



# Ελεγκτική Λογιστική

Ν. Ηρειώτης / Ι. Πλουμπής

# Βασικά χαρακτηριστικά μαθήματος

## Ελεγκτική Λογιστική

1. Εισαγωγή στην Ελεγκτική και τον Εξωτερικό Έλεγχο (External Audit)
2. Εισαγωγή στην Εταιρική Διακυβέρνηση και τον Εσωτερικό Έλεγχο (Corporate Governance & Internal Audit)
3. Εισαγωγή στο Σύστημα Εσωτερικού Ελέγχου ( COSO Integrated Framework )
4. Πρακτικά Παραδείγματα - Case Studies Ελεγκτικών Εργασιών (Μέρος 1ο)
5. Πρακτικά Παραδείγματα - Case Studies Ελεγκτικών Εργασιών (Μέρος 2ο)

# Διδακτικές Ενότητες

## 1. Εισαγωγή στην Ελεγκτική και τον Εξωτερικό Έλεγχο (External Audit)

- Ορισμός και Σκοπός του Εξωτερικού Ελέγχου
- Τι είναι ο εξωτερικός έλεγχος και ποιος είναι ο ρόλος του.
- Διαφορές μεταξύ εξωτερικού και εσωτερικού ελέγχου.
- Το Ρυθμιστικό Πλαίσιο του Εξωτερικού Ελέγχου
- Διεθνή Ελεγκτικά Πρότυπα (ISA – International Standards on Auditing).
- Κανονισμοί από φορείς όπως το IFAC (International Federation of Accountants).
- Βασικές Αρχές και Διαδικασίες Εξωτερικού Ελέγχου
- Προγραμματισμός Ελέγχου (Audit Planning).
- Αξιολόγηση Κινδύνων και Σχεδιασμός Δοκιμών (Risk Assessment & Testing Strategy).
- Αποδεικτικά στοιχεία και τεκμηρίωση (Audit Evidence & Documentation).
- Έκθεση Ελέγχου (Audit Report).
- Ανεξαρτησία και Ηθική του Ελεγκτή
- Ο ρόλος της ανεξαρτησίας των εξωτερικών ελεγκτών.
- Ηθικά διλήμματα και επαγγελματική δεοντολογία (IESBA Code of Ethics).
- Επιπτώσεις του Εξωτερικού Ελέγχου στις Επιχειρήσεις
- Πώς ο εξωτερικός έλεγχος συμβάλλει στη διαφάνεια και στη χρηματοοικονομική σταθερότητα.

# Διδακτικές Ενότητες

## 2. Εισαγωγή στην Εταιρική Διακυβέρνηση και τον Εσωτερικό Έλεγχο (Corporate Governance & Internal Audit)

- Ορισμός και Σημασία της Εταιρικής Διακυβέρνησης
- Τι είναι η εταιρική διακυβέρνηση και πώς συνδέεται με τη χρηστή διοίκηση.
- Θεσμικό και κανονιστικό πλαίσιο (OECD Principles of Corporate Governance).
- Ο ρόλος των Διοικητικών Συμβουλίων & Επιτροπών Ελέγχου
- Καθήκοντα των ανεξάρτητων μελών και της Επιτροπής Ελέγχου.
- Συνεργασία μεταξύ εξωτερικών ελεγκτών και διοικητικών συμβουλίων.
- Εισαγωγή στον Εσωτερικό Έλεγχο (Internal Audit)
- Τι είναι ο εσωτερικός έλεγχος και πώς διαφέρει από τον εξωτερικό έλεγχο.
- Βασικές αρχές και πρακτικές του IIA (Institute of Internal Auditors).
- Ο Εσωτερικός Έλεγχος ως Μηχανισμός Διαχείρισης Κινδύνων
- Ο ρόλος του εσωτερικού ελέγχου στην ανίχνευση και πρόληψη απάτης (Fraud Detection & Prevention).
- Σύνδεση με το Σύστημα Εσωτερικού Ελέγχου (Internal Control System - ICS).

# Διδακτικές Ενότητες

## 3. Εισαγωγή στο Σύστημα Εσωτερικού Ελέγχου (COSO Integrated Framework)

- Τι είναι το COSO και γιατί είναι σημαντικό
- Ανάλυση του COSO (Committee of Sponsoring Organizations of the Treadway Commission).
- Εξέλιξη του COSO Framework από το 1992 έως σήμερα.
- Τα Πέντε Στοιχεία του Συστήματος Εσωτερικού Ελέγχου (COSO Framework)
- Περιβάλλον Ελέγχου (Control Environment).
- Αξιολόγηση Κινδύνων (Risk Assessment).
- Δραστηριότητες Ελέγχου (Control Activities).
- Πληροφόρηση και Επικοινωνία (Information & Communication).
- Παρακολούθηση και Βελτίωση (Monitoring Activities).
- Εφαρμογές του COSO στην Πρακτική
- Πώς εφαρμόζεται το COSO Framework σε εταιρείες και οργανισμούς.
- Παραδείγματα πραγματικών περιπτώσεων.
- Σχέση COSO & SOX (Sarbanes-Oxley Act)
- Ο ρόλος του COSO στη συμμόρφωση με τη νομοθεσία Sarbanes-Oxley (SOX).

# Διδακτικές Ενότητες

## 4. Πρακτικά Παραδείγματα - Case Studies Ελεγκτικών Εργασιών (Μέρος 1ο)

Η ανάλυση πραγματικών περιπτώσεων (case studies) είναι ένας από τους πιο αποτελεσματικούς τρόπους κατανόησης των ελεγκτικών διαδικασιών και των προκλήσεων που αντιμετωπίζουν οι ελεγκτές. Στο πρώτο μέρος εστιάζουμε στην Έναρξη και τον Σχεδιασμό του ελέγχου καθώς και στην Υλοποίηση ελεγκτικών διαδικασιών στις παρακάτω περιοχές:

- Πάγια και Λοιπός Εξοπλισμός
- Αποθέματα και Αγορές
- Ταμειακά Διαθέσιμα

# Διδακτικές Ενότητες

## 5. Πρακτικά Παραδείγματα - Case Studies Ελεγκτικών Εργασιών (Μέρος 2ο)

Η ανάλυση πραγματικών περιπτώσεων (case studies) είναι ένας από τους πιο αποτελεσματικούς τρόπους κατανόησης των ελεγκτικών διαδικασιών και των προκλήσεων που αντιμετωπίζουν οι ελεγκτές. Στο δεύτερο μέρος εστιάζουμε στην Ολοκλήρωση του ελέγχου και την Κατάρτιση της σχετικής αναφοράς (έκθεσης ελέγχου) ενώ ταυτόχρονα εξετάζουμε τις ελεγκτικές διαδικασίες στις παρακάτω περιοχές:

- Απαιτήσεις και Έσοδα
- Έξοδα και Υποχρεώσεις

# Τι είναι το COSO και γιατί είναι σημαντικό

Το COSO (Committee of Sponsoring Organizations of the Treadway Commission) είναι ένα διεθνώς αναγνωρισμένο πλαίσιο που βοηθά τους οργανισμούς να σχεδιάζουν, να εφαρμόζουν και να αξιολογούν τα συστήματα εσωτερικού ελέγχου και διαχείρισης κινδύνου.

Το COSO αποτελεί πρωτοβουλία πέντε μεγάλων επαγγελματικών οργανώσεων των ΗΠΑ (όπως το AICPA) και σχεδιάστηκε για να προωθήσει:

- Τη διακυβέρνηση
- Τη διαχείριση κινδύνου
- Την αποτελεσματικότητα του εσωτερικού ελέγχου
- Τη συμμόρφωση με κανονιστικά πλαίσια

Το πιο γνωστό του μοντέλο είναι το "COSO Internal Control – Integrated Framework", το οποίο περιγράφει πέντε βασικά στοιχεία ενός αποτελεσματικού συστήματος εσωτερικού ελέγχου.

# Τι είναι το COSO και γιατί είναι σημαντικό

Γιατί είναι σημαντικό το COSO;

Διασφαλίζει την αξιοπιστία των οικονομικών καταστάσεων

Μειώνει τον κίνδυνο απάτης και λαθών

Υποστηρίζει την επίτευξη επιχειρηματικών στόχων

Ενισχύει τη συμμόρφωση με νόμους όπως ο Sarbanes-Oxley Act (SOX)

Προάγει διαρκή βελτίωση μέσω της παρακολούθησης

# Ανάλυση του COSO (Committee of Sponsoring Organizations of the Treadway Commission)

Το COSO (Committee of Sponsoring Organizations of the Treadway Commission) ιδρύθηκε το 1985 στις ΗΠΑ με σκοπό την πρόληψη της απάτης στις χρηματοοικονομικές αναφορές και τη βελτίωση της εταιρικής διακυβέρνησης. Παρόλο που ξεκίνησε για λόγους ελέγχου λογιστικών απατών, εξελίχθηκε σε πλαίσιο διαχείρισης επιχειρηματικών κινδύνων και εσωτερικού ελέγχου που χρησιμοποιείται διεθνώς.

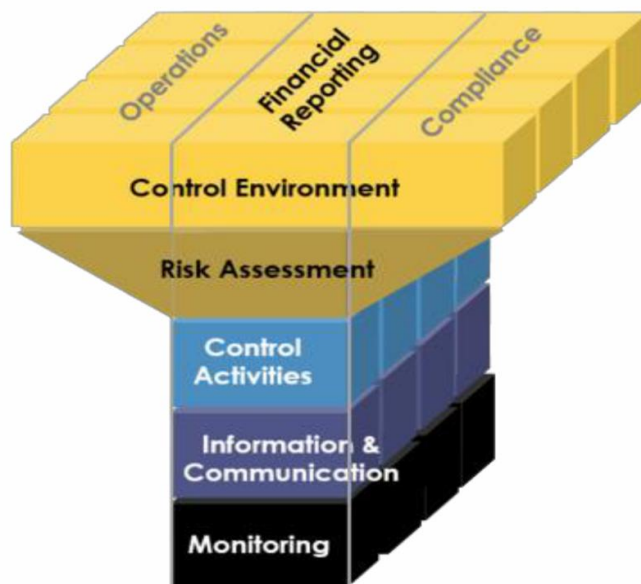
## Πλαίσιο Περιγραφή

COSO - Internal Control (2013) - Πλαίσιο Εσωτερικού Ελέγχου για τον σχεδιασμό, εφαρμογή και αξιολόγηση του ελέγχου

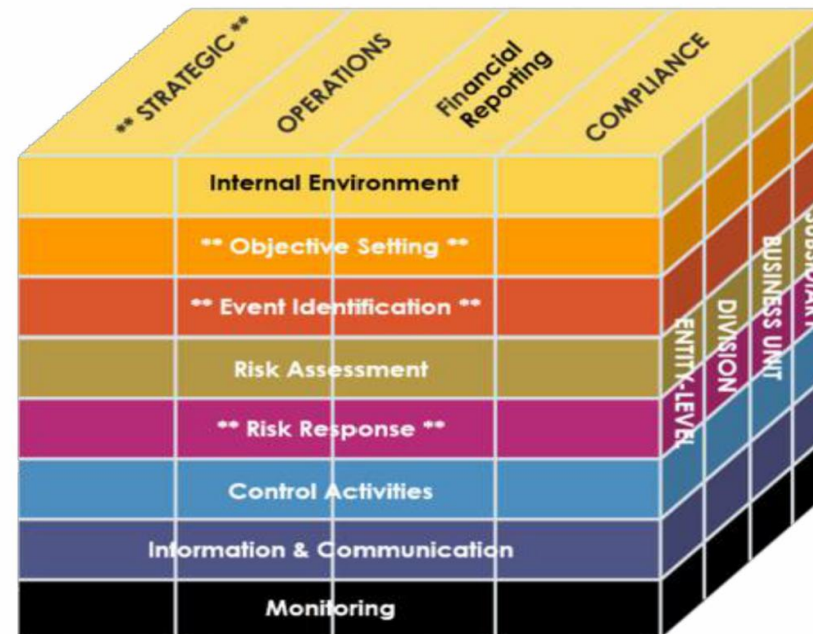
COSO - Enterprise Risk Management (ERM) (2017)-Πλαίσιο Διαχείρισης Επιχειρηματικών Κινδύνων (συνδέεται με στρατηγικούς στόχους)

# Ανάλυση του COSO (Committee of Sponsoring Organizations of the Treadway Commission)

**"SOX"**  
COSO 2013 Framework



**"ERM"**  
COSO 2004 ERM Framework



# Ανάλυση του COSO (Committee of Sponsoring Organizations of the Treadway Commission)



**COSO Cube (2013 Edition)**

\*Ο κύβος COSO απεικονίζει τρεις διαστάσεις που συνδυάζονται για να προσδιορίσουν το σύστημα εσωτερικού ελέγχου

# Ανάλυση του COSO (Committee of Sponsoring Organizations of the Treadway Commission)

Αποτελείται από 5 Συστατικά και 17 Αρχές (Principles).

## **Περιβάλλον Ελέγχου (Control Environment)**

- Αξίες, ηγεσία, οργανωτική δομή

## **Αξιολόγηση Κινδύνου (Risk Assessment)**

- Εντοπισμός, ανάλυση και διαχείριση κινδύνων

## **Δραστηριότητες Ελέγχου (Control Activities)**

- Πολιτικές και διαδικασίες για την άμβλυνση των κινδύνων

## **Πληροφορία & Επικοινωνία (Information & Communication)**

- Ροή σχετικών και αξιόπιστων πληροφοριών

## **Παρακολούθηση (Monitoring Activities)**

- Συνεχής ή περιοδικός έλεγχος και βελτίωση

# Εξέλιξη του COSO Framework από το 1992 έως σήμερα

## 1. COSO 1992 – Internal Control: Integrated Framework

Η πρώτη έκδοση του πλαισίου εισήχθη το 1992. Ήταν η πρώτη οργανωμένη προσπάθεια να τυποποιηθεί το σύστημα εσωτερικού ελέγχου, με στόχο:

- Τη διασφάλιση αξιοπιστίας οικονομικών αναφορών
- Τη συμμόρφωση με νόμους
- Τη λειτουργική αποτελεσματικότητα

## 2. COSO 2004 – Enterprise Risk Management (ERM) Framework

Το 2004, η COSO επεκτείνει την προσέγγισή της με το ERM – Integrated Framework, εισάγοντας:

- Τη σύνδεση διαχείρισης κινδύνου με στρατηγική
- 8 συστατικά ERM (π.χ. objective setting, risk response)
- Εστίαση στον “risk appetite” και “risk tolerance”

Αυτό το μοντέλο θεωρήθηκε επαναστατικό, αλλά θεωρήθηκε και περίπλοκο για πολλούς οργανισμούς.

# Εξέλιξη του COSO Framework από το 1992 έως σήμερα

## 3. COSO 2013 – Αναθεώρηση Internal Control Framework

Η έκδοση του 2013 ενημέρωσε την αρχική έκδοση του 1992. Περιλαμβάνει:

- 17 βασικές αρχές εσωτερικού ελέγχου
- Ενσωμάτωση νέων τεχνολογιών, κανονισμών και ψηφιακού περιβάλλοντος
- Ευθυγράμμιση με τον Sarbanes-Oxley Act (SOX)

## 4. COSO 2017 – Enterprise Risk Management (ERM): Integrating with Strategy and Performance

Η πιο πρόσφατη επαναστατική ανανέωση του ERM ήρθε το 2017, με έμφαση στη:

- Ευθυγράμμιση διαχείρισης κινδύνου με στρατηγική & επίδοση
- Ενίσχυση της εταιρικής κουλτούρας κινδύνου
- Δομή 5 στοιχείων και 20 αρχών
- Δυναμική προσέγγιση με συνεχείς κύκλους βελτίωσης

# Τα Πέντε Στοιχεία του Συστήματος Εσωτερικού Ελέγχου (COSO Framework)

## Περιβάλλον Ελέγχου (Control Environment)

Αποτελεί τη **βάση** για όλα τα υπόλοιπα στοιχεία. Περιλαμβάνει:

- Ηγεσία με **ηθικές αξίες**
- **Δομή οργανισμού** & κατανομή αρμοδιοτήτων
- **Δέσμευση** στη γνώση, στην ανεξαρτησία και στον έλεγχο

📌 *Παράδειγμα:* Η Διοίκηση καθορίζει πολιτικές ηθικής και ενθαρρύνει υπεύθυνη συμπεριφορά.

## Εκτίμηση Κινδύνου (Risk Assessment)

Αφορά τη διαδικασία με την οποία ο οργανισμός:

- **Αναγνωρίζει** και **αξιολογεί** πιθανούς κινδύνους
- **Συσχετίζει κινδύνους με στόχους**
- Αντιμετωπίζει **απάτες** και **εξωτερικές απειλές**

📌 *Παράδειγμα:* Ανάλυση κινδύνου για απώλεια δεδομένων σε περιβάλλον cloud.

# Τα Πέντε Στοιχεία του Συστήματος Εσωτερικού Ελέγχου (COSO Framework)

## Δραστηριότητες Ελέγχου (Control Activities)

Οι πολιτικές και οι διαδικασίες που καθιερώνει ένας οργανισμός ώστε:

- Να μειώνει τους κινδύνους
- Να εξασφαλίζει την εκτέλεση αποφάσεων
- Να εφαρμόζει τεχνολογικούς και χειροκίνητους ελέγχους

 *Παράδειγμα:* Εγκρίσεις πληρωμών άνω ενός ποσού από διπλό έλεγχο.

## Πληροφορία και Επικοινωνία (Information and Communication)

Το στοιχείο αυτό διασφαλίζει ότι:

- Οι σωστές πληροφορίες μεταφέρονται στους κατάλληλους ανθρώπους
- Υπάρχουν κατάλληλα συστήματα αναφορών
- Η κάθετη και οριζόντια επικοινωνία είναι ενεργή

 *Παράδειγμα:* Η Διεύθυνση Οικονομικών ενημερώνει άμεσα για αλλαγές στις λογιστικές πολιτικές.

# Τα Πέντε Στοιχεία του Συστήματος Εσωτερικού Ελέγχου (COSO Framework)

## Δραστηριότητες Παρακολούθησης (Monitoring Activities)

Αναφέρεται στη **συνεχή ή περιοδική αξιολόγηση** του εσωτερικού ελέγχου. Περιλαμβάνει:

- **Δείκτες επίδοσης**
- **Αναφορές ελέγχου**
- **Διορθωτικές ενέργειες**

*Παράδειγμα:* Ετήσιος εσωτερικός έλεγχος συμμόρφωσης με GDPR.

## Πώς συνεργάζονται τα 5 στοιχεία;

Σκέψου το COSO σαν **οργανωμένο δίκτυο**:







- Το **Περιβάλλον Ελέγχου** είναι η βάση.
- Η **Εκτίμηση Κινδύνου** προσδιορίζει τους κινδύνους.
- Οι **Δραστηριότητες Ελέγχου** είναι οι άμυνες.
- Η **Πληροφορία & Επικοινωνία** ενώνει τα τμήματα.
- Η **Παρακολούθηση** εξασφαλίζει ότι όλα λειτουργούν σωστά.

# Περιβάλλον Ελέγχου (Control Environment)

Το Περιβάλλον Ελέγχου (Control Environment) είναι το πρώτο και θεμελιώδες στοιχείο του πλαισίου COSO για τον Εσωτερικό Έλεγχο. Ουσιαστικά, είναι το "DNA" ενός οργανισμού ως προς την κουλτούρα ελέγχου, τις αξίες, τη δομή, και τη συμπεριφορά της ηγεσίας.

Το Control Environment καθορίζει το “τόνο από την κορυφή” (tone at the top) και αντανακλά τον χαρακτήρα και τις αξίες της διοίκησης. Είναι το θεμέλιο πάνω στο οποίο στηρίζονται όλα τα άλλα στοιχεία ελέγχου.

## Ενότητα

-  Ακεραιότητα και Ηθικές Αξίες
-  Διοικητική Δομή & Αρμοδιότητες
-  Δέσμευση στην Ικανότητα
-  Διοικητικό Συμβούλιο & Εποπτεία
-  Ανάθεση Αρμοδιοτήτων και Εξουσιοδοτήσεις
-  Πολιτικές Ελέγχου Ανθρώπινου Δυναμικού

## Περιγραφή

Η διοίκηση προωθεί διαφάνεια, ειλικρίνεια και εντιμότητα  
Καθαρός διαχωρισμός αρμοδιοτήτων και λογοδοσίας  
Επιλογή και εκπαίδευση προσωπικού με τις κατάλληλες ικανότητες  
Ανεξάρτητη και ισχυρή εποπτεία του οργανισμού  
Σαφής κατανομή καθηκόντων και εξουσιών  
Η κουλτούρα του οργανισμού αντικατοπτρίζεται στη διαχείριση του προσωπικού

# Αξιολόγηση Κινδύνων (Risk Assessment)

Η Αξιολόγηση Κινδύνων (Risk Assessment) είναι το δεύτερο βασικό στοιχείο του πλαισίου COSO Internal Control Framework και αποτελεί έναν κρίσιμο πυλώνα για τον εντοπισμό, την κατανόηση και την αντιμετώπιση των κινδύνων που απειλούν την επίτευξη των στόχων ενός οργανισμού.

Η Risk Assessment είναι η διαδικασία μέσω της οποίας ένας οργανισμός:

- Καθορίζει στόχους (operational, reporting, compliance)
- Εντοπίζει κινδύνους που μπορεί να παρεμποδίσουν την επίτευξη αυτών των στόχων
- Αναλύει τη φύση, την πιθανότητα και τις επιπτώσεις αυτών των κινδύνων
- Προσδιορίζει απατεωνικές δραστηριότητες (fraud risk)

# Αξιολόγηση Κινδύνων (Risk Assessment)

Τύποι Κινδύνων που Εξετάζονται:

- Λειτουργικοί Κίνδυνοι (Operational Risks)
- Οικονομικοί / Λογιστικοί (Financial Reporting Risks)
- Κανονιστικοί (Compliance Risks)
- Τεχνολογικοί (Cybersecurity, IT)
- Στρατηγικοί Κίνδυνοι (Strategy misalignment, market shifts)

Εργαλεία και Μέθοδοι:

- SWOT Analysis
- Risk Matrix (πιθανότητα x σοβαρότητα)
- Monte Carlo Simulation (σε πιο εξελιγμένες αναλύσεις)
- Workshops & Interviews με προσωπικό
- Fraud Tree από το ACFE






# Δραστηριότητες Ελέγχου (Control Activities)

Οι Δραστηριότητες Ελέγχου (Control Activities) είναι το τρίτο βασικό στοιχείο του πλαισίου COSO Internal Control Framework και αναφέρονται σε όλες εκείνες τις πολιτικές, διαδικασίες και ενέργειες που εφαρμόζονται για να μειώσουν ή να εξαλείψουν τους κινδύνους που εντοπίζονται κατά την Αξιολόγηση Κινδύνων (Risk Assessment).

Οι Control Activities είναι:

- Συγκεκριμένες ενέργειες πρόληψης ή ανίχνευσης σφαλμάτων και παρατυπιών
- Ενσωματωμένες σε όλες τις λειτουργίες (λειτουργικές, οικονομικές, κανονιστικές)
- Χειροκίνητες ή αυτοματοποιημένες

# Δραστηριότητες Ελέγχου (Control Activities)

Κατηγορία	Παράδειγμα
 Εγκρίσεις	Έγκριση δαπανών από υπεύθυνο πριν από την πληρωμή
 Επαληθεύσεις	Διασταύρωση στοιχείων προμηθευτών με Τιμολόγια
 Αναλύσεις	Συγκριτική ανάλυση προϋπολογισμού με πραγματικά δεδομένα
 Καταμετρήσεις	Απογραφή υλικών ή μετρητών
 Διαχωρισμός Καθηκόντων (Segregation of Duties)	Το ίδιο άτομο δεν εκτελεί και πληρώνει τιμολόγια

# Πληροφόρηση και Επικοινωνία (Information & Communication).

Η Πληροφόρηση και Επικοινωνία (Information & Communication) είναι το τέταρτο στοιχείο του πλαισίου COSO Internal Control και λειτουργεί ως νευρικό σύστημα για τη λειτουργία των υπολοίπων στοιχείων ελέγχου. Στόχος της είναι να εξασφαλίζει τη ροή αξιόπιστης, έγκαιρης και σχετικής πληροφορίας στα κατάλληλα άτομα, τόσο εντός όσο και εκτός του οργανισμού.

## Πηγές και Ροή Πληροφόρησης

- Εσωτερικά συστήματα πληροφορικής (π.χ. ERP, CRM)
- Αναφορές προσωπικού, οικονομικών, συμμόρφωσης
- Διαύλους επικοινωνίας όπως email, intranet, dashboards, reports
- Εκπαίδευση και ενημέρωση προσωπικού σε πολιτικές και διαδικασίες

# Παρακολούθηση και Βελτίωση (Monitoring Activities)

Η Παρακολούθηση και Βελτίωση (Monitoring Activities) είναι το πέμπτο και τελευταίο στοιχείο του πλαισίου COSO Internal Control Framework. Παίζει κρίσιμο ρόλο στην εξασφάλιση της συνεχούς αποτελεσματικότητας του συστήματος εσωτερικού ελέγχου, βοηθώντας τους οργανισμούς να εντοπίζουν προβλήματα και να τα διορθώνουν έγκαιρα και ουσιαστικά.

Η παρακολούθηση αφορά τη συνεχή αξιολόγηση ή την περιοδική επανεξέταση του τρόπου λειτουργίας των εσωτερικών ελέγχων. Η βελτίωση είναι η διαδικασία κατά την οποία διορθώνονται οι αδυναμίες που εντοπίζονται. Το ζητούμενο δεν είναι μόνο να υπάρχουν έλεγχοι, αλλά να λειτουργούν σωστά και διαχρονικά.

# Παρακολούθηση και Βελτίωση (Monitoring Activities)

## Ο Στόχος: «Κλείσιμο του Κύκλου»

Η παρακολούθηση αποτελεί το τελικό αλλά και επαναλαμβανόμενο στάδιο που:

- Ελέγχει την ποιότητα και τη συνέπεια των ελέγχων
- Τροφοδοτεί με πληροφορία τις διορθωτικές ενέργειες
- Υποστηρίζει την κουλτούρα βελτίωσης και λογοδοσίας

Σύνδεση με τα άλλα στοιχεία του COSO:

- Risk Assessment: Αν εντοπιστεί νέος κίνδυνος, επαναξιολογείται
- Control Activities: Αν δεν λειτουργούν σωστά, επανασχεδιάζονται
- Information & Communication: Η επικοινωνία ευρημάτων είναι απαραίτητη

# Εφαρμογές του COSO στην Πρακτική

## Εφαρμογή στην Τραπεζική – Citibank (ΗΠΑ)

Μετά το 2008, πολλές τράπεζες ενίσχυσαν το εσωτερικό τους σύστημα ελέγχου. Η Citibank εφάρμοσε το COSO για:

- Ανίχνευση λειτουργικών κινδύνων (π.χ. cyber threats)
- Ενσωμάτωση ERM στη στρατηγική λήψης αποφάσεων
- Συμμόρφωση με SOX & Basel II

## Εφαρμογή στο Δημόσιο – Υπουργεία Οικονομικών (Ελλάδα & Ε.Ε.)

Το COSO χρησιμοποιείται για την:

- Καταπολέμηση της διαφθοράς και την ενίσχυση διαφάνειας
- Ενσωμάτωση του Εσωτερικού Ελέγχου στους ΟΤΑ
- Τεκμηρίωση αναφορών προς την Ευρωπαϊκή Επιτροπή

## Νοσοκομεία & Οργανισμοί Υγείας

Τα δημόσια νοσοκομεία υιοθετούν το COSO:

- Για παρακολούθηση ιατρικών λαθών
- Για αξιολόγηση κινδύνου απώλειας ασθενών δεδομένων
- Για τη δημιουργία μοντέλων compliance με το GDPR

# Εφαρμογές του COSO στην Πρακτική

## 4 Επιχειρήσεις Τεχνολογίας – SAP

Η SAP ενσωμάτωσε το COSO στο GRC μοντέλο της (Governance, Risk, Compliance) για:

- Διαχείριση επιχειρησιακών κινδύνων
- Ανίχνευση εσωτερικής απάτης
- Ελεγχόμενη κατανομή δικαιωμάτων πρόσβασης

## 5 Εφαρμογή σε Πολυεθνικές – Nestlé

Η Nestlé ανέπτυξε internal control self-assessments (ICSAs) βασισμένα στο COSO, ώστε να:

- Εντοπίζει τρωτά σημεία στην εφοδιαστική αλυσίδα
- Εκπαιδεύει προσωπικό σε ethical conduct
- Εφαρμόζει συστηματικά εργαλεία monitoring

## 6 Εταιρείες Παροχής Υπηρεσιών – Deloitte

Η Deloitte αξιοποιεί το COSO σε projects αξιολόγησης εσωτερικού ελέγχου σε πελάτες:

- Σχεδιασμός tailored μοντέλων για κάθε τμήμα (HR, Πληροφορική, Προμήθειες)
- Πλήρης κάλυψη και των 5 στοιχείων του πλαισίου
- Χρήση Data Analytics για ongoing monitoring

## Σχέση COSO & SOX (Sarbanes-Oxley Act)

Η σχέση μεταξύ του πλαισίου COSO και του νόμου Sarbanes-Oxley (SOX) είναι άμεση, συμπληρωματική και ουσιαστική. Το COSO λειτουργεί ως το πρότυπο πλαίσιο για την εφαρμογή των απαιτήσεων του SOX, ειδικά όσον αφορά το Section 404, το οποίο αφορά τη διασφάλιση της αποτελεσματικότητας των εσωτερικών ελέγχων στις χρηματοοικονομικές αναφορές.

Ο νόμος Sarbanes-Oxley Act του 2002 θεσπίστηκε στις ΗΠΑ μετά τα οικονομικά σκάνδαλα Enron, WorldCom, Tyco κ.ά. Στόχος του ήταν η αποκατάσταση της εμπιστοσύνης των επενδυτών μέσω αυστηρότερων προτύπων διαφάνειας, εταιρικής διακυβέρνησης και εσωτερικού ελέγχου.

Το COSO αποτελεί τον “χάρτη” που οδηγεί τις επιχειρήσεις στην ασφαλή συμμόρφωση με τον SOX. Ειδικά για εταιρείες εισηγμένες σε αμερικανικά χρηματιστήρια, το COSO δεν είναι απλώς επιλογή – είναι σχεδόν αναγκαιότητα.



ΣΑΣ ΕΥΧΑΡΙΣΤΩ !