνου στο IT Audit:

1. **Διαχείριση Κινδύνων Κυβερνοασφάλειας:** Στον τομέα της κυβερνοασφάλειας, η AI μπορεί να αναλύσει επιθέσεις σε πραγματικό χρόνο και να προτείνει αυτόματα μέτρα για τη μείωση των κινδύνων. Επίσης, συμβάλλει στη δημιουργία μοντέλων που βοηθούν τους οργανισμούς να προβλέψουν τις πιο πιθανές μορφές κυβερνοεπιθέσεων.
2. **Αξιολόγηση και Ιεράρχηση Κινδύνων:** Η AI βοηθά στην αξιολόγηση της σοβαρότητας των κινδύνων και στην ιεράρχηση τους με βάση την πιθανότητα εμφάνισης και τον αντίκτυπό τους. Αυτό βοηθά τους IT auditors να εστιάσουν στους πιο σημαντικούς κινδύνους και να λάβουν πιο αποτελεσματικά μέτρα πρόληψης ή αντιμετώπισης.
3. **Προγνωστική Ανάλυση Κινδύνων:** Η AI επιτρέπει την εφαρμογή προγνωστικών μοντέλων για την ανάλυση ιστορικών δεδομένων και τον εντοπισμό πιθανών μελλοντικών κινδύνων. Με τη χρήση machine learning, τα συστήματα μπορούν να μάθουν από προηγούμενα περιστατικά κινδύνου και να προβλέψουν πού είναι πιθανότερο να εμφανιστούν μελλοντικές απειλές.

Τεχνολογίες και Μέθοδοι που Χρησιμοποιούνται:

1. **Machine Learning:** Η μηχανική μάθηση χρησιμοποιείται για την ανάλυση τεράστιων όγκων δεδομένων και την ανίχνευση μοτίβων κινδύνων που δεν είναι άμεσα εμφανή. Τα μοντέλα machine learning μπορούν να αυτοβελτιώνονται με την πάροδο του χρόνου, καθιστώντας τα πιο αποδοτικά στον εντοπισμό και την πρόβλεψη κινδύνων.
2. **Automated Risk Scoring:** Η AI μπορεί να αναλύσει τις πιθανότητες εμφάνισης ενός κινδύνου και να δώσει ένα "score" (βαθμολογία κινδύνου) για κάθε απειλή, βοηθώντας τους υπεύθυνους να λαμβάνουν αποφάσεις με βάση τα πιο κρίσιμα ζητήματα.

Παραδείγματα Εφαρμογών AI για Ανάλυση Κινδύνου στο IT Audit:

1. **LogicGate:** Η LogicGate προσφέρει λύσεις διαχείρισης κινδύνων που ενσωματώνουν AI για τον εντοπισμό και την ανάλυση κινδύνων. Οι χρήστες μπορούν να αυτοματοποιούν τη διαδικασία ανάλυσης κινδύνων και να διαχειρίζονται τις προτεραιότητες με βάση τα αποτελέσματα ανάλυσης.
2. **IBM Risk Analytics:** Η πλατφόρμα IBM Risk Analytics χρησιμοποιεί AI για την πρόβλεψη και την ανάλυση κινδύνων. Η τεχνολογία της επιτρέπει στους οργανισμούς να εκτιμούν τους

κινδύνους σε σχέση με τα κανονιστικά πλαίσια, τις απειλές κυβερνοασφάλειας και τις επιχειρησιακές λειτουργίες.

Αυτοματοποιημένος Έλεγχος Συμμόρφωσης (Compliance Auditing)

Ο Αυτοματοποιημένος Έλεγχος Συμμόρφωσης (Compliance Auditing) με τη χρήση της τεχνητής νοημοσύνης (AI) στο IT audit φέρνει επανάσταση στη διαδικασία ελέγχου, επιτρέποντας την ταχύτερη και πιο ακριβή ανάλυση των συστημάτων και διαδικασιών σε σχέση με κανονιστικά πλαίσια, πολιτικές ασφάλειας και πρότυπα συμμόρφωσης. Η αυτοματοποίηση εξαλείφει πολλές από τις χειροκίνητες εργασίες που απαιτούνται σε παραδοσιακούς ελέγχους και επιτρέπει στους οργανισμούς να διατηρούν τη συμμόρφωση σε συνεχή βάση.

Πώς η AI Ενισχύει τον Αυτοματοποιημένο Έλεγχο Συμμόρφωσης:

1. **Σύγκριση Δεδομένων με Πρότυπα Συμμόρφωσης:** Η AI συγκρίνει τα δεδομένα με τα πρότυπα συμμόρφωσης που εφαρμόζει ο οργανισμός (όπως GDPR, PCI DSS, HIPAA, ISO 27001 κ.λπ.). Ανιχνεύει παραβιάσεις και αποκλίσεις από τις απαιτούμενες διαδικασίες, δημιουργώντας αναφορές και ειδοποιήσεις για τυχόν προβλήματα.
2. **Εκτέλεση Συνεχών Ελέγχων:** Η AI μπορεί να εκτελεί ελέγχους συμμόρφωσης σε συνεχή βάση, επιτρέποντας τον διαρκή εντοπισμό και διόρθωση προβλημάτων πριν αυτά οδηγήσουν σε μεγαλύτερα ρίσκα. Αυτοί οι συνεχείς έλεγχοι βοηθούν τις επιχειρήσεις να διατηρούν τη συμμόρφωση χωρίς να περιμένουν την παραδοσιακή ετήσια ή περιοδική ελεγκτική διαδικασία.
3. **Αυτοματοποιημένη Παραγωγή Αναφορών Ελέγχου:** Η AI δημιουργεί αυτόματα αναφορές για τη συμμόρφωση, οι οποίες είναι πλήρως διαφανείς και μπορούν να παρασχεθούν στους ενδιαφερόμενους φορείς ή στις ρυθμιστικές αρχές. Αυτές οι αναφορές παρέχουν λεπτομερή δεδομένα για τα σημεία συμμόρφωσης και τις περιοχές όπου μπορεί να υπάρχουν αποκλίσεις.

Παραδείγματα εργαλείων για Αυτοματοποιημένο Έλεγχο:

1. **AuditBoard:** Το AuditBoard προσφέρει μια πλατφόρμα διαχείρισης κινδύνων και συμμόρφωσης που αξιοποιεί την AI για την αυτοματοποίηση των διαδικασιών ελέγχου συμμόρφωσης. Οι χρήστες μπορούν να δημιουργούν αυτόματα αναφορές και να παρακολουθούν συνεχώς την κατάσταση της συμμόρφωσης.
2. **Vanta:** Το Vanta χρησιμοποιείται για τον αυτοματοποιημένο έλεγχο συμμόρφωσης με πλαίσια όπως το SOC 2, το ISO 27001, και το GDPR. Η AI ελέγχει συνεχώς τις διαδικασίες και τα συστήματα IT και ενημερώνει για τυχόν αποκλίσεις.

3.3 Ανάλυση δεδομένων και λήψη αποφάσεων με AI.

Παραδοσιακά, η διαδικασία ελέγχου ήταν μια χειρωνακτική και χρονοβόρα διαδικασία που βασιζόταν σε μεγάλο βαθμό στην κρίση και την τεχνογνωσία του ελεγκτή. Ωστόσο, η τεχνολογία μεταμορφώνει τη διαδικασία ελέγχου εισάγοντας εργαλεία όπως η τεχνητή νοημοσύνη (AI) και η

ανάλυση δεδομένων που μπορούν να βελτιώσουν την ταχύτητα, την ακρίβεια και το εύρος των δραστηριοτήτων ελέγχου.

Ανάλυση δεδομένων:

1. **Αυτοματοποίηση διαδικασιών ανάλυσης**: Οι αλγόριθμοι μηχανικής μάθησης (machine learning) μπορούν να επεξεργαστούν τεράστιους όγκους δεδομένων πολύ πιο γρήγορα από τους παραδοσιακούς ελεγκτές, εντοπίζοντας ανωμαλίες, απάτες ή αποκλίσεις στα δεδομένα με μεγαλύτερη ακρίβεια.Πλατφόρμες όπως Hadoop, Spark, AWS, Azure και GCP επιτρέπουν την απορρόφηση και επεξεργασία μεγάλων όγκων δεδομένων με εργαλεία όπως το Spark και το AWS Glue, προσφέροντας ταχύτερη πρόσβαση σε καθαρά δεδομένα. Αυτές οι πλατφόρμες επιτρέπουν στους επαγγελματίες ελέγχου να έχουν πρόσβαση σε βασικά δεδομένα με ευκολία, μειώνοντας το χρόνο ελέγχου κατά 30% και βελτιώνοντας την ποιότητα των υπηρεσιών τους.

2. **Προγνωστική ανάλυση για τη διαχείριση κινδύνων :**Το Predictive Analytics, μια βασική πτυχή του ελέγχου, αξιοποιεί στατιστικά μοντέλα και αλγόριθμους για την πρόβλεψη μελλοντικών τάσεων και τον εντοπισμό πιθανών κινδύνων. Η χρήση πλατφορμών προγνωστικής ανάλυσης κινδύνων με AI μπορεί να ενισχύσει δραστικά την ποιότητα και την αποδοτικότητα του IT audit, προσφέροντας έγκαιρη πληροφόρηση και αναλύσεις που ενισχύουν την ασφάλεια και τη συμμόρφωση.

- Η πλατφόρμα Watson της IBM προσφέρει προηγμένες δυνατότητες ανάλυσης κινδύνων, χρησιμοποιώντας AI και machine learning για να αναλύει μεγάλα σύνολα δεδομένων και να εντοπίζει πιθανούς κινδύνους στον τομέα του IT. Η Watson μπορεί να ενσωματωθεί σε IT audit διαδικασίες για προγνωστική ανάλυση και ανίχνευση απειλών.
- Η πλατφόρμα Google Cloud προσφέρει προγνωστικά εργαλεία βασισμένα σε AI μέσω του BigQuery και των machine learning μοντέλων της. Αυτή η πλατφόρμα μπορεί να αξιοποιηθεί για IT audit μέσω ανάλυσης μεγάλων δεδομένων και προβλεπτικών μοντέλων που βοηθούν στον εντοπισμό και στην πρόληψη κινδύνων.

3. **Ανάλυση ιστορικών δεδομένων:**Τα ιστορικά δεδομένα παρέχουν πληροφορίες σχετικά με προηγούμενα γεγονότα, τάσεις, και ανωμαλίες, τα οποία μπορούν να χρησιμοποιηθούν για την αναγνώριση μοτίβων και την πρόβλεψη μελλοντικών κινδύνων.

- Αναγνώριση μοτίβων και ανωμαλιών: Η AI μπορεί να αναλύσει μεγάλα σύνολα ιστορικών δεδομένων για την αναγνώριση μοτίβων κανονικής συμπεριφοράς και να εντοπίσει ανωμαλίες που θα μπορούσαν να υποδηλώνουν σφάλματα, απάτες ή κινδύνους ασφάλειας. Για παράδειγμα, αν σε παλαιότερους ελέγχους υπήρχαν συγκεκριμένες επαναλαμβανόμενες παραβιάσεις, η AI μπορεί να προβλέψει την πιθανότητα εμφάνισης παρόμοιων προβλημάτων στο μέλλον.

4. **Ανάλυση συμπεριφοράς χρηστών:** Χρησιμοποιώντας ιστορικά δεδομένα σχετικά με τη συμπεριφορά των χρηστών, όπως η πρόσβαση σε συστήματα, η αλλαγή ρυθμίσεων ή η χρήση δεδομένων, η AI μπορεί να αναγνωρίσει ύποπτες ή μη φυσιολογικές συμπεριφορές που ενδέχεται να υποδεικνύουν απειλές ασφαλείας. Αυτή η τεχνική επιτρέπει τον εντοπισμό και την πρόληψη παραβιάσεων προτού προκαλέσουν σημαντικά προβλήματα.

Οι ελεγκτές μπορούν να χρησιμοποιήσουν την τεχνητή νοημοσύνη για να παράγουν πληροφορίες και απεικονίσεις βάσει δεδομένων για την αναφορά της επιτροπής ελέγχου και του συμβουλίου. Η τεχνητή νοημοσύνη μπορεί να δημιουργήσει αναφορές και απεικονίσεις που παρουσιάζουν σύνθετες πληροφορίες, επιτρέποντας στους ελεγκτές να κοινοποιούν τα ευρήματα και τις συστάσεις πιο αποτελεσματικά στους ενδιαφερόμενους. Μια μελλοντική κατάσταση για την αναφορά της επιτροπής ελέγχου θα μπορούσε να χρησιμοποιήσει την τεχνητή νοημοσύνη για την ανάπτυξη προγνωστικών μοντέλων που εκτιμούν την πιθανότητα μελλοντικών κινδύνων με βάση τα τρέχοντα αποτελέσματα, διευκολύνοντας βαθύτερες συζητήσεις μεταξύ των ηγετών ελέγχου και της επιτροπής ελέγχου.

Παράδειγμα Αυτοματοποιημένης Τεκμηρίωσης και Αναφοράς μέσω AI:

Σενάριο: Έλεγχος Ασφαλείας Εφαρμογής

1. **Συλλογή Δεδομένων**: Το σύστημα AI συνδέεται με τα αρχεία καταγραφής των servers, την εφαρμογή και τη βάση δεδομένων.
2. **Ανάλυση Δεδομένων**: Η AI ελέγχει αν οι χρήστες που έχουν πρόσβαση στην εφαρμογή πληρούν τα κριτήρια ασφαλείας, αν υπάρχουν απρόβλεπτες μεταβολές στον αριθμό των χρηστών που συνδέονται ταυτόχρονα ή αν εντοπίζονται πιθανές επιθέσεις (π.χ. SQL injection).
3. **Αυτοματοποιημένη Ανίχνευση Ανωμαλιών**: Η AI ανιχνεύει ότι η εφαρμογή έχει μια ασυνήθιστη αύξηση σε αριθμό login από μία συγκεκριμένη IP, κάτι που μπορεί να υποδεικνύει απόπειρα επίθεσης.
4. **Δημιουργία Αναφοράς**: Το σύστημα αυτοματοποιημένα δημιουργεί αναφορά που περιγράφει τη δραστηριότητα, την ανωμαλία και την πιθανή αιτία της απειλής, και προσφέρει προτάσεις για τη βελτίωση της ασφάλειας.
5. **Ειδοποίηση Υπεύθυνου Ασφαλείας**: Η αναφορά αποστέλλεται αυτόματα στον υπεύθυνο ασφαλείας, ο οποίος μπορεί να λάβει άμεσα μέτρα.

3.4 Οφέλη της Λήψης Αποφάσεων με AI

Τα ολοκληρωμένα πλεονεκτήματα της Υποβοηθούμενης Λήψης Αποφάσεων περιλαμβάνουν:

1. **Προσδιορισμός κινδύνου βάσει δεδομένων:** Ένα από τα βασικά χαρακτηριστικά είναι η ικανότητά περιήγησης σε τεράστιες ποσότητες δεδομένων με αστραπιαία ταχύτητα. Χρησιμοποιώντας προηγμένους αλγόριθμους,αναλύονται οικονομικές καταστάσεις, αρχεία συναλλαγών και άλλες σχετικές πηγές δεδομένων για να εντοπιστούν πρότυπα, ανωμαλίες και πιθανοί κινδυνοι. Αυτή η προσέγγιση βάσει δεδομένων διασφαλίζει μια ολοκληρωμένη και ακριβή εκτίμηση κινδύνου, εξοικονομώντας πολύτιμο χρόνο στους ελεγκτές.

2. **Απρόσκοπτη ενσωμάτωση σε υπάρχουσες ροές εργασίας:** Μία από τις ανησυχίες κατά την υιοθέτηση νέας τεχνολογίας σε οποιονδήποτε κλάδο είναι η πιθανή διακοπή των καθιερωμένων ροών εργασίας.Η Thomson Reuters κατάλαβε αυτήν την πρόκληση και ανέπτυξε τη σουίτα ελέγχου Cloud με έμφαση στην απρόσκοπτη ενοποίηση.Η λειτουργία Υποβοηθούμενης λήψης αποφάσεων λειτουργεί παράλληλα με τις υπάρχουσες διαδικασίες της εταιρείας,παρέχοντας πληροφορίες σε πραγματικό χρόνο χωρίς να απαιτείται πλήρης αναθεώρηση της ροής εργασιών σας.
3. **Σημαντικές πληροφορίες από την ελεγκτική κοινότητα:** Η Υποβοηθούμενη Λήψη Αποφάσεων χρησιμοποιεί τεχνητή νοημοσύνη για τον εντοπισμό κινδύνων που σχετίζονται με τη δέσμευσή σας και δείχνει προληπτικά κινδύνους που εντοπίζονται από άλλους ελεγκτές. Αυτά τα δεδομένα είναι ανώνυμα για την κατάργηση των ονομάτων εταιρειών και πελατών. Βλέποντας τι έχουν κάνει άλλοι ελεγκτές σε παρόμοια κατάσταση, η ομάδα ελέγχου σας μπορεί να αισθάνεται σίγουρη ότι έχετε λάβει υπόψη όλους τους κινδύνους κατά την ολοκλήρωση του ελέγχου σας.

<u>Βασικά ζητήματα για την ενσωμάτωση των αναλύσεων δεδομένων βάσει τεχνητής νοημοσύνης στους ελέγχους</u>

Αν και οι αναλύσεις δεδομένων που βασίζονται στην τεχνητή νοημοσύνη μπορούν να επιταχύνουν τις διαδικασίες ελέγχου, ενδέχεται να συνοδεύονται από ορισμένα σημεία συμφόρησης που πρέπει να αντιμετωπιστούν έξυπνα από τους ελεγκτές. Μερικά από τα πράγματα που πρέπει να έχετε κατά νου είναι:

1. Διασφάλιση του απορρήτου των δεδομένων πελάτη:

Η πρακτική του ελέγχου βασίζεται κατά κύριο λόγο στην εμπιστοσύνη. Το πιο σημαντικό πράγμα που πρέπει να λάβουν υπόψη οι ελεγκτές κατά την εφαρμογή της τεχνητής νοημοσύνης είναι το απόρρητο των δεδομένων πελατών. Μια πλατφόρμα ελέγχου με τεχνητή νοημοσύνη απαιτεί συνεχώς πολλά δεδομένα καλής ποιότητας για να αυτομάθη και να οδηγήσει σε έξυπνη λήψη αποφάσεων σε παρόμοια σενάρια στο μέλλον. Η Πλατφόρμα, επομένως, απαιτεί πρόσβαση στα εμπιστευτικά δεδομένα του πελάτη, τα οποία ενδέχεται να μην παρέχονται εύκολα από τους πελάτες, εάν δεν υπάρχει ασφαλής πρακτική για την προστασία των δεδομένων. Επομένως, για τη σωστή διαχείριση των δεδομένων πελατών και την προστασία τους από παραβιάσεις δεδομένων, οι ελεγκτές πρέπει να λαμβάνουν προληπτικά μέτρα ασφαλείας. Η εφαρμογή μιας ισχυρής διαδικασίας ανωνυμοποίησης δεδομένων για την ανωνυμοποίηση PII πελάτη (Προσωπικά αναγνωρίσιμα στοιχεία) πριν από την απορρόφηση δεδομένων μπορεί να βοηθήσει στην εξάλειψη αυτής της ανησυχίας. Αυτή η διαδικασία συμμορφώνεται με το απόρρητο του πελάτη, καθώς δεν υπάρχει ανησυχία σχετικά με το ότι το μοντέλο τεχνητής νοημοσύνης απορροφά πληροφορίες PII πελάτη και προκαλεί παραβίαση της εμπιστοσύνης.

2. Επιβεβαίωση της αξιοπιστίας των δεδομένων εκπαίδευσης:

Το γεγονός ότι η τεχνητή νοημοσύνη εκπαιδεύεται σε σύνολα δεδομένων για να λειτουργεί σωστά εγείρει μια άλλη ανησυχία. Τι θα συνέβαινε εάν τα σύνολα δεδομένων δεν είναι ακριβή και αξιόπιστα; Η τεχνητή νοημοσύνη ενδέχεται να μην παράγει τα επιδιωκόμενα αποτελέσματα και να παρέχει ανακριβείς προβλέψεις εάν τα δεδομένα εκπαίδευσης δεν είναι καλής ποιότητας. Οι ελεγκτές πρέπει να λάβουν προληπτικά μέτρα - **επικύρωση δεδομένων εισόδου, διατήρηση διαδρομής ελέγχου κ.λπ.** - για να διασφαλίσουν ότι τα δεδομένα που συλλέγονται από συστήματα πελατών είναι αξιόπιστα και ακριβή. Διαφορετικά, η τεχνητή νοημοσύνη θα γίνει δυσλειτουργική.

3. Παροχή επεξηγήσεων για αποτελέσματα τεχνητής νοημοσύνης:

Το AI μπορεί να προσφέρει ακριβείς προβλέψεις και επιθυμητά αποτελέσματα. Ωστόσο, οι ελεγκτές πρέπει να αναπτύξουν τις απαιτούμενες διαδικασίες για την παρακολούθηση του εργαλείου ελέγχου τεχνητής νοημοσύνης τους, για να εξηγήσουν γιατί το εργαλείο έχει αναγνωρίσει ορισμένες συναλλαγές ως «ανώμαλες» και «ασυνήθιστες» και να αιτιολογήσει τα αποτελέσματα της τεχνητής νοημοσύνης. Αλλά αυτό που αποτελεί πρόκληση εδώ είναι ότι η τεχνητή νοημοσύνη μπορεί να είχε πάρει έναν συνδυασμό παραγόντων για να καταλήξει στα αντίστοιχα συμπεράσματα, και αυτό μπορεί να είναι αρκετά περίπλοκο. Αν και η τεχνητή νοημοσύνη παρέχει ακριβή αποτελέσματα, οι ελεγκτές θα πρέπει να εφαρμόσουν την επαγγελματική τους κρίση για να επικυρώσουν αυτά τα συμπεράσματα. Και αυτό απαιτεί από τους ελεγκτές να επεκτείνουν την τεχνογνωσία τους πέρα από τον έλεγχο και τη λογιστική και να εξοικειωθούν με την ανάλυση δεδομένων, την πληροφορική και πολλά άλλα. **[13]**

Είναι απαραίτητο να αντιληφθούμε αυτές τις λύσεις ως επιταχυντές και όχι ως υποκατάστατο των ελεγκτών. Οι έλεγχοι που βασίζονται σε τεχνητή νοημοσύνη απαιτούν λίγη ανθρώπινη παρέμβαση γύρω από επαναλαμβανόμενες και βασισμένες σε κανόνες εργασίες και επιτρέπουν στους ελεγκτές να εστιάζουν περισσότερο σε συναλλαγές υψηλού κινδύνου. Αυτό καθιστά ολόκληρη τη διαδικασία ελέγχου αποτελεσματική, μειώνοντας τον φόρτο εργασίας των ελεγκτών, το λειτουργικό κόστος και την επικοινωνία μεταξύ των πελατών.

3.5 Πλαίσια όπου χρησιμοποιείται η A.I. στο Audit

Ενώ πολλά πλαίσια ελέγχου τεχνητής νοημοσύνης έχουν αναπτυχθεί για να βοηθήσουν τους οργανισμούς να πλοηγηθούν στην πολυπλοκότητα των συστημάτων τεχνητής νοημοσύνης, εξακολουθούν να υπάρχουν προκλήσεις λόγω της σχετικής ανωριμότητας αυτών των πλαισίων και του γρήγορου ρυθμού προόδου της τεχνητής νοημοσύνης. Τα διαθέσιμα πλαίσια, όπως αυτά του Ινστιτούτου Εσωτερικών Ελεγκτών (IIA), του Εθνικού Ινστιτούτου Προτύπων και Τεχνολογίας (NIST) και του Γραφείου του Επιτρόπου Πληροφοριών (ICO), παρέχουν πολύτιμη καθοδήγηση, αλλά εξακολουθούν να εξελίσσονται για να συμβαδίζουν με νέες εξελίξεις και κινδύνους στην τεχνητή νοημοσύνη. Ακολουθούν ορισμένα αξιοσημείωτα πλαίσια ελέγχου AI:

1. Το Πλαίσιο Ελέγχου AI της IIA

Το Ινστιτούτο Εσωτερικών Ελεγκτών (IIA) έχει αναπτύξει ένα ολοκληρωμένο πλαίσιο ελέγχου τεχνητής νοημοσύνης για να βοηθήσει τους οργανισμούς να κατανοήσουν τους κινδύνους και να εφαρμόσουν βέλτιστες πρακτικές για συστήματα τεχνητής νοημοσύνης. Περιλαμβάνει τρία βασικά

στοιχεία—Στρατηγική AI, Διακυβέρνηση και Ανθρώπινος Παράγοντας—και επτά στοιχεία: Ανθεκτικότητα στον κυβερνοχώρο, Ικανότητες τεχνητής νοημοσύνης, ηθική τεχνητή νοημοσύνη, διαχείριση κινδύνου, κανονιστική συμμόρφωση, διαφάνεια και υπευθυνότητα. Αυτό το πλαίσιο διασφαλίζει ότι τα συστήματα τεχνητής νοημοσύνης ευθυγραμμίζονται με τους οργανωτικούς στόχους, διαχειρίζονται δεοντολογικά και συμμορφώνονται με τους κανονισμούς.

2. Πλαίσιο Διαχείρισης Κινδύνων NIST AI

Το NIST δημοσίευσε το Πλαίσιο Διαχείρισης Κινδύνων AI για τη διαχείριση κινδύνων που σχετίζονται με συστήματα τεχνητής νοημοσύνης. Επικεντρώνεται στη χαρτογράφηση των κινδύνων της τεχνητής νοημοσύνης, στη μέτρηση του αντικτύπου τους, στην αποτελεσματική διαχείρισή τους και στη συνεχή παρακολούθηση των στρατηγικών διαχείρισης κινδύνου. Αυτό το πλαίσιο είναι ζωτικής σημασίας για την ενίσχυση της εμπιστοσύνης στις τεχνολογίες τεχνητής νοημοσύνης και για τη διασφάλιση της υπεύθυνης ανάπτυξής τους.

3. Πλαίσιο ελέγχου AI της ICO

Το Γραφείο του Επιτρόπου Πληροφοριών (ICO) στο Ηνωμένο Βασίλειο προσφέρει ένα λεπτομερές πλαίσιο ελέγχου τεχνητής νοημοσύνης με επίκεντρο τη συμμόρφωση με την προστασία δεδομένων. Δίνει έμφαση στη διακυβέρνηση, τη νομιμότητα, τη δικαιοσύνη, τη διαφάνεια, την ελαχιστοποίηση των δεδομένων, την ακρίβεια, την ασφάλεια και τον σεβασμό των ατομικών δικαιωμάτων. Αυτό το πλαίσιο είναι απαραίτητο για τους οργανισμούς να διασφαλίζουν ότι τα συστήματα τεχνητής νοημοσύνης τους τηρούν τα πρότυπα απορρήτου και δεοντολογίας.

4. Πλαίσιο COBIT

Το πλαίσιο COBIT , που παρέχεται από την ISACA, προσφέρει μια δομημένη προσέγγιση για τη διακυβέρνηση και τη διαχείριση εταιρικών IT, συμπεριλαμβανομένων των συστημάτων τεχνητής νοημοσύνης. Επικεντρώνεται στην ευθυγράμμιση των στρατηγικών πληροφορικής με τους επιχειρηματικούς στόχους, στην παροχή αξίας από επενδύσεις πληροφορικής, στη βελτιστοποίηση της χρήσης πόρων, στη διαχείριση των κινδύνων και στη μέτρηση της απόδοσης. Αυτό το ολοκληρωμένο πλαίσιο βοηθά τους οργανισμούς να δημιουργήσουν αξία διατηρώντας παράλληλα ισχυρή διακυβέρνηση και έλεγχο στις τεχνολογίες τεχνητής νοημοσύνης. **[20]**

3.6 Case Studies όπου χρησημοποιείται AI στο IT Audit

1. Case Study: Baker Tilly

Η **Baker Tilly** έχει εφαρμόσει την τεχνητή νοημοσύνη σε διάφορους τομείς, συμπεριλαμβανομένων των IT audit, για να ενισχύσει τη λήψη αποφάσεων βάσει δεδομένων και την επιχειρησιακή αποδοτικότητα. Ένα αξιοσημείωτο παράδειγμα αφορά τη χρήση προηγμένων εργαλείων ανάλυσης δεδομένων, όπως το **Microsoft Power BI**, το **Tableau** και το **Qlik**, για να βοηθήσουν τους πελάτες να κατανοήσουν καλύτερα τα δεδομένα τους και να τα ευθυγραμμίσουν με τους επιχειρηματικούς τους στόχους. Για παράδειγμα, η **Baker Tilly** ενσωμάτωσε την τεχνητή νοημοσύνη στη διαδικασία του ελέγχου για να βελτιώσει τη διαφάνεια και να επιτρέψει την ανάλυση σε πραγματικό χρόνο,

δίνοντας τη δυνατότητα στις εταιρείες να προβλέπουν τους κινδύνους πιο αποτελεσματικά και να βελτιστοποιούν τις λειτουργίες τους.

Ένα παράδειγμα είναι η χρήση προγνωστικής ανάλυσης για IT audits, όπου η Baker Tilly βοήθησε εταιρείες να εντοπίσουν αναδυόμενους κινδύνους αναλύοντας ιστορικά δεδομένα και IT συστήματα. Αυτή η προσέγγιση επέτρεψε στις επιχειρήσεις να μετριάσουν τους πιθανούς IT κινδύνους και να βελτιώσουν τη συμμόρφωση με κανονιστικά πρότυπα.

Επιπλέον, η εξαγορά της Talavant, μιας εταιρείας ανάλυσης δεδομένων από την **Baker Tilly**, ενίσχυσε περαιτέρω τις δυνατότητες AI τους στα IT audits, επιτρέποντας να προσφέρουν πιο εξατομικευμένες και προληπτικές λύσεις στους πελάτες, ιδιαίτερα σε κλάδους που βασίζονται σε δεδομένα σε πραγματικό χρόνο.

2. Case Study: KPGM Ignite

Ένα χαρακτηριστικό παράδειγμα χρήσης AI από την KPMG είναι η πλατφόρμα **KPMG Ignite**, που εφαρμόζεται σε διαδικασίες IT audit και ελέγχους οικονομικών καταστάσεων. Η πλατφόρμα αυτή χρησιμοποιεί τεχνητή νοημοσύνη για την ανάλυση μεγάλων όγκων δεδομένων, την αυτοματοποίηση χειρωνακτικών διαδικασιών, και την ανίχνευση ανωμαλιών σε πραγματικό χρόνο.

Σε ένα παράδειγμα χρήσης, η KPMG συνεργάστηκε με έναν διεθνή χρηματοοικονομικό οργανισμό για να ενσωματώσει AI στις διαδικασίες ελέγχου τους. Η πλατφόρμα χρησιμοποίησε AI για να αναλύσει μεγάλες ποσότητες δεδομένων συναλλαγών και να εντοπίσει ανωμαλίες ή ενδεχόμενα σημάδια απάτης. Ο οργανισμός είχε προηγουμένως δυσκολία να διαχειριστεί τον όγκο των δεδομένων, καθώς χρησιμοποιούσε χειρωνακτικές μεθόδους για τη διεξαγωγή του ελέγχου.

Αποτέλεσμα:

Η εφαρμογή του AI στην ανάλυση των δεδομένων μείωσε τον χρόνο που απαιτείται για τους ελέγχους κατά 30%, αυξάνοντας παράλληλα την ακρίβεια στην ανίχνευση πιθανών κινδύνων και την ικανότητα να προβλέπουν μελλοντικά περιστατικά απάτης. Οι ελεγκτές μπορούσαν να επικεντρωθούν σε πιο κρίσιμα ζητήματα, αφήνοντας τις αυτοματοποιημένες διαδικασίες AI να χειρίζονται τα μεγαλύτερα σε όγκο δεδομένα και τις βασικές αναλύσεις(KPMG).

Αυτό το παράδειγμα δείχνει πώς η KPMG εκμεταλλεύεται την τεχνητή νοημοσύνη για τη βελτίωση της αποδοτικότητας και της ακρίβειας των ελέγχων σε μεγάλες επιχειρήσεις, προσφέροντας γρηγορότερα και πιο ακριβή αποτελέσματα στις διαδικασίες IT audit.

****Για λόγους εμπιστευτικότητας και τήρησης νομοθετικών πλαισίων(GDPR στην Ε.Ε) ,οι δυο παραπάνω συμβουλευτικές-ελεγκτικές εταιρείες απέφυγαν να αναφέρουν τα ονόματα των πελατών τους.**

3. Case Study: Yapi Kredi

Η αυτοματοποίηση με τεχνολογία AI έχει επιτρέψει στη **Yapi Kredi**, μια τουρκική τράπεζα, να συμμορφώνεται καλύτερα με συγκεκριμένους κανονισμούς, ειδικά στην εκτέλεση ελέγχων, στη διεξαγωγή συμφωνιών, στην έκδοση προειδοποιήσεων και στον εντοπισμό ύποπτων συναλλαγών.

Η Yapı Kredi έχει πλέον αρχίσει να ενσωματώνει την τεχνητή νοημοσύνη στις αυτοματοποιήσεις διακυβέρνησης, κινδύνου και συμμόρφωσης (**GRC**). Για παράδειγμα, στη διαδικασία ελέγχου, η τράπεζα έχει εφαρμόσει AI, κατανόηση εγγράφων και επεξεργασία εικόνας, όχι μόνο για να αυτοματοποιήσει διάφορες διαδικασίες, αλλά και για να χρησιμοποιήσει τις αυτοματοποιήσεις ως «έξυπνους βοηθούς» για τους ελεγκτές, επιτρέποντάς τους να επικεντρωθούν σε πιο ουσιαστικές δραστηριότητες.

Η διαδικασία ελέγχου λειτουργεί τώρα ως εξής: το ρομπότ συλλέγει τα σχετικά έγγραφα και τις πληροφορίες, τα οποία στη συνέχεια ελέγχονται μέσω αλγορίθμου AI για υπογραφές και άλλους ελέγχους. Τυχόν εξαιρέσεις επισημαίνονται πρώτα από το ρομπότ και έπειτα ελέγχονται από έναν ανθρώπινο ελεγκτή. Αυτό έχει επιστρέψει σημαντικό χρόνο στους ελεγκτές, οι οποίοι τώρα ασχολούνται λιγότερο με επαναλαμβανόμενες και λειτουργικές εργασίες. **[23]**

4.Πλεονεκτήματα και προκλήσεις

4.1 Πλεονεκτήματα της AI στο IT audit

Στο σημερινό ταχέως εξελισσόμενο επιχειρηματικό τοπίο, η τεχνολογία διαμορφώνει όλο και περισσότερο το τοπίο του ελέγχου, οδηγώντας σε σημαντικές διακοπές και ευκαιρίες. Καθώς οι επιχειρήσεις δημιουργούν μεγαλύτερα και πιο σύνθετα σύνολα δεδομένων, οι παραδοσιακές προσεγγίσεις ελέγχου γίνονται γρήγορα ξεπερασμένες. Η ενσωμάτωση της τεχνητής νοημοσύνης (AI) μεταμορφώνει τις πρακτικές ελέγχου, βελτιώνει την αποτελεσματικότητα και ενισχύει την ακρίβεια.Στο άρθρο «**How AI is Transforming the Audit Process in Europe>> του** δρ.Anton Todorov διερευνάτε η ενσωμάτωση της τεχνητής νοημοσύνης στις μεθόδους ελέγχου και τον αντίκτυπο στην αποτελεσματικότητα και την ακρίβεια.

Βελτιωμένη αποτελεσματικότητα και ακρίβεια:Ένα από τα πιο σημαντικά οφέλη της τεχνητής νοημοσύνης στον έλεγχο είναι η βελτίωση της αποτελεσματικότητας και της ακρίβειας. Οι αλγόριθμοι μηχανικής μάθησης και άλλα εργαλεία που τροφοδοτούνται με AI μπορούν να εκτελούν εργασίες ρουτίνας με μεγάλη ταχύτητα και ακρίβεια, μειώνοντας τον χρόνο και την προσπάθεια που απαιτείται για την ολοκλήρωση των ελέγχων. Αυτό επιτρέπει στους ελεγκτές να εστιάζουν σε πιο υψηλής αξίας καθήκοντα, όπως η αξιολόγηση κινδύνου και η στρατηγική ανάλυση, οδηγώντας σε βελτιωμένη ποιότητα ελέγχου. Με τη δυνατότητα ανάλυσης μεγάλων συνόλων δεδομένων, η τεχνητή νοημοσύνη μπορεί να βρει κρυφές τάσεις και ανωμαλίες, οδηγώντας σε καλύτερες πληροφορίες.

Βελτιωμένη αξιολόγηση κινδύνου:Η ικανότητα του AI να αναλύει μεγάλες ποσότητες δεδομένων γρήγορα και με ακρίβεια έχει σημαντικά οφέλη για τις διαδικασίες αξιολόγησης κινδύνου. Οι αλγόριθμοι τεχνητής νοημοσύνης μπορούν να επεξεργάζονται δεδομένα από πολλαπλές πηγές, παρέχοντας στους ελεγκτές μια ολοκληρωμένη εικόνα των λειτουργιών, των κινδύνων και του περιβάλλοντος ελέγχου ενός οργανισμού. Αυτό επιτρέπει στους ελεγκτές να εντοπίζουν πιθανούς κινδύνους και να ελέγχουν τις αδυναμίες, οδηγώντας σε καλύτερα ενημερωμένες ελεγκτικές γνώμες.

Βελτιστοποίηση δειγματοληψίας ελέγχου:Παραδοσιακά, οι ελεγκτές χρησιμοποιούν μια δειγματοληπτική προσέγγιση κατά τη διεξαγωγή ελέγχων, επιλέγοντας ένα κλάσμα συναλλαγών και υποθέτοντας ότι είναι αντιπροσωπευτικοί ολόκληρου του πληθυσμού. Ωστόσο, τα εργαλεία ανάλυσης δεδομένων με δυνατότητα AI μπορούν πλέον να επεξεργάζονται ολόκληρα σύνολα δεδομένων, οδηγώντας σε πιο ολοκληρωμένη και ακριβή κάλυψη ελέγχου. Αυτό επιτρέπει στους ελεγκτές να εντοπίζουν τυχόν ανωμαλίες ή πιθανά σφάλματα προτού γίνουν σημαντικά ζητήματα και να παρέχουν συστάσεις για βελτίωση.

Βελτιωμένη ανίχνευση απάτης:Οι διαδικασίες ελέγχου έχουν σχεδιαστεί για να εντοπίζουν δόλιες δραστηριότητες που μπορούν να επηρεάσουν σημαντικά την οικονομική απόδοση και τη φήμη των οργανισμών. Τα εργαλεία που υποστηρίζονται από AI μπορούν να εντοπίσουν ύποπτες συναλλαγές μέσω προηγμένης αναγνώρισης προτύπων, μηχανικής μάθησης και άλλων αλγορίθμων, οδηγώντας σε πιο αποτελεσματικό εντοπισμό απάτης. Η τεχνητή νοημοσύνη μπορεί να ανιχνεύσει ανωμαλίες

που μπορεί να είναι δύσκολο να αναγνωρίσουν οι άνθρωποι, χρησιμοποιώντας επεξεργασία φυσικής γλώσσας για τον εντοπισμό ασυνήθιστων μοτίβων στις ηλεκτρονικές επικοινωνίες, όπως τα email.

Βελτιωμένη Επικοινωνία και Συνεργασία:Η ενσωμάτωση της τεχνητής νοημοσύνης στις ελεγκτικές διαδικασίες μπορεί να οδηγήσει σε ενισχυμένη συνεργασία και επικοινωνία μεταξύ ελεγκτών, ρυθμιστικών αρχών και επιχειρήσεων. Η χρήση ψηφιακών εργαλείων επιτρέπει στους ελεγκτές να επικοινωνούν σε πραγματικό χρόνο, να μοιράζονται δεδομένα απρόσκοπτα και να παρακολουθούν την πρόοδο του ελέγχου. Η βελτιωμένη συνεργασία μπορεί να οδηγήσει σε πιο αποτελεσματικούς και αποτελεσματικούς ελέγχους, βελτιώνοντας τη συνολική ποιότητα του ελέγχου. **[21]**

Τα οφέλη της τεχνητής νοημοσύνης στον έλεγχο είναι ξεκάθαρα. Από τη βελτίωση της ακρίβειας και της αποτελεσματικότητας μέχρι τον εντοπισμό κινδύνων και τη δημιουργία πληροφοριών, η τεχνητή νοημοσύνη φέρνει επανάσταση στον κλάδο των ελεγκτών.

Καθώς η τεχνολογία AI συνεχίζει να εξελίσσεται, ο αντίκτυπός της στον έλεγχο είναι πιθανό να αυξηθεί, καθιστώντας την ένα ουσιαστικό εργαλείο για τους ελεγκτές.

Αποτελέσματα ερωτηματολογίου της **DatasSnipper:**

Η εταιρεία **DatasSnipper,** η οποία έχει κατασκευάσει την ομώνυμη πλατφόρμα-εργαλείο για να υποστηρίζει τις διαδικασίες ελέγχου και λογιστικής,εστιάζοντας στην αυτοματοποίηση,εξέθεσε τα αποτελέσματα του ερωτηματολόγιου <<AI Report 2024-The AI Revolution in Audit and Finance>> το οποίο διερευνά πως η τεχνητή νοημοσύνη μεταμορφώνει τον κλάδο ελέγχου,ενισχύοντας τις ροές εργασίας και την παραγωγικότητα. **[22]**

Η έρευνά συγκέντρωσε πάνω από 150 απαντήσεις από ένα ευρύ φάσμα φάσμα επαγγελματιών ελέγχου και χρηματοοικονομικών. Όσον αφορά τα επίπεδα εμπειρίας η έρευνα περιελάμβανε 27% Ατομικά Συνεισφέροντες, 23% Manager, 25% Διευθυντές και 25% Συνεργάτες-Στελέχη.

Figure 6- Κατανομή των συμμετεχόντων στην έρευνα ανά επαγγελματικό επίπεδο: 27% μεμονωμένοι συνεργάτες, 23% διευθυντές τμημάτων, 25% ανώτερα διευθυντικά στελέχη και 25% ανώτατα στελέχη/εταίροι.

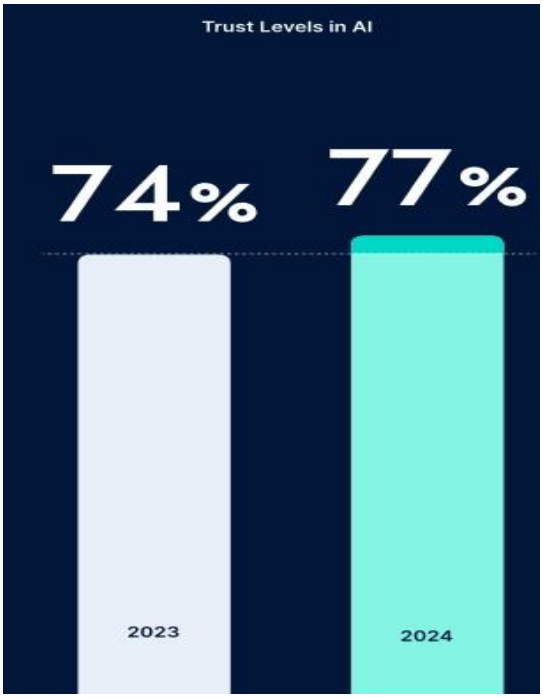


Figure 7- Επίπεδα εμπιστοσύνης στην τεχνητή νοημοσύνη: αύξηση από 74% το 2023 σε 77% το 2024.

Συγκριτικά αποτελέσματα 2023 -2024

AI: Φίλος ή εχθρός;

Η εμπιστοσύνη στην τεχνητή νοημοσύνη είναι απαραίτητη για την υιοθέτησή της.Η έρευνα διαπίστωσε ότι η εμπιστοσύνη των ελεγκτών απέναντι της,ως αξιόπιστο εργαλείο,αυξήθηκε κατά 3 μονάδες ,φτάνοντας στο 77%,σχεδόν δηλαδή οι 112 από τους 150 συμμετέχοντες. Η εμπιστοσύνη είναι ζωτικής σημασίας για τη συνεχή ενσωμάτωση των τεχνολογιών τεχνητής νοημοσύνης.

"Η τεχνητή νοημοσύνη έχει πραγματικά κερδίσει την εμπιστοσύνη μας. Έχει ενισχύσει την ακρίβεια στη δουλειά μας σε μεγάλο βαθμό. Είναι σαν να έχουμε έναν επιπλέον συνεργάτη στον οποίο μπορούμε πάντα να υπολογίζουμε," είπε ένας συμμετέχων.

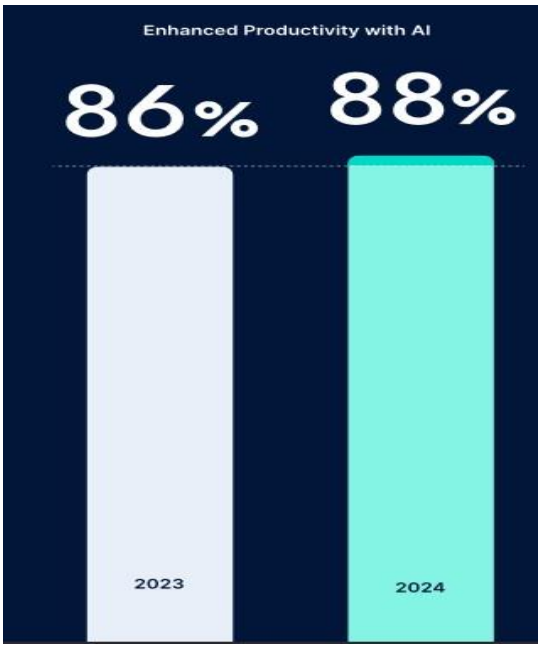


Figure 8- Αύξηση της παραγωγικότητας με τη χρήση τεχνητής νοημοσύνης: από 86% το 2023 σε 88% το 2024

Η τεχνητή νοημοσύνη επαναστατεί τον τρόπο που οι ελεγκτές διαχειρίζονται τα καθήκοντά τους, ειδικά τα επαναλαμβανόμενα και χειροκίνητα. Ένα εντυπωσιακό 88% των συμμετεχόντων δηλώνει ότι η τεχνητή νοημοσύνη βοηθά στη μείωση του χρόνου που δαπανάται σε αυτές τις εργασίες, επιτρέποντάς τους να επικεντρωθούν σε πιο πολύπλοκες και ενδιαφέρουσες δραστηριότητες. Αυτό είναι μια ελαφρά αύξηση από το 86% στην έρευνα της περασμένης χρονιάς. Τα οφέλη της αποδοτικότητας είναι προφανή, με την τεχνητή νοημοσύνη να επιτρέπει ταχύτερη ανάλυση δεδομένων και πιο απλοποιημένες ροές εργασίας.

"Η τεχνητή νοημοσύνη έχει μειώσει τον χρόνο επεξεργασίας δεδομένων κατά το ήμισυ, επιτρέποντάς μας να αφιερώσουμε περισσότερο
χρόνο στις αλληλεπιδράσεις με τους πελάτες και τον στρατηγικό προγραμματισμό," μοιράστηκε ένας συμμετέχων. Ένας άλλος σημείωσε: "Η ανάλυση δεδομένων και η διαχείριση των λογιστικών μου καθηκόντων έχουν γίνει σημαντικά πιο εύκολες με την τεχνητή νοημοσύνη." *είπε ένας συμμετέχων* .

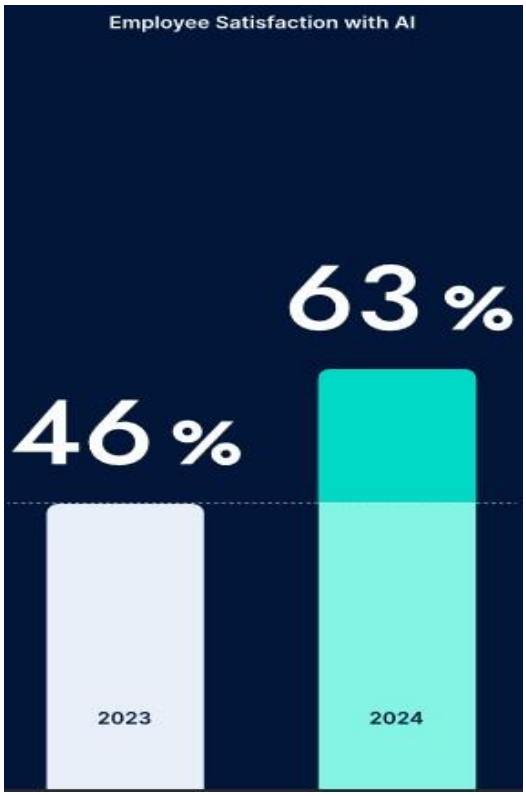


Figure 9-Ικανοποίηση υπαλλήλων με χρήση AI

Η τεχνητή νοημοσύνη βελτιώνει την ισορροπία επαγγελματικής και προσωπικής ζωής, με το 63% φέτος (έναντι 46% πέρυσι) να δηλώνει λιγότερη εξάντληση και μεγαλύτερη ικανοποίηση. Όπως είπε ένας υπάλληλος, «η AI μειώνει τον χρόνο σε επαναλαμβανόμενες εργασίες και αυξάνει τη συνολική μου ευτυχία».

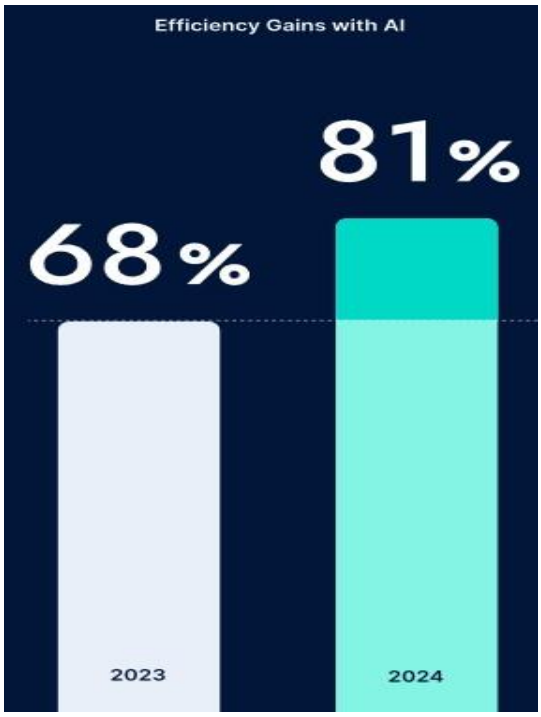


Figure 10-Αύξηση απόδοσης με χρήση AI,από 68% το 2023 σε 81% το 2024.

Η Τεχνητή Νοημοσύνη στη Διάσωση κατά τις πολυάσχολες περιόδους

Κατά τις περιόδους αυξημένης δραστηριότητας, η τεχνητή νοημοσύνη βοηθά τους ελεγκτές να διαχειρίζονται τον φόρτο εργασίας, αυξάνοντας την αποδοτικότητα και μειώνοντας τα λάθη. Φέτος, το 81% των επαγγελματιών ανέφερε βελτίωση, έναντι 68% πέρυσι. Όπως είπε χαρακτηριστικά ένας ελεγκτής, «η AI αναλαμβάνει τις επαναλαμβανόμενες εργασίες, ώστε να επικεντρωνόμαστε στην κρίσιμη ανάλυση και αναφορά».

Figure 11-Το 88% των συμμετοχόντων αναμένει σημαντική πρόοδο με χρήση της AI.

Μέλλοντική Επέκταση

Τα επόμενα δύο χρόνια υπόσχονται σημαντική ανάπτυξη στην υιοθέτηση της τεχνητής νοημοσύνης στους τομείς του ελέγχου και των οικονομικών. Το 88% των συμμετεχόντων στην έρευνά μας αναμένει σημαντικές προόδους και αυξημένη εφαρμογή εργαλείων AI στις εταιρείες τους κατά τους επόμενους
24 μήνες. Αυτή η προβλεπόμενη ανάπτυξη υπογραμμίζει την αναγνώριση της αξίας της τεχνητής νοημοσύνης από τον κλάδο και τη δέσμευση για την ενσωμάτωσή αυτών των τεχνολογιών για τη βελτίωση της αποδοτικότητας, της ακρίβειας και των στρατηγικών πληροφοριών.

"Η ικανότητα να προσαρμόζεσαι στην τεχνολογία είναι κρίσιμη για να παραμείνεις ανταγωνιστικός σε αυτόν τον τομέα." Senior Auditor.

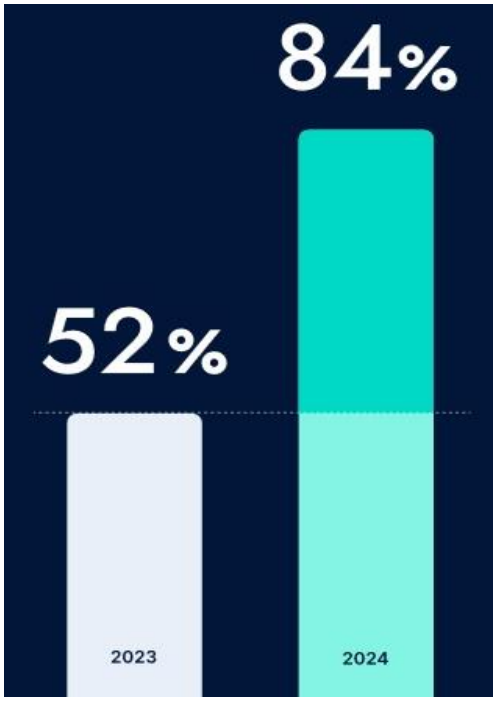


Figure 12-Αύξηση του ποσοστού εργαζομένων από 52% σε 84% όπου πιστεύουν ότι η AI θα επψφελήσει την εργασία τους.

Μέλλουσα Προοπτική: Μηχανή x Ανθρώπος

Το 84% των ελεγκτών πιστεύει ότι η τεχνητή νοημοσύνη δεν θα αντικαταστήσει τις δουλειές τους, σε σύγκριση με το 52% πέρυσι, αλλά θα ενισχύσει τις ικανότητές τους. Η προσαρμογή απαιτεί συνεχή μάθηση, όμως η προοπτική είναι θετική. Όπως είπε ένας επαγγελματίας, «η AI είναι ευκαιρία για βελτίωση δεξιοτήτων και πιο στρατηγικούς ρόλους», ενώ άλλος τόνισε πως «η προληπτική σκέψη είναι κρίσιμη για την αποτελεσματική αξιοποίησή της».

Τα Μεγάλα Συμπεράσματα

Η Έκθεση AI 2024 αναδεικνύει μια σαφή τάση: η τεχνητή νοημοσύνη ήρθε για να μείνει και έχει σημαντικές θετικές επιδράσεις στον τομέα του ελέγχου και των οικονομικών. Από την αύξηση της αποδοτικότητας και τη διατήρηση ταλέντου έως τη βελτίωση της ισορροπίας μεταξύ επαγγελματικής και προσωπικής ζωής, τα οφέλη της τεχνητής νοημοσύνης είναι πολλά. Οι επιχειρήσεις που υιοθετούν την τεχνητή νοημοσύνη όχι μόνο προστατεύουν τις λειτουργίες τους για το μέλλον, αλλά δημιουργούν επίσης πιο ικανοποιημένα και παραγωγικά εργατικά δυναμικά.

4.2 Προκλήσεις και Ηθικά Διλήμματα της Τεχνητής Νοημοσύνης στους Ελέγχους Συστημάτων

Η ενσωμάτωση της τεχνητής νοημοσύνης (ΤΝ) στους ελέγχους συστημάτων φέρνει νέες ευκαιρίες αλλά και σημαντικές προκλήσεις και ηθικά διλήμματα. Οι τεχνολογίες ΤΝ έχουν τη δυνατότητα να βελτιώσουν την αποτελεσματικότητα, την ακρίβεια και τη διαφάνεια στους ελέγχους, ωστόσο η χρήση τους προκαλεί ερωτήματα σχετικά με την αμεροληψία, την ιδιωτικότητα, την ασφάλεια και την υπευθυνότητα.

1.Προκλήσεις: Μεροληψία στα Συστήματα ΤΝ: Η μεροληψία είναι μία από τις σημαντικότερες προκλήσεις που ανακύπτουν κατά τη χρήση της ΤΝ στους ελέγχους συστημάτων. Όπως αναφέρεται, τα δεδομένα που χρησιμοποιούνται για την εκπαίδευση των αλγορίθμων ΤΝ μπορούν να περιέχουν έμφυτες προκαταλήψεις (Crawford & Whittaker, 2019). Αυτό σημαίνει ότι τα συστήματα που βασίζονται σε τέτοια δεδομένα μπορεί να επηρεάζουν τις αποφάσεις τους με τρόπους που δημιουργούν αδικίες και ανισότητες, όπως οι διακρίσεις εις βάρος ορισμένων κοινωνικών ομάδων. Οι προκαταλήψεις αυτές μπορούν να εμφανιστούν είτε λόγω ανεπαρκούς εκπροσώπησης διαφορετικών δημογραφικών ομάδων είτε λόγω κοινωνικών ανισοτήτων που έχουν καταγραφεί ιστορικά στα δεδομένα.

Έλλειψη Διαφάνειας: Τα συστήματα ΤΝ, και ιδιαίτερα τα λεγόμενα <<black box*>> μοντέλα, συχνά χαρακτηρίζονται από έλλειψη διαφάνειας. Οι πολύπλοκοι αλγόριθμοι και η αδυναμία κατανόησης του τρόπου λήψης αποφάσεων από αυτά τα συστήματα αποτελούν σοβαρό πρόβλημα στους ελέγχους συστημάτων, καθώς οι ελεγκτές πρέπει να είναι σε θέση να ερμηνεύουν τις αποφάσεις της ΤΝ για να εντοπίζουν σφάλματα ή αδυναμίες (Miller et al., 2019). Η έλλειψη διαφάνειας υπονομεύει τη λογοδοσία και την εμπιστοσύνη στους ελέγχους που βασίζονται σε ΤΝ.

Ασφάλεια Δεδομένων και Ιδιωτικότητα: Η ΤΝ βασίζεται σε μεγάλους όγκους δεδομένων, συμπεριλαμβανομένων ευαίσθητων πληροφοριών που αφορούν οικονομικά στοιχεία, προσωπικά δεδομένα και άλλες κρίσιμες πληροφορίες (Ohm, 2019). Η διαχείριση αυτών των δεδομένων δημιουργεί προκλήσεις για την ασφάλεια και την ιδιωτικότητα. Ειδικά στους ελέγχους συστημάτων, η διασφάλιση ότι τα δεδομένα προστατεύονται από διαρροές, κακόβουλες επιθέσεις και μη εξουσιοδοτημένη πρόσβαση είναι ζωτικής σημασίας. Η αποτυχία διασφάλισης της ιδιωτικότητας και της ασφάλειας μπορεί να οδηγήσει σε σοβαρές συνέπειες για τις επιχειρήσεις και τους πελάτες.

*Ο όρος **black box** στην τεχνητή νοημοσύνη αναφέρεται σε μοντέλα ή αλγορίθμους των οποίων η εσωτερική λειτουργία είναι δύσκολο να κατανοηθεί ή να αναλυθεί από τους ανθρώπους. Αυτό συμβαίνει συχνά με πολύπλοκες διαδικασίες, όπως οι νευρωνικές δίκτυα, όπου οι διαδικασίες που οδηγούν σε συγκεκριμένες αποφάσεις ή αποτελέσματα είναι κρυμμένες και δεν είναι άμεσα ορατές.*

2.Ηθικά Διλήμματα: Ιδιωτικότητα και Υπερβολική Συλλογή Δεδομένων: Η χρήση ΤΝ στους ελέγχους συστημάτων μπορεί να απαιτεί τη συλλογή και ανάλυση μεγάλων όγκων δεδομένων, κάτι που εγείρει ηθικά διλήμματα γύρω από την υπερβολική χρήση ή κατάχρηση των προσωπικών πληροφοριών (AICPA, 2023). Η ΤΝ συλλέγει συχνά περισσότερα δεδομένα από ό,τι χρειάζεται, και αυτό μπορεί να παραβιάζει τα δικαιώματα των ατόμων σχετικά με την ιδιωτικότητα τους. Το ηθικό δίλημμα έγκειται στην ανάγκη για επαρκή δεδομένα ώστε να λειτουργεί σωστά η ΤΝ, χωρίς όμως να θυσιάζονται τα δικαιώματα ιδιωτικότητας.

Παράδειγμα**:** Ένας οργανισμός αναπτύσσει παρακολούθηση δικτύου βάσει τεχνητής νοημοσύνης, καταγράφοντας ακούσια ευαίσθητες πληροφορίες εργαζομένων στην καθημερινή διαδικασία παρακολούθησης. Η εξισορρόπηση της ασφάλειας με το απόρρητο γίνεται μια πρόκληση, καθώς το σύστημα πρέπει να ρυθμιστεί με ακρίβεια ώστε να ελαχιστοποιήσει τη συλλογή προσωπικών και άλλων μη σχετιζόμενων με την εργασία δεδομένων, ενώ παράλληλα εντοπίζει αποτελεσματικά τις απειλές.

Διαφάνεια και Λογοδοσία των Αλγορίθμων: Η διαφάνεια των αλγορίθμων ΤΝ είναι θεμελιώδης για τη διασφάλιση της δικαιοσύνης και της λογοδοσίας, αλλά η επίτευξή της συχνά συγκρούεται με τα εμπορικά συμφέροντα των επιχειρήσεων που αναπτύσσουν τα εν λόγω συστήματα (Lundberg & Lee, 2017). Οι εταιρείες ενδέχεται να αρνούνται να αποκαλύψουν πλήρως τις εσωτερικές λειτουργίες των αλγορίθμων τους, προβάλλοντας ανησυχίες περί πνευματικής ιδιοκτησίας. Αυτό οδηγεί σε ηθικά διλήμματα σχετικά με το ποιος πρέπει να ελέγχει και να επιβλέπει τη χρήση αυτών των συστημάτων, καθώς και το ποιος φέρει την ευθύνη για τυχόν λάθη ή αδικίες που προκαλούνται από τα αποτελέσματά τους.

Παράδειγμα**:** Ένας αναλυτής κυβερνοασφάλειας πρέπει να υπερασπιστεί την απόφασή του να ενεργήσει ενάντια σε μια ύποπτη απειλή που επισημαίνεται από ένα σύστημα AI. Ωστόσο, δεν μπορούν να δώσουν μια σαφή εξήγηση για το γιατί η τεχνητή νοημοσύνη έκανε αυτόν τον προσδιορισμό, καθιστώντας δύσκολη την αιτιολόγηση των μεταγενέστερων ενεργειών τους στους ενδιαφερόμενους.

Μεροληψία και Ανισότητες: Η μεροληψία στους αλγόριθμους ΤΝ, η οποία μπορεί να οδηγήσει σε άδικες αποφάσεις, συνιστά ένα ακόμα ηθικό δίλημμα (Prabhakar et al., 2021). Για παράδειγμα, αν οι αλγόριθμοι που χρησιμοποιούνται σε ελέγχους συστημάτων βασίζονται σε δεδομένα που εμπεριέχουν ιστορικές διακρίσεις, τότε τα συστήματα ΤΝ μπορεί να αναπαράγουν αυτές τις διακρίσεις. Η ηθική πρόκληση εδώ αφορά το πώς μπορούμε να σχεδιάσουμε και να εκπαιδεύσουμε αλγόριθμους που όχι μόνο θα αποφεύγουν τέτοια σφάλματα, αλλά θα ενισχύουν τη δικαιοσύνη και την ισότητα.

Παράδειγμα: Ένα εργαλείο κυβερνοασφάλειας επισημαίνει το νόμιμο λογισμικό που χρησιμοποιείται κυρίως από μια συγκεκριμένη πολιτισμική ομάδα ως κακόβουλο λόγω μεροληψίας στα δεδομένα εκπαίδευσης. Αυτό εγείρει ερωτήματα σχετικά με τη δικαιοσύνη και τη δυνατότητα για άδικες και δυσανάλογες ενέργειες και συνέπειες.

3.Στρατηγικές Αντιμετώπισης:

Για να αντιμετωπιστούν οι προκλήσεις και τα ηθικά διλήμματα της ΤΝ στους ελέγχους συστημάτων, προτείνονται διάφορες στρατηγικές:

Τακτικοί έλεγχοι και αναλύσεις αμεροληψίας: Η συνεχής παρακολούθηση των συστημάτων ΤΝ για πιθανές μεροληψίες και αδικίες μπορεί να συμβάλλει στην αποφυγή των διακρίσεων (Selbst et al., 2019).

Διασφάλιση διαφάνειας και εξηγήσιμης ΤΝ: Η χρήση εξηγήσιμων μοντέλων ΤΝ που επιτρέπουν στους χρήστες να κατανοούν πώς λαμβάνονται οι αποφάσεις από τους αλγόριθμους αποτελεί ένα σημαντικό εργαλείο για την προώθηση της διαφάνειας (Miller et al., 2019).

Αυστηρή τήρηση των κανονισμών περί προστασίας δεδομένων: Η συμμόρφωση με κανονισμούς όπως ο GDPR διασφαλίζει ότι η χρήση της ΤΝ δεν θα παραβιάζει τα δικαιώματα ιδιωτικότητας των χρηστών (Wolters Kluwer, 2023).

Συμπέρασμα: Η εφαρμογή της τεχνητής νοημοσύνης στους ελέγχους συστημάτων φέρνει τόσο δυνατότητες όσο και κινδύνους. Οι προκλήσεις της μεροληψίας, της έλλειψης διαφάνειας και της προστασίας της ιδιωτικότητας αναδεικνύουν την ανάγκη για προσεκτικό σχεδιασμό και συνεχή εποπτεία. Τα ηθικά διλήμματα που προκύπτουν απαιτούν την ανάπτυξη στρατηγικών που θα διασφαλίσουν ότι η ΤΝ θα χρησιμοποιείται με τρόπο δίκαιο, διαφανή και υπεύθυνο, συμβάλλοντας στην επίτευξη αξιόπιστων και ακριβών ελέγχων. **[23]**

4.3 Ανθρώπινος παράγοντας και AI: Συνδυασμός ή αντικατάσταση;

Ενώ η τεχνητή νοημοσύνη υπόσχεται πολλά για το επάγγελμα του ελεγκτή, οι ελεγκτές πρέπει να γνωρίζουν τις προκλήσεις που σχετίζονται με τη χρήση της και να λαμβάνουν μέτρα για την αντιμετώπισή τους. Κεντρικά ζητήματα που αναδεικνύονται περιλαμβάνουν:

- **Ηθική διακυβέρνηση:** Η ανάπτυξη και χρήση της ΤΝ πρέπει να βασίζεται σε αρχές που προάγουν την ανθρώπινη ευημερία, την προστασία των θεμελιωδών δικαιωμάτων και την αποφυγή διακρίσεων ή προκαταλήψεων. Η ηθική διακυβέρνηση επιδιώκει να θέσει σαφείς κανόνες και πλαίσια για τη δημιουργία υπεύθυνων συστημάτων ΤΝ.
- **Αλγοριθμική υπευθυνότητα:** Τα συστήματα ΤΝ συχνά λειτουργούν ως «μαύρα κουτιά», με αλγορίθμους που λαμβάνουν αποφάσεις χωρίς πλήρη διαφάνεια ή εξήγηση. Η ανάγκη για υπευθυνότητα σημαίνει ότι πρέπει να υπάρχει σαφής προσδιορισμός των υπευθύνων και μηχανισμοί ελέγχου για τις επιπτώσεις των αποφάσεων αυτών.
- **Διαφάνεια και εξηγησιμότητα:** Η κατανόηση και η εξήγηση των τρόπων λειτουργίας των αλγορίθμων είναι κρίσιμης σημασίας, ειδικά όταν τα αποτελέσματα επηρεάζουν ανθρώπους ή

σημαντικές επιχειρησιακές αποφάσεις. Η διαφάνεια ενισχύει την εμπιστοσύνη και επιτρέπει την ορθή αξιολόγηση και εποπτεία.

Αντιμετωπίζοντας αυτές τις προκλήσεις, οι ελεγκτές μπορούν να αξιοποιήσουν τη δύναμη της τεχνητής νοημοσύνης για τη βελτίωση της ποιότητας και της αποτελεσματικότητας των ελέγχων, διατηρώντας παράλληλα την ακεραιότητα της διαδικασίας ελέγχου. **[18]**

5.Νομικό & Κανονιστικό Πλαίσιο

Οι νόμοι και οι κανονισμοί που ισχύουν σε κάθε κράτος,μπορεί να διαφέρουν μεταξύ τους, επιβάλλοντας συγκεκριμένες απαιτήσεις συμμόρφωσης στις επιχειρήσεις. Οι ελεγκτές πληροφορικής πρέπει να γνωρίζουν αυτές τις απαιτήσεις και να προσαρμόζουν τις αναφορές τους αναλόγως.

Κάθε κράτος έχει δικούς του κανόνες που αφορούν διάφορες πτυχές του IT audit, όπως οι νόμοι για την ειδοποίηση σε περίπτωση παραβίασης δεδομένων, οι οποίοι απαιτούν από τις εταιρείες να ενημερώνουν τους χρήστες αν τα προσωπικά τους στοιχεία έχουν υποκλαπεί. Οι ελεγκτές πρέπει να είναι ενημερωμένοι με τις απαιτήσεις κάθε κράτους ώστε να διασφαλίζουν ότι η εταιρεία συμμορφώνεται.

Επίσης, κάποια κράτη έχουν θεσπίσει συγκεκριμένους νόμους για την κυβερνοασφάλεια, που μπορεί να περιλαμβάνουν τακτικούς ελέγχους ευπάθειας, δοκιμές διείσδυσης και εφαρμογή συγκεκριμένων μέτρων ασφαλείας. Οι ελεγκτές πρέπει να γνωρίζουν καλά αυτούς τους κανόνες για να παρέχουν ακριβείς και ολοκληρωμένες εκθέσεις.

Επιπλέον, οι νόμοι σε κάθε κράτος μπορεί να καλύπτουν ζητήματα όπως η προστασία προσωπικών δεδομένων, η αποθήκευση ηλεκτρονικών αρχείων και η χρήση υπηρεσιών cloud. Οι ελεγκτές πρέπει να μπορούν να κινηθούν μέσα σε αυτό το σύνθετο νομικό πλαίσιο για να διασφαλίσουν ότι οι επιχειρήσεις ακολουθούν τους ισχύοντες κανόνες.

Τελικά, το νομικό πλαίσιο για τον έλεγχο των πληροφοριακών συστημάτων είναι σύνθετο, με νόμους σε ομοσπονδιακό και πολιτειακό επίπεδο. Οι ελεγκτές πληροφορικής είναι κρίσιμοι για την εξασφάλιση της συμμόρφωσης και την προστασία ευαίσθητων πληροφοριών, παρέχοντας πολύτιμες προτάσεις για τη βελτίωση της ασφάλειας των συστημάτων.

5.1 Νομοθεσία και κανονισμοί που αφορούν την Τεχνητή Νοημοσύνη.

Οι νομοθεσίες που αφορούν την τεχνητή νοημοσύνη (AI) εξελίσσονται ταχύτατα καθώς οι κυβερνήσεις προσπαθούν να ρυθμίσουν τη χρήση της με σκοπό να προστατεύσουν την ασφάλεια, τα ανθρώπινα δικαιώματα και την ιδιωτικότητα.

Τι είναι ο νόμος AI ACT της Ευρωπαϊκής Ένωσης για την Τεχνητή Νοημοσύνη;

Η χρήση της τεχνητής νοημοσύνης στην ΕΕ θα ρυθμίζεται από τον νόμο **AI ACT**, ***Κανονισμός (ΕΕ) 2024/1689 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Ιουνίου 2024, για τη θέσπιση εναρμονισμένων κανόνων για την τεχνητή νοημοσύνη και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 300/2008, (ΕΕ) αριθ. 167/2013, (ΕΕ) αριθ. /2013, (ΕΕ) 2018/858, (ΕΕ) 2018/1139 και (ΕΕ) 2019/2144 και Οδηγίες 2014/90/ΕΕ, (ΕΕ) 2016/797 και (ΕΕ) 2020/1828 (Artifical Intelligence) Κείμενο με συνάφεια στον ΕΟΧ)***[25], τον πρώτο ολοκληρωμένο νόμο στον κόσμο για την τεχνητή νοημοσύνη.

Ο **AI Act** της Ευρωπαϊκής Ένωσης, Κανονισμός (ΕΕ) 2024/1689 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 13ης Ιουνίου 2024, αποτελεί το πρώτο ολοκληρωμένο νομοθετικό πλαίσιο παγκοσμίως για την τεχνητή νοημοσύνη. Στόχος του είναι η ρύθμιση των συστημάτων AI στην ΕΕ βάσει του επιπέδου κινδύνου που αυτά ενέχουν.

Τα συστήματα AI που χρησιμοποιούνται στο IT auditing ενδέχεται να καταταγούν ως υψηλού κινδύνου, λόγω της κρίσιμης σημασίας τους στις διαδικασίες ελέγχου και αξιολόγησης. Ο κανονισμός θέτει αυστηρές απαιτήσεις για διαφάνεια, αξιοπιστία, διαχείριση κινδύνων και ανθρώπινη εποπτεία.

Διασφάλιση συμμόρφωσης και συνεχής παρακολούθηση

Η συμμόρφωση με τον νόμο της ΕΕ για την τεχνητή νοημοσύνη δεν τελειώνει με την αρχική ανάπτυξη συστημάτων τεχνητής νοημοσύνης. Απαιτείται συνεχής παρακολούθηση για τη διασφάλιση της συνεχούς συμμόρφωσης. Οι εσωτερικοί ελεγκτές πρέπει να επαληθεύουν ότι τα συστήματα τεχνητής νοημοσύνης υψηλού κινδύνου υποβάλλονται σε κατάλληλες αξιολογήσεις και να κατανοούν πότε απαιτούνται εξωτερικές αξιολογήσεις. Οι ελεγκτές θα πρέπει επίσης να αξιολογήσουν εάν υπάρχουν κατάλληλοι μηχανισμοί για συνεχή παρακολούθηση, συμπεριλαμβανομένης της αναφοράς περιστατικών και των έγκαιρων διορθωτικών ενεργειών. Λαμβάνοντας μια πιο προληπτική προσέγγιση, οι ελεγκτές μπορούν να συμβάλουν στη διασφάλιση της αντιμετώπισης πιθανών κινδύνων και ότι αυτά τα συστήματα παραμένουν συμβατά καθ' όλη τη διάρκεια του κύκλου ζωής τους. Τα δεδομένα εσωτερικού ελέγχου που χρησιμοποιούνται από συστήματα τεχνητής νοημοσύνης είναι επίσης σημαντικά, επομένως η αξιολόγηση των δομών και διαδικασιών διακυβέρνησης δεδομένων του οργανισμού είναι απαραίτητη. Οι ελεγκτές θα πρέπει να επαληθεύουν ότι χρησιμοποιούνται δεδομένα υψηλής ποιότητας, ότι τηρείται η κατάλληλη τεκμηρίωση και ότι ακολουθούνται οι ισχύουσες πρακτικές τήρησης αρχείων. Οι ελεγκτές θα πρέπει να λάβουν υπόψη:

- Από πού προήλθαν τα δεδομένα;
- Έχουν σχεδιαστεί και λειτουργούν αποτελεσματικά οι διαδικασίες και οι έλεγχοι που παρήγαγαν τα δεδομένα;
- Είναι τα δεδομένα πλήρη, ακριβή και αξιόπιστα;
- Πώς χρησιμοποιούνται τα δεδομένα από το AI;

Δεοντολογικά ζητήματα και θεμελιώδη δικαιώματα

Ο νόμος της Ευρωπαϊκής Ένωσης για την τεχνητή νοημοσύνη διατηρεί σημαντική εστίαση στους ηθικούς λόγους και στην προστασία των θεμελιωδών δικαιωμάτων. Για το σκοπό αυτό, οι εσωτερικοί ελεγκτές θα πρέπει να αξιολογούν εάν τα συστήματα τεχνητής νοημοσύνης αναπτύσσονται και χρησιμοποιούνται με τρόπο που δεν εισάγει διακρίσεις, προωθεί την ισότητα και ενθαρρύνει την πολιτιστική πολυμορφία. Ορισμένοι τομείς που πρέπει να εξετάσουν οι εσωτερικοί ελεγκτές σχετικά με τον σεβασμό των θεμελιωδών δικαιωμάτων περιλαμβάνουν το απόρρητο, την προστασία δεδομένων, την ελευθερία της έκφρασης και τη μη διάκριση. **[25]**

Επιπλέον νόμοι που αφορούν την AI στο IT Audit:

GDPR (Γενικός Κανονισμός για την Προστασία Δεδομένων): Ο GDPR επηρεάζει τη χρήση της AI στο IT audit, ιδιαίτερα όσον αφορά τη συλλογή, επεξεργασία και προστασία προσωπικών δεδομένων.

Κύριες αρχές του GDPR που σχετίζονται με την AI στο IT audit:

1. **Διαφάνεια και ενημέρωση (Άρθρα 12-14)**: Όταν χρησιμοποιούνται συστήματα AI για την επεξεργασία προσωπικών δεδομένων κατά τη διάρκεια ενός IT audit, πρέπει να υπάρχει διαφάνεια σχετικά με τη χρήση της τεχνολογίας. Οι οργανισμοί οφείλουν να ενημερώνουν τους χρήστες για το πώς τα δεδομένα τους συλλέγονται, επεξεργάζονται και χρησιμοποιούνται από συστήματα AI κατά τη διάρκεια του ελέγχου.
2. **Ελαχιστοποίηση δεδομένων (Άρθρο 5)**: Τα συστήματα AI που χρησιμοποιούνται στο IT audit πρέπει να περιορίζουν τη συλλογή προσωπικών δεδομένων μόνο σε εκείνα που είναι απολύτως απαραίτητα για τους σκοπούς του ελέγχου. Η υπερβολική συλλογή δεδομένων αντίκειται στην αρχή της ελαχιστοποίησης.
3. **Δικαίωμα πρόσβασης και διαγραφής δεδομένων (Άρθρα 15-17)**: Οι πολίτες έχουν το δικαίωμα να γνωρίζουν αν τα προσωπικά τους δεδομένα υποβάλλονται σε επεξεργασία από ένα σύστημα AI κατά τη διάρκεια ενός IT audit και να ζητούν πρόσβαση ή διαγραφή των δεδομένων τους, εφόσον δεν είναι απαραίτητα για τον έλεγχο ή για άλλους νόμιμους λόγους.
4. **Λήψη συγκατάθεσης (Άρθρο 6)**: Η επεξεργασία προσωπικών δεδομένων μέσω AI στο IT audit απαιτεί τη νόμιμη βάση για την επεξεργασία, όπως η συγκατάθεση των υποκειμένων των δεδομένων. Ειδικά σε περιπτώσεις όπου χρησιμοποιούνται δεδομένα που μπορεί να περιέχουν ευαίσθητες πληροφορίες, οι οργανισμοί πρέπει να εξασφαλίζουν τη συγκατάθεση ή να βασίζονται σε άλλες νόμιμες βάσεις, όπως η εκπλήρωση νόμιμων υποχρεώσεων.
5. **Αυτοματοποιημένες αποφάσεις και προφίλ (Άρθρο 22)**: Ο GDPR περιορίζει τις **αυτοματοποιημένες αποφάσεις** που λαμβάνονται αποκλειστικά από συστήματα AI και επηρεάζουν σημαντικά τα υποκείμενα των δεδομένων, όπως η αξιολόγηση κινδύνων ή η απόδοση ποινών με βάση ένα audit. Τα άτομα έχουν το δικαίωμα να ζητούν την ανθρώπινη παρέμβαση σε τέτοιες αποφάσεις, γεγονός που είναι σημαντικό για το IT audit όταν οι AI αλγόριθμοι συμμετέχουν σε τέτοιες διαδικασίες.
6. **Εκτίμηση Αντικτύπου στην Προστασία Δεδομένων (DPIA) (Άρθρο 35)**: Όταν η χρήση της AI στο IT audit παρουσιάζει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των ατόμων (όπως συμβαίνει με την επεξεργασία μεγάλου όγκου ευαίσθητων δεδομένων), απαιτείται να πραγματοποιηθεί μια **εκτίμηση αντικτύπου στην προστασία δεδομένων (DPIA)**. Αυτό βοηθά να αναγνωριστούν οι κίνδυνοι και να ληφθούν μέτρα για την προστασία των δεδομένων. **[10]**

Άλλες συναφείς ρυθμίσεις:

- **Sarbanes-Oxley Act (SOX)**: Πρόκειται για αμερικανικό νόμο που επιβάλλει αυστηρούς κανόνες εσωτερικού ελέγχου για εταιρείες εισηγμένες στο χρηματιστήριο των ΗΠΑ. Αν και δεν σχετίζεται άμεσα με την AI, η χρήση αλγορίθμων στις χρηματοοικονομικές ροές ή στη

διαχείριση κινδύνων υπόκειται στους μηχανισμούς διαφάνειας και λογοδοσίας που επιβάλλει η SOX.

- **Οδηγία NIS 2**: Αποτελεί το νέο κανονιστικό πλαίσιο για την κυβερνοασφάλεια κρίσιμων υποδομών και υπηρεσιών στην ΕΕ. Η AI μπορεί να χρησιμοποιηθεί τόσο για ανίχνευση κυβερνοαπειλών όσο και να αποτελέσει δυνητικό σημείο ευπάθειας, γι' αυτό και ενσωματώνεται στις υποχρεώσεις διαχείρισης κινδύνων των φορέων.

Συμπέρασμα : Νέος ρόλος των εσωτερικών ελεγκτών

Στο νέο αυτό ρυθμιστικό πλαίσιο, οι **εσωτερικοί ελεγκτές** πρέπει να προσαρμόσουν τα ελεγκτικά τους πρότυπα, ώστε να καλύπτουν και τη χρήση της AI:

- Να διασφαλίζουν ότι η **τεκμηρίωση και η ιχνηλασιμότητα** των αποφάσεων μέσω AI είναι πλήρεις.
- Να εφαρμόζουν **μηχανισμούς ελέγχου συμμόρφωσης** τόσο με τον AI Act όσο και με άλλες ισχύουσες νομοθεσίες.
- Να αξιολογούν τον **αντίκτυπο της AI στα δικαιώματα των υποκειμένων**, τις **δεοντολογικές επιπτώσεις**, και να προτείνουν κατάλληλα **πλαίσια διακυβέρνησης AI**.

5.2 Ηθικές και Δεοντολογικές Προκλήσεις της Τεχνητής Νοημοσύνηςστον Εσωτερικό Έλεγχο.

Η ενσωμάτωση τεχνητής νοημοσύνης (AI) στις διαδικασίες εσωτερικού ελέγχου μεταμορφώνει ριζικά το πλαίσιο λήψης αποφάσεων, εντοπισμού κινδύνων και αξιολόγησης αποτελεσματικότητας των εσωτερικών διαδικασιών. Ωστόσο, η χρήση AI δημιουργεί και ένα νέο φάσμα **ηθικών και δεοντολογικών διλημμάτων**, τα οποία οφείλουν να αντιμετωπιστούν υπεύθυνα από τους οργανισμούς και, κυρίως, από τους επαγγελματίες του εσωτερικού ελέγχου που λειτουργούν ως θεματοφύλακες της ακεραιότητας.

1. Αλγοριθμική προκατάληψη (algorithmic bias) και δικαιοσύνη

Ένα από τα σοβαρότερα ηθικά ζητήματα είναι η **αλγοριθμική προκατάληψη**. Τα συστήματα AI βασίζονται σε δεδομένα εκπαίδευσης, τα οποία μπορεί να αντανακλούν κοινωνικές ανισότητες, προκαταλήψεις ή στρεβλώσεις. Αν αυτά τα δεδομένα δεν είναι αντιπροσωπευτικά ή έχουν ενσωματωμένες προκαταλήψεις, το σύστημα θα τις αναπαράγει.

Για παράδειγμα, ένα AI που αξιολογεί την πιστοληπτική ικανότητα εργαζομένων μπορεί να εμφανίσει **αρνητικές αποκλίσεις προς ομάδες που ιστορικά έχουν λιγότερη πρόσβαση σε χρηματοδότηση**, ακόμα κι αν τα μεμονωμένα άτομα δεν παρουσιάζουν τέτοιο ρίσκο.

Ο εσωτερικός έλεγχος οφείλει να εστιάσει στον **έλεγχο της δίκαιης μεταχείρισης** και της ισότητας, αξιολογώντας αν τα αποτελέσματα του συστήματος είναι **διαφανή, τεκμηριωμένα και απαλλαγμένα από διακρίσεις**. Οι ελεγκτές πρέπει να εντοπίζουν πηγές δυνητικής προκατάληψης

και να εισηγούνται διαδικασίες απομεροληψίας (debiasing), είτε στο επίπεδο των δεδομένων είτε στο σχεδιασμό των μοντέλων.

2. Διαφάνεια και ιχνηλασιμότητα αποφάσεων (explainability)

Η λειτουργία πολλών συστημάτων AI, και ιδιαίτερα των συστημάτων μηχανικής μάθησης, χαρακτηρίζεται από **περιορισμένη διαφάνεια**. Σε περιπτώσεις όπου το αποτέλεσμα μιας απόφασης βασίζεται σε πολύπλοκους υπολογισμούς χωρίς δυνατότητα εύκολης ερμηνείας (black box models), προκύπτει το ζήτημα της **λογοδοσίας**.

Οι εσωτερικοί ελεγκτές πρέπει να εξετάζουν:

- αν είναι **τεκμηριωμένο το πώς προκύπτει μια απόφαση**,
- αν ο οργανισμός μπορεί να **παρέχει επαρκή εξήγηση** σε ένα ενδιαφερόμενο μέρος (π.χ. εργαζόμενο ή πελάτη),
- και αν υπάρχει **μηχανισμός αναθεώρησης ή προσφυγής** σε περίπτωση σφάλματος ή αδικίας.

Η **ιχνηλασιμότητα (traceability)** είναι κρίσιμη: κάθε βήμα της διαδικασίας απόφασης πρέπει να μπορεί να αποτυπωθεί και να επαληθευτεί σε ενδεχόμενο έλεγχο.

Ανθρώπινη εποπτεία και ευθύνη

Η AI επιτρέπει την αυτοματοποίηση πολλών ελεγκτικών διαδικασιών – όπως η ανίχνευση απάτης ή η αξιολόγηση συναλλαγών. Ωστόσο, όσο μεγαλύτερη είναι η αυτονομία του συστήματος, τόσο πιο θολή γίνεται η **ευθύνη για τις αποφάσεις** που αυτό λαμβάνει.

Ποιος ευθύνεται όταν ένα σύστημα καταλήγει σε λανθασμένο ή επιβλαβές αποτέλεσμα;

- Ο προγραμματιστής του μοντέλου;
- Ο χρήστης;
- Ή ο οργανισμός ως σύνολο;

Οι δεοντολογικές αρχές απαιτούν **σαφή καταμερισμό ευθύνης και ανθρώπινη εποπτεία (human oversight)**. Οι εσωτερικοί ελεγκτές έχουν ρόλο-κλειδί στο να διασφαλίζουν ότι:

- η λήψη κρίσιμων αποφάσεων **δεν γίνεται αποκλειστικά από μηχανές**,
- και ότι οι ανθρώπινοι επαγγελματίες έχουν το δικαίωμα και την ικανότητα να παρέμβουν, να διορθώσουν ή να ακυρώσουν μια απόφαση που κρίνεται ακατάλληλη.

3. Προστασία ιδιωτικότητας και δεδομένων

Η χρήση AI προϋποθέτει συχνά την επεξεργασία μεγάλου όγκου προσωπικών δεδομένων, όπως βιομετρικά χαρακτηριστικά, συνήθειες, ή εργασιακές επιδόσεις. Εάν δεν υπάρχουν αυστηροί μηχανισμοί προστασίας, είναι πιθανό να θιγούν θεμελιώδη δικαιώματα των εργαζομένων ή των πελατών.

Οι ελεγκτές οφείλουν να ελέγχουν:

- αν τηρούνται οι αρχές του GDPR (ελαχιστοποίηση δεδομένων, σκοπός επεξεργασίας, συγκατάθεση),
- αν εφαρμόζονται μέτρα **ανωνυμοποίησης ή ψευδωνυμοποίησης**,
- και αν οι τεχνικές ασφαλείας που εφαρμόζονται είναι επαρκείς απέναντι σε κυβερνοαπειλές.

Επιπλέον, πρέπει να διασφαλίζεται η **συγκατάθεση των υποκειμένων**, όχι απλώς ως τυπική διαδικασία, αλλά με ουσιαστική ενημέρωση και δυνατότητα άρνησης χωρίς επιπτώσεις.

Ο εσωτερικός έλεγχος δεν περιορίζεται μόνο σε τεχνικά ζητήματα, αλλά οφείλει να αξιολογεί και τη **συνολική επίδραση της τεχνολογίας στην οργανωσιακή κουλτούρα, την ψυχολογική ασφάλεια και την εταιρική ηθική**.

Οι παραπάνω ηθικές προκλήσεις καθιστούν απαραίτητη τη δημιουργία ενός ισχυρού πλαισίου κανονισμών και κατευθυντήριων γραμμών για την υπεύθυνη χρήση της AI στο IT auditing, κάτι που αντικατοπτρίζεται και στον **Κανονισμό (ΕΕ) 2024/1689 (AI ACT)**.

5.3 Ο Ρόλος του Εσωτερικού Ελεγκτή στο Νέο Πλαίσιο Συμμόρφωσης και Ηθικής Διακυβέρνησης

Η ταχεία υιοθέτηση της τεχνητής νοημοσύνης στους οργανισμούς μετασχηματίζει τον ρόλο του εσωτερικού ελεγκτή. Από έναν παραδοσιακό επόπτη ελέγχων, καλείται πλέον να λειτουργεί ως **στρατηγικός συνεργάτης**, συνδυάζοντας τεχνική κατανόηση, δεοντολογική κρίση και συμβουλευτική ικανότητα. Το νέο πλαίσιο συμμόρφωσης και ηθικής διακυβέρνησης επιβάλλει μια σειρά από διευρυμένες ευθύνες για τον ελεγκτή, οι οποίες αναλύονται παρακάτω.

1. Επιτήρηση της συμμόρφωσης με κανονιστικά και ηθικά πρότυπα

Ο εσωτερικός ελεγκτής δεν περιορίζεται στον έλεγχο της εφαρμογής των υπαρχόντων πολιτικών· είναι υπεύθυνος για την **επαλήθευση της συμμόρφωσης με ταχύτατα εξελισσόμενα κανονιστικά πλαίσια**, όπως ο GDPR, οι ευρωπαϊκές οδηγίες για την AI (AI Act), ή και εσωτερικοί κώδικες δεοντολογίας.

Ειδικότερα:

- Πρέπει να εντοπίζει αν τα συστήματα AI **συμβαδίζουν με τις αρχές διαφάνειας, ισότητας και ασφάλειας**, και αν ενσωματώνουν μηχανισμούς ελέγχου.
- Πρέπει να αξιολογεί αν οι **πολιτικές προστασίας προσωπικών δεδομένων** είναι εφαρμόσιμες και κατανοητές.
- Ο ρόλος του αποκτά προληπτικό χαρακτήρα, προτείνοντας **διορθωτικές ενέργειες πριν την πρόκληση νομικών ή ηθικών ζητημάτων**.

2. Ανάπτυξη μηχανισμών ηθικού ελέγχου και λογοδοσίας των συστημάτων AI

Ο εσωτερικός ελεγκτής καλείται να συμβάλει στη **δημιουργία πλαισίων λογοδοσίας (accountability frameworks)** για την τεχνητή νοημοσύνη. Τα πλαίσια αυτά καθορίζουν:

- Ποιος ελέγχει το μοντέλο;
- Πώς διασφαλίζεται η διαφάνεια;
- Ποιος φέρει την ευθύνη σε περίπτωση σφάλματος ή βλαπτικής απόφασης;

*Ηθική διακυβέρνηση σημαίνει ότι κάθε σύστημα AI πρέπει να λειτουργεί εντός **σαφώς καθορισμένων αξιακών ορίων** και με **διακριτή ανθρώπινη εποπτεία**. Ο ελεγκτής αξιολογεί όχι μόνο τις τεχνικές πτυχές, αλλά και τον βαθμό στον οποίο η τεχνολογία ανταποκρίνεται στις αξίες του οργανισμού.*

3. Συμβολή στον σχεδιασμό πολιτικών χρήσης της τεχνητής νοημοσύνης

Πέρα από τον έλεγχο, ο εσωτερικός ελεγκτής συμμετέχει ενεργά και στη **διαμόρφωση στρατηγικών πολιτικών χρήσης της AI**. Αυτές οι πολιτικές καθορίζουν:

- τα αποδεκτά πεδία εφαρμογής της AI (π.χ. παρακολούθηση προσωπικού),
- τις απαιτήσεις για **συγκατάθεση**,
- τις **ελάχιστες απαιτήσεις ηθικής διασφάλισης**.

Ο ελεγκτής οφείλει να **συνεργάζεται με τα τμήματα IT, νομικής υπηρεσίας και ανθρώπινου δυναμικού**, προκειμένου να διασφαλίζει ότι οι πολιτικές αυτές είναι **συνεκτικές, εφαρμόσιμες και προσανατολισμένες στην ηθική υπευθυνότητα**.

5.4 Νομικές Επιπτώσεις της Αυτοματοποιημένης Διεξαγωγής Ελέγχου μέσω AI

Η αυτοματοποίηση των διαδικασιών ελέγχου μέσω τεχνητής νοημοσύνης (όπως περιγράφηκε στο Κεφάλαιο 3.2) έχει δημιουργήσει νέες νομικές και κανονιστικές προκλήσεις. Στην Ευρωπαϊκή Ένωση, η χρήση της AI ρυθμίζεται πλέον από τον **Κανονισμό (ΕΕ) 2024/1689 – AI Act**, που θεσπίστηκε στις 13 Ιουνίου 2024 και αποτελεί το πρώτο ολοκληρωμένο νομικό πλαίσιο παγκοσμίως για την τεχνητή νοημοσύνη.

Ο AI Act εισάγει ένα σύστημα κατηγοριοποίησης με βάση τον κίνδυνο. Τα συστήματα AI που εμπλέκονται σε ελεγκτικές διαδικασίες συχνά κατατάσσονται στην κατηγορία «υψηλού κινδύνου», καθώς επηρεάζουν κρίσιμες λειτουργίες, όπως η ανάλυση οικονομικών στοιχείων ή η αξιολόγηση συμμόρφωσης. Αυτό συνεπάγεται αυξημένες απαιτήσεις για διαφάνεια, αξιοπιστία, διαχείριση κινδύνων και ανθρώπινη εποπτεία.

Η αυτοματοποίηση των διαδικασιών ελέγχου μέσω AI δημιουργεί νέες νομικές και κανονιστικές προκλήσεις. Η χρήση εργαλείων που εκτελούν αυτοματοποιημένη συλλογή, επεξεργασία και αξιολόγηση δεδομένων πρέπει να συμμορφώνεται με ένα ευρύ πλαίσιο κανόνων που διασφαλίζουν τη νομιμότητα, την ακεραιότητα των διαδικασιών και τον σεβασμό των δικαιωμάτων των εμπλεκομένων.

5.4.1 Συμμόρφωση με το GDPR και την αυτοματοποιημένη λήψη αποφάσεων

Σύμφωνα με το άρθρο 22 του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR), κάθε άτομο έχει δικαίωμα να μην υπόκειται σε απόφαση που βασίζεται αποκλειστικά σε αυτοματοποιημένη επεξεργασία, εφόσον αυτή έχει έννομες συνέπειες. Στο πλαίσιο του IT audit, αυτό σημαίνει ότι τα αποτελέσματα που παράγει η AI πρέπει να συνοδεύονται από ανθρώπινη αξιολόγηση, επεξηγησιμότητα (explainability) και επαρκή τεκμηρίωση.

5.4.2 Κατηγοριοποίηση της AI βάσει του AI Act (Κανονισμός ΕΕ 2024/1689)

Τα συστήματα AI που χρησιμοποιούνται σε ελέγχους υψηλού ρίσκου απαιτούν τεχνική τεκμηρίωση, συνεχή εποπτεία από ανθρώπους, περιοδική αξιολόγηση και ενσωμάτωση ισχυρών μηχανισμών ασφάλειας. Επιπλέον, ο AI Act απαιτεί διασφάλιση της ακρίβειας των δεδομένων εισόδου, καταγραφή σφαλμάτων και ύπαρξη διαδικασιών για τον εντοπισμό και την αντιμετώπιση αποκλίσεων..

5.4.3 Ευθύνες του εσωτερικού ελεγκτή στην εποχή της AI

Ο ρόλος του εσωτερικού ελεγκτή δεν περιορίζεται πλέον στον έλεγχο των αποτελεσμάτων. Περιλαμβάνει την αξιολόγηση του τρόπου με τον οποίο σχεδιάζονται, υλοποιούνται και χρησιμοποιούνται τα εργαλεία AI, την επιβεβαίωση της συμμόρφωσης με τα νομικά πλαίσια, καθώς και τη διασφάλιση της αξιοπιστίας και εγκυρότητας των αναλύσεων που προκύπτουν.

5.4.4 Νομική απαίτηση για καταγραφή και τεκμηρίωση (Auditability)

Η ύπαρξη λεπτομερών αρχείων καταγραφής (logs) και ιχνών ελέγχου (audit trails) είναι θεμελιώδης απαίτηση, όχι μόνο για λόγους λογοδοσίας, αλλά και για την τεκμηρίωση της συμμόρφωσης σε περίπτωση ελέγχου από ρυθμιστικές αρχές. Αυτά τα δεδομένα επιτρέπουν την αναδρομική εξέταση των αυτοματοποιημένων ενεργειών και ενισχύουν την εμπιστοσύνη στα συστήματα.

6. Υιοθέτηση της AI στο IT Audit

6.1 Τεχνολογίες και Εργαλεία AI διαθέσιμα για auditing

Μηχανική Μάθηση στον Έλεγχο Πληροφορικής:

Οι αλγόριθμοι μηχανικής μάθησης επιτρέπουν στα συστήματα τεχνητής νοημοσύνης να μαθαίνουν από ιστορικά δεδομένα και να κάνουν προβλέψεις ή να αναλαμβάνουν ενέργειες χωρίς να είναι ρητά προγραμματισμένοι για κάθε σενάριο. Στο πλαίσιο του ελέγχου πληροφορικής, η μηχανική μάθηση μπορεί να χρησιμοποιηθεί για την ανάλυση μεγάλων συνόλων δεδομένων, τον εντοπισμό προτύπων, τον εντοπισμό ανωμαλιών και την πρόβλεψη πιθανών κινδύνων.

Μια ειδική εφαρμογή της μηχανικής μάθησης στον έλεγχο πληροφορικής είναι η ανίχνευση ανωμαλιών. Εκπαιδεύοντας ένα μοντέλο μηχανικής μάθησης σε ιστορικά δεδομένα ελέγχου IT, το σύστημα μπορεί να μάθει να εντοπίζει πρότυπα κανονικής συμπεριφοράς. Οποιεσδήποτε αποκλίσεις από τα μαθησιακά πρότυπα μπορούν να επισημανθούν ως πιθανές ανωμαλίες όταν αναλύονται νέα δεδομένα. Αυτό μπορεί να βοηθήσει τους ελεγκτές να εντοπίσουν και να διερευνήσουν γρήγορα ύποπτες δραστηριότητες ή πιθανές παραβιάσεις ασφάλειας.

Μια άλλη εφαρμογή της μηχανικής μάθησης στον έλεγχο πληροφορικής είναι η προγνωστική ανάλυση. Τα μοντέλα μηχανικής μάθησης μπορούν να προσδιορίσουν τάσεις και μοτίβα που μπορεί να υποδεικνύουν μελλοντικούς κινδύνους ή τρωτά σημεία αναλύοντας ιστορικά δεδομένα σχετικά με συστήματα και διαδικασίες πληροφορικής. Αυτό μπορεί να βοηθήσει τους ελεγκτές να αντιμετωπίσουν προληπτικά πιθανά ζητήματα προτού κλιμακωθούν σε μεγάλα προβλήματα.

Επιπλέον, η μηχανική εκμάθηση μπορεί να χρησιμοποιηθεί για την αυτοματοποίηση επαναλαμβανόμενων εργασιών στον έλεγχο πληροφορικής, όπως η εξαγωγή και η ανάλυση δεδομένων. Εκπαιδεύοντας μοντέλα για την αναγνώριση και εξαγωγή σχετικών πληροφοριών από διάφορες πηγές, οι ελεγκτές μπορούν να εξοικονομήσουν χρόνο και να επικεντρωθούν σε πιο σύνθετες εργασίες που απαιτούν ανθρώπινη κρίση και τεχνογνωσία.

Επεξεργασία Φυσικής Γλώσσας στον Έλεγχο Πληροφορικής:

Η επεξεργασία φυσικής γλώσσας (NLP) είναι ο κλάδος της τεχνητής νοημοσύνης που εστιάζει στην αλληλεπίδραση μεταξύ υπολογιστών και ανθρώπινης γλώσσας. Στον έλεγχο πληροφορικής, το NLP μπορεί να χρησιμοποιηθεί για την ανάλυση μη δομημένων δεδομένων, όπως εκθέσεις ελέγχου, μηνύματα ηλεκτρονικού ταχυδρομείου και διαδικτυακό περιεχόμενο, εξάγοντας σχετικές πληροφορίες και εντοπίζοντας πιθανά ζητήματα.

Μια εφαρμογή του NLP στον έλεγχο πληροφορικής είναι η ανάλυση συναισθήματος. Οι αλγόριθμοι NLP μπορούν να εντοπίσουν θετικές ή αρνητικές τάσεις αναλύοντας τον τόνο και το συναίσθημα των αναφορών ελέγχου ή των σχολίων των πελατών. Αυτό μπορεί να βοηθήσει τους ελεγκτές να κατανοήσουν το συνολικό επίπεδο ικανοποίησης των συστημάτων και υπηρεσιών πληροφορικής και να εντοπίσουν τομείς προς βελτίωση.

Μια άλλη εφαρμογή του NLP στον έλεγχο πληροφορικής είναι η αναγνώριση οντοτήτων. Οι αλγόριθμοι NLP μπορούν να προσδιορίσουν και να ταξινομήσουν οντότητες, όπως ονόματα,

οργανισμούς ή τοποθεσίες που αναφέρονται σε εκθέσεις ελέγχου ή άλλα έγγραφα, αναλύοντας δεδομένα κειμένου. Αυτό μπορεί να βοηθήσει τους ελεγκτές να εντοπίζουν και να αναλύουν γρήγορα πληροφορίες που σχετίζονται με συγκεκριμένες οντότητες, βελτιώνοντας την αποτελεσματικότητα της διαδικασίας ελέγχου.

Επιπλέον, το NLP μπορεί να χρησιμοποιηθεί για την αυτοματοποίηση της κατηγοριοποίησης και της επισήμανσης εκθέσεων ελέγχου ή άλλων δεδομένων κειμένου. Εκπαιδεύοντας μοντέλα NLP για την αναγνώριση συγκεκριμένων λέξεων-κλειδιών ή θεμάτων, οι ελεγκτές μπορούν γρήγορα να ταξινομήσουν και να οργανώσουν μεγάλους όγκους πληροφοριών, διευκολύνοντας τον εντοπισμό σχετικών ευρημάτων και γνώσεων.

Συμπερασματικά, η χρήση εργαλείων και τεχνικών τεχνητής νοημοσύνης, όπως η μηχανική εκμάθηση και η επεξεργασία φυσικής γλώσσας, στον έλεγχο πληροφορικής μπορεί να ενισχύσει σημαντικά την αποδοτικότητα και την αποτελεσματικότητα της διαδικασίας ελέγχου. Αξιοποιώντας ιστορικά δεδομένα και προηγμένους αλγόριθμους, οι ελεγκτές μπορούν να αποκτήσουν πολύτιμες γνώσεις, να εντοπίσουν ανωμαλίες και να αντιμετωπίσουν προληπτικά πιθανούς κινδύνους. Η συνεχής πρόοδος της τεχνητής νοημοσύνης στον έλεγχο πληροφορικής υπόσχεται πολλά για το μέλλον του τομέα. **[27]**

Επιπλέον, σημαντικά εργαλεία που χρησιμοποιούνται σήμερα στην πράξη περιλαμβάνουν πλατφόρμες όπως το **MindBridge AI**, το οποίο εφαρμόζει τεχνικές μηχανικής μάθησης για την ανίχνευση ανωμαλιών σε οικονομικά δεδομένα, καθώς και το **CaseWare IDEA**, το οποίο αξιοποιείται για την ανάλυση μεγάλων όγκων συναλλαγών. Επίσης, εργαλεία όπως το **DataSnipper** ενσωματώνονται απευθείας σε εφαρμογές υπολογιστικών φύλλων, διευκολύνοντας τον ελεγκτή να συγκρίνει και να επιβεβαιώσει δεδομένα με μεγαλύτερη ταχύτητα και ακρίβεια. Η ενσωμάτωση αυτών των εργαλείων σε διαδικασίες IT audit ενισχύει την αποδοτικότητα και μειώνει την πιθανότητα ανθρώπινου λάθους.

6.2 Επιμόρφωση επαγγελματιών IT audit στην AI.

Η επιμόρφωση των επαγγελματιών IT audit στην τεχνητή νοημοσύνη (AI) είναι ζωτικής σημασίας, καθώς η ενσωμάτωση της AI στις διαδικασίες ελέγχου απαιτεί από τους ελεγκτές να αποκτήσουν νέες γνώσεις και δεξιότητες. Η σωστή επιμόρφωση θα τους επιτρέψει να χρησιμοποιούν αποτελεσματικά τις AI τεχνολογίες και να κατανοούν τις δυνατότητες, τους κινδύνους και τις ηθικές επιπτώσεις που συνεπάγεται η χρήση τους. Τα βασικά στοιχεία για την επιμόρφωση περιλαμβάνουν:

- **Βασικές γνώσεις για την τεχνητή νοημοσύνη:** Οι επαγγελματίες IT audit θα πρέπει να κατανοούν τις βασικές αρχές της AI, συμπεριλαμβανομένων των τύπων αλγορίθμων που χρησιμοποιούνται, όπως το machine learning, το deep learning και τα συστήματα αυτόματης μάθησης. Θα πρέπει επίσης να γνωρίζουν πώς λειτουργούν αυτά τα συστήματα και πώς να τα εφαρμόσουν σε περιβάλλον ελέγχου.
- **Εκπαίδευση σε AI-based εργαλεία:** Υπάρχουν διάφορα εργαλεία AI που χρησιμοποιούνται στο IT audit, όπως λογισμικά για την ανάλυση μεγάλων δεδομένων, αυτοματοποιημένες πλατφόρμες ανάλυσης κινδύνων, και εργαλεία ανίχνευσης απάτης. Οι ελεγκτές θα πρέπει να εκπαιδευτούν στη χρήση αυτών των εργαλείων για την ανάλυση δεδομένων και την εντοπισμό

αδύναμων σημείων στους ελέγχους, καθώς και στη διαμόρφωση των παραμέτρων για τη σωστή εφαρμογή τους.

- **Αντιμετώπιση ηθικών και κανονιστικών θεμάτων:** Οι επαγγελματίες IT audit θα πρέπει να εκπαιδευτούν για τις ηθικές προκλήσεις και τα κανονιστικά πλαίσια που σχετίζονται με τη χρήση της AI. Η κατανόηση του Κανονισμού (ΕΕ) 2024/1689 και των αρχών που αφορούν τη διαφάνεια, την αμεροληψία και την προστασία των δεδομένων είναι απαραίτητη για τη σωστή εφαρμογή της AI με υπευθυνότητα.
- **Συνεχής εκπαίδευση και ανάπτυξη:** Η AI είναι μια ταχέως εξελισσόμενη τεχνολογία. Οι επαγγελματίες του IT audit πρέπει να συμμετέχουν σε συνεχή εκπαίδευση για να ενημερώνονται για τις νέες τάσεις και εξελίξεις. Προγράμματα πιστοποίησης και εξειδικευμένα μαθήματα μπορούν να βοηθήσουν τους ελεγκτές να παραμείνουν ανταγωνιστικοί και καλά καταρτισμένοι στις τελευταίες τεχνολογίες.

Η επιμόρφωση είναι κρίσιμη για τη διασφάλιση ότι οι IT auditors μπορούν να ανταποκριθούν στις απαιτήσεις των νέων τεχνολογιών και να αξιοποιήσουν την AI με αποτελεσματικότητα και υπευθυνότητα.

7. Μελλοντικές Τάσεις

Το μέλλον της τεχνητής νοημοσύνης στον έλεγχο πληροφορικής

Η τεχνητή νοημοσύνη αναμένεται να διαδραματίσει ολοένα και πιο σημαντικό ρόλο στον έλεγχο πληροφορικής. Η προγνωστική ανάλυση, ο εντοπισμός ανωμαλιών και η αυτοματοποιημένη αξιολόγηση κινδύνου είναι μόνο ορισμένοι τομείς στους οποίους η τεχνητή νοημοσύνη θα συνεχίσει να έχει αντίκτυπο. Καθώς η τεχνολογία εξελίσσεται, οι ελεγκτές πληροφορικής πρέπει να παραμένουν ενημερωμένοι με τις τελευταίες τάσεις και εξελίξεις στην τεχνητή νοημοσύνη για να παραμείνουν σχετικοί στον τομέα.

7.1 Πρόβλεψη τάσεων στον έλεγχο τεχνητής νοημοσύνης και πληροφορικής

Ενώ είναι αδύνατο να προβλεφθεί το μέλλον με βεβαιότητα, πολλές τάσεις αναδύονται στον τομέα της τεχνητής νοημοσύνης και του ελέγχου της πληροφορικής. Αυτά περιλαμβάνουν τη χρήση εικονικών βοηθών με τεχνητή νοημοσύνη για ελεγκτές, τεχνολογία blockchain για ασφαλείς και διαφανείς ελέγχους και πλατφόρμες τεχνητής νοημοσύνης που βασίζονται σε cloud για πιο αποτελεσματική ανάλυση δεδομένων.

Οι εικονικοί βοηθοί με τεχνητή νοημοσύνη έχουν τη δυνατότητα να φέρουν επανάσταση στον τρόπο εργασίας των ελεγκτών. Αυτοί οι βοηθοί μπορούν να βοηθήσουν τους ελεγκτές να αυτοματοποιήσουν επαναλαμβανόμενες εργασίες, όπως η συλλογή και ανάλυση δεδομένων, επιτρέποντάς τους να επικεντρωθούν σε πιο σύνθετες και στρατηγικές πτυχές της εργασίας τους. Οι εικονικοί βοηθοί μπορούν επίσης να παρέχουν πληροφορίες και συστάσεις σε πραγματικό χρόνο με βάση τα δεδομένα που αναλύουν, βοηθώντας τους ελεγκτές να λαμβάνουν πιο ενημερωμένες αποφάσεις.

Η τεχνολογία Blockchain, με την αποκεντρωμένη και διαφανή φύση της, μπορεί να βελτιώσει σημαντικά την ασφάλεια και την ακεραιότητα των ελέγχων. Με τη χρήση του blockchain, οι ελεγκτές μπορούν να δημιουργήσουν ένα αμετάβλητο αρχείο των ιχνών ελέγχου, διασφαλίζοντας ότι οι πληροφορίες που συλλέγουν είναι ασφαλείς και αξιόπιστες. Αυτή η τεχνολογία μπορεί επίσης να επιτρέψει στους ελεγκτές να επαληθεύουν την αυθεντικότητα των δεδομένων και των συναλλαγών, μειώνοντας τον κίνδυνο απάτης και χειραγώγησης.

Οι πλατφόρμες τεχνητής νοημοσύνης που βασίζονται στο cloud προσφέρουν στους ελεγκτές τη δυνατότητα να αναλύουν μεγάλους όγκους δεδομένων γρήγορα και αποτελεσματικά. Αυτές οι πλατφόρμες αξιοποιούν τη δύναμη του υπολογιστικού νέφους για την επεξεργασία και ανάλυση δεδομένων σε πραγματικό χρόνο, παρέχοντας στους ελεγκτές πολύτιμες πληροφορίες και μοτίβα. Αξιοποιώντας την επεκτασιμότητα και τις υπολογιστικές δυνατότητες του cloud, οι ελεγκτές

μπορούν να εκτελούν πιο ολοκληρωμένους και ακριβείς ελέγχους, ακόμη και σε πολύπλοκα και διαφορετικά σύνολα δεδομένων.

Αναμένεται ότι τα επόμενα 5–10 χρόνια, η έννοια του **continuous auditing** θα ενισχυθεί ακόμη περισσότερο, με χρήση AI για **πραγματικό χρόνο ανάλυση δεδομένων** και αυτόματη δημιουργία αναφορών. Παράλληλα, τεχνολογίες όπως το **explainable AI (XAI)** θα είναι κρίσιμες, ώστε οι αλγόριθμοι να παρέχουν κατανοητές εξηγήσεις για τις αποφάσεις τους, ενισχύοντας τη διαφάνεια και τη συμμόρφωση.

7.2 Πώς η AI μπορεί να αλλάξει τον τρόπο διεξαγωγής των IT audits τα επόμενα χρόνια.

Η τεχνητή νοημοσύνη (AI) αναμένεται να επιφέρει μεγάλες αλλαγές στον τρόπο διεξαγωγής των IT audits τα επόμενα χρόνια, κάνοντας τις διαδικασίες πιο αποτελεσματικές και ακριβείς. Αυτές οι αλλαγές θα περιλαμβάνουν:

1. **Ανάλυση μεγάλων δεδομένων**: Η AI θα μπορεί να επεξεργάζεται τεράστιες ποσότητες δεδομένων πολύ πιο γρήγορα και λεπτομερώς από ό,τι οι άνθρωποι, χωρίς να χρειάζεται να γίνεται δειγματοληψία. Αυτό θα επιτρέψει στους ελεγκτές να εξετάζουν όλα τα δεδομένα μιας επιχείρησης, βελτιώνοντας σημαντικά την ακρίβεια των ελέγχων.
2. **Ανίχνευση ανωμαλιών**: Με τη χρήση αλγορίθμων μηχανικής μάθησης, η AI θα μπορεί να αναγνωρίζει ασυνήθιστες συμπεριφορές ή μοτίβα στα δεδομένα και τα συστήματα, εντοπίζοντας πιθανά σφάλματα ή απειλές πιο γρήγορα από τους παραδοσιακούς ελέγχους.
3. **Συνεχής παρακολούθηση**: Αντί οι έλεγχοι να γίνονται μία φορά το χρόνο ή ανά τακτά χρονικά διαστήματα, η AI θα μπορεί να παρακολουθεί τα συστήματα μιας εταιρείας συνεχώς, αναγνωρίζοντας προβλήματα σε πραγματικό χρόνο και διορθώνοντάς τα άμεσα.
4. **Αυτοματοποίηση επαναλαμβανόμενων διαδικασιών**: Εργασίες όπως η συλλογή και η επεξεργασία δεδομένων θα γίνονται αυτόματα από την AI, επιτρέποντας στους ελεγκτές να επικεντρώνονται σε πιο σημαντικά καθήκοντα που απαιτούν κρίση και ανάλυση. 5. **Αλλαγή του ρόλου του ελεγκτή**: Ο ρόλος του IT auditor θα αλλάξει, καθώς αντί να ασχολείται με χειροκίνητους ελέγχους, θα εστιάζει περισσότερο στη διαχείριση και την αξιολόγηση των αποτελεσμάτων που παράγει η AI, καθώς και στη στρατηγική λήψη αποφάσεων.
6. **Ενσωμάτωση νέων τεχνολογιών**: Καθώς οι νέες τεχνολογίες όπως το blockchain και τα κρυπτονομίσματα γίνονται πιο διαδεδομένες, η AI θα μπορεί να ενσωματώσει τη γνώση αυτών των τεχνολογιών στους ελέγχους, διασφαλίζοντας ότι καλύπτονται όλες οι νέες τεχνολογικές εξελίξεις.

Συνολικά, η τεχνητή νοημοσύνη θα αλλάξει τη φύση των IT audits, καθιστώντας τα πιο γρήγορα, ακριβή και συνεχώς ενεργά, ενώ οι ελεγκτές θα έχουν πιο σύνθετους και στρατηγικούς ρόλους, βοηθώντας στην κατανόηση και διαχείριση των τεχνολογικών κινδύνων.

Προετοιμασία για ένα Μέλλον Ελέγχου Πληροφορικής με γνώμονα το AI

Οι ελεγκτές πληροφορικής πρέπει να αγκαλιάσουν τη συνεχή μάθηση και την επαγγελματική εξέλιξη για να προετοιμαστούν για ένα μέλλον που βασίζεται στην τεχνητή νοημοσύνη. Θα πρέπει να εξοικειωθούν με τα εργαλεία και τις τεχνικές τεχνητής νοημοσύνης, να ενημερώνονται για τις βέλτιστες πρακτικές του κλάδου και να αναπτύξουν τις απαραίτητες δεξιότητες για την αποτελεσματική χρήση της τεχνητής νοημοσύνης στις ελεγκτικές πρακτικές τους.

Η συνεχής μάθηση είναι απαραίτητη για τους ελεγκτές IT ώστε να συμβαδίζουν με τις ραγδαίες εξελίξεις στην τεχνολογία AI. Θα πρέπει να αναζητούν ενεργά προγράμματα κατάρτισης, πιστοποιήσεις και εργαστήρια που εστιάζουν στην τεχνητή νοημοσύνη στον έλεγχο. Επεκτείνοντας τις γνώσεις και τις δεξιότητές τους στην τεχνητή νοημοσύνη, οι ελεγκτές μπορούν με σιγουριά να περιηγηθούν στο εξελισσόμενο τοπίο του ελέγχου πληροφορικής και να αξιοποιήσουν την τεχνητή νοημοσύνη για να βελτιώσουν το έργο τους.

Η συνεργασία και η ανταλλαγή γνώσεων εντός της ελεγκτικής κοινότητας είναι επίσης ζωτικής σημασίας για την προετοιμασία για ένα μέλλον που βασίζεται στην τεχνητή νοημοσύνη. Οι ελεγκτές πληροφορικής θα πρέπει να συμμετέχουν ενεργά σε επαγγελματικά δίκτυα, να παρακολουθούν συνέδρια και να συμμετέχουν σε συζητήσεις με ομοτίμους για την ανταλλαγή ιδεών και γνώσεων. Μαθαίνοντας ο ένας από τις εμπειρίες του άλλου και ανταλλάσσοντας βέλτιστες πρακτικές, οι ελεγκτές μπορούν συλλογικά να προσαρμοστούν στις μεταβαλλόμενες απαιτήσεις του κλάδου.

Η τεχνητή νοημοσύνη (AI) αναμένεται να φέρει σημαντικές αλλαγές στον τομέα του auditing τα επόμενα χρόνια, βελτιώνοντας την αποδοτικότητα, την ακρίβεια και την ευελιξία των ελέγχων. Μια από τις κύριες εξελίξεις θα είναι η δυνατότητα αυτοματοποιημένων, σε πραγματικό χρόνο ελέγχων, επιτρέποντας την παρακολούθηση των συναλλαγών και των δραστηριοτήτων μιας εταιρείας συνεχώς, αντί για περιοδικούς ελέγχους. Επιπλέον, η AI θα μπορεί να προβλέπει πιθανά προβλήματα μέσω της ανάλυσης ιστορικών δεδομένων, επιτρέποντας στους ελεγκτές να δρουν προληπτικά. Καθώς οι νέες τεχνολογίες, όπως το blockchain και τα κρυπτονομίσματα, γίνονται πιο διαδεδομένες, η AI θα προσαρμόζεται για να τις ενσωματώνει στους ελέγχους, διασφαλίζοντας την πλήρη κάλυψή τους. Η τεχνολογία αυτή θα μειώσει επίσης τα ανθρώπινα λάθη, καθώς η αυτοματοποίηση των επαναλαμβανόμενων διαδικασιών θα αυξήσει την ακρίβεια και την ταχύτητα των ελέγχων. Παρά την αυτοματοποίηση, η ανθρώπινη παρέμβαση θα παραμένει κρίσιμη, με τους ελεγκτές να λαμβάνουν κρίσιμες αποφάσεις και να χρησιμοποιούν την AI ως εργαλείο ανάλυσης και υποστήριξης. Ταυτόχρονα, η AI θα βελτιώσει τη διαφάνεια των ελέγχων, παρέχοντας σαφείς εξηγήσεις για τα αποτελέσματα και τις αποφάσεις που λαμβάνονται, ενώ θα λειτουργεί και ως εργαλείο διαχείρισης κινδύνων, εντοπίζοντας περιοχές ευπάθειας και προτείνοντας μέτρα για τη μείωση του κινδύνου. Τέλος, η AI θα ενισχύσει την ικανότητα των ελεγκτών να παρακολουθούν τη συμμόρφωση των οργανισμών με τις κανονιστικές απαιτήσεις σε πραγματικό χρόνο, διευκολύνοντας την έγκαιρη διόρθωση παραβάσεων. Συνολικά, η τεχνητή νοημοσύνη δεν θα

αντικαταστήσει τους ελεγκτές, αλλά θα βελτιώσει τον τρόπο που εργάζονται, καθιστώντας τους ελέγχους πιο ακριβείς, γρήγορους και αποτελεσματικούς.

8.Συμπεράσματα

8.1 Σύνοψη βασικών ευρημάτων

Η τεχνητή νοημοσύνη διαδραματίζει ολοένα και σημαντικότερο ρόλο στη διαδικασία ελέγχου των πληροφοριακών συστημάτων (IT audit). Η ενσωμάτωση έξυπνων αλγορίθμων και τεχνικών μηχανικής μάθησης έχει επιφέρει σημαντικές βελτιώσεις τόσο στην αποδοτικότητα όσο και στην ακρίβεια των ελέγχων. Η αυτοματοποίηση των διαδικασιών επιτρέπει τη γρήγορη και αποτελεσματική ανάλυση μεγάλου όγκου δεδομένων, μειώνοντας τα περιθώρια ανθρώπινου λάθους και επιταχύνοντας τις ελεγκτικές διαδικασίες.

Επιπλέον, η εφαρμογή των ελέγχων συμμόρφωσης SOC 2 ενισχύει τη διαφάνεια και την ασφάλεια των πληροφοριακών συστημάτων. Μέσα από αυστηρές προδιαγραφές και διαδικασίες αξιολόγησης, οι οργανισμοί διασφαλίζουν ότι πληρούν τα απαραίτητα κριτήρια για την προστασία των δεδομένων τους, ενισχύοντας παράλληλα την εμπιστοσύνη πελατών και συνεργατών.

Η ανάλυση κινδύνων και η χαρτογράφηση των ελέγχων αποτελούν θεμελιώδη στάδια για την επιτυχή προετοιμασία ενός ελέγχου. Η σωστή αναγνώριση και κατανόηση των πιθανών απειλών επιτρέπει την ανάπτυξη κατάλληλων στρατηγικών μετριασμού των κινδύνων, μειώνοντας τις πιθανότητες παραβίασης των δεδομένων ή δυσλειτουργιών στα πληροφοριακά συστήματα

8.2 Συμβολή της τεχνητής νοημοσύνης στη βελτίωση του IT audit.

Η τεχνητή νοημοσύνη (AI) αναδιαμορφώνει ουσιαστικά το πεδίο του IT audit, ενισχύοντας την αποδοτικότητα, την ακρίβεια και τη διαφάνεια των ελέγχων. Μέσω αλγορίθμων μηχανικής μάθησης και αυτοματοποιημένων εργαλείων, καθίσταται δυνατός ο εντοπισμός ανωμαλιών και πιθανών απειλών σε πραγματικό χρόνο, γεγονός που μειώνει σημαντικά τον κίνδυνο παραβιάσεων ασφαλείας. Μία από τις βασικές εφαρμογές της AI στον ελεγκτικό τομέα είναι η αυτοματοποίηση της ανάλυσης μεγάλων όγκων δεδομένων· αντί της χειροκίνητης επεξεργασίας, τα συστήματα AI μπορούν να διασταυρώνουν και να αξιολογούν πληροφορίες με υψηλή ακρίβεια, εντοπίζοντας αποκλίσεις ή ύποπτες συναλλαγές. Παράλληλα, η AI διευκολύνει την πρόβλεψη κινδύνων μέσω της ανάλυσης ιστορικών δεδομένων και της ανίχνευσης προτύπων που ενδέχεται να υποδηλώνουν επικείμενες απειλές, επιτρέποντας την έγκαιρη λήψη προληπτικών μέτρων. Επιπλέον, συμβάλλει ουσιαστικά στη συμμόρφωση με κανονιστικά πλαίσια και βέλτιστες πρακτικές, παρέχοντας αυτοματοποιημένη τεκμηρίωση και αναφορές, ενώ παράλληλα μειώνει τον διοικητικό φόρτο μέσω συνεχούς παρακολούθησης της εφαρμογής των ελέγχων. Σημαντικό είναι ότι η ενσωμάτωση της AI στο IT audit δεν αντικαθιστά τον ανθρώπινο παράγοντα· αντίθετα, ενισχύει τη δυνατότητα των ελεγκτών να λαμβάνουν τεκμηριωμένες και στρατηγικές αποφάσεις, αναβαθμίζοντας την ποιότητα και την ταχύτητα των ελεγκτικών διαδικασιών.

Σύμφωνα με πρόσφατες μελέτες, η χρήση εργαλείων AI στο auditing έχει οδηγήσει σε **αύξηση της αποδοτικότητας κατά 30–40%**, ενώ η ακρίβεια στην ανίχνευση ανωμαλιών βελτιώθηκε έως και **25%** σε σχέση με παραδοσιακές μεθόδους. Η δυνατότητα ανάλυσης δεδομένων σε πραγματικό χρόνο συμβάλλει στη μείωση του χρόνου εκτέλεσης ενός audit, ενώ παράλληλα ενισχύει την ικανότητα πρόβλεψης πιθανών κινδύνων.

8.3 Προτάσεις για μελλοντική έρευνα.

Η συνεχής εξέλιξη της τεχνητής νοημοσύνης και των πληροφοριακών συστημάτων δημιουργεί νέες προκλήσεις και ευκαιρίες για το IT audit. Για τον λόγο αυτό, η μελλοντική έρευνα θα μπορούσε να εστιάσει στους ακόλουθους τομείς:

- Ανάπτυξη προηγμένων αλγορίθμων ανίχνευσης απειλών: Η βελτίωση των τεχνικών μηχανικής μάθησης θα μπορούσε να ενισχύσει την ικανότητα των συστημάτων AI να εντοπίζουν νέες και άγνωστες απειλές στον κυβερνοχώρο.
- Διερεύνηση της ηθικής διάστασης της AI στο IT audit: Η χρήση τεχνητής νοημοσύνης στους ελέγχους συμμόρφωσης δημιουργεί ερωτήματα σχετικά με τη διαφάνεια, την προκατάληψη των αλγορίθμων και την ευθύνη λήψης αποφάσεων.
- Αυτοματοποιημένα συστήματα IT audit: Η μελέτη και η εφαρμογή πλήρως αυτοματοποιημένων ελέγχων θα μπορούσε να μειώσει τον απαιτούμενο χρόνο και κόστος για τους οργανισμούς, διατηρώντας παράλληλα υψηλή ακρίβεια.
- Ενσωμάτωση AI με blockchain για μεγαλύτερη ασφάλεια: Ο συνδυασμός αυτών των τεχνολογιών θα μπορούσε να αυξήσει τη διαφάνεια και την ασφάλεια των διαδικασιών IT audit, διασφαλίζοντας την ακεραιότητα των δεδομένων.
- Δυναμικά συστήματα συμμόρφωσης: Η ανάπτυξη συστημάτων που προσαρμόζονται αυτόματα στις μεταβαλλόμενες ρυθμιστικές απαιτήσεις θα μπορούσε να βελτιώσει τη διαχείριση της συμμόρφωσης για τους οργανισμούς.

Η έρευνα σε αυτούς τους τομείς μπορεί να συμβάλει στη διαμόρφωση ενός πιο εξελιγμένου και αποτελεσματικού πλαισίου IT audit, που θα ανταποκρίνεται στις διαρκώς μεταβαλλόμενες απαιτήσεις της τεχνολογίας και της κυβερνοασφάλειας.

9. Βιβλιογραφία

1. **Ν. Τσέλιος, *Εισαγωγή στην Τεχνητή Νοημοσύνη*. Θεσσαλονίκη, Ελλάδα: Εκδόσεις Τζιόλα, 2019.**
2. **ISO Experts, "ISO 27001:2022," [Online]. Available: https://isoexperts.gr/our-services/iso-iec-27001-2022/** [Accessed: Nov. 2024].
3. **Udemy, "IT Audit Complete Course.[Online].Available:** https://www.udemy.com/course/it-audit-completecourse/learn/lecture/36049760?start=0#overview [Accessed: Oct. , 2024].
4. **Sprinto, "SOC 2 Report Examples (Broken down into each section)." [Online]. Available:** https://sprinto.com/blog/soc-2report-example/ [Accessed: Nov. , 2024].
5. **Sprinto, "SOC 2 Audit: A Way to Ensuring Data Security." [Online]. Available:** https://sprinto.com/blog/soc-2-audit/ [Accessed: Nov. , 2024].
6. **Zapier, "IT Audit Checklist." [Online]. Available:** https://cdn.zapier.com/storage/files/f6c3c258624c2aa92cea49bc5fcb7749.pdf [Accessed: Nov. , 2024].
7. **G2, "Τι είναι ο έλεγχος πληροφορικής; Ένας οριστικός οδηγός για την προστασία των δεδομένων σας," [Online]. Available: https://track.g2.com/resources/it-audit** [Accessed: Oct. 2024].
8. **Audit Guru, "What Are The Types of IT Audits?" [Online]. Available: https://audit.guru/what-are-the-types-of-it-audits/** [Accessed: Apr. 2025].
9. **Wikipedia, "Certified Public Accountant," [Online]. Available: https://en.wikipedia.org/wiki/Certified_Public_Accountant** [Accessed: Jan. 2025].
10. **Thoropass, "What is SOC 1 compliance?" [Online]. Available: https://thoropass.com/blog/compliance/what-is-soc-1-compliance/** [Accessed: Apr. 2025].
11. **Vanta, "SOC 2 compliance requirements: What does SOC 2 compliance involve?" [Online]. Available: https://www.vanta.com/collection/soc-2/soc-2-compliance-requirements** [Accessed: Apr. 2025].
12. **Sprinto, "SOC 2 Audit: A Way to Ensuring Data Security," [Online]. Available: https://sprinto.com/blog/soc-2-audit/** [Accessed: Nov. 2024].
13. **Sprinto, "SOC 2 Report Examples (Broken down into each section)," [Online]. Available: https://sprinto.com/blog/soc-2-report-example/** [Accessed: Nov. 2024].
14. **Secureframe, "A Real-World SOC 2 Report Example," [Online]. Available: https://secureframe.com/hub/soc-2/report-example** [Accessed: Dec. 2024].
15. **Wikipedia, "ISO/IEC 27001," [Online]. Available: https://en.m.wikipedia.org/wiki/ISO/IEC_27001** [Accessed: Nov. 2024].
16. **OpenAI, "Powered by ChatGPT," [Online]. Available: https://chatgpt.com/** [Accessed: Dec. 2024].
17. **SAP, "Τι είναι η τεχνητή νοημοσύνη;" [Online]. Available: https://www.sap.com/greece/products/artificial-intelligence/what-is-artificial-intelligence.html** [Accessed: Dec. 2024].

18. **Wolters Kluwer, "Internal audit's role in the new European Union's Artificial Intelligence Act," [Online]. Available:** https://www.wolterskluwer.com/en/expert-insights/internal-audits-role-new-european-union-ai-act [Accessed: Jun. 2025].
19. **S. Ahmedislam, "Help of Artificial Intelligence to the Audit Profession," LinkedIn, [Online]. Available:** https://www.linkedin.com/pulse/help-artificial-intelligence-audit-profession-salih-ahmedislam/ [Accessed: Jun. 2025].
20. **UiPath, "Modernizing risk management: How AI-powered automation is redefining audit and controls testing," [Online]. Available:** https://www.uipath.com/blog/industry-solutions/modernizing-risk-management-redefining-audit-and-controls-testing [Accessed: Jun. 2025].
21. **C. Todorov, "The Rise of Technology in Auditing - How AI is Transforming the Audit Process in Europe," LinkedIn, [Online]. Available:** https://www.linkedin.com/pulse/rise-technology-auditing-how-ai-transforming-audit-process-todorov-cdy7f/ [Accessed: Jun. 2025].
22. **DataSnipper, "The AI Revolution in Audit and Finance," [Online]. Available:** https://cdn.prod.website-files.com/60816e54c89f06e2dcc2e65c/66684af416972d38ae1ee62c_DataSnipper%20AI%20Report%202024%20(1).pdf [Accessed: Jun. 2025].
23. **Centraleyes, "AI Auditing: Ensuring Ethical and Efficient AI Systems," [Online]. Available:** https://www.centraleyes.com/ai-auditing/ [Accessed: Jun. 2025].
24. **Vanta, "ISO 27001 vs. SOC 2: What is the difference?" [Online]. Available:** https://www.vanta.com/collection/soc-2/iso-27001-vs-soc-2 [Accessed: Apr. 2025].
25. ***Journal of Accounting, Ethics and Public Policy*, "Artificial Intelligence (AI) Ethics in Accounting," [Online]. Available:** https://www.jaepp.org/index.php/jaepp/article/download/349/329/445 [Accessed: Jun. 2025].
26. **OpenAI, "Powered by ChatGPT," [Online]. Available:** https://chatgpt.com/ [Accessed: Jul. 2025].
27. **Audit Guru, "Artificial Intelligence in IT Auditing," [Online]. Available:** https://audit.guru/artificial-intelligence-in-it-auditing/ [Accessed: Jul. 2025].