



## **Πολιτική και Μεθοδολογία (Διαδικασίες) Διαχείρισης Κινδύνων**

**ΝΟΕΜΒΡΙΟΣ 2023**

**ΠΙΝΑΚΑΣ ΑΝΑΘΕΩΡΗΣΕΩΝ ΕΓΓΡΑΦΟΥ**

<b>A/A</b>	<b>Ημερομηνία σύνταξης / αναθεώρησης</b>	<b>Σύντομη περιγραφή αλλαγής</b>	<b>Εισήγηση από</b>	<b>Έγκριση από</b>
<b>Έκδοση 1</b>	<b>30.11.2023</b>	<b>Αρχική έκδοση</b>	<b>Υπεύθυνος Υπηρεσίας Διαχείρισης Κινδύνων</b>	<b>Διοικητικό Συμβούλιο</b>
<b>Έκδοση 2</b>				

## ΠΕΡΙΕΧΟΜΕΝΑ

1.	Εισαγωγή.....	4
2.	Σύντομη αναφορά στο πλαίσιο COSO ERM .....	5
3.	Κύρια χαρακτηριστικά της Διαδικασίας Διαχείρισης Κινδύνων.....	5
3.1.	Αναγνώριση Κινδύνων .....	6
3.2.	Εκτίμηση Κινδύνων .....	7
3.3.	Διαχείριση Κινδύνων.....	10
3.4.	Παρακολούθηση Κινδύνων.....	10
4.	Αναγνώριση των ρόλων των εμπλεκόμενων μερών.....	11
4.1.	Ο ρόλος του Συμβουλίου Διεύθυνσης και του Διοικητικού Συμβουλίου .....	11
4.2.	Ο ρόλος των Υπεύθυνων Διαχείρισης Κινδύνων («Ιδιοκτήτης Κινδύνου») .....	11
4.3.	Ο ρόλος της Υπηρεσίας Διαχείρισης Κινδύνων .....	11
4.4.	Ο ρόλος της Λειτουργίας Κανονιστικής Συμμόρφωσης .....	12
4.5.	Ο ρόλος της Υπηρεσίας Εσωτερικού Ελέγχου.....	12
4.6.	Ο ρόλος του προσωπικού .....	13
5.	Εργαλεία μεθοδολογίας και σύνοψη ροής βασικής διαδικασίας.....	13
	Παράρτημα Α / Υπόδειγμα Μητρώου Κινδύνων .....	17
	Παράρτημα Β / Συνοπτική απεικόνιση του Πλαισίου COSO ERM .....	18

## 1. Εισαγωγή

Η παρούσα Πολιτική και Μεθοδολογία (Διαδικασίες) Διαχείρισης Κινδύνων εγκρίθηκε και τίθεται σε ισχύ με την από 01/12/2023 απόφαση του Διοικητικού Συμβουλίου της «ΑΒΑΞ ΑΝΩΝΥΜΗ ΕΤΑΙΡΕΙΑ – ΕΡΓΟΛΗΠΤΙΚΗ – ΤΟΥΡΙΣΤΙΚΗ – ΕΜΠΟΡΙΚΗ – ΒΙΟΜΗΧΑΝΙΚΗ – ΟΙΚΟΔΟΜΙΚΩΝ ΥΛΙΚΩΝ ΚΑΙ ΜΗΧΑΝΗΜΑΤΩΝ», με διακριτικό τίτλο "ΑΒΑΞ ΑΕ» (εφεξής «Εταιρεία»)

Η Διαχείριση Κινδύνων είναι ένα από τα βασικά στοιχεία του Συστήματος Εσωτερικού Ελέγχου της Εταιρείας (στο εξής και «ΣΕΕ»). Σε συνδυασμό με τα λοιπά στοιχεία που συνθέτουν ένα αποτελεσματικό ΣΕΕ όπως οι λειτουργίες της Κανονιστικής Συμμόρφωσης, της Διασφάλισης Ποιότητας και του Εσωτερικού Ελέγχου, συνθέτουν ένα Πλαίσιο που έχει ως στόχο την αποτελεσματική διαχείριση των κινδύνων της Εταιρείας και την επίτευξη των στόχων της.

Η Εταιρεία εφαρμόζει κατάλληλη Πολιτική και Μεθοδολογία (Διαδικασίες) Διαχείρισης Κινδύνων η οποία εγκρίνεται με ξεχωριστή απόφαση του ΔΣ. Περιλαμβάνει διαδικασίες, έντυπα και εργαλεία διαχείρισης ενώ λαμβάνει υπόψη διεθνή πλαίσια όπως το COSO ERM.

## 2. Σύνοψη αναφορά στο πλαίσιο COSO ERM

Η μεθοδολογία που εφαρμόζει η Εταιρεία λαμβάνει υπόψη το διεθνές πλαίσιο «**Committee of Sponsoring Organizations of the Treadway Commission (“COSO”), Enterprise Risk Management - Integrated Framework, 2017**». Το συγκεκριμένο πλαίσιο βοηθάει τόσο στο σχεδιασμό όσο και στην αξιολόγηση της διαδικασίας διαχείρισης κινδύνων. Αναπτύσσεται σε είκοσι βασικές αρχές οι οποίες παρατίθενται, συνοπτικά στο Appendix I.

## 3. Κύρια χαρακτηριστικά της Διαδικασίας Διαχείρισης Κινδύνων

Ως «κίνδυνος» (risk) ορίζεται η πιθανότητα έλευσης ενός συμβάντος (event) το οποίο μπορεί να επηρεάσει αρνητικά τη λειτουργία και την επίτευξη της στρατηγικής και των στόχων της Εταιρείας.

Η Διαχείριση Κινδύνων είναι μία συνεχής και επαναληπτική διαδικασία η οποία επιτρέπει στη Διοίκηση της Εταιρείας να εντοπίσει, αξιολογήσει και διαχειριστεί τους κινδύνους και τις αβεβαιότητες. Η διαδικασία αυτή είναι απόλυτα συνδεδεμένη με την επίτευξη των στρατηγικών στόχων της Εταιρείας και με τη διατήρηση και την αύξηση της αξίας της. Η Διαδικασία Διαχείρισης Κινδύνων συνίσταται από την κουλτούρα, τις αξίες, τις δυνατότητες, τις πολιτικές, διαδικασίες και πρακτικές της Εταιρείας και λειτουργεί σε συνδυασμό με την διαμόρφωση στρατηγικής και την επίτευξη των στόχων της.

Η επάρκεια και η αποτελεσματικότητα του ΣΕΕ σε κάθε Εταιρεία βασίζεται:

- α) στη φύση και έκταση των κινδύνων που αντιμετωπίζει
- β) στην έκταση και τις κατηγορίες των κινδύνων που το ΔΣ αποδέχεται να αναλάβει
- γ) στην πιθανότητα επέλευσης των παραπάνω κινδύνων
- δ) στην ικανότητα της Εταιρείας να μειώσει την επίπτωση των κινδύνων που τελικώς επέρχονται και
- ε) στο κόστος λειτουργίας συγκεκριμένων δικλίδων ασφαλείας, σε σχέση με το όφελος από τη διαχείριση των κινδύνων.

Η Διαχείριση Κινδύνων έχει ως προϋπόθεση τον προσδιορισμό σαφών και μετρήσιμων λειτουργικών στόχων (objective setting) τόσο σε επίπεδο Εταιρείας όσο και σε επίπεδο των επιμέρους λειτουργιών και δραστηριοτήτων. Ακολούθως, θα πρέπει να αναγνωρίζονται τα σημαντικά γεγονότα που μπορούν να επηρεάσουν αρνητικά αυτούς τους στόχους (event identification), να αξιολογούνται οι σχετικοί κίνδυνοι (risk assessment) και να αποφασίζεται η απόκριση της Εταιρείας σε αυτούς (risk response).

Ουσιαστικά, η Διαδικασία Διαχείρισης Κινδύνων αποτελείται από τις εξής υπό-διαδικασίες:

1. Αναγνώριση Κινδύνων (risk identification)
2. Εκτίμηση Κινδύνων (risk assessment)
3. Διαχείριση Κινδύνων (risk management)
4. Παρακολούθηση εξέλιξης κινδύνων (risk monitoring)

### 3.1. Αναγνώριση Κινδύνων

Οι κίνδυνοι που αντιμετωπίζει η Εταιρεία διαφέρουν από την άποψη:

α) της πηγής του κινδύνου

- Εξωγενείς κίνδυνοι: προέρχονται από το εξωτερικό περιβάλλον
- Ενδογενείς κίνδυνοι.

β) της φύσης των κινδύνων και των στόχων που απειλούν. Ενδεικτικά αναφέρονται:

- Κίνδυνοι που απειλούν στρατηγικούς στόχους (strategic objectives / strategic risks)
- Κίνδυνοι που απειλούν λειτουργικούς /επιχειρησιακούς στόχους και στόχους των επιμέρους λειτουργιών, διευθύνσεων και τμημάτων της Εταιρείας (Operational objectives /Operational risks).
- Κίνδυνοι κανονιστικής συμμόρφωσης (compliance objectives / compliance risks)
- Κίνδυνοι που σχετίζονται με τις αναφορές (reporting objectives / reporting risks).

Κάθε κίνδυνος είναι πιθανό να κατατάσσεται σε περισσότερες από μία κατηγορίες (πχ να απειλεί λειτουργικούς στόχους αλλά και στόχους αναφορών αλλά και κανονιστικής συμμόρφωσης).

Σημαντικές υποκατηγορίες υπο-κατηγορίες στόχων και αντίστοιχων κινδύνων είναι (ενδεικτικά και όχι περιοριστικά):

- περιβαλλοντικοί κίνδυνοι
- κίνδυνοι σχετιζόμενοι με την υγεία και ασφάλεια
- κίνδυνοι σχετιζόμενοι με την κλιματική αλλαγή
- χρηματοοικονομικοί κίνδυνοι
- γεωπολιτικοί κίνδυνοι
- κίνδυνοι αγοράς και ανταγωνισμού
- κίνδυνοι φήμης
- κίνδυνοι πληροφοριακών συστημάτων,
- Κίνδυνοι σχετιζόμενοι με την κυβερνοασφάλεια,
- κίνδυνοι που έχουν σχέση με το ανθρώπινο κεφάλαιο (εύρεση, διατήρηση, εκπαίδευση, διαχείριση προσωπικού)
- Λοιποί κίνδυνοι

Η αναγνώριση κινδύνων γίνεται εφικτή με τη συνεχή, μεθοδική και επαναληπτική επικοινωνία μεταξύ όλων των εμπλεκόμενων μερών μέσω:

- διενέργειας συζητήσεων και συναντήσεων εργασίας
- καταχώρησης πληροφόρησης στα διαθέσιμα εργαλεία (όπως το μητρώο κινδύνων)
- ερωτηματολογίων
- ερευνών

### 3.2. Εκτίμηση Κινδύνων

Η εκτίμηση κινδύνων πραγματοποιείται με την αξιολόγηση και την κατάταξή τους σε κλίμακες που έχουν σχέση με:

- Την πιθανότητα έλευσης του κινδύνου (event likelihood)
- Την επίπτωση του κινδύνου (impact)

Οι κλίμακες μέτρησης τόσο της πιθανότητας όσο και της επίπτωσης του κινδύνου έχουν πέντε βαθμίδες ως εξής:

#### Α) Κλίμακα πιθανότητας

Επίπεδο Πιθανότητας	ΠΙΘΑΝΟΤΗΤΑ
5	Έχει ήδη επέλθει το γεγονός που επιφέρει κίνδυνο (risk event) ή είναι σχεδόν βέβαιο ότι θα επέλθει άμεσα
4	Πολύ πιθανό να επέλθει τους επόμενους 12 μήνες (άνω του 50%)
3	20%-50% πιθανότητα να επέλθει τους επόμενους 12 μήνες
2	10%-20% πιθανότητα ότι θα επέλθει τους επόμενους 12-24 μήνες
1	Πολύ χαμηλή πιθανότητα να συμβεί

#### Β) Κλίμακα επίδρασης

ΕΠΙΔΡΑΣΗ				
Επίπεδο Επίδρασης	Χρηματοοικονομική	Συμμόρφωσης στους νόμους και τους κανονισμούς	Φήμης	Λειτουργία / Επιχειρησιακή Απόδοση
5	Πολύ κρίσιμη επίδραση στην οικονομική θέση (ενεργητικό-παθητικό-ίδια κεφάλαια) ή στα αναμενόμενα αποτελέσματα	Πολύ κρίσιμη παραβίαση νόμων και κανονισμών που θα μπορούσαν να οδηγήσουν σε σημαντικά πρόστιμα ή συνέπειες στην Εταιρία ή/και στα μέλη Διοίκησης	Πολύ κρίσιμο αντίκτυπο στη φήμη ή το εμπορικό σήμα της Εταιρείας που θα μπορούσε να απειλήσει τη μελλοντική της βιωσιμότητα	Πολύ κρίσιμο αντίκτυπο στην λειτουργία /αποτελεσματικότητα
4	Κρίσιμη επίδραση στην οικονομική θέση (ενεργητικό-παθητικό-ίδια κεφάλαια) ή στα	Σημαντική παραβίαση των νόμων και κανονισμών με	Σημαντικό αντίκτυπο στη φήμη ή το εμπορικό σήμα της Εταιρείας	Σημαντικό αντίκτυπο στην λειτουργία /αποτελεσματικότητα

	αναμενόμενα αποτελέσματα	αποτέλεσμα σημαντικά πρόστιμα και συνέπειες		
3	Μέτρια επίδραση στην οικονομική θέση (ενεργητικό-παθητικό- ίδια κεφάλαια) ή στα αναμενόμενα αποτελέσματα	Μέτρια παραβίαση νόμων και κανονισμών με μέτριες συνέπειες	Μέτρια επίδραση στη φήμη της Εταιρείας	Μέτρια επίδραση στην λειτουργία /αποτελεσματικότητα
2	Μικρές (κάτω του μετρίου) επιπτώσεις στην οικονομική θέση (ενεργητικό-παθητικό- ίδια κεφάλαια) ή στα αναμενόμενα αποτελέσματα	Μικρή (κάτω του μετρίου) παραβίαση νόμων και κανονισμών με περιορισμένες συνέπειες	Μικρές (κάτω του μετρίου) επιπτώσεις στη φήμη της Εταιρείας	Μικρή (κάτω του μετρίου) επίδραση στην λειτουργία /αποτελεσματικότητα
1	Ελάχιστη επίδραση στην οικονομική θέση (ενεργητικό-παθητικό- ίδια κεφάλαια) ή στα αναμενόμενα αποτελέσματα	Ελάχιστη παραβίαση των νόμων και των κανονισμών με μικρή συνέπεια	Ελάχιστη επίδραση στη φήμη της Εταιρείας	Ελάχιστη επίδραση στην λειτουργία /αποτελεσματικότητα



**Γ) Συνολική αξιολόγηση: Συνδυασμός επίπεδου πιθανότητας και επιπέδου επίδρασης**

ΕΠΙΠΕΔΟ ΠΙΘΑΝΟΤΗΤΑΣ	ΕΠΙΠΕΔΟ ΕΠΙΔΡΑΣΗΣ				
	1	2	3	4	5
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5

<b>Υψηλός Κίνδυνος</b>	Απαιτούνται άμεσες ενέργειες και συνεχής παρακολούθηση από ανώτατη διοίκηση και εκτελεστικούς διευθυντές και καθορισμός σχεδίων δράσης με μετρήσιμη απόδοση
<b>Μεσαίος προς Υψηλός Κίνδυνος</b>	Απαιτείται επαυξημένη παρακολούθηση και εξέταση για άμεσες ενέργειες από ανώτατη διοίκηση και εκτελεστικούς διευθυντές
<b>Μεσαίος Κίνδυνος</b>	Απαιτείται συνεχής παρακολούθηση και διαχείριση ως μέρος των εργασιών της εταιρείας
<b>Χαμηλός προς Μεσαίος Κίνδυνος</b>	Απαιτείται περιοδική παρακολούθηση και διαχείριση ως μέρος των εργασιών της εταιρείας και περιοδική επανεκτίμηση αλλαγών
<b>Χαμηλός κίνδυνος</b>	Απαιτείται περιοδική παρακολούθηση κυρίως μέσω αναφοράς συμβάντων έλευσης κινδύνου (risk event) που πιθανώς αυξάνουν την πιθανότητα ή την επίδραση.

Οι ανωτέρω κλίμακες μπορεί να εξειδικεύονται περαιτέρω με απόφαση του Υπεύθυνου Διαχείρισης Κινδύνων. Τυχόν αλλαγές μπορούν να γίνονται κυρίως για την ευθυγράμμιση της μεθοδολογίας της ΥΔΚ με τις λειτουργίες και μονάδες που διενεργούν επίσης εκτιμήσεις κινδύνων (ως παράδειγμα αναφέρεται η Λειτουργία Εσωτερικού Ελέγχου, η Λειτουργία Κανονιστικής Συμμόρφωσης και η Λειτουργία Ποιότητας και η Λειτουργία Πληροφορικής).

Οι ανωτέρω κλίμακες εφαρμόζονται σε δύο «επίπεδα» κινδύνων:

1. Ενδογενής κίνδυνος (inherent risk): εκτίμηση κινδύνου σε κλίμακες πιθανότητας και επίδρασης χωρίς να λαμβάνεται υπόψη το σύστημα εσωτερικού ελέγχου (δικλίδες ασφαλείας) της Εταιρείας.
2. Υπολειπόμενος κίνδυνος (residual risk): εκτίμηση κινδύνου σε κλίμακες πιθανότητας και επίδρασης έχοντας λάβει υπόψη το σύστημα εσωτερικού ελέγχου (δικλίδες ασφαλείας) της Εταιρείας.

Στην περίπτωση που η διοίκηση εκτιμά ότι ο υπολειπόμενος κίνδυνος πρέπει να μειωθεί σε χαμηλότερο επίπεδο, θα πρέπει να προσδιορίζεται ένα τρίτο επίπεδο κινδύνου, ο «στοχευόμενος κίνδυνος» (target residual risk")

Η μέτρηση των κινδύνων γίνεται εφικτή με τη συνεχή, μεθοδική και επαναληπτική διενέργεια συζητήσεων και συναντήσεων εργασίας εντός της Εταιρείας μεταξύ όλων των εμπλεκόμενων μερών και με τη χρησιμοποίηση κατάλληλων αναλύσεων, μεθοδολογίας και εργαλείων.

Το βασικότερα εργαλεία και διαδικασίες που θα χρησιμοποιηθούν είναι:

- ✓ Εργαλεία αποτύπωσης κινδύνων.
- ✓ Διαδικασία διενέργειας επαναληπτικών «κύκλων αυτοαξιολόγησης κινδύνων» / Risk Controls Self Assessment Cycles. Οι κύκλοι συναντήσεων θα προγραμματίζονται σε συνεργασία με τη Διοίκηση σε συχνότητα που θα αξιολογείται ανάλογα με τις περιστάσεις.

Είναι προφανές ότι πολλοί κίνδυνοι δεν είναι εύκολα ποσοτικοποιήσιμοι και μετρήσιμοι. Στην περίπτωση αυτή λαμβάνονται ποιοτικά κριτήρια για την κατάταξη του κινδύνου σε μία από τις ανωτέρω κατηγορίες.

### **3.3. Διαχείριση Κινδύνων**

Η Διοίκηση της Εταιρείας καλείται να διαχειριστεί τους κινδύνους στους οποίους υπόκειται. Οι ενέργειες /απόκριση της Διοίκησης μπορεί να είναι:

- Αποδοχή του κινδύνου (risk acceptance)
- Περιορισμός του κινδύνου (risk mitigation), μέσω του περιορισμού της επίδρασης ή της πιθανότητας. Ο περιορισμός του κινδύνου γίνεται είτε με την ενίσχυση των δικλίδων ασφαλείας (internal controls) είτε και με την υλοποίηση ενεργειών διοίκησης (management actions)
- Μεταφορά του κινδύνου σε τρίτους (risk transfer)
- Απόρριψη /αποφυγή του κινδύνου (risk avoidance).

Η απόφαση για τον τρόπο διαχείρισης των κινδύνων λαμβάνεται από τη Διοίκηση και συγκεκριμένα τους εκάστοτε «ιδιοκτήτες» των κινδύνων (risk owners) σύμφωνα με:

- Το προφίλ κινδύνου της Εταιρείας (Risk Profile)
- Γενικό επίπεδο αποδεκτού κινδύνου (Risk Appetite Statement)
- Επιμέρους αποδεκτά επίπεδα κινδύνου/απόδοσης (Performance Tolerance Levels)

Οι ανωτέρω δηλώσεις και όρια προσδιορίζονται από τη Διοίκηση και τους εκάστοτε «ιδιοκτήτες» των κινδύνων (risk owners) και υπόκεινται σε αλλαγές καθώς πρόκειται για μία δυναμική διαδικασία. «Ιδιοκτήτης κινδύνων» μπορεί να είναι οποιασδήποτε (στέλεχος ή ομάδα) έχει τη συνολική ευθύνη για τη διαχείριση του κινδύνου.

### **3.4. Παρακολούθηση Κινδύνων**

Η Διοίκηση της Εταιρείας είναι συνεχώς ενήμερη για την πορεία διαχείρισης και εξέλιξης των κινδύνων σύμφωνα με τις αποφάσεις της αλλά και διαρκώς ενημερώνεται για αναδυόμενους κινδύνους που δεν είχαν αρχικά εντοπιστεί και αξιολογηθεί.

Η παρακολούθηση κινδύνων γίνεται με τα κατάλληλα εργαλεία και αναφορές προς τη Διοίκηση. Σχετικά με τις αναφορές της ΥΔΚ, η συχνότητα των αναφορών είναι περιοδική και ορίζεται τουλάχιστον εξαμηνιαία. Ωστόσο προβλέπεται και η δυνατότητα για έκτακτων αναφορών ανάλογα με τις περιστάσεις.

#### **4. Αναγνώριση των ρόλων των εμπλεκόμενων μερών**

##### **4.1. Ο ρόλος του Συμβουλίου Διεύθυνσης και του Διοικητικού Συμβουλίου**

Το Διοικητικό Συμβούλιο και το Συμβούλιο Διεύθυνσης διενεργεί εποπτεία και παρακολούθηση της αποτελεσματικότητας της διαδικασίας διαχείρισης κινδύνων κυρίως μέσω:

- Λήψης και αξιολόγησης των κατάλληλων αναφορών
- Διενέργειας δημιουργικών συζητήσεων και σχετικών παρουσιάσεων στο πλαίσιο της λειτουργίας του
- Παροχής σχετικών συστάσεων στα εμπλεκόμενα μέρη
- Λήψης σχετικών αποφάσεων

##### **4.2. Ο ρόλος των Υπεύθυνων Διαχείρισης Κινδύνων («Ιδιοκτήτης Κινδύνου»)**

Η διαχείριση κινδύνων είναι μία συνεχής και επαναληπτική διαδικασία (on going & iterative process) και αποτελεί μία από τις βασικές αρμοδιότητες των στελεχών που είναι επιφορτισμένα με τη διοίκηση των επιμέρους οργανωτικών μονάδων («πρώτη γραμμή άμυνας»).

«Ιδιοκτήτης κινδύνων» μπορεί να είναι οποιασδήποτε (στέλεχος ή ομάδα) έχει τη συνολική ευθύνη για τη διαχείριση του συγκεκριμένου κινδύνου.

##### **4.3. Ο ρόλος της Υπηρεσίας Διαχείρισης Κινδύνων**

Η συμβολή της Υπηρεσίας Διαχείρισης Κινδύνων (Risk Function) και του Υπεύθυνου αυτής είναι να υποστηριχθεί η Διοίκηση και τα στελέχη της Εταιρείας σε ενέργειες που έχουν σχέση με τη διαχείριση κινδύνων και να αποτυπωθεί η πληροφόρηση στα κατάλληλα εργαλεία, τα οποία θα είναι εύχρηστα αρχικά για τα ίδια αυτά τα στελέχη.

Η Διοίκηση της Εταιρείας, συνδυάζοντας τις απαιτήσεις του Εσωτερικού Κανονισμού Λειτουργίας της, των σχετικών νομοθετικών απαιτήσεων αλλά και των διεθνών καλών πρακτικών έχει προβλέψει τη λειτουργία διακριτής Υπηρεσίας Διαχείρισης Κινδύνων (στο εξής και «ΥΔΚ» και τον ορισμό Υπεύθυνου Διαχείρισης Κινδύνων (στο εξής και «ΥπΔΚ»).

Ο ΥπΔΚ απαιτείται να έχει επαρκείς γνώσεις και εμπειρία και τη δυνατότητα πρόσβασης σε όλες τις απαιτούμενες πηγές πληροφόρησης..

Ο υπεύθυνος της ΥΔΚ αναφέρεται λειτουργικά στο Συμβούλιο Διεύθυνσης και διοικητικά στον ορισμένο Εντεταλμένο Σύμβουλο. Επίσης, ο ΥΠΔΚ αναφέρεται σε περιοδική βάση προς την Επιτροπή Ελέγχου ενημερώνοντάς την για τη δραστηριότητα της ΥΔΚ.

Ο ΥΠΔΚ :

- υποστηρίζει τις δραστηριότητες διαχείρισης κινδύνων εντός της Εταιρείας.
- προάγει την κουλτούρα της Εταιρείας σχετικά με τη διαχείριση κινδύνων (risk culture).
- διασφαλίζει την ύπαρξη και εφαρμογή κατάλληλης πολιτικής και μεθοδολογίας διαχείρισης κινδύνων.
- μπορεί να συμμετέχει συμβουλευτικά, εφόσον ζητηθεί, στη διαδικασία λήψης αποφάσεων σχετικά με τη διαχείριση κινδύνων.
- παρακολουθεί την ορθή τήρηση και αναφορά επί ορίων και περιορισμών που θέτει η Διοίκηση για τη διαχείριση κινδύνων, καθώς και τυχόν σχετικών εποπτικών απαιτήσεων, κυρίως μέσω των κύκλων αυτοαξιολόγησης κινδύνων.
- υποστηρίζει το ΔΣ και τις Επιτροπές του σε θέματα που άπτονται της διαχείρισης των κινδύνων της Εταιρείας.
- μεριμνά για τη διαρκή εκπαίδευση και ανάπτυξη των γνώσεων και δεξιοτήτων τόσο του ιδίου όσο και του προσωπικού της ΥΔΚ, εφόσον υφίσταται.

#### **4.4. Ο ρόλος της Λειτουργίας Κανονιστικής Συμμόρφωσης**

Η Υπηρεσία Διαχείρισης Κινδύνων, όπως και η Μονάδα Κανονιστικής Συμμόρφωσης ανήκουν στην ονομαζόμενη «δεύτερη γραμμή» (“Three lines model” / The Institute of Internal Auditors). και υποστηρίζουν τη Διοίκηση («πρώτη γραμμή») για θέματα αρμοδιότητάς της. Ακολούθως, και οι δύο λειτουργίες υπόκεινται σε έλεγχο από την «τρίτη γραμμή»τη λειτουργία Εσωτερικού Ελέγχου. Μεγάλο μέρος των κινδύνων, όπως έχει ήδη αναφερθεί, έχει σχέση με την τήρηση των κανονιστικών υποχρεώσεων και κατά συνέπεια οι λειτουργίες διαχείρισης κινδύνων και κανονιστικής συμμόρφωσης συνδέονται και συνεργάζονται στενά.

#### **4.5. Ο ρόλος της Υπηρεσίας Εσωτερικού Ελέγχου**

Η σύγχρονη οργάνωση του Εσωτερικού Ελέγχου ενός οργανισμού (χαρακτηριζόμενη και ως «τρίτη γραμμή») βασίζεται στην αναγνώριση, τη μέτρηση, την ανάλυση και την ιεράρχηση των κινδύνων (risk based internal audit). Η προσέγγιση αυτή είναι απαραίτητη λόγω του ότι, τόσο η προσοχή της Διοίκησης της Εταιρείας όσο και οι πόροι του Εσωτερικού Ελέγχου, πρέπει να στραφούν σε περιοχές που είναι περισσότερο επικίνδυνες για την Εταιρεία αναφορικά είτε σε μετρήσιμα (χρηματικά) στοιχεία είτε σε μη άμεσα μετρήσιμα ποιοτικά στοιχεία. Επίσης, η ίδια η Διαδικασία Διαχείρισης Κινδύνων, ελέγχεται από την Υπηρεσία Εσωτερικού Ελέγχου (αποτελεί ένα από βασικά αντικείμενα ελέγχου). Για τους λόγους αυτούς η Υπηρεσία Εσωτερικού Ελέγχου (Internal Audit Function) συνεργάζεται άμεσα τόσο με την Εκτελεστική Διοίκηση όσο και με την Υπηρεσία Διαχείρισης Κινδύνων.

#### 4.6. Ο ρόλος του προσωπικού

Η Διαχείριση Κινδύνων είναι μια βασική εταιρική διαδικασία και αναπόσπαστο μέρος της καθημερινότητας. Όλα τα άτομα που εργάζονται στην Εταιρεία, συνεργάζονται για την κατανόηση και την αποτελεσματική διαχείριση των κινδύνων της Εταιρείας και την επίτευξη των εταιρικών στόχων. Κατά συνέπεια είναι ιδιαίτερα κρίσιμος ο ρόλος του συνόλου του προσωπικού στην διαδικασία διαχείρισης κινδύνων.

### 5. Εργαλεία μεθοδολογίας και σύνοψη ροής βασικής διαδικασίας

Κάθε στάδιο της διαχείρισης κινδύνων πρέπει να είναι κατάλληλα αποτυπωμένο με τρόπο που να επιτρέπει την επεξεργασία των πληροφοριών και δεδομένων και τη λήψη ενημερωμένων αποφάσεων. Βασικό ρόλο, όπως προαναφέρθηκε, έχει ο Υπεύθυνος Διαχείρισης Κινδύνων, ο οποίος ενεργεί ως σύμβουλος της Διοίκησης αλλά και ως συντονιστής της συνολικής διαδικασίας, υπό την άμεση επίβλεψη του Συμβουλίου Διεύθυνσης και του Εντεταλμένου Συμβούλου στον οποίο αναφέρεται διοικητικά.

Τα βασικότερα εργαλεία της μεθοδολογίας είναι τα εξής:

- ✓ Διενέργεια «κύκλων αυτοαξιολόγησης κινδύνου» (RCSA / Risk And Controls Self Assessment workshops): Πρόκειται συνεχή και περιοδική διαδικασία, η οποία προάγει την συμμετοχή των στελεχών της Εταιρείας στη διαδικασία και γενικότερα ενισχύει την κουλτούρα διαχείρισης κινδύνων. Η διαδικασία RCSA αφορά:
  - Ομαδικές Συναντήσεις Εργασίας (workshops) με μέλη ΔΣ, στελέχη διοίκησης, ΔΣ προσωπικό και λοιπά ενδιαφερόμενα μέρη
  - Ατομικές συζητήσεις εργασίας (interviews & meetings)
- ✓ Δημιουργία και συντήρηση κατάλληλων εργαλείων παρακολούθησης, όπως για παράδειγμα το «Μητρώο Κινδύνων» (Objectives-Risks-Control matrix / “ORC matrix”). Το Μητρώο Κινδύνων περιλαμβάνει (ενδεικτικά):
  - Περιγραφή του κινδύνου
  - Κατηγοριοποίηση και πληροφόρηση σχετικά με τον κίνδυνο
  - Σύνδεση με τον αντίστοιχο αντικειμενικό στόχο του Οργανισμού (objective)
  - Κύριες δικλίδες ασφαλείας (key controls) που σχετίζονται με / τον κίνδυνο
  - Μέτρηση κινδύνου (σε κλίμακες πιθανότητας και επίπτωσης)
  - Αποτύπωση συμβάντων κινδύνου (risk events)
  - Δείκτης παρακολούθησης απόδοσης (key performance indicators) που σχετίζονται με τους κινδύνους
  - Αποτύπωση του «αποδεκτού επίπεδου κινδύνου» (target residual risk) σύμφωνα με τη Διοίκηση (risk appetite /risk tolerance)
  - Σχέδια δράσης / διαχείρισης κινδύνων

Στο παράρτημα Α υπάρχει το προτεινόμενο υπόδειγμα του μητρώου κινδύνων. Υπόκειται σε αλλαγές ωστόσο και αναθεώρηση ανάλογα με την εξέλιξη της διαδικασίας.

- ✓ Δημιουργία και επικοινωνία κατάλληλων περιοδικών αναφορών.
- ✓ Συνεργασία με τις λειτουργίες Κανονιστικής Συμμόρφωσης και Εσωτερικού Ελέγχου, με σκοπό την αποφυγή του κινδύνου της επικάλυψης ενεργειών.

**Η ροή της διαδικασίας, όπως προκύπτει από τις προηγούμενες παραγράφους, συνοψίζεται ως εξής:**

- ✓ Η Υπηρεσία Διαχείρισης Κινδύνων διοργανώνει (facilitates) «κύκλους αυτοαξιολόγησης κινδύνων» (RCSA / Risk And Controls Self Assessment workshops”) Πρόκειται για συναντήσεις και συζητήσεις εργασίας με στελέχη Διοίκησης και υπεύθυνους διευθύνσεων, λειτουργιών και λοιπών οργανωτικών μονάδων κλπ. Στις συζητήσεις αυτές μπορούν να συμμετέχουν και λοιπά στελέχη, ανάλογα με την περίπτωση και σε σύμφωνα με την κρίση των συμμετεχόντων. Στους κύκλους αυτοαξιολόγησης λαμβάνεται χρήσιμη πληροφόρηση σχετικά με τους κινδύνους, τις δικλίδες ασφαλείας, τα σχέδια δράσης (action plans), τα συμβάντα κινδύνου (risk events), την μέτρηση επιδόσεων (performance indicators) και την παρακολούθηση των σχεδίων δράσης.
- ✓ Για την καλύτερη προετοιμασία των κύκλων αυτοαξιολόγησης κινδύνων μπορούν να χρησιμοποιούνται συμπληρωματικά εργαλεία όπως ερωτηματολόγια και αποστολή σχετικού υλικού πληροφόρησης και προετοιμασίας. Η συχνότητα των κύκλων αυτοαξιολόγησης είναι τουλάχιστον ετήσια.
- ✓ Η Υπηρεσία Διαχείρισης Κινδύνων ενημερώνει με τη σχετική πληροφόρηση σε εργαλείο παρακολούθησης (όπως το «Μητρώο Κινδύνων») περιοδικά ανάλογα με τη πορεία των συναντήσεων.
- ✓ Η πληροφορία που καταχωρείται στο εργαλείο παρακολούθησης και η βαθμολόγηση των κινδύνων δίνεται από τους Ιδιοκτήτες κινδύνων σε συνεργασία με την ΥΔΚ. Για το σκοπό αυτό, προβλέπεται και ενθαρρύνεται η σχετική επικοινωνία μεταξύ των μερών ώστε αν επιτυγχάνεται μια «κοινή αντίληψη» επί των κινδύνων. Τυχόν σοβαρές διαφωνίες μεταξύ των Ιδιοκτητών Κινδύνων και του Υπεύθυνου Διαχείρισης Κινδύνων επικοινωνούνται κατάλληλα μέσω των αναφορών της Υπηρεσίας Διαχείρισης Κινδύνων.
- ✓ Οι «Ιδιοκτήτες Κινδύνων» (risk owners) μπορούν να καταχωρούν απευθείας σχετική πληροφόρηση στο τηρούμενο εργαλείο. Ως παράδειγμα αναφέρεται η καταχώριση σημαντικών συμβάντων κινδύνου.
- ✓ Η Υπηρεσία Διαχείρισης Κινδύνων υποβάλει σε περιοδική βάση αναφορές με την πρόοδο της εργασίας και σχετική πληροφόρηση, σύμφωνα με τα οριζόμενα στην Πολιτική και Μεθοδολογία Διαχείρισης Κινδύνων.
- ✓ Σε περιπτώσεις που οι ιδιοκτήτες κινδύνων προσδιορίζουν το «στοχευόμενο επίπεδο κινδύνου» (target risk) σε μικρότερο επίπεδο από το «υπολειπόμενο επίπεδο κινδύνου» (residual risk), υποχρεωτικά αναφέρονται σχέδια δράσης. Τα σχέδια δράσης πρέπει να είναι, κατά το δυνατό, συγκεκριμένα και με σαφή χρονοδιαγράμματα και ρόλους.
- ✓ Σχέδια δράσης μπορούν να καταχωρούνται και σε λοιπές περιπτώσεις.
- ✓ Η Υπηρεσία Διαχείρισης Κινδύνων μπορεί να διοργανώνει ειδικές συναντήσεις σε ανώτατο επίπεδο με τη γραμμή αναφοράς της (Συμβούλιο Διεύθυνσης και Εντεταλμένος Σύμβουλος). Στις συναντήσεις αυτές ενδεχομένως θα μπορούν να προκύψουν ανάγκες για αλλαγές σε διάφορα σχετικά θέματα (risk calibration).





## Παράρτημα Α / Υπόδειγμα Μητρώου Κινδύνων

Το προτεινόμενο υπόδειγμα του μητρώου κινδύνων υπόκειται σε αλλαγές ωστόσο και αναθεώρηση ανάλογα με την εξέλιξη της διαδικασίας.

Πιθανές πρόσθετες στήλες (ενδεικτικά):

- Συμβάντα επέλευσης κινδύνου (risk events)
- Πληροφόρηση σχετικά με αξιολόγηση από μηχανισμούς ελέγχου
- Πληροφόρηση σε σχέση με την μέγιστη ανοχή στο κίνδυνο (risk capacity) και την επιθυμητή απόδοση (Δείκτες απόδοσης / performance indicators)

ΜΗΤΡΩΟ ΚΙΝΔΥΝΩΝ																	
Α/Α	Σχετικός Στόχος (Στρατηγικός /Επιχειρησιακός)	Κίνδυνος / Σύντομη Περιγραφή Κινδύνου	Πηγή Κινδύνου Ενδογενής/ Εξωγενής	Κύριος Τύπος Στρατηγ. / Λειτουργ. / Χρηματ. / Κανον. συμμόρφ.	Υπεύθυνος για τον κίνδυνο	Αξιολόγηση κινδύνου (εγγενής κινδύνος / inherent risk)				Απόκριση στον κίνδυνο	Δικλείδες ασφαλείας που περιορίζουν τον κίνδυνο (βασικά σημεία)	Αξιολόγηση κινδύνου (υπολειπόμενος κινδύνος / residual risk)				Στοχευόμενο επίπεδο κινδύνου /target risk	Προγραμματισμένες ενέργειες (σχέδια δράσης)
						Επίδραση (1-5)	Πιθανότητα (1-5)	Επίδραση x Πιθανότητα	Κατάταξη κινδύνου			Επίδραση (1-5)	Πιθανότητα (1-5)	Επίδραση x Πιθανότητα	Κατάταξη κινδύνου		
1																	
2																	
3																	
4																	

## Παράρτημα Β / Συνοπτική απεικόνιση του Πλαισίου COSO ERM

Η μεθοδολογία που εφαρμόζει η Εταιρεία λαμβάνει υπόψη το διεθνές πλαίσιο «**Committee of Sponsoring Organizations of the Treadway Commission (“COSO”), Enterprise Risk Management - Integrated Framework, 2017**». Το συγκεκριμένο πλαίσιο βοηθάει τόσο στο σχεδιασμό όσο και στην αξιολόγηση της διαδικασίας διαχείρισης κινδύνων. Αναπτύσσεται σε είκοσι βασικές αρχές οι οποίες παρατίθενται, συνοπτικά πιο κάτω.



