Ε.Ε. Παρ. III(I)
Αρ. 4808, 8.8.2014

Κ.Δ.Π. 375/2014

Αριθμός 375

ΚΕΝΤΡΙΚΗ ΤΡΑΠΕΖΑ ΤΗΣ ΚΥΠΡΟΥ

ΟΔΗΓΙΑ ΠΡΟΣ ΤΑ ΠΙΣΤΩΤΙΚΑ ΙΔΡΥΜΑΤΑ ΣΧΕΤΙΚΑ ΜΕ ΤΙΣ ΡΥΘΜΙΣΕΙΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ ΚΑΙ ΔΙΑΧΕΙΡΙΣΗΣ

ΙΟΥΛΙΟΣ 2014

ΠΕΡΙΕΧΟΜΕΝΑ

Τμήμα 5 - Ρόλος και αρμοδιότητες του προέδρου του διοικητικού οργάνου

27 Κύριες αρμοδιότητες του προέδρου του διοικητικού οργάνου.
28 Διασφάλιση της αποτελεσματικής λειτουργίας του διοικητικού οργάνου.
29 Διασφάλιση της εισαγωγής, ανάπτυξης και αξιολόγησης των επιδόσεων.
30 Διασφάλιση αποτελεσματικής επικοινωνίας με τις εποπτικές αρχές και τους μετόχους.

Τμήμα 6 - Ρόλος και ευθύνες του ανώτερου ανεξάρτητου μέλους του διοικητικού οργάνου.

31 Ρόλοι και αρμοδιότητες του ανώτερου ανεξάρτητου μέλους του διοικητικού οργάνου.

Τμήμα 7 - Ρόλοι και ευθύνες του γραμματέα της εταιρείας

32 Ευθύνη για το διορισμό γραμματέα της εταιρείας.
33 Διευκόλυνση της λειτουργίας του διοικητικού οργάνου.
34 Διευκόλυνση της επαγωγής, ανάπτυξης και αξιολόγησης των μελών του διοικητικού οργάνου.

ΜΕΡΟΣ IV - ΕΠΙΤΡΟΠΕΣ ΤΟΥ ΔΙΟΙΚΗΤΙΚΟΥ ΟΡΓΑΝΟΥ

Τμήμα 1 - Γενικές απαιτήσεις

35 Απαίτηση για σύσταση επιτροπών.
36 Σύνθεση και οργάνωση των επιτροπών.
37 Όροι εντολής των επιτροπών.

Τμήμα 2 – Επιτροπή Ελέγχου

38 Κριτήρια επιλεξιμότητας των μελών της επιτροπής ελέγχου.
39 Καθήκοντα της επιτροπής ελέγχου.

Τμήμα 3 – Επιτροπή Κινδύνων

40 Κριτήρια επιλεξιμότητας των μελών της επιτροπής κινδύνων.
41 Καθήκοντα της επιτροπής κινδύνων.

Τμήμα 4 – Επιτροπή Αποδοχών

42 Κριτήρια επιλεξιμότητας των μελών της επιτροπής αποδοχών.
43 Καθήκοντα της επιτροπής αποδοχών.

Τμήμα 5 - Επιτροπή ανάδειξης υποψηφίων

44 Κριτήρια επιλεξιμότητας των μελών της επιτροπής ανάδειξης υποψηφίων.

ΜΕΡΟΣ V - ΑΝΩΤΑΤΑ ΔΙΟΙΚΗΤΙΚΑ ΣΤΕΛΕΧΗ

45 Σύνθεση των ανώτατων διοικητικών στελεχών.
46 Επιλογή, ανάπτυξη και διαδοχή των ανώτατων διοικητικών στελεχών.
47 Ρόλοι και ευθύνες των ανώτατων διοικητικών στελεχών.
48 Επίβλεψη των εργασιών του ιδρύματος και καθοδήγηση σε καθημερινή βάση.
49 Παροχή εισηγήσεων στο διοικητικό όργανο.

ΜΕΡΟΣ VI - ΠΛΑΙΣΙΟ ΑΠΟΔΟΧΩΝ

50 Πολιτικές αποδοχών.
51 Μεταβλητά στοιχεία αποδοχών.
52 Ιδρύματα που επωφελούνται από κυβερνητική παρέμβαση.

ΜΕΡΟΣ VII - ΠΛΑΙΣΙΟ ΕΠΙΧΕΙΡΗΣΙΑΚΗΣ ΔΕΟΝΤΟΛΟΓΙΑΣ

53 Εταιρικές αξίες και κώδικας επιχειρησιακής δεοντολογίας.
54 Οι υπηρεσίες που προσφέρονται στους πελάτες.
55 Σύγκρουση συμφερόντων και διαχωρισμός καθηκόντων.
56 Μη τυποποιημένες ή μη διαφανείς δραστηριότητες.
57 Διαδικασίες προειδοποίησης.

ΜΕΡΟΣ VIII - ΡΥΘΜΙΣΕΙΣ ΚΑΝΟΝΙΣΤΙΚΗΣ ΣΥΜΜΟΡΦΩΣΗΣ

58 Κουλτούρα κανονιστικής συμμόρφωσης.
59 Απαιτήσεις για τη δημιουργία πλαισίου κανονιστικής συμμόρφωσης.

ΜΕΡΟΣ IX - ΠΛΑΙΣΙΟ ΓΙΑ ΤΗΝ ΑΝΤΙΜΕΤΩΠΙΣΗ ΤΩΝ ΚΙΝΔΥΝΩΝ

Τμήμα 1 – Κουλτούρα διαχείρισης κινδύνων και διάθεση ανάληψης κινδύνων

60 Κουλτούρα διαχείρισης κινδύνων.
61 Πλαίσιο διάθεσης ανάληψης κινδύνων.

Τμήμα 2 – Πλαίσιο διαχείρισης κινδύνων

Υποτμήμα 2.1 – Γενικές απαιτήσεις

62 Γενικές απαιτήσεις για τη διαχείριση κινδύνων.

Υποτμήμα 2.2 – Αντιμετώπιση συγκεκριμένων κινδύνων

63 Πιστωτικός κίνδυνος και κίνδυνος αντισυμβαλλομένου.
64 Υπολειπόμενος κίνδυνος.
65 Κίνδυνος συγκέντρωσης.
66 Κίνδυνος τιτλοποίησης.
67 Κίνδυνος αγοράς.
68 Κίνδυνος επιτοκίου από δραστηριότητες εκτός χαρτοφυλακίου.
69 Κίνδυνος υπερβολικής μόχλευσης.
70 Λειτουργικός κίνδυνος.
71 Κίνδυνος ρευστότητας.

Υποτμήμα 2.3 – Νέα προϊόντα και αγορές και μη τυποποιημένες ή μη διαφανείς δραστηριότητες

72 Νέα προϊόντα και υπηρεσίες.
73 Μη τυποποιημένες ή μη διαφανείς δραστηριότητες.

ΜΕΡΟΣ X - ΠΛΑΙΣΙΟ ΕΣΩΤΕΡΙΚΟΥ ΕΛΕΓΧΟΥ
Τμήμα 1 - Γενικές απαιτήσεις

74 Απαιτήσεις για τη θέσπιση πλαισίου εσωτερικού ελέγχου.

Τμήμα 2 – Συστήματα εσωτερικού ελέγχου

75 Απαιτήσεις για τη δημιουργία συστημάτων ελέγχου.

Τμήμα 3- Τμήματα Ελέγχου

Υποτμήμα 3.1- Γενικές απαιτήσεις των τμημάτων ελέγχου

76 Απαιτήσεις για τη θέσπιση τμημάτων ελέγχου.
77 Ανεξαρτησία τμήματος ελέγχου.
78 Επικεφαλής τμήματος ελέγχου.
79 Προσόντα υπαλλήλων τμήματος ελέγχου.
80 Εναλλαγή προσωπικού τμημάτων ελέγχου.
81 Σχέσεις μεταξύ τμημάτων ελέγχου.
82 Καταστατικό τμήματος ελέγχου.
83 Ο ρόλος των τμημάτων ελέγχου σε ομίλους.

Υποτμήμα 3.1 – Τμήμα διαχείρισης κινδύνων

84 Γενικές απαιτήσεις του τμήματος διαχείρισης κινδύνων.
85 Ο ρόλος του τμήματος διαχείρισης κινδύνων στη διαμόρφωση στρατηγικής, διάθεσης ανάληψης κινδύνων και λήψης αποφάσεων.
86 Ο ρόλος του τμήματος διαχείρισης κινδύνων στη διαχείριση κινδύνων.
87 Ο ρόλος του τμήματος διαχείρισης κινδύνων στην ανάπτυξη και έγκριση νέων προϊόντων.
88 Συγκεκριμένες απαιτήσεις του επικεφαλής του τμήματος διαχείρισης κινδύνων.
89 Απαιτήσεις για υποβολή αναφορών του τμήματος διαχείρισης κινδύνων.

Υποτμήμα 3.2 – Τμήμα Κανονιστικής Συμμόρφωσης

90 Ρόλος και ευθύνες του τμήματος κανονιστικής συμμόρφωσης.
91 Ρόλος του τμήματος κανονιστικής συμμόρφωσης στην παρεμπόδιση νομιμοποίησης εσόδων από παράνομες δραστηριότητες.
92 Ρόλος του τμήματος κανονιστικής συμμόρφωσης στην παροχή επενδυτικών υπηρεσιών και δραστηριοτήτων.
93 Καταστατικό του τμήματος κανονιστικής συμμόρφωσης.
94 Απαιτήσεις για υποβολή αναφορών.

Υποτμήμα 3.4 – Τμήμα ασφάλειας πληροφοριών

95 Ρόλος και ευθύνες του τμήματος ασφάλειας πληροφοριών..
96 Απαιτήσεις για υποβολή αναφορών.

Υποτμήμα 3.5 – Τμήμα εσωτερικής επιθεώρησης

97 Ρόλος και ευθύνες του τμήματος εσωτερικής επιθεώρησης.
98 Καταστατικό του τμήματος εσωτερικής επιθεώρησης.
99 Αποστολές ελέγχου.
100 Σχέδιο ελέγχου.
101 Υποβολή εκθέσεων στο διοικητικό όργανο.
102 Συνεργασία του τμήματος εσωτερικής επιθεώρησης με την Κεντρική Τράπεζα.
103 Προσόντα και δεξιότητες και επαγγελματική επιμέλεια του προσωπικού εσωτερικής επιθεώρησης.

ΟΙ ΠΕΡΙ ΕΡΓΑΣΙΩΝ ΠΙΣΤΩΤΙΚΩΝ ΙΔΡΥΜΑΤΩΝ ΝΟΜΟΙ ΤΟΥ 1997 ΕΩΣ (ΑΡ.4) ΤΟΥ 2013

Οδηγία δυνάμει των άρθρων 19 και 41(1) και (2)

Η Κεντρική Τράπεζα, ασκώντας τις εξουσίες που παρέχονται σ' αυτή σύμφωνα με τις διατάξεις των άρθρων 19 και 41(1)-(2) των περί Εργασιών Πιστωτικών Ιδρυμάτων Νόμων του 1997 έως (Αρ.4) του 2013, εκδίδει την παρούσα Οδηγία.

ΜΕΡΟΣ Ι

ΤΙΤΛΟΣ, ΣΚΟΠΟΣ ΚΑΙ ΕΠΙΠΕΔΟ ΕΦΑΡΜΟΓΗΣ ΚΑΙ ΕΡΜΗΝΕΙΑ

Συνοπτικός τίτλος.

1. Η παρούσα Οδηγία θα αναφέρεται ως η περί Ρυθμίσεων Διακυβέρνησης και Διαχείρισης Οδηγία του 2014.

Σκοπός της Οδηγίας.

2 . Σκοπός της παρούσας Οδηγίας είναι:

(α) ο καθορισμός απαιτήσεων σχετικά με τις δομές διακυβέρνησης των πιστωτικών ιδρυμάτων,

(β) ο καθορισμός απαιτήσεων σχετικά με τους ρόλους και τις αρμοδιότητες των διοικητικών οργάνων και των ανώτατων διοικητικών στελεχών,

(γ) ο καθορισμός απαιτήσεων σχετικά με την ανάπτυξη, την εφαρμογή και τον αποτελεσματικό έλεγχο των πλαισίων κανονιστικής συμμόρφωσης, διαχείρισης κινδύνων και εσωτερικού ελέγχου.

Πεδίο εφαρμογής.

3.(1) Η παρούσα Οδηγία εφαρμόζεται μόνο σε αδειοδοτημένα πιστωτικά ιδρύματα που εδρεύουν στη Δημοκρατία σε ατομική βάση, εκτός εάν η Κεντρική Τράπεζα κάνει χρήση της παρέκκλισης που προβλέπεται στο άρθρο 7 του Κανονισμού (ΕΕ) αρ. 575/ 2013.

(2) Μητρικές εταιρείες και θυγατρικές για τις οποίες ισχύει η παρούσα Οδηγία δυνάμει της υποπαραγράφου (1) οφείλουν να –

(α) συμμορφώνονται με τις υποχρεώσεις που απορρέουν από την παρούσα Οδηγία σε ενοποιημένη ή υπο-ενοποιημένη βάση για να διασφαλιστεί ότι οι ρυθμίσεις, οι διαδικασίες και οι μηχανισμοί που διατηρούν κατά τα προβλεπόμενα στην παρούσα Οδηγία είναι συνεπείς και ολοκληρωμένοι και ότι μπορούν να εξαχθούν οποιαδήποτε δεδομένα και πληροφορίες σχετικές με το σκοπό της εποπτείας,

(β) εφαρμόζουν τέτοιες ρυθμίσεις, διαδικασίες και μηχανισμούς στις θυγατρικές τους εταιρείες που δεν υπόκεινται στην παρούσα Οδηγία δυνάμει της υποπαραγράφου (1) έτσι ώστε να διασφαλίζεται ότι οι ρυθμίσεις, οι διαδικασίες και οι μηχανισμοί αυτοί είναι συνεπείς και ολοκληρωμένοι και ότι οι θυγατρικές αυτές είναι σε θέση να παράγουν οποιαδήποτε δεδομένα και πληροφορίες σχετικές με το σκοπό της εποπτείας,

(3) Υποχρεώσεις που απορρέουν από την παρούσα Οδηγία σχετικά με θυγατρικές εταιρείες, που δεν υπόκεινται οι ίδιες στις πρόνοιες της παρούσας Οδηγίας, δεν εφαρμόζονται εάν το μητρικό ίδρυμα εγκατεστημένο στην ΕΕ ή τα ιδρύματα που ελέγχονται από μητρική χρηματοδοτική εταιρεία συμμετοχών εγκατεστημένη στην ΕΕ ή από μητρική μεικτή χρηματοδοτική εταιρεία συμμετοχών εγκατεστημένη στην ΕΕ, μπορεί να αποδείξει στην Κεντρική Τράπεζα ότι η εφαρμογή της παρούσας Οδηγίας είναι αντισυνταγματική σύμφωνα με το νομικό πλαίσιο της τρίτης χώρας όπου είναι εγκατεστημένη η θυγατρική.

(4) Οι διατάξεις του μέρους VI εφαρμόζονται σε επίπεδο ομίλου, μητρικής εταιρείας και θυγατρικής, συμπεριλαμβανομένων όσων έχουν συσταθεί σε υπεράκτια χρηματοπιστωτικά κέντρα.

(5) Η Κεντρική Τράπεζα δύναται να ζητήσει τη συμμόρφωση των πιστωτικών ιδρυμάτων που έχουν συσταθεί σε κράτος μέλος και λειτουργούν μέσω υποκαταστήματος στη Δημοκρατία, με τις διατάξεις της παρούσας Οδηγίας όσον αφορά τα υποκαταστήματά τους στην Κύπρο, εάν τα υποκαταστήματα τους με έδρα την Κύπρο θεωρούνται σημαντικά σύμφωνα με το άρθρο 27Ε του Νόμου.

(6) Η Κεντρική Τράπεζα δύναται να ζητήσει τη συμμόρφωση των πιστωτικών ιδρυμάτων που έχουν συσταθεί σε τρίτη χώρα και λειτουργούν μέσω υποκαταστήματος στη Δημοκρατία, με τις διατάξεις της παρούσας Οδηγίας όσον αφορά τα υποκαταστήματά τους στην Κύπρο, αφού ληφθεί υπόψη η σημαντικότητα των δραστηριοτήτων τους στη Δημοκρατία, η σταθερότητα του τραπεζικού συστήματος,ο όμιλος στον οποίο ανήκουν και η έκταση της διαχείρισης και ελέγχου του ιδρύματος που ασκείται στη ή από τη Δημοκρατία.

Ερμηνεία.

4. Για τους σκοπούς της παρούσας Οδηγίας, οι ερμηνείες που αναφέρονται στο Νόμο και στον Κανονισμό (ΕΕ) αριθ. 575/2013 εφαρμόζονται, εκτός αν από το κείμενο προκύπτει διαφορετική ερμηνεία· επιπλέον, οι ακόλουθες ερμηνείες έχουν εφαρμογή, εκτός εάν από το κείμενο προκύπτει διαφορετική ερμηνεία:

«εσωτερικές μέθοδοι» σημαίνει τη μέθοδο που βασίζεται στις εσωτερικές αξιολογήσεις, τη μέθοδο των εσωτερικών υποδειγμάτων, τη μέθοδο εσωτερικών διαβαθμίσεων, τις εξελιγμένες μεθόδους μέτρησης, τη μέθοδο εσωτερικών υποδειγμάτων και τη μέθοδο του εποπτικού υποδείγματος που αναφέρεται στα άρθρα 143(1), 221, 225, 259 (3), 283 και 312(2) του Κανονισμού (ΕΕ) αριθ. 575/2013·

«κώδικας επιχειρησιακής δεοντολογίας και εταιρικών αξιών» σημαίνει το σύνολο των αρχών, αξιών, προτύπων, ή κανόνων συμπεριφοράς που καθοδηγούν τις αποφάσεις, τις διαδικασίες και τα συστήματα ενός ιδρύματος σύμφωνα με το Μέρος VII·

«επιτροπή» σημαίνει υποομάδα του διοικητικού οργάνου εντεταλμένη για την εκτέλεση συγκεκριμένων λειτουργιών ή έργων που της ανατίθενται·

«γραμματέας εταιρείας» σημαίνει τον ανώτερο διοικητικό λειτουργό εταιρείας που έχει συσταθεί δυνάμει του περί Εταιρειών Νόμου και ο οποίος έχει διοριστεί σύμφωνα με το άρθρο 171 του περί Εταιρειών Νόμου και είναι υπεύθυνος μαζί με τους διευθυντές για την εκτέλεση συγκεκριμένων καθηκόντων που απορρέουν από τον περί Εταιρειών Νόμο, καθώς και οποιοδήποτε άλλο πρόσωπο που μπορεί να ασκήσει καθήκοντα γραμματέα της εταιρείας σύμφωνα με την παρούσα Οδηγία·

«κουλτούρα κανονιστικής συμμόρφωσης» σημαίνει το συνδυασμένο σύνολο ατομικών και εταιρικών αξιών, στάσεων, δεξιοτήτων και συμπεριφορών που καθορίζουν τη δέσμευση του ιδρύματος και τον τρόπο συμμόρφωσης με εσωτερικούς και εξωτερικούς κανόνες και κανονισμούς·

«εκτελεστικό μέλος του διοικητικού οργάνου» έχει την έννοια που αποδίδεται στον όρο αυτό στην παράγραφο 2 της περί της Αξιολόγησης για την Ικανότητα και Καταλληλότητα των Μελών Διοικητικού Οργάνου και των Διευθυντών των ΑΠΙ Οδηγία του 2014·

«εξωτερικός ελεγκτής» σημαίνει το νόμιμο ελεγκτή ή ελεγκτικό γραφείο κατά τα προβλεπόμενα στον περί Ελεγκτών και Υποχρεωτικών Ελέγχων των Ετήσιων και των Ενοποιημένων Λογαριασμών Νόμος του 2009 ως εκάστοτε τροποποιείται ή αντικαθίσταται και περιλαμβάνει τον εγκεκριμένο ελεγκτή του ιδρύματος·

«ανεξάρτητο μέλος του διοικητικού οργάνου" έχει την έννοια που αποδίδεται στον όρο αυτό στην παράγραφο 2 της περί της Αξιολόγησης για την Ικανότητα και Καταλληλότητα των Μελών Διοικητικού Οργάνου και των Διευθυντών των ΑΠΙ Οδηγία του 2014·

«ιδρυμα» σημαίνει αδειοδοτημένο πιστωτικο ίδρυμα και σημαντικό υποκατάστημα πιστωτικού ιδρύματος που είναι εγκατεστημένο στην ΕΕ και υπόκειται στις διατάξεις της παρούσας Οδηγίας·

«Νόμος» σημαίνει τον περί Πιστωτικών Ιδρυμάτων Νόμο του 1997 έως (Αρ. 4) του 2013·

«κίνδυνος του υποδείγματος» σημαίνει τη ζημία που κινδυνεύει να υποστεί ένα ίδρυμα συνεπεία αποφάσεων που βασίζονται κυρίως στα αποτελέσματα εσωτερικών υποδειγμάτων, λόγω σφαλμάτων στη θέσπιση, την εφαρμογή ή τη χρήση αυτών των υποδειγμάτων.

«ανάθεση εργασιών σε τρίτους» σημαίνει τη χρήση ενός τρίτου προσώπου για την εκτέλεση υπηρεσιών ή δραστηριοτήτων, οι οποίες σε διαφορετική περίπτωση, κανονικά, θα τις εκτελούσε το ίδιο το ίδρυμα στο παρόν στάδιο ή στο μέλλον. και δεν περιλαμβάνει την αγορά προϊόντων ή υπηρεσιών·

«αγορά προϊόντων ή υπηρεσιών» σημαίνει μεταξύ άλλων την προμήθεια:

(i) τυποποιημένων προϊόντων ή υπηρεσιών, όπως πληροφορίες σχετικά με τις τρέχουσες τιμές και την αγορά εμπορευμάτων και άλλων αγαθών και αναλώσιμων· και

(i) συμβουλευτικών και άλλων υπηρεσιών που δεν αποτελούν μέρος των επιχειρηματικών και επενδυτικών δραστηριοτήτων του ιδρύματος, συμπεριλαμβανομένων των νομικών συμβουλών·

«διάθεση ανάληψης κινδύνων» σημαίνει το συνολικό επίπεδο και είδη κινδύνου που ένα ίδρυμα είναι διατεθειμένο να αναλάβει στο πλαίσιο της δυνατότητας του για ανάληψη κινδύνων, για την επίτευξη των επιχειρηματικών του στόχων και στρατηγικών·

«δυνατότητα ανάληψης κινδύνων» σημαίνει το μέγιστο επίπεδο κινδύνου που το ίδρυμα μπορεί να αναλάβει πριν από την παραβίαση των περιορισμών που καθορίζονται για τα εποπτικά κεφάλαια και τις ανάγκες για ρευστότητα και τις υποχρεώσεις του προς τους καταθέτες, λοιπούς πελάτες και μετόχους·

«κουλτούρα διαχείρισης κινδύνων» σημαίνει το σύνολο των ατομικών και εταιρικών αξιών, στάσεων, δεξιοτήτων και συμπεριφορών που καθορίζουν τον τρόπο διαχείριση κινδύνου του ιδρύματος·

«προφίλ κινδύνου» σημαίνει την αξιολόγηση των κινδύνων στους οποίους εκτίθεται το ίδρυμα σε ένα χρονικό σημείο, αφού ληφθούν υπόψη οι τεχνικές μετριασμού των κινδύνων, συγκεντρωτικά, εντός και διαμέσου κάθε σχετικής κατηγορίας κινδύνου, στη βάση υποθέσεων για το μέλλον.

ΜΕΡΟΣ ΙΙ
ΓΕΝΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ

Γενικές απαιτήσεις.

5.(1) Το διοικητικό όργανο έχει την κύρια ευθύνη για την εσωτερική διακυβέρνηση ανά πάσα στιγμή· ορίζει, επιβλέπει και λογοδοτεί για την υλοποίηση των ρυθμίσεων διακυβέρνησης που διασφαλίζουν την αποτελεσματική και συνετή διοίκηση ενός ιδρύματος, συμπεριλαμβανομένου του διαχωρισμού αρμοδιοτήτων και της πρόληψης αντικρουόμενων συμφερόντων.

(2) Οι ρυθμίσεις που αναφέρονται στην υποπαράγραφο (1) συμμορφώνονται με τις ακόλουθες αρχές:

(α) το διοικητικό όργανο έχει τη γενική ευθύνη του ιδρύματος και εγκρίνει και επιβλέπει την υλοποίηση των στρατηγικών στόχων, της στρατηγικής κινδύνου και της εσωτερικής διακυβέρνησης του ιδρύματος·

(β) το διοικητικό όργανο διασφαλίζει την αρτιότητα των λογιστικών συστημάτων και συστημάτων χρηματοοικονομικών αναφορών, περιλαμβανομένων των χρηματοοικονομικών και επιχειρησιακών ελέγχων και της συμμόρφωσης με τον Νόμο και τα συναφή πρότυπα·

(γ) το διοικητικό όργανο επιβλέπει τη διαδικασία δημοσιοποίησης και επικοινωνίας·

(δ) το διοικητικό όργανο είναι υπεύθυνο για την αποτελεσματική επίβλεψη των ανώτατων διοικητικών στελεχών.

(3) Το διοικητικό όργανο παρακολουθεί και αξιολογεί περιοδικά την αποτελεσματικότητα των ρυθμίσεων διακυβέρνησης του ιδρύματος και προβαίνει στις δέουσες ενέργειες για την αντιμετώπιση τυχόν ελλείψεων.

(4) Όπου το ίδρυμα είναι μητρικό ίδρυμα ομίλου εταιρειών, το διοικητικό όργανο του ιδρύματος έχει τη συνολική ευθύνη για την επαρκή εσωτερική διακυβέρνηση σε όλο τον όμιλο· προκειμένου να εκπληρώνει τις αρμοδιότητες του για εσωτερική διακυβέρνηση, το διοικητικό όργανο οφείλει να:

(α) εγκαθιδρύει μια δομή διακυβέρνησης η οποία να συμβάλλει στην αποτελεσματική εποπτεία των θυγατρικών του ιδρύματος και να λαμβάνει υπόψη τη φύση, την κλίμακα και την πολυπλοκότητα των διαφόρων κινδύνων στους οποίους ο όμιλος και οι θυγατρικές του εκτίθενται·

(β) εγκρίνει μια πολιτική εσωτερικής διακυβέρνησης σε επίπεδο ομίλου η οποία περιλαμβάνει την υποχρέωση των θυγατρικών να πληρούν όλες τις εφαρμοστέες απαιτήσεις διακυβέρνησης·

(γ) διασφαλίζει ότι σε κάθε θυγατρική είναι διαθέσιμοι επαρκείς πόροι έτσι ώστε να πληρούνται τόσο τα πρότυπα του ομίλου όσο και τα τοπικά πρότυπα διακυβέρνησης·

(δ) διαθέτει κατάλληλα μέσα για την παρακολούθηση της συμμόρφωσης κάθε θυγατρικής με όλες τις ισχύουσες απαιτήσεις εσωτερικής διακυβέρνησης· και

(ε) διασφαλίζει ότι οι δίαυλοι αναφοράς στον όμιλο είναι σαφείς και διαφανείς, ιδίως όπου υπάρχει αναντιστοιχία των επιχειρηματικών γραμμών με τη νομική διάρθρωση του ομίλου.

(5) Σε περίπτωση όπου το ίδρυμα είναι μέλος ομίλου, και αποτελεί θυγατρική εταιρεία, το διοικητικό του όργανο εφαρμόζει τις ρυθμίσεις διακυβέρνησης, τις διαδικασίες και τους μηχανισμούς που έχουν αναπτυχθεί σε επίπεδο ομίλου, εκτός εάν νομικές και εποπτικές απαιτήσεις στη Δημοκρατία ή θέματα αναλογικότητας καθορίζουν διαφορετικά· σε αυτό το πλαίσιο, το διοικητικό όργανο του ιδρύματος αξιολογεί τυχόν αποφάσεις διακυβέρνησης σε επίπεδο ομίλου ή πρακτικές για να διασφαλίζει ότι –

(α) δεν είναι κατά παράβαση των διατάξεων του Κανονισμού (ΕΕ) αριθ. 575/2013, του Νόμου και των Οδηγιών που εκδίδονται δυνάμει του Νόμου και, όπου εφαρμόζεται, άλλων νομοθετικών πράξεων ή προτύπων·

(β) δεν είναι επιζήμιες για –

(i) την ορθή και συνετή διαχείριση του ιδρύματος·
(ii) την οικονομική ευρωστία του ιδρύματος·
(iii) τα έννομα συμφέροντα των ενδιαφερόμενων μερών του ιδρύματος.

ΜΕΡΟΣ ΙΙΙ
ΔΙΟΙΚΗΤΙΚΟ ΟΡΓΑΝΟ

Τμήμα 1 - Σύνθεση, οργάνωση και λειτουργία του διοικητικού οργάνου και πρόσβαση σε πληροφορίες και πόρους

Μέγεθος και σύνθεση διοικητικού οργάνου.

6. Το μέγεθος και η σύνθεση του διοικητικού οργάνου καθορίζεται λαμβάνοντας υπόψη το μέγεθος και την πολυπλοκότητα του ιδρύματος και τη φύση και το πεδίο εφαρμογής των δραστηριοτήτων του, διασφαλίζοντας ότι–

(α) το διοικητικό όργανο αποτελείται από τουλάχιστον επτά (7) μέλη και όχι περισσότερα από δεκατρία (13) μέλη·

(β) τουλάχιστον το πενήντα τοις εκατό (50%) των μελών του διοικητικού οργάνου στρογγυλοποιημένο προς τα κάτω συν ένα (1) μέλος είναι ανεξάρτητα σύμφωνα με το άρθρο 19Β του Νόμου·

(γ) τα εκτελεστικά μέλη πρέπει να είναι τουλάχιστον δύο (2) και όχι περισσότερο από είκοσι πέντε τοις εκατό (25%) των μελών του διοικητικού οργάνου στρογγυλοποιημένο προς τα κάτω, ένα εκ των οποίων πρέπει να είναι ο διευθύνων σύμβουλος·

(δ) το διοικητικό όργανο είναι επαρκώς διαφοροποιημένο όσον αφορά την ηλικία, το φύλο και το εκπαιδευτικό και επαγγελματικό υπόβαθρο ώστε να αποτυπώνει ένα αρκούντως ευρύ φάσμα εμπειριών και να διευκολύνει την εξαγωγή μιας ποικιλίας ανεξάρτητων γνωμοδοτήσεων και κριτικών προκλήσεων·

(ε) το διοικητικό όργανο κατέχει συνολικά επαρκείς γνώσεις, δεξιότητες και εμπειρία ώστε να μπορεί να κατανοήσει τις δραστηριότητες του ιδρύματος, συμπεριλαμβανομένων των κυριότερων κινδύνων·

Νοείται ότι, τα μέλη του δεν δύνανται να ορίσουν αναπληρωματικά μέλη για την εκπροσώπησή τους σε περίπτωση απουσίας τους.

Οργάνωση και λειτουργία διοικητικού οργάνου.

7. Τα ιδρύματα διαθέτουν κατάλληλες πολιτικές, πρακτικές και διαδικασίες εσωτερικής διακυβέρνησης για την οργάνωση και λειτουργία του διοικητικού οργάνου, σύμφωνα με τον Νόμο και την παρούσα Οδηγία διασφαλίζοντας τα ακόλουθα:

(1) Σε σχέση με την οργανωτική δομή του διοικητικού οργάνου:

(α) τη θέση του προέδρου του διοικητικού οργάνου σύμφωνα με τις διατάξεις του άρθρου 19Β του Νόμου κατέχει ανεξάρτητο μέλος του διοικητικού οργάνου·

(β) τη θέση του αντιπροέδρου του διοικητικού οργάνου κατέχει μη εκτελεστικό μέλος, και αναλαμβάνει τους ρόλους και τις αρμοδιότητες του προέδρου σε περίπτωση απουσίας του τελευταίου·

(γ) ένα ανεξάρτητο μέλος του διοικητικού οργάνου διορίζεται ως ανώτερο ανεξάρτητο μέλος·

νοείται ότι το ανώτερο ανεξάρτητο μέλος του διοικητικού οργάνου δεν μπορεί να κατέχει τη θέση του προέδρου ή του αντιπροέδρου·

(δ) επιτροπές κατάλληλου μεγέθους, σύνθεσης, δομής και αρμοδιοτήτων εγκαθιδρύονται για την αποτελεσματική εκτέλεση των ρόλων και των αρμοδιοτήτων του διοικητικού οργάνου, σύμφωνα με τις διατάξεις του Μέρους IV.

(2) Σε σχέση με τη διοργάνωση των συνεδριάσεων του διοικητικού οργάνου και των επιτροπών του:

(α) το διοικητικό όργανο πραγματοποιεί τακτικές συνεδριάσεις για την επαρκή και αποτελεσματική εκτέλεση των καθηκόντων του·

(β) καταβάλλεται κάθε δυνατή προσπάθεια για τη διεξαγωγή τουλάχιστον μία φορά το χρόνο τακτικής συνεδρίασης του διοικητικού οργάνου με τη φυσική παρουσία όλων των μελών·

(γ) τα μη εκτελεστικά μέλη του διοικητικού οργάνου πραγματοποιούν χωρίς την παρουσία των εκτελεστικών μελών, τακτικές συνεδριάσεις, οι οποίες δύναται να είναι με την παρουσία των εξωτερικών ελεγκτών και/ή των επικεφαλής των τμημάτων ελέγχου, ανάλογα με την περίπτωση, και τουλάχιστον σε εξαμηνιαία βάση·

(δ) τα μη εκτελεστικά μέλη του διοικητικού οργάνου συναντώνται χωρίς την παρουσία του προέδρου τουλάχιστον ετησίως για εκτίμηση της απόδοσης του προέδρου·

(ε) η ρυθμίση για τη συμμετοχή σε τακτικές ή έκτακτες συνεδριάσεις μέσω τηλεδιάσκεψης ή βιντεοδιάσκεψης δεν πρέπει να χρησιμοποιείται καταχρηστικά αλλά με προσοχή στο επίπεδο του μέλους ή του διοικητικού οργάνου διασφαλίζοντας ότι τουλάχιστον το πενήντα τοις εκατό (50%) του διοικητικού οργάνου συν ένα (1) μέλος, στρογγυλοποιημένο προς τα κάτω, των μελών είναι φυσικά παρόντες σε έκαστη τακτική συνεδρίαση·

(στ) τα μέλη του διοικητικού οργάνου δεν δύνανται να απουσιάζουν από τις συνεδριάσεις του διοικητικού οργάνου, είτε φυσικά είτε μέσω τηλεδιάσκεψης/βιτεοδιάσκεψης, για περισσότερο από δύο (2) συνεχόμενες συνεδριάσεις ή είκοσι πέντε τοις εκατό (25%) των ετήσιων συνεδριάσεων·

(ζ) η άσκηση δικαιώματος ψήφου μέσω πληρεξουσίου αντιπροσώπου δύναται να επιτραπεί σε μέλος που απουσιάζει από συνεδρίαση, εφόσον η άσκηση ψήφου μέσω πληρεξούσιου περιορίζεται σε μία (1) για κάθε μέλος που συμμετέχει στη συνεδρία, και τα μέλη που ψηφίζουν μέσω πληρεξουσίου είναι υπόλογοι για τη ψήφο του πληρεξούσιου αντιπροσώπου τους·

(η) κανένα άλλο πρόσωπο δεν είναι παρών, εκτός εάν έχει προσκληθεί επισήμως να παραστεί ενόψει συζήτησης συγκεκριμένου θέματος/των στην ημερήσια διάταξη· οποιοδήποτε τέτοιο πρόσωπο είναι παρών μόνο κατά τη συζήτηση του συγκεκριμένου θέματος και εγκαταλείπει την αίθουσα συσκέψεων αμέσως μετά, χωρίς καμία συμμετοχή στη διαδικασία λήψης αποφάσεων.

(3) Όσον αφορά το χειρισμό των συμφερόντων ή σύγκρουσης συμφερόντων ή δυνητικών συμφερόντων ή σύγκρουσης συμφερόντων των μελών του διοικητικού οργάνου:

(α) υπάρχει καταγεγραμμένη διαδικασία εξέτασης ή έγκρισης συμμετοχής μελών του διοικητικού οργάνου σε συγκεκριμένες δραστηριότητες, όπως η συμμετοχή σε διοικητικό όργανο άλλης οντότητας, για να διασφαλίζεται ότι τέτοια συμμετοχή δεν θα δημιουργεί σύγκρουση συμφερόντων·

(β) υπάρχει απαίτηση γνωστοποίησης από τα μέλη τυχόν συγκρούσεων συμφερόντων τους και αποχής τους από τη διαδικασία λήψης αποφάσεων ή ψηφοφορίας για οποιοδήποτε θέμα

όπου δύνανται να έχουν σύγκρουση συμφερόντων· ειδικότερα:

(i) πριν από την έναρξη κάθε συνεδρίασης ο προεδρεύων της συνεδρίασης οφείλει να διαβάζει όλα τα θέματα της ημερήσιας διάταξης, ένα προς ένα, και να ζητάει όπως ο κάθε συμμετέχοντας, συμπεριλαμβανομένων του ιδίου, αναφέρει σαφώς για κάθε θέμα κατά πόσον έχει ή όχι συμφέρον ή σύγκρουση συμφερόντων ή δυνητικού συμφέροντος ή σύγκρουσης συμφερόντων·

Νοείται ότι, μέλος που ενεργεί ως πληρεξούσιος αντιπρόσωπος αναφέρει επιπρόσθετα για κάθε θέμα κατά πόσον το μέλος που του έχει χορηγήσει πληρεξούσιο έχει ή όχι συμφέρον ή σύγκρουση συμφερόντων ή δυνητικό συμφέρον ή σύγκρουση συμφέροντος·

(ii) κατά την ολοκλήρωση της διαδικασίας που αναφέρεται στο υποσημείο (i), ο πρόεδρος καλεί όλα τα μέλη που συμμετέχουν στη συνεδρίαση να υποβάλουν τα σχόλια τους αναφορικά με τις δηλώσεις που έχουν δηλωθεί·

(iii) εάν εντοπιστεί σύγκρουση συμφερόντων για θέμα της ημερήσιας διάταξης, τότε το εμπλεκόμενο μέλος πρέπει να απέχει από τη συζήτηση και από τη ψηφοφορία του συγκεκριμένου θέματος, είτε αυτοπροσώπως είτε μέσω πληρεξούσιου αντιπροσώπου·

(iii) ανάλογη διαδικασία πρέπει να ακολουθείται για οποιαδήποτε άλλα/ειδικά θέματα συζητούνται·

(γ) τον τρόπο με τον οποίο το διοικητικό όργανο αντιμετωπίζει οποιαδήποτε μη συμμόρφωση με τις πολιτικές, πρακτικές και διαδικασίες σχετικά με τις συγκρούσεις συμφερόντων· η μη συμμόρφωση πρέπει να γνωστοποιείται άμεσα στην Κεντρική Τράπεζα.

(4) Όσον αφορά την τήρηση των πρακτικών των συνεδριάσεων του διοικητικού οργάνου και των επιτροπών του:

(α) λεπτομερή πρακτικά τηρούνται για κάθε συνεδρίαση τα οποία οριστικοποιούνται το αργότερο εντός δέκα (15) εργάσιμων ημερών μετά τη συνεδρίαση και εγκρίνονται επισήμως στην επόμενη συνεδρίαση·

(β) στα πρακτικά της συνεδρίασης καταγράφεται –

(i) ο χρόνος της συνεδρίασης, η τοποθεσία διεξαγωγής και οι παρευρισκόμενοι συμπεριλαμβανομένων των προσκεκλημένων, με φυσική παρουσία και μέσω ηλεκτρονικών μέσων·

(ii) τους λόγους για πρόσκληση ατόμων να παραστούν στη συνεδρίαση, σύμφωνα με την υποπαράγραφο 2(η), το σχετικό θέμα στην ημερήσια διάταξη και τις θέσεις και/ή τις απόψεις τους·

(ii) όλα τα θέματα της ημερήσιας διάταξης και οι αντίστοιχες συζητήσεις, οι αποφάσεις, τα αποτελέσματα της ψηφοφορίας, γνώμες και απόψεις της μειοψηφίας, καθώς και οι ανησυχίες που δεν έχουν επιλυθεί·

(iii) οι δηλώσεις που αναφέρονται στο σημείο (β) της υποπαραγράφου (3) καταγράφονται ξεχωριστά υπό τον τίτλο «αναγνώριση των συμφερόντων ή συγκρούσεων συμφερόντων ή δυνητικών συμφερόντων ή σύγκρουση συμφερόντων".

(5) Όλα τα μέλη του διοικητικού οργάνου, ιδίως τα μη εκτελεστικά μέλη:

(α) λαμβάνουν στοχευμένη εκπαίδευση για την ανάπτυξη και/ή ανανέωση των γνώσεων και των δεξιοτήτων τους· και

(β) έχουν πρόσβαση στις συμβουλές και υπηρεσίες του γραμματέα της εταιρείας.

(6) Σχετικά με την αντιμετώπιση της μη συμμόρφωσης με τις πολιτικές και διαδικασίες του διοικητικού οργάνου –

(α) υπάρχει κατάλληλη διαδικασία για την παρακολούθηση της συμμόρφωσης με τις πολιτικές,

διεργασίες και διαδικασίες του διοικητικού οργάνου·

(β) υπάρχει επίσημος και καλά τεκμηριωμένος μηχανισμός για την παροχή οδηγιών και την ανάθεση αρμοδιοτήτων για–

(i) την αξιολόγηση των αιτίων μη συμμόρφωσης·

(ii) την έναρξη, απαίτηση, εφαρμογή και παρακολούθηση της αποτελεσματικότητας των διορθωτικών μέτρων· και

(iii) την τεκμηρίωση της όλης διαδικασίας και του αποτελέσματος της διαδικασίας·

(γ) την κοινοποίηση σε εύθετο χρόνο μη συμμόρφωσης με τον Νόμο και την παρούσα Οδηγία στην Κεντρική Τράπεζα, και –

(i) εντός προθεσμίας ενός (1) μηνός από την ημερομηνία εντοπισμού περίπτωσης μη συμμόρφωσης, της διαδικασίας που ακολουθήθηκε και τα πρόσωπα που εμπλέκονται στην επίλυση αυτών των περιπτώσεων μη συμμόρφωσης· και

(ii) εντός δύο (2) μηνών από την ημερομηνία εντοπισμού περίπτωσης μη συμμόρφωσης, τα επανορθωτικά / διορθωτικά μέτρα που λήφθηκαν για την αντιμετώπιση αυτών των περιπτώσεων μη συμμόρφωσης.

Πρόσβαση σε πληροφορίες και πόρους του διοικητικού οργάνου κατά την άσκηση εποπτείας.

8. (1) Το διοικητικό όργανο, κατά την άσκηση των εποπτικών του αρμοδιοτήτων, και η επιτροπή κινδύνων, σε περίπτωση που έχει συσταθεί τέτοια, έχουν επαρκή πρόσβαση σε πληροφορίες ως προς την κατάσταση κινδύνου του ιδρύματος και, εάν απαιτείται και κρίνεται σκόπιμο, σε πληροφορίες που αφορούν το τμήμα διαχείρισης κινδύνων και σε ειδικούς εξωτερικούς συμβούλους.

(2) Το διοικητικό όργανο, κατά την άσκηση των εποπτικών του αρμοδιοτήτων, και η επιτροπή κινδύνων, σε περίπτωση που έχει συσταθεί τέτοια, καθορίζουν το είδος, την ποσότητα, τη μορφή και τη συχνότητα των πληροφοριών που πρέπει να λαμβάνουν σχετικά με θέματα κινδύνου. Με σκοπό την υποβοήθηση της δημιουργίας υγιών πολιτικών και πρακτικών αποδοχών, η επιτροπή κινδύνων, τηρουμένων των καθηκόντων της επιτροπής αποδοχών, εξετάζει κατά πόσο τα κίνητρα που προβλέπει το σύστημα αποδοχών λαμβάνουν υπόψη τον κίνδυνο, το κεφάλαιο, τη ρευστότητα και την πιθανότητα και το χρονοδιάγραμμα εσόδων.

Τμήμα 2 - Απαιτήσεις για την ανάδειξη υποψηφίων, την επιλογή και διαδοχή των μελών του διοικητικού οργάνου και την αξιολόγηση της διοικητικού οργάνου

Ανάδειξη υποψηφίων, επιλογή και διαδοχή των μελών του διοικητικού οργάνου.

9. (1) Οι επιτροπές ανάδειξης υποψηφίων των ιδρυμάτων, πρέπει να υιοθετούν ένα ευρύ φάσμα προσόντων και δεξιοτήτων κατά την πρόσληψη μελών και τον επαναδιορισμό υφιστάμενων μελών στο διοικητικό όργανο και να εφαρμόζουν για το σκοπό αυτό πολιτική που να προωθεί το αρμόζον επίπεδο ποικιλομορφίας του διοικητικού οργάνου.

(2) Τα ιδρύματα εφαρμόζουν κατάλληλη πολιτική πρόσληψης για την ανάδειξη υποψηφίων, επιλογή, επαναδιορισμό και τη διαδοχή μελών του διοικητικού οργάνου η οποία να περιλαμβάνει, τουλάχιστο, τα ακόλουθα:

(α) περιγραφή των απαραίτητων ικανοτήτων, δεξιοτήτων, και ακαδημαϊκών ή επαγγελματικών προσόντων για τη διασφάλιση επαρκούς τεχνογνωσίας και συμμόρφωσης με τις απαιτήσεις της παρούσας Οδηγίας και τις διατάξεις της Περί της Αξιολόγησης για την Ικανότητα και Καταλληλότητα των Μελών Διοικητικού Οργάνου και των Διευθυντών των ΑΠΙ Οδηγία του 2014·

(β) την απαίτηση ότι, πριν από το διορισμό νέων μελών, οι υποψήφιοι βεβαιώνονται ότι έχουν τις γνώσεις, δεξιότητες, εμπειρία και χρόνο για να συμβάλουν θετικά στο διοικητικό όργανο·

(γ) την απαίτηση ότι, η επιτροπή ανάδειξης υποψηφίων ετοιμάζει για το διοικητικό όργανο έκθεση στην οποία αναφέρεται στο πώς κατέληξε στην ανάδειξη των υποψηφίων για την πλήρωση των κενών θέσεων στο διοικητικό όργανο·

(δ) την υποχρέωση παροχής επαρκών πληροφορίων στους μετόχους για την επιλογή προσώπου ως μέλους του διοικητικού οργάνου, συμπεριλαμβανομένων:

(i) περιγραφής των προσόντων, εμπειριών και ικανοτήτων του ατόμου·

(ii) περιγραφής των ρόλων και καθηκόντων της συγκεκριμένης κενής θέσης·

(iii) του αναμενόμενου χρόνου δέσμευσης·

(iv) επεξήγησης του λόγου που ο διορισμός του συγκεκριμένου ατόμου κρίθηκε κατάλληλος·

(ε) τη διάρκεια της θητείας και του αριθμού επαναδιορισμού εκτελεστικών και μη εκτελεστικών καθώς και ανεξάρτητων μελών του διοικητικού οργάνου·

(στ) την απαίτηση ότι ο επαναδιορισμός γίνεται με βάση την απόδοση του μέλους, όπως τεκμηριώνεται από τις εκθέσεις αξιολόγησης·

(ζ) κατάλληλο σχέδιο διαδοχής των μελών του, το οποίο να λαμβάνει υπόψη, μεταξύ άλλων, την ημερομηνία λήξης της σύμβασης του κάθε μέλους ή με στόχο να αποτρέπει την ταυτόχρονη αντικατάσταση πολλών μελών.

(3) Τα ιδρύματα οφείλουν να καθορίσουν ένα μέγιστο αριθμό θητειών που δύναται να υπηρετεί ένα μέλος ως μη εκτελεστικό μέλος του διοικητικού οργάνου· σε κάθε περίπτωση, μέλος μπορεί να υπηρετήσει ως μη εκτελεστικό μέλος ενός ιδρύματος για μέγιστο χρονικό διάστημα δώδεκα (12) ετών συμπεριλαμβανομένων των διορισμών σε οποιαδήποτε διοικητικά όργανα του ομίλου.

(4) Τα ιδρύματα οφείλουν να καθορίσουν ένα μέγιστο αριθμό θητειών που δύναται να υπηρετεί ένα άτομο ως πρόεδρος του διοικητικού οργάνου ή επιτροπής του διοικητικού οργάνου· σε κάθε περίπτωση, άτομο μπορεί να υπηρετήσει στη θέση του προέδρου του διοικητικού οργάνου για μέγιστο χρονικό διάστημα έξι (6) χρόνια είτε αυτά είναι συνεχόμενα είτε όχι.

(5) Τα ιδρύματα αφιερώνουν επαρκές προσωπικό και οικονομικούς πόρους για την υποδοχή και εκπαίδευση των μελών του διοικητικού οργάνου.

Αξιολόγηση του διοικητικού οργάνου.

10. (1) Τα ιδρύματα οφείλουν να διαθέτουν κατάλληλη μεθοδολογία και διαδικασία για την εις βάθος και με βάση κανόνων αξιολόγηση της απόδοσης του διοικητικού οργάνου στο σύνολό του, κάθε επιτροπής και κάθε μέλους του διοικητικού οργάνου τουλάχιστο σε ετήσια βάση· η διαδικασία αξιολόγησης πρέπει να καλύπτει, τουλάχιστο, τα ακόλουθα:

(α) την απόδοση του διοικητικού οργάνου στο σύνολό του, των επιτροπών και των μεμονωμένων μελών·

(β) τη συμβολή του διοικητικού οργάνου στο σύνολό του, των επιτροπών και των μεμονωμένων μελών –

(i) στην ανάπτυξη των επιχειρηματικών στόχων, της διάθεσης ανάληψης κινδύνων και των στρατηγικών·

(ii) στον καθορισμό και την επίβλεψη των πλαισίων διαχείρισης κινδύνων και κανονιστικής συμμόρφωσης·

(iii) στη δημιουργία και διατήρηση συνεπών οργανωτικών και λειτουργικών ρυθμίσεων και μηχανισμών εσωτερικού ελέγχου·

(γ) τη σύνθεση του διοικητικού οργάνου και των επιτροπών του·

(δ) την επικοινωνία με τη διοίκηση, τους μετόχους και τις αρμόδιες αρχές·

(ε) το ρόλο του προέδρου του διοικητικού οργάνου, του γραμματέα εταιρείας και του ανώτερου ανεξάρτητου μέλους του διοικητικού οργάνου·

(στ) τη δέσμευση χρόνου των μη εκτελεστικών μελών και την ικανότητα κριτικής εξέτασης πληροφοριών·

(ζ) την αξιολόγηση της ικανότητας και καταλληλότητας κάθε μέλους του διοικητικού οργάνου με βάση τα ισχύοντα κριτήρια της περί της Αξιολόγησης της Ικανότητας και Καταλληλότητας των Μελών Διοικητικού Οργάνου και Διευθυντών ΑΠΙ Οδηγίας του 2014 και ιδιαίτερα της ανεξαρτησίας κάθε ανεξάρτητου μέλους με βάση τα ισχύοντα κριτήρια της εν λόγω Οδηγία:

Νοείται ότι, αν σε οποιαδήποτε χρονική στιγμή, τα πρόσωπα που κατέχουν θέση ανεξάρτητου μέλους, λόγω εξελίξεων δεν πληρούν ή φαίνεται να μην πληρούν οποιοδήποτε από τα κριτήρια ανεξαρτησίας, τότε το διοικητικό όργανο επιλαμβάνεται άμεσα του εν λόγω θέματος σύμφωνα με την παράγραφο 7(6), προχωρώντας με τη λήψη των αναγκαίων διορθωτικών μέτρων, συμπεριλαμβανομένης της απομάκρυνσης του εν λόγω μέλους από το διοικητικό όργανο ή τον επαναπροσδιορισμό του ρόλου του στο διοικητικό όργανο και / ή το διορισμό νέου ανεξάρτητου μέλους· η χρονική περίοδος για την εφαρμογή όλων των αναγκαίων μέτρων αποκατάστασης δεν θα πρέπει να υπερβαίνει τον ένα (1) μήνα:

Νοείται περαιτέρω ότι το εν λόγω μέλος πρέπει να απαλλαγεί από τα καθήκοντα που διεξάγει ως ανεξάρτητο μέλος του διοικητικού οργάνου από την ημερομηνία που εντοπίζεται η μη συμμόρφωση του/της με τα κριτήρια ανεξαρτησίας.

(2) Ως μέρος της διαδικασίας αξιολόγησης, τα ιδρύματα οφείλουν να διασφαλίζουν ότι τα μη εκτελεστικά μέλη του διοικητικού οργάνου αξιολογούν οι ίδιοι τις ατομικές τους δεξιότητες, γνώσεις και εμπειρία, και καθορίζουν κατά πόσο περαιτέρω επαγγελματική ανάπτυξη θα τους βοηθήσει να αναπτύξουν την τεχνογνωσία τους και να εκπληρώσουν τις υποχρεώσεις τους.

(3) Τα ιδρύματα οφείλουν να αναθέτουν την πραγματοποίηση τουλάχιστον κάθε τρία (3) χρόνια, της εξέτασης και αξιολόγησης της σύνθεσης, της αποδοτικότητας και της αποτελεσματικότητας του διοικητικού οργάνου και των επιτροπών του σε ανεξάρτητο εξωτερικό σύμβουλο, λαμβάνοντας υπόψη τις απαιτήσεις της παρούσας Οδηγίας και για να αποκομίσουν μια αντικειμενική άποψη και για να ενημερωθούν για τις βέλτιστες πρακτικές του κλάδου.

Τμήμα 3 – Σημαντικοί ρόλοι και αρμοδιότητες του διοικητικού οργάνου

Καθορισμός και επίβλεψη στρατηγικής.

11. (1) Το διοικητικό όργανο είναι υπεύθυνο για τον καθορισμό, την περιοδική επίβλεψη και επανεξέταση της εφαρμογής των επιχειρηματικών στόχων του ιδρύματος καθώς επίσης και των στρατηγικών του ιδρύματος για την επίτευξη των στόχων αυτών, συμπεριλαμβανομένων των στρατηγικών αντιμετώπισης κινδύνων και των σχεδίων εσωτερικού κεφαλαίου, λαμβάνοντας υπόψη τη φερεγγυότητα και τα μακροπρόθεσμα οικονομικά συμφέροντα του ιδρύματος, καθώς και τα συμφέροντα των καταθετών, των μετόχων και άλλων ενδιαφερομένων μερών.

(2) Το διοικητικό όργανο διασφαλίζει ότι το ίδρυμα διαθέτει σχεδιασμό για την ανάπτυξη των επιχειρηματικών στόχων και στρατηγικών· ο εν λόγω σχεδιασμός διασφαλίζει ότι:

(α) ο κώδικας επιχειρηματικής δεοντολογίας του ιδρύματος και οι εταιρικές αξίες αντικατοπτρίζονται στους επιχειρηματικούς στόχους και στρατηγικές· και

(β) οι ρόλοι του επικεφαλής του τμήματος διαχείρισης κινδύνων, της διαχείρισης διαθεσίμων και του οικονομικού διευθυντή στην ανάπτυξη στρατηγικών είναι καταλλήλως και σαφώς διαφοροποιημένοι.

(3) Κατά τη διαμόρφωση των στρατηγικών, το διοικητικό όργανο οφείλει να:

(α) καθορίζει και να θέτει προτεραιότητες για την εκπλήρωση των άμεσων καθώς και των μελλοντικών επιχειρησιακών στόχων τόσο του ιδρύματος όσο και του ομίλου του, σε περίπτωση που το ίδρυμα είναι η μητρική εταιρεία, λαμβάνοντας υπόψη το εφαρμοστέο νομοθετικό και ρυθμιστικό πλαίσιο·

(β) καθορίζει τη διάθεση ανάληψης κινδύνων του ιδρύματος, μέσω της διατύπωσης σε γραπτή μορφή μίας δήλωσης για τη διάθεση ανάληψης κινδύνων και ορίων κινδύνων σύμφωνα με τις διατάξεις της παραγράφου 61 και τη διαδοχική και κλιμακωτή εφαρμογή τους στον οργανισμό·

και

(γ) αξιολογεί σε συνεχή βάση και υπό εναλλακτικά σενάρια σύμφωνα με τις παραγράφους (6) και (8)-(12), τα ποσά, τους τύπους και την κατανομή των εσωτερικών κεφαλαίων και των ρευστών διαθεσίμων και εγκρίνει τα κεφαλαία και τη χρηματοδότηση σχεδίων και προϋπολογισμό αναλογικό με το είδος και το μέγεθος των δραστηριοτήτων του, τη διάθεση ανάληψης κινδύνων του ιδρύματος και τα εκτιμώμενα χρηματοοικονομικά αποτελέσματα.

(5) Το διοικητικό όργανο διασφαλίζει ότι το ίδρυμα διαθέτει μια αποτελεσματική διαδικασία για την πληροφόρηση και συνεχή ενημέρωση του προσωπικού για τις σχετικές με τα καθήκοντά του στρατηγικές του ιδρύματος, με σαφή και συνεπή τρόπο.

(6) Το διοικητικό όργανο οφείλει να έχει μια διαδικασία για την αναθεώρηση των επιχειρηματικών στόχων και στρατηγικών σε τακτική βάση, τουλάχιστον ετησίως, για να διασφαλιστεί ότι παραμένουν περιεκτικοί και αναλογικοί προς τη φύση, κλίμακα και πολυπλοκότητα των δραστηριοτήτων του εν λόγω ιδρύματος.

(7) Το διοικητικό όργανο οφείλει να έχει διαδικασίες για την αξιολόγηση του κατά πόσο το ίδρυμα λειτουργεί εντός των εγκεκριμένων στρατηγικών του· για το σκοπό αυτό το διοικητικό όργανο καθορίζει και επικοινωνεί στα ανώτατα διοικητικά στελέχη σαφή και αντικειμενικούς στόχους απόδοσης και μέτρα, που αφορούν τόσο το ίδρυμα όσο και τα ανώτατα διοικητικά στελέχη.

Καθορισμός και επίβλεψη δομής του ιδρύματος και του ομίλου.

12. (1) Το διοικητικό όργανο οφείλει να κατανοεί τη δομή του ιδρύματος και τον τρόπο που οι διάφορες συνιστώσες της δομής αλληλοσυμπληρώνονται και αλληλεπιδρούν, να αναγνωρίζει τους περιορισμούς της, να αξιολογεί τους κινδύνους που δύναται να προκληθούν ένεκα των περιορισμών και της πολυπλοκότητα της δομής και να κατευθύνει την εξέλιξη της, κατά τρόπο που να διασφαλίζει ότι η δομή του ιδρύματος –

(α) είναι δικαιολογημένη και ευθυγραμμισμένη με την εγκεκριμένη επιχειρηματική στρατηγική και τη διάθεση ανάληψης κινδύνων του ιδρύματος·

(β) δεν ενέχει υπερβολική ή ακατάλληλη πολυπλοκότητα που να εμποδίζει την ικανότητα του διοικητικού οργάνου για αποτελεσματική εποπτεία και διαχείριση των κινδύνων που αντιμετωπίζει το ίδρυμα· και

(γ) είναι διαφανής στα ενδιαφερόμενα μέρη.

(2) Σε περίπτωση που το ίδρυμα είναι η μητρική εταιρεία ομίλου, το διοικητικό όργανο οφείλει –

(α) να κατανοεί τη δομή του ομίλου, το σκοπό των διαφορετικών μονάδων και οντοτήτων του ομίλου και τις συνδέσεις και σχέσεις τόσο μεταξύ τους όσο και με το ίδρυμα· αυτό προϋποθέτει την αξιολόγηση των ειδικών λειτουργικών κινδύνων του ομίλου, των ανοιγμάτων εντός του ομίλου και τον τρόπο που θα μπορούσε να επηρεαστεί η χρηματοδότηση, το κεφάλαιο και το προφίλ κινδύνου του ομίλου, υπό κανονικές και αντίξοες συνθήκες·

(β) να τηρείται ενήμερο για τους κινδύνους που δύναται να προκαλεί η δομή του ομίλου· η πληροφόρηση αυτή να περιλαμβάνει:

(i) πληροφορίες για τις κύριες αιτίες κινδύνου· και

(ii) τακτικές εκθέσεις αξιολόγησης της γενικής δομής του ιδρύματος και αξιολόγησης της συμμόρφωσης των δραστηριοτήτων της κάθε οντότητας με την εγκεκριμένη στρατηγική·

(γ) να αξιολογεί τις συνέπειες που συνεπάγονται από αλλαγές στη δομή του ομίλου, όπως είναι η σύσταση νέων θυγατρικών, συγχωνεύσεις ή εξαγορές, αναστολή της λειτουργίας τμημάτων του ιδρύματος ή του ομίλου, ή μεταβολές που οφείλονται σε εξωτερικές εξελίξεις, όσον αφορά την οικονομική ευρωστία του και να προβαίνει εγκαίρως στις αναγκαίες προσαρμογές.

(3) Το διοικητικό όργανο εγκρίνει υγιείς στρατηγικές και πολιτικές για τη σύσταση νέων δομών και διασφαλίζει ότι οι εν λόγω πολιτικές και διαδικασίες γνωστοποιούνται στην Κεντρική Τράπεζα· όταν ένα ίδρυμα ή ένας όμιλος λειτουργεί ή προτίθεται να λειτουργήσει μέσω οντοτήτων ειδικού σκοπού ή άλλων παρόμοιων δομών ή σε δικαιοδοσίες οι οποίες εμποδίζουν τη διαφάνεια ή δεν πληρούν τα διεθνή τραπεζικά πρότυπα, οι πολιτικές αυτές πρέπει να διασφαλίζουν ότι:

(α) οι εν λόγω δομές και δραστηριότητες –

(i) είναι αποδεκτές μόνο όταν εντοπίζονται οι συναφείς κίνδυνοι, αξιολογούνται δεόντως και το ίδρυμα βεβαιώνεται ότι οι κίνδυνοι αυτοί μπορούν να τύχουν κατάλληλης διαχείρισης ή μετριασμού·

(ii) υπόκεινται σε κατάλληλα όρια·

(β) αξιολογείται περιοδικά η ανάγκη άσκησης δραστηριοτήτων μέσω τέτοιων δομών.

(4) Το διοικητικό όργανο διασφαλίζει την ύπαρξη υγιών και αποτελεσματικών μέτρων και συστημάτων για τη παραγωγή και ανταλλαγή πληροφοριών μεταξύ και εντός των διάφορων μονάδων του ιδρύματος και στην περίπτωση κατά την οποία το ίδρυμα είναι η μητρική εταιρεία ενός ομίλου, τη παραγωγή και ανταλλαγή πληροφοριών μεταξύ και εντός των διαφόρων οντοτήτων του ομίλου, συμπεριλαμβανομένων του τύπου, του καταστατικού, της ιδιοκτησιακής δομής και επιχειρηματικών δραστηριοτήτων κάθε νομικής οντότητας.

(5) Το διοικητικό όργανο διασφαλίζει ότι κάθε ροή σημαντικών πληροφοριών σχετικών με την επιχειρησιακή λειτουργία του ιδρύματος και του επικεφαλής ομίλου είναι τεκμηριωμένη και τίθεται στη διάθεση του διοικητικού οργάνου, του τμήματος ελέγχου και των εποπτικών αρχών, συμπεριλαμβανομένων πληροφοριών που αφορούν την έγκριση και συντήρηση οντοτήτων ειδικού σκοπού ή συναφών δομών ή σε δικαιοδοσίες που παρεμποδίζουν τη διαφάνεια ή δεν πληρούν τα διεθνή τραπεζικά πρότυπα.

Ρύθμιση και επίβλεψη της κατανομής αρμοδιοτήτων και εξουσίας.

13. (1) Το διοικητικό όργανο διασφαλίζει ότι υπάρχουν σαφείς γραμμές ευθύνης και λογοδοσίας σε ολόκληρο το ίδρυμα, συμπεριλαμβανομένων των θυγατρικών, των συνδεδεμένων οντοτήτων και λοιπών συμβατικών σχέσεων, οι οποίες να είναι συμβατές με τη λειτουργική δομή του ιδρύματος.

(2) Το διοικητικό όργανο διασφαλίζει την ύπαρξη σαφούς και τεκμηριωμένης κατανομής των ρόλων, ευθυνών και εξουσιών του διοικητικού οργάνου και των επιτροπών του διοικητικού οργάνου ως σώματα και των μελών του διοικητικού οργάνου ως πρόσωπα, των ανώτατων διοικητικών στελεχών και των τμημάτων ελέγχου, σύμφωνα με τις διατάξεις του Νόμου και της παρούσας Οδηγίας, κατά τέτοιο τρόπο ώστε:

(α) η κατανομή των ρόλων, ευθυνών και εξουσιών να προάγει τον ουσιαστικό διαχωρισμό των λειτουργιών εποπτείας και διαχείρισης·

(β) να είναι σαφές ποιός έχει ποιόν από αυτούς τους ρόλους, ευθύνες και εξουσίες·

(γ) στη περίπτωση που οι ευθύνες έχουν κατανεμηθεί σε περισσότερα από ένα τμήματα του ιδρύματος, ο τρόπος που αυτές οι ευθύνες επιμερίζονται ή κατανέμονται μεταξύ των υπό αναφορά τμημάτων , να είναι κατάλληλος και σαφώς τεκμηριωμένος·

(δ) οι εργασίες και οι υποθέσεις του ιδρύματος να μπορούν να παρακολουθούνται επαρκώς και να ελέγχονται από το διοικητικό όργανο και από τα ανώτατα διοικητικά στελέχη·

(ε) να τηρείται αρχείο των διευθετήσεων κατανομής ευθυνών και εξουσιών για επτά (7) χρόνια από την ημερομηνία κατά την οποία αντικαταστάθηκε από ένα πιο ενήμερο αρχείο.

(3) Το διοικητικό όργανο διασφαλίζει ότι η κατανομή αρμοδιοτήτων σε έκαστο μέλος του διοικητικού οργάνου λαμβάνει δεόντως υπόψη το κατά πόσο το εκάστοτε μέλος έχει την τεχνογνωσία και το βαθμό ανεξαρτησίας και την αντικειμενικότητα που απαιτείται για την εκτέλεση των καθηκόντων που του κατανεμήθηκαν.

(4) Το διοικητικό όργανο ελέγχει και βεβαιώνεται ως προς την ικανότητα των μελών των επιτροπών να διαθέσουν τον απαραίτητο χρόνο για τις επιτροπές· όπου ένα μέλος της επιτροπής δεν είναι σε θέση να διαθέσει επαρκή χρόνο για συμμετοχή στις συνεδρίες της επιτροπής, το διοικητικό όργανο οφείλει να τον/την αντικαταστήσει με άλλο μέλος το οποίο να διαθέτει τον απαραίτητο χρόνο, εμπειρία και τεχνογνωσία.

(5) Το διοικητικό όργανο διασφαλίζει ότι οι επικεφαλής των τμημάτων ελέγχου έχουν την απαραίτητη εξουσία για την άσκηση των καθηκόντων τους και έχουν άμεση πρόσβαση στο διοικητικό όργανο.

Καθορισμός και επίβλεψη και διαδοχή των βασικών λειτουργιών.

14.(1) Το διοικητικό όργανο θεσπίζει και επιβλέπει τις πολιτικές για την επιλογή νέων μελών του διοικητικού οργάνου και τον επαναδιορισμό των υφιστάμενων μελών, σύμφωνα με τις διατάξεις της παραγράφου 9.

(2) Το διοικητικό όργανο θεσπίζει κατάλληλες πρακτικές και διαδικασίες για την παρακολούθηση και περιοδική επανεξέταση:

(α) της επάρκειας και καταλληλότητας του μεγέθους και της σύνθεσης του διοικητικού οργάνου δυνάμει της παραγράφου 6·

(β) της σχετικής τεχνογνωσίας και δεξιοτήτων των μελών της επιτροπής και την ικανότητά τους να αφιερώνουν ικανοποιητικό χρόνο στην επιτροπή·

(γ) της ικανότητας και καταλληλότητας των υφιστάμενων μελών, σύμφωνα με τις διατάξεις της περί της Αξιολόγησης της Ικανότητας και Καταλληλότητας των Μελών του Διοικητικού Οργάνου και των Διευθυντών ΑΠΙ Οδηγίας του 2014.

(3) Το διοικητικό όργανο θεσπίζει και επιβλέπει τις πολιτικές για την επιλογή, ανάπτυξη και αντικατάσταση των ανώτατων διοικητικών στελεχών και των επικεφαλής του τμήματος εσωτερικού ελέγχου δυνάμει των άρθρων 46, 78 και 80.

(4) Το διοικητικό όργανο θεσπίζει κατάλληλες πρακτικές και διαδικασίες για την παρακολούθηση και την περιοδική εξέταση:

(α) της επάρκειας και αποτελεσματικότητας της σύνθεσης και δομής των ανώτατων διοικητικών στελεχών σύμφωνα με τις διατάξεις της παραγράφου 45·

(β) της ικανότητας και την καταλληλότητας των ανώτατων διοικητικών στελεχών, σύμφωνα με τις διατάξεις της περί της Αξιολόγησης της Ικανότητας και Καταλληλότητας των Μελών του Διοικητικού Οργάνου και των Διευθυντών ΑΠΙ Οδηγίας του 2014·

(γ) της ανεξαρτησίας και αντικειμενικότητας των επικεφαλής των τμημάτων ελέγχου.

(5) Το διοικητικό όργανο εγκρίνει και ελέγχει περιοδικά την πολιτική προσλήψεων, εσωτερικών μετακινήσεων και προαγωγών του προσωπικού.

Επίβλεψη των ανώτατων διοικητικών στελεχών.

15.(1) Το διοικητικό όργανο έχει την ευθύνη για τη διεξαγωγή αποτελεσματικής επίβλεψης των ανώτατων διοικητικών στελεχών· συναφώς, θεσπίζει κατάλληλες πολιτικές, πρακτικές και διαδικασίες που να διασφαλίζουν ότι τα ανώτατα διοικητικά στελέχη διεκπεραιώνουν τους ρόλους και τις ευθύνες τους, σύμφωνα με τις διατάξεις των παραγράφων 47 έως 49.

(2) Οι πρακτικές και οι διαδικασίες που αναφέρονται στην υποπαράγραφο (1) περιλαμβάνουν τα ακόλουθα:

(α) τακτικές συναντήσεις με τα ανώτατα διοικητικά στελέχη·

(β) υποβολή ερωτήσεων και κριτική εξέταση των επεξηγήσεων και πληροφοριών που παρέχονται από τα ανώτατα διοικητικά στελέχη·

(γ) καθορισμό των επίσημων στόχων απόδοσης των ανώτατων διοικητικών στελεχών σύμφωνα με τους μακροπρόθεσμους στόχους, στρατηγική και οικονομική ευρωστία του ιδρύματος, και παρακολούθηση της απόδοσης των ανώτατων διοικητικών στελεχών σε σχέση με τους στόχους αυτούς.

Καθορισμός και επίβλεψη του κώδικα επιχειρησιακής δεοντολογίας και των διαδικασιών προειδοποιητικών μηνυμάτων.

16. (1)Το διοικητικό όργανο θα πρέπει να δίνει το παράδειγμα ηγεσίας για την αποτελεσματική εφαρμογή των κατάλληλων προτύπων για τη διαμόρφωση επαγγελματικής και υπεύθυνης συμπεριφορά σε ολόκληρο το ίδρυμα.

(2) Το διοικητικό όργανο διασφαλίζει ότι υπάρχουν κατάλληλες και σαφείς πολιτικές, διεργασίες και διαδικασίες για –

(α) την εφαρμογή και περιοδική εξέταση του κώδικα επιχειρηματικής δεοντολογίας και των εταιρικών αξιών, σύμφωνα με τις διατάξεις της παραγράφου 53· και

(β) την παρακολούθηση και υποβολή αναφορών σχετικά με τη συμμόρφωση με αυτά τα πρότυπα και τις εταιρικές αξίες.

(3) Το διοικητικό όργανο διασφαλίζει ότι το ίδρυμα θεσπίζει κατάλληλες διαδικασίες έγκαιρης εσωτερικής προειδοποίησης που να επιτρέπουν στους υπαλλήλους να κοινοποιούν δυνητικές ή πραγματικές παραβάσεις των εσωτερικών ή κανονιστικών απαιτήσεων ή ανησυχίες τους για ατασθαλίες εντός του ιδρύματος μέσω ενός συγκεκριμένου, ανεξάρτητου και αυτόνομου διαύλου αναφοράς χωρίς το φόβο επιβολής αντίποινων, σύμφωνα με τις διατάξεις της παραγράφου 57.

Έγκριση και περιοδική επανεξέταση τεχνικών κριτηρίων για την οργάνωση και αντιμετώπιση των κινδύνων.

17. (1) Το διοικητικό όργανο εγκρίνει και επανεξετάζει περιοδικά τις στρατηγικές και τις πολιτικές για την ανάληψη, διαχείριση, παρακολούθηση και το μετριασμό των κινδύνων στους οποίους είναι ή θα μπορούσε να είναι εκτεθειμένο το ίδρυμα, περιλαμβανομένων εκείνων που προκαλούνται από το μακροοικονομικό περιβάλλον στο οποίο ασκεί τις δραστηριότητές του, λαμβανομένης υπόψη της φάσης του οικονομικού κύκλου.

(2) Το διοικητικό όργανο αφιερώνει αρκετό χρόνο στην εκτίμηση των θεμάτων κινδύνου. Το διοικητικό όργανο συμμετέχει ενεργά και διασφαλίζει ότι διατίθενται επαρκείς πόροι για τη διαχείριση όλων των σημαντικών κινδύνων που εξετάζονται στην παρούσα οδηγία και στον κανονισμό (ΕΕ) αριθ. 575/2013, καθώς και στην αποτίμηση των στοιχείων ενεργητικού, τη χρήση εξωτερικών αξιολογήσεων πιστοληπτικής ικανότητας και εσωτερικών υποδειγμάτων σε σχέση με τους εν λόγω κινδύνους. Το ίδρυμα εισάγει διαύλους αναφοράς στο διοικητικό όργανο, που να καλύπτουν όλους τους σημαντικούς κινδύνους και τις πολιτικές διαχείρισης κινδύνων καθώς και τις αλλαγές τους.

(3) Το διοικητικό όργανο έχει την κύρια ευθύνη για τον καθορισμό, την παρακολούθηση και αξιολόγηση της κουλτούρας διαχείρισης κινδύνων του ιδρύματος σύμφωνα με τις πρόνοιες της παραγράφου 60 κατά τρόπο που να διασφαλίζεται μια κοινή κατανόηση και επίγνωση των κινδύνων, ενθαρρύνεται η έκφραση, συζήτηση και παραπομπή των προβληματισμών/ ανησυχιών αναφορικά με την ύπαρξη κινδύνων στα κατάλληλα επίπεδα αναφοράς και λήψης αποφάσεων και θέτει τους υπαλλήλους, σε όλα τα επίπεδα αρμοδιοτήτων, υπόλογους των πράξεων τους που οδηγούν στην ανάληψη κινδύνων από το ίδρυμα· το διοικητικό όργανο δίνει το παράδειγμα ηγεσίας διατυπώνοντας με σαφήνεια τις υποκείμενες αξίες της κουλτούρας διαχείρισης κινδύνων και διασφαλίζοντας ότι η συμπεριφορά του οργάνου αντανακλά τις αξίες που ασπάζεται.

(4) Το διοικητικό όργανο καθορίζει και επιβλέπει την εφαρμογή του πλαισίου της διάθεσης ανάληψης κινδύνων σύμφωνα με τις διατάξεις τις παραγράφου 61· συναφώς, το διοικητικό όργανο –

(α) υιοθετεί και ελέγχει την εφαρμογή μίας σαφώς τεκμηριωμένης δήλωσης για τη διάθεση ανάληψης κινδύνων·

(β) περιλαμβάνει την αξιολόγηση της διάθεσης ανάληψης κινδύνων κατά τις συζητήσεις στρατηγικής, συμπεριλαμβανομένων των αποφάσεων που αφορούν συγχωνεύσεις, εξαγορές και ανάπτυξη των επιχειρηματικών δραστηριοτήτων ή προϊόντων·

(γ) τακτικά και τουλάχιστον κάθε έξι (6) μήνες, επανεξετάζει και παρακολουθεί τα πραγματικά επίπεδα κινδύνου σε σχέση με τα εγκεκριμένα όρια ανάληψης κινδύνων συμπεριλαμβανομένων ποιοτικών παραμέτρων των κινδύνων που δεν είναι εύκολο να μετρηθούν·

(δ) διαβεβαιώνεται για την ύπαρξη μηχανισμών που διασφαλίζουν την αποτελεσματική διαχείριση των σημαντικά δυσμενών ανοιγμάτων σε κινδύνους, και, όπου χρειάζεται, το μετριασμό των κινδύνων, κυρίως εκείνων που βρίσκονται κοντά στα όρια ανάληψης κινδύνων που έχουν τεθεί.

(5) Το διοικητικό όργανο διασφαλίζει ότι το ίδρυμα διαθέτει κατάλληλο πλαίσιο διαχείρισης κινδύνων, λαμβάνοντας υπόψη το επιχειρηματικό μοντέλο, την πολυπλοκότητα των δραστηριοτήτων και το μέγεθος του ιδρύματος, το οποίο ενσωματώνεται στη κουλτούρα διαχείρισης κινδύνων του ιδρύματος και συνάδει με τις διατάξεις του Μέρους IX· το διοικητικό όργανο συμμετέχει ενεργά και διασφαλίζει ότι –

(α) οι στόχοι διαχείρισης κινδύνων, οι βασικές αρχές διαχείρισης κινδύνων και η ανάθεση αρμοδιοτήτων διαχείρισης κινδύνων σε όλα τα τμήματα του ιδρύματος είναι σαφείς, τεκμηριωμένες και συνάδουν με τους επιχειρηματικούς στόχους και στρατηγικές·

(β) οι εξωτερικές αξιολογήσεις δεν χρησιμοποιούνται αποκλειστικά ή μηχανιστικά για σκοπούς αξιολόγησης των κινδύνων αλλά αναπτύσσεται και μία κατάλληλη ικανότητα αξιολόγησης εσωτερικών κινδύνων, ανάλογη με τη φύση, την κλίμακα και την πολυπλοκότητα των δραστηριοτήτων του ιδρύματος·

(γ) η διαχείριση κινδύνων υποστηρίζεται από ένα επαρκές και εύρωστο σύστημα διαχείρισης πληροφοριών που επιτρέπει την αναγνώριση, μέτρηση, αξιολόγηση και αναφορά των κινδύνων κατά τρόπο έγκαιρο και ακριβή·

(δ) οι σημαντικές αλλαγές στο σύστημα διαχείρισης κινδύνων είναι τεκμηριωμένες και υπόκεινται σε έγκριση από το διοικητικό όργανο·

(ε) η ανάπτυξη νέων αγορών, προϊόντων και υπηρεσιών που προσφέρονται στους πελάτες από κάθε επιχειρηματική μονάδα του ιδρύματος και οι σημαντικές αλλαγές στις υφιστάμενες αγορές, προϊόντα και υπηρεσίες διέπονται από μία καλά τεκμηριωμένη πολιτική έγκρισης νέων προϊόντων, σύμφωνα με τις διατάξεις της παραγράφου 72·

(στ) το πλαίσιο διαχείρισης κινδύνων επανεξετάζεται τακτικά έτσι ώστε να διασφαλιστεί ότι οι απαραίτητες τροποποιήσεις και βελτιώσεις εντοπίζονται και διαπεραιώνονται σε εύθετο χρόνο.

(5) Το διοικητικό όργανο υιοθετεί και εφαρμόζει πολιτική σχετικά με το περιεχόμενο, τη μορφή και τη συχνότητα αναφορών που αναμένει να λαμβάνει από τα ανώτατα διοικητικά στελέχη και των τμημάτων ελέγχου.

(6) Το διοικητικό όργανο διασφαλίσει ότι το ίδρυμα αξιολογεί την αναγκαιότητα χρήσης εσωτερικών μεθόδων για τον υπολογισμό των απαιτήσεων ιδίων κεφαλαίων σύμφωνα τη φύση και την πολυπλοκότητα των ανοιγμάτων και της εσωτερικής του οργάνωσης.

Κανονιστική συμμόρφωση.

18. (1) Το διοικητικό όργανο οφείλει να γνωρίζει το κανονιστικό περιβάλλον στο οποίο δραστηριοποιείται το ίδρυμα, να διασφαλίζει ότι το ίδρυμα διαθέτει κατάλληλο πλαίσιο κανονιστικής συμμόρφωσης σύμφωνα με τις διατάξεις του Μέρους VIII, και να διατηρεί μια αποτελεσματική και παραγωγική σχέση με τις αρμόδιες αρχές.

(2) Το διοικητικό όργανο εγκρίνει την πολιτική κανονιστικής συμμόρφωσης του ιδρύματος που αναφέρεται στην παράγραφο 59(2)(δ) και αξιολογεί τουλάχιστον μια φορά το χρόνο το βαθμό αποτελεσματικότητας της διαχείρισης από το ίδρυμα του κινδύνου κανονιστικής συμμόρφωσης.

Σχεδιασμός και εφαρμογή ενός υγιούς πλαισίου εσωτερικού ελέγχου.

19. Το διοικητικό όργανο διασφαλίζει ότι το ίδρυμα έχει θεσπίσει ένα κατάλληλο πλαίσιο εσωτερικού ελέγχου σύμφωνα με τις διατάξεις του Μέρους X· στο πλαίσιο αυτό, το διοικητικό όργανο διασφαλίζει ότι:

(α) ο σχεδιασμός των συστημάτων εσωτερικού ελέγχου και η σύνθεση των τμημάτων ελέγχου είναι κατάλληλοι για το μέγεθος και την πολυπλοκότητα του ιδρύματος και ότι τα συστήματα και τα τμήματα αυτά λειτουργούν αποτελεσματικά και όπως είχε προβλεφθεί·

(β) υπάρχουν οι κατάλληλοι έλεγχοι για κάθε σημαντική επιχειρηματική διαδικασία και πολιτική και για τους συναφής κινδύνους και υποχρεώσεις·

(γ) όλοι οι έλεγχοι και διαδικασίες, συμπεριλαμβανομένων των διαδικασιών έγκρισης, τεκμηριώνονται επαρκώς και κοινοποιούνται στο προσωπικό που είναι αρμόδιο για την εκτέλεση και τον έλεγχο τους·

(δ) το προσωπικό καθίσταται υπόλογο για την αποτελεσματική εφαρμογή των ελέγχων και των διαδικασιών στο πλαίσιο των καθηκόντων τους·

(ε) τουλάχιστον δύο μέλη του προσωπικού εμπλέκονται άμεσα ή έμμεσα σε κάθε δραστηριότητα ή τμήμα ελέγχου μέχρι την ολοκλήρωσή της·

(στ) μόνο το κατάλληλα εξουσιοδοτημένο προσωπικό έχει πρόσβαση στα περιουσιακά στοιχεία του ιδρύματος, στα λογιστικά αρχεία και σε εμπιστευτικές πληροφορίες γενικότερα·

(ζ) στα τμήματα ελέγχου διορίζονται ικανά πρόσωπα·

(η) τα τμήματα ελέγχου συμμετέχουν, έχοντας συμβουλευτικό ρόλο, στη θέσπιση νέων διαδικασιών·

(θ) το τμήμα εσωτερικής επιθεώρησης έχει την αρμοδιότητα να διεξάγει αξιολογήσεις του πλαισίου διαχείρισης κινδύνων, των πλαισίων κανονιστικής συμμόρφωσης και του πλαισίου εσωτερικού ελέγχου·

(ι) το πλαίσιο εσωτερικού ελέγχου αξιολογείται από εξωτερικό ελεγκτή κατά τα προβλεπόμενα στην παράγραφο 104·για το σκοπό αυτό, το διοικητικό όργανο διασφαλίζει ότι η σχέση με τον εξωτερικό ελεγκτή είναι ίδια με τη σχέση που διατηρεί με τον εγκεκριμένο ελεγκτή κατά τα προβλεπόμενα στη παράγραφο 22(4).

Καθορισμός και επίβλεψη της πολιτικής και των πρακτικών αποδοχών.

20. (1) Το διοικητικό όργανο υιοθετεί και επανεξετάζει περιοδικά την πολιτική αποδοχών σύμφωνα με τις διατάξεις του Μέρους VI και επιβλέπει την αποτελεσματική εφαρμογή της.

(2) Το διοικητικό όργανο διασφαλίζει ότι η πολιτική και οι πρακτικές αποδοχών είναι συνεπείς με τη διάθεση ανάληψης κινδύνων του ιδρύματος, αποτρέπουν τις συγκρούσεις συμφερόντων και προωθούν την υγιή και αποτελεσματική διαχείριση των κινδύνων.

Έγκριση των διαδικασιών εφοδιασμού και ανάθεσης εργασιών σε τρίτους.

21. (1) Το διοικητικό όργανο διασφαλίζει ότι το ίδρυμα διαθέτει καταγεγραμμένες διαδικασίες διαχείρισης προσφορών και σύναψης συμβάσεων για την αγορά προϊόντων ή υπηρεσιών, συμπεριλαμβανομένων ορίων έγκρισης· οι διαδικασίες αυτές διασφαλίζουν ότι οι συμβάσεις για την αγορά προϊόντων ή υπηρεσιών συνάπτονται με βάση αντικειμενικά κριτήρια τα οποία -

(α) διασφαλίζουν τη συμμόρφωση με τις αρχές της διαφάνειας, της μη διάκρισης και της ίσης μεταχείρισης· και

(β) εγγυώνται την αξιολόγηση των προσφορών υπό συνθήκες πραγματικού ανταγωνισμού.

(2) Το διοικητικό όργανο εγκρίνει και επανεξετάζει τακτικά, και σε κάθε περίπτωση τουλάχιστο κάθε τρία (3) χρόνια την πολιτική ανάθεσης εργασιών σε τρίτους του ιδρύματος και επιβλέπει την εφαρμογή της· η ανάθεση εργασιών σε τρίτους σχεδιάζεται και υλοποιείται σύμφωνα με το πλαίσιο των αρχών για ανάθεση εργασιών σε τρίτους, το οποίο περιγράφεται στο Παράρτημα 2.

Διασφάλιση αξιόπιστων και διαφανών χρηματοοικονομικών εκθέσεων.

22.(1) το διοικητικό όργανο διασφαλίζει την ακεραιότητα των συστημάτων λογιστικής και χρηματοοικονομικών εκθέσεων, περιλαμβανομένων των χρηματοοικονομικών και επιχειρησιακών ελέγχων και της συμμόρφωσης με ρυθμιστικές και εποπτικές απαιτήσεις και συναφή πρότυπα.

(2) Το διοικητικό όργανο διασφαλίζει την ύπαρξη αξιόπιστης διαδικασίας για την ετοιμασία χρηματοοικονομικών εκθέσεων η οποία υποστηρίζεται από τους σαφώς καθορισμένους ρόλους και αρμοδιότητες του διοικητικού οργάνου, των ανώτατων διοικητικών στελεχών και του εγκεκριμένου ελεγκτή.

(3) Το διοικητικό όργανο εγκρίνει και επιβλέπει την αποτελεσματική εφαρμογή των εν λόγω συστημάτων και ελέγχων, έτσι ώστε να διασφαλίζεται ότι οι χρηματοοικονομικές εκθέσεις του ιδρύματος παρουσιάζουν μια ισορροπημένη και ακριβή εικόνα της οικονομικής κατάστασης και της κερδοφορίας του ιδρύματος, σύμφωνα με τα Διεθνή Πρότυπα Χρηματοοικονομικής Αναφοράς.

(4) Το διοικητικό όργανο προωθεί και διατηρεί μια αποδοτική σχέση με τον εγκεκριμένο ελεγκτή, διασφαλίζοντας ότι:

(α) οι όροι εμπλοκής του εγκεκριμένου ελεγκτή είναι σαφείς και κατάλληλοι για το πεδίο εφαρμογής του ελέγχου και των πόρων που απαιτούνται για τη διενέργεια του ελέγχου, και προσδιορίζουν το επίπεδο των αμοιβών που θα καταβληθούν·

(β) ο εγκεκριμένος ελεγκτής αναλαμβάνει συγκεκριμένη ευθύνη, σύμφωνα με τους όρους ανάθεσης του ελέγχου, για την εκτέλεση του υποχρεωτικού ελέγχου σύμφωνα με τα ισχύοντα διεθνή πρότυπα ελέγχου·

(γ) υπάρχουν κατάλληλες πολιτικές και διαδικασίες για τη διασφάλιση της ανεξαρτησίας του εγκεκριμένου ελεγκτή·

(δ) υπάρχει επαρκής διάλογος με τον εγκεκριμένο ελεγκτή σχετικά με το πεδίο εφαρμογής και το χρονοδιάγραμμα του ελέγχου έτσι ώστε να κατανοεί τα θέματα που αφορούν τους κινδύνους, τις πληροφορίες για το περιβάλλον λειτουργίας του ιδρύματος που είναι σχετικές με τον έλεγχο, καθώς και οποιουσδήποτε τομείς για τους οποίους ζητείται από το διοικητικό όργανο η διεξαγωγή ελέγχου από τον εγκεκριμένο ελεγκτή, είτε ως μέρος ή ως επέκταση της ανάθεσης ελέγχου .

(ε) διεξάγονται τακτικές συναντήσεις μεταξύ του διοικητικού οργάνου και του εγκεκριμένου ελεγκτή κατά τη διάρκεια της διενέργειας του ελέγχου, συμπεριλαμβανομένων των συνεδριάσεις χωρίς την παρουσία των ανώτατων διοικητικών στελεχών·

(στ) χρησιμοποιούνται, κατά τρόπο έγκαιρο και αποτελεσματικό, τα ευρήματα του εξωτερικού ελεγκτή και επιλύουν εγκαίρως τυχόν αδυναμίες.

Εξασφάλιση αποτελεσματικής και διαφανούς επικοινωνίας.

23.(1) Το διοικητικό όργανο διασφαλίζει ότι το ίδρυμα υιοθετεί και εφαρμόζει κατάλληλες πολιτικές, διαδικασίες, συστήματα και ελέγχους για την προώθηση της έγκαιρης και αποτελεσματικής δημοσιοποίησης πληροφοριών στα ενδιαφερόμενα μέρη, σύμφωνα με τις διατάξεις του Μέρους Χ.

(2) Το διοικητικό όργανο διασφαλίζει ότι οι χρηματοοικονομικές πληροφορίες και τα λοιπά στοιχεία που υποβάλλονται στην Κεντρική Τράπεζα και σε άλλες αρμόδιες αρχές–

(α) είναι πλήρεις και έγκυρες και βασίζονται σε αντίστοιχες λογιστικές εγγραφές·

(β) στην περίπτωση εκτιμήσεων που δεν βασίζονται σε λογιστικές εγγραφές, έχουν διεξαχθεί κατά τρόπο ορθό και κατάλληλα τεκμηριωμένο·

(γ) υποβάλλονται εντός των προβλεπόμενων προθεσμιών.

(3) Το διοικητικό όργανο επιβλέπει τη διαδικασία δημοσιοποίησης και επικοινωνίας.

Διασφάλιση της εφαρμογής των κατάλληλων πολιτικών ασφάλειας πληροφοριών, προτύπων και διαδικασιών.

24. Το διοικητικό όργανο διασφαλίζει ότι το ίδρυμα διαθέτει κατάλληλο πλαίσιο ασφάλειας πληροφοριών για την προστασία των εμπιστευτικών και ιδιόκτητων πληροφοριών του ιδρύματος· προς το σκοπό αυτό –

(α) εγκρίνει και επανεξετάζει περιοδικά την πολιτική ασφάλειας πληροφοριών του ιδρύματος· η πολιτική ασφάλειας των πληροφοριών θα πρέπει να παρουσιάζεται υπό τη μορφή αρχών και υποχρεώσεων του ιδρύματος υποτυπώνοντας τις κατευθύνσεις και τους στόχους του ιδρύματος για την αποτελεσματική διαχείριση, προστασία και κατανομή όλων των πληροφοριών που βρίσκονται στην ιδιοκτησία του, σε ηλεκτρονική μορφή, σε έντυπη μορφή ή άλλως πως·

(β) διασφαλίζει ότι οι κατάλληλες ενότητες της πολιτικής ασφάλειας πληροφοριών κοινοποιούνται στα ανώτατα διοικητικά στελέχη και στο προσωπικό, με βάση την ανάγκη να γνωρίζουν, σύμφωνα με τα καθήκοντα και τις ευθύνες τους·

(γ) διασφαλίζει ότι το ίδρυμα έχει καταρτίσει διοικητική δομή που να επιβλέπει την ασφάλεια των επιχειρησιακών πληροφοριών·

(δ) εξετάζει τις αναφορές σχετικά με την αποτελεσματικότητα του προγράμματος ασφάλειας των πληροφοριών.

Συνεχής παρακολούθηση και αξιολόγηση του πλαισίου διακυβέρνησης.

25. (1) Το διοικητικό όργανο παρακολουθεί και αξιολογεί περιοδικά την αποτελεσματικότητα των ρυθμίσεων διακυβέρνησης του ιδρύματος και λαμβάνει τα κατάλληλα μέτρα για την αντιμετώπιση τυχόν ελλείψεων.

(2) Στην περίπτωση κατά την οποία το ίδρυμα είναι η μητρική εταιρεία ομίλου, το διοικητικό του όργανο διασφαλίζει, σε περιοδική βάση, ότι διαθέτει τα κατάλληλα μέσα για την παρακολούθηση και αξιολόγηση της δομής διακυβέρνησης του ομίλου κατά τρόπο που να διασφαλίζει ότι αυτή παραμένει κατάλληλη υπό το πρίσμα της ανάπτυξης και της αυξανόμενης πολυπλοκότητας του ομίλου και ότι συμμορφώνεται με όλες τις εφαρμοστέες απαιτήσεις διακυβέρνησης.

Τμήμα 4 - Καθήκοντα κάθε μέλους του διοικητικού οργάνου

Καθήκοντα μελών του διοικητικού οργάνου.

26.(1) Τα μέλη του διοικητικού οργάνου συμμετέχουν ενεργά στην επιχειρηματική δραστηριότητα του ιδρύματος και οφείλουν να είναι σε θέση να διαμορφώνουν τις δικές τους λογικές, τεκμηριωμένες, αντικειμενικές και ανεξάρτητες θέσεις και αποφάσεις για την εκπλήρωση των προσωπικών και συλλογικών αρμοδιοτήτων τους· ως εκ τούτου, κάθε μέλος του διοικητικού οργάνου –

(α) διασφαλίζει ότι έχει πλήρη επίγνωση των ρυθμίσεων διακυβέρνησης του ιδρύματος και του ρόλου του σε αυτές·

(β) διασφαλίζει ότι έχει ενημερωμένη αντίληψη των εργασιών του ιδρύματος συμπεριλαμβανομένων των τομέων για τους οποίους δεν είναι άμεσα υπεύθυνο, αλλά είναι συλλογικά υπόλογο·

(γ) αφιερώνει αρκετό χρόνο στην εκτέλεση των καθηκόντων του στο ίδρυμα συμπεριλαμβανομένης της προετοιμασίας των συνεδριάσεων του διοικητικού οργάνου·

(δ) ενεργεί με ειλικρίνεια, ακεραιότητα και ανεξάρτητη βούληση ώστε να εκτιμά και να αμφισβητεί τις αποφάσεις των ανώτατων διοικητικών στελεχών όποτε αυτό χρειάζεται και να επιβλέπει αποτελεσματικά και να παρακολουθεί τη λήψη των αποφάσεων από τη διοίκηση·

(ε) δεν χρησιμοποιεί τη θέση του για την απόκτηση προσωπικού οφέλους ή για να προκαλέσει οποιαδήποτε ζημιά στο ίδρυμα·

(στ) γνωστοποιεί στο ίδρυμα οποιοδήποτε θέμα το οποίο μπορεί να οδηγήσει, ή έχει ήδη οδηγήσει, σε σύγκρουση συμφερόντων ή σε μη συμμόρφωση με τις απαιτήσεις της περί της Αξιολόγησης για την Ικανότητα και Καταλληλότητα των Μελών Διοικητικού Οργάνου και των Διευθυντών των ΑΠΙ Οδηγία του 2014·

(ζ) διασφαλίζει ότι οι όποιες ανησυχίες του για τη διοίκηση του ιδρύματος, οι οποίες δεν μπορούν να επιλυθούν, καταγράφονται στις συνεδριάσεις του διοικητικού οργάνου·

(η) αποκτά, συντηρεί και εμβαθύνει τις γνώσεις και δεξιότητές του για εκπλήρωση των υποχρεώσεών του.

(2) Τα εκτελεστικά μέλη του διοικητικού οργάνου είναι αρμόδια για την υποβολή εισηγήσεων στρατηγικής στο διοικητικό όργανο και την εκτέλεση των στρατηγικών που υιοθετεί το διοικητικό όργανο με τις υψηλότερες δυνατές προδιαγραφές.

(3) Τα μη εκτελεστικά μέλη του διοικητικού οργάνου είναι αρμόδια για την παρακολούθηση των ενεργειών των ανώτατων διοκητικών στελεχών και συμβάλλουν στην ανάπτυξη των στρατηγικών· στο πλαίσιο αυτό, τα μη εκτελεστικά μέλη του διοικητικού οργάνου, επιπρόσθετα των υποχρεώσεων τους κατά τα προβλεπόμενα στην υποπαράγραφο (1), οφείλουν να:

(α) αμφισβητούν και να συμβάλλουν εποικοδομητικά στην ανάπτυξη στρατηγικών·

(β) εξετάζουν λεπτομερώς την απόδοση των ανώτατων διοικητικών στελεχών ως προς την εκπλήρωση των συμφωνηθέντων στόχων και επιδιώξεων και παρακολουθούν τις αναφορές απόδοσης·

(γ) βεβαιώνονται ότι οι οικονομικές πληροφορίες είναι ακριβείς και ότι τα πλαίσια διαχείρισης κινδύνων και κανονιστικής συμμόρφωσης καθώς και το πλαίσιο εσωτερικού ελέγχου είναι εύρωστα και αξιόπιστα·

(δ) έχουν κεντρικό ρόλο στο διορισμό, και όπου χρειάζεται, στην απομάκρυνση των ανώτατων διοικητικών στελεχών και των στελεχών σε θέσεις κλειδιά των τμημάτων ελέγχου, και στον προγραμματισμό της διαδοχής του εν λόγω προσωπικού·

(ε) έχουν πρωταρχικό ρόλο στον καταρτισμό και την επίβλεψη της πολιτικής αποδοχών του διοικητικού οργάνου που αναφέρεται στο Μέρος VI,·

(στ) παρέχουν αντικειμενικές απόψεις για τους πόρους, διορισμούς και τα πρότυπα συμπεριφοράς.

(4) Τα ανεξάρτητα μέλη του διοικητικού οργάνου διατηρούν, σε κάθε περίπτωση, ανεξαρτησία σκέψης και γνώμης.

(5) Τα μέλη του διοικητικού οργάνου οφείλουν να έχουν πάντοτε καλή φήμη και να διαθέτουν επαρκείς γνώσεις, δεξιότητες και εμπειρία κατά την εκτέλεση των καθηκόντων τους.

Τμήμα 5 - Ρόλος και αρμοδιότητες του προέδρου του διοικητικού οργάνου

Κύριες αρμοδιότητες του προέδρου του διοικητικού οργάνου.

27. Ο ι κύριες αρμοδιότητες του προέδρου του διοικητικού οργάνου περιλαμβάνουν:

(α) τη διασφάλιση της αποτελεσματικής λειτουργίας του διοικητικού οργάνου·

(β) τη διασφάλιση της καταλληλότητας του μεγέθους και της σύνθεσης του διοικητικού οργάνου, υπό το πρίσμα της ανάπτυξης και αύξησης της πολυπλοκότητας του ιδρύματος ή του ομίλου και σύμφωνα με την παράγραφο 5 και άλλες εφαρμοστέες απαιτήσεις διακυβέρνησης·

(γ) τη διασφάλιση της αποτελεσματικής επικοινωνίας με τις εποπτικές αρχές και τα ενδιαφερόμενα μέρη.

Διασφάλιση της αποτελεσματικής λειτουργίας του διοικητικού οργάνου.

28. Ο πρόεδρος του διοικητικού οργάνου έχει την κύρια ευθύνη για την αποτελεσματική λειτουργία του διοικητικού οργάνου σε όλες τις πτυχές των ρόλων διοίκησης και εποπτείας του· στο πλαίσιο αυτό, ο πρόεδρος είναι υπεύθυνος για –

(α) την τακτική πραγματοποίηση συνεδριάσεων του διοικητικού οργάνου, σύμφωνα με τις σχετικές διατάξεις της παραγράφου 7(2)·

(β) τον καθορισμό της ημερήσιας διάταξης των συνεδριάσεων, λαμβάνοντας υπόψη τα θέματα και τις ανησυχίες όλων των μελών του διοικητικού οργάνου·

(γ) τη διάθεση στα μέλη του διοικητικού οργάνου ακριβούς, έγκαιρης και σαφής πληροφόρησης που να επιτρέπει στο διοικητικό όργανο να εκτελεί ως σώμα τις διοικητικές και εποπτικές του εργασίες·

(δ) τη διάθεση επαρκούς χρόνου στα μέλη του διοικητικού οργάνου για την εξέταση σημαντικών θεμάτων και τη λήψη απαντήσεων σε οποιεσδήποτε ερωτήσεις ή ανησυχίες που δύναται να έχουν χωρίς να έρχονται αντιμέτωποι με μη ρεαλιστικές προθεσμίες για τη λήψη αποφάσεων·

(ε) την ενθάρρυνση της ενεργού συμμετοχής των μελών του διοικητικού οργάνου·

(στ) την κοινοποίηση των συγκρουόμενων συμφερόντων και την αποχή των μελών από τη διαδικασία λήψης αποφάσεων ή ψηφοφορίας για οποιοδήποτε θέμα για το οποίο δύναται να έχουν σύγκρουση συμφερόντων, σύμφωνα με την παράγραφο 7(3)·

(ζ) τον καθορισμό του ύφους και τόνου των συζητήσεων του διοικητικού οργάνου με τρόπο που να προωθεί την αποτελεσματική λήψη αποφάσεων και εποικοδομητικής συζήτησης·

(η) τη διάθεση αρκετού χρόνο για συζήτηση των πολύπλοκων ή επίμαχων θεμάτων και, όπου κρίνεται σκόπιμο, την οργάνωση ανεπίσημων συναντήσεων εκ των προτέρων για να καταστεί δυνατή η ενδελεχή προετοιμασία για τη συζήτηση·

(i) την τήρηση πρακτικών της συνεδρίασης σύμφωνα με την παράγραφο 7(4).

Διασφάλιση της εισαγωγής, ανάπτυξης και αξιολόγησης των επιδόσεων.

29. (1) Ο πρόεδρος του διοικητικού οργάνου διασφαλίζει ότι τα μέλη του διοικητικού οργάνου διαθέτουν ανά πάσα στιγμή επαρκή γνώση και δεξιότητες για την εκτέλεση των καθηκόντων τους· ο πρόεδρος οφείλει –

(α) να διασφαλίζει ότι τα νέα μέλη του διοικητικού οργάνου συμμετέχουν σε επίσημο, ολοκληρωμένο και εξατομικευμένο εισαγωγικό πρόγραμμα επιμόρφωσης, το οποίο προετοιμάζεται από τον γραμματέα του ιδρύματος·

(β) να αναγνωρίζει τις ανάγκες κατάρτισης των μελών του διοικητικού οργάνου ως άτομα καθώς και του διοικητικού οργάνου ως σύνολο, για ενίσχυση της συνολικής αποτελεσματικότητας του διοικητικού οργάνου ως σώμα και να διασφαλίζει ότι οι ανάγκες αυτές ικανοποιούνται.

(2) Ο πρόεδρος του διοικητικού οργάνου διασφαλίζει ότι η αξιολόγηση του διοικητικού οργάνου, των επιτροπών του και εκάστου μέλους του διοικητικού οργάνου διεξάγεται σύμφωνα με τις διατάξεις της παραγράφου 10 και προβαίνει σε ενέργειες ανάλογες με τα αποτελέσματα των αξιολογήσεων αυτών, αναγνωρίζοντας τις δυνατότητες και αντιμετωπίζοντας τις αδυναμίες του διοικητικού οργάνου.

Διασφάλιση αποτελεσματικής επικοινωνίας με τις εποπτικές αρχές και τους μετόχους.

30. (1) Ο πρόεδρος του διοικητικού οργάνου διατηρεί επαρκή επαφή με την Κεντρική Τράπεζα και άλλες εποπτικές αρχές και διαμορφώνει αντίληψη των απόψεων και των ανησυχιών των κύριων μετόχων και επενδυτών του ιδρύματος.

(2) Ο πρόεδρος του διοικητικού οργάνου διασφαλίζει ότι οι απόψεις και οι ανησυχίες της Κεντρικής Τράπεζας, άλλων εποπτικών αρχών και των κύριων μέτοχων και επενδυτών κοινοποιούνται στο σύνολο τους στο διοικητικό όργανο.

Τμήμα 6 - Ρόλος και ευθύνες του ανώτερου ανεξάρτητου μέλους του διοικητικού οργάνου

Ρόλοι και αρμοδιότητες του ανώτερου ανεξάρτητου μέλους του διοικητικού οργάνου.

31. (1) Τα καθήκοντα του ανώτερου ανεξάρτητου μέλους του διοικητικού οργάνου περιλαμβάνουν, μεταξύ άλλων, τα ακόλουθα:

(α) να ενεργεί ως σημείο επαφής για τους μετόχους και άλλους ενδιαφερόμενους σχετικά με ανησυχίες οι οποίες δεν κατέστει δυνατό να επιλυθούν ή που δεν ήταν ορθό να επιλυθούν μέσω των συνήθων διαύλων επικοινωνίας με τον πρόεδρο του διοικητικού οργάνου ή τα ανώτατα διοικητικά στελέχη·

(β) να διασφαλιζεί ότι το διοικητικό όργανο έχει ισορροπημένη αντίληψη των σημαντικότερων θεμάτων και ανησυχιών των μετόχων·

(γ) να προεδρεύει της συνεδρίασης με τα μη εκτελεστικά μέλη του διοικητικού οργάνου, χωρίς την παρουσία του προέδρου, τουλάχιστον ετησίως, προκειμένου να αξιολογήσει την απόδοση του προέδρου σύμφωνα με την παράγραφο 10·

(δ) να προεδρεύει του διοικητικού οργάνου κατά την εξέταση διαδοχής του προέδρου του διοικητικού οργάνου και διασφαλίζει την ομαλή διαδικασία της διαδοχής.

Τμήμα 7 - Ρόλοι και ευθύνες του γραμματέα της εταιρείας

Ευθύνη για το διορισμό γραμματέα της εταιρείας.

32. (1) Λαμβάνοντας υπόψη τις διατάξεις των Άρθρων 172 και 173 του περί Εταιρειών Νόμου, τα ιδρύματα οφείλουν να φροντίζουν για την αποφυγή οποιασδήποτε σύγκρουσης συμφερόντων όσον αφορά το διορισμό γραμματέα της εταιρείας, σύμφωνα με το Άρθρο 171 του περί Εταιρειών Νόμου.

(2) Ανεξαρτήτως των διατάξεων της Οδηγίας Σύνδεσης των Συνεργατικών Πιστωτικών Ιδρυμάτων με τον Κεντρικό Φορέα του 2013 ως εκάστοτε τροποποιείται ή αντικαθίσταται, τα συνεργατικά πιστωτικά ιδρύματα διασφαλίζουν ότι το άτομο που εκτελεί τα καθήκοντα γραμματέα της εταιρείας όπως προβλέπονται στο παρόν Τμήμα λαμβάνει τη δέουσα προσοχή για την αποφυγή συγκρούσεων συμφερόντων.

(3) Ανεξαρτήτως των διατάξεων του περί Εταιρειών Νόμου, ο γραμματέας της εταιρείας δύναται να αναθέσει καθήκοντα που αναφέρονται στο παρόν Τμήμα σε τρίτα πρόσωπα εφόσον δεν προκύπτει σύγκρουση συμφερόντων και ο γραμματέας της εταιρείας ελέγχει και υπογράφει τα σχετικά πρακτικά

και έγγραφα και παραμένει υπεύθυνος και υπόλογος για τα αποτελέσματα της ανάθεσης·

Νοείται ότι ο γραμματέας της εταιρείας δεν μπορεί να αναθέσει τα καθήκοντά του στους επικεφαλής των τμημάτων ελέγχου.

Διευκόλυνση της λειτουργίας του διοικητικού οργάνου.

33.(1) Ο γραμματέας της εταιρείας διασφαλίζει ότι το διοικητικό όργανο και οι επιτροπές του έχουν συσταθεί και λειτουργούν σύμφωνα με τους εσωτερικούς κανόνες και κανονισμούς του διοικητικού οργάνου, τις διατάξεις της παρούσας Οδηγίας και των άλλων εφαρμοστέων νομικών και εποπτικών απαιτήσεων.

(2) Ο γραμματέας της εταιρείας ενεργεί ως πηγή πληροφοριών και συμβουλών στα μέλη του διοικητικού οργάνου· ο γραμματέας της εταιρείας διασφαλίζει την ύπαρξη επαρκούς ροής πληροφοριών εντός του διοικητικού οργάνου και των επιτροπών του, μεταξύ των ανώτατων διοικητικών στελεχών και των μη εκτελεστικών μελών και μεταξύ των επικεφαλής των τμημάτων ελέγχου και των μη εκτελεστικών μελών.

(3) Ο γραμματέας της εταιρείας διασφαλίζει ότι εάν χρειαστεί τα μη εκτελεστικά μέλη έχουν πρόσβαση σε ανεξάρτητες επαγγελματικές συμβουλές με έξοδα του ιδρύματος, σύμφωνα με την παράγραφο 7.

(4) Ο γραμματέας της εταιρείας συμμετέχει ενεργά στην προετοιμασία του προγράμματος όλων των συνεδριάσεων του διοικητικού οργάνου και των επιτροπών· ο γραμματέας της εταιρείας οφείλει να:

(α) προετοιμάζει, σε συνεργασία με τον πρόεδρο, την ημερήσια διάταξη των συνεδριάσεων αυτών διασφαλίζοντας ότι τα θέματα που απαιτούν την προσοχή ή τις ενέργειες του διοικητικού οργάνου ή επιτροπής περιλαμβάνονται στην ημερήσια διάταξη·

(β) διασφαλίζει ότι οι σχετικές πληροφορίες αποστέλλονται έγκαιρα σε όλα τα μέλη του διοικητικού οργάνου, ώστε να προετοιμαστούν επαρκώς για τις συναντήσεις αυτές.

(5) Ο γραμματέας της εταιρείας διασφαλίζει ότι τηρούνται τα πρακτικά, σύμφωνα με τις διατάξεις της παραγράφου 7· ο γραμματέας της εταιρείας οφείλει να –

(α) εκφράζει ρητά, σε ξεχωριστή παράγραφο, την εκτίμηση του ως προς το αν η συνάντηση είχε πραγματοποιηθεί σύμφωνα με τους εσωτερικούς κανόνες και κανονισμούς του διοικητικού οργάνου, τις διατάξεις της παρούσας Οδηγίας και των άλλων εφαρμοστέων ρυθμιστικών και εποπτικών απαιτήσεων·

(β) διασφαλίζει την κυκλοφορία, ολοκλήρωση και έγκριση των πρακτικών σε εύθετο χρόνο από όλα τα μέλη που ήταν παρόντα στη συνεδρίαση·

(γ) διασφαλίζει τη διανομή των τελικών πρακτικών σε εύθετο χρόνο σε όλους τους παραλήπτες·

(δ) διασφαλίζει την κατάλληλη κοινοποίηση των αποφάσεων που έχουν ληφθεί, επιδιώκει την πραγματοποίηση των μετέπειτα ενεργειών και αναφέρει τα θέματα που προκύπτουν.

(6) Ο γραμματέας της εταιρείας παρέχει υποστήριξη στο διοικητικό όργανο για τον καθορισμό σχεδιασμού διαδοχής και την εποπτεία της διαδοχής και εναλλαγής καθηκόντων των μη εκτελεστικών μελών του διοικητικού οργάνου.

Διευκόλυνση της επαγωγής, ανάπτυξης και αξιολόγησης των μελών του διοικητικού οργάνου.

34. (1) Ο γραμματέας της εταιρείας οργανώνει εισαγωγικά προγράμματα επιμόρφωσης για τα μη εκτελεστικά μέλη του διοικητικού οργάνου τα οποία παρέχουν επίσημη, πλήρη και εξατομικευμένη εισαγωγή στο ίδρυμα και στα καθήκοντα και τις ευθύνες τους.

(2) Ο γραμματέας της εταιρείας βοηθά τον πρόεδρο στην αξιολόγηση και ικανοποίηση των αναγκών κατάρτισης των μελών του διοικητικού οργάνου και διασφαλίζει ότι υπάρχει ένα εν εξελίξει πρόγραμμα για την καλή ενημέρωση των μελών όσον αφορά τις εξελίξεις στην εταιρεία και θέματα που σχετίζονται με τις ευθύνες τους γενικότερα.

(3) Ο γραμματέας της εταιρείας παρέχει βοήθεια και υποστήριξη στον πρόεδρο του διοικητικού

οργάνου για την ανάπτυξη και πραγματοποίηση αξιολογήσεων της απόδοσης του διοικητικού οργάνου στο σύνολό του, των επιτροπών και εκάστου μέλους, σύμφωνα με τις διατάξεις της παραγράφου 10.

ΜΕΡΟΣ IV
ΕΠΙΤΡΟΠΕΣ ΤΟΥ ΔΙΟΙΚΗΤΙΚΟΥ ΟΡΓΑΝΟΥ

Τμήμα 1 - Γενικές απαιτήσεις

Απαίτηση για σύσταση επιτροπών.

35.(1) Τα ιδρύματα συστήνουν επιτροπές του διοικητικού οργάνου οι οποίες είναι κατάλληλες για το μέγεθος, την εσωτερική οργάνωση και τη φύση, το πεδίο εφαρμογής και την πολυπλοκότητα των δραστηριοτήτων τους.

(2) Τα ιδρύματα συστήνουν επιτροπή κινδύνου, επιτροπή ανάδειξης υποψηφίων και επιτροπή αποδοχών.

Νοείται ότι τα ιδρύματα συστήνουν επίσης επιτροπή ελέγχου σύμφωνα με τις διατάξεις του Άρθρου 46 του περί Ελεγκτών και Υποχρεωτικών Ελέγχων των Ετήσιων και των Ενοποιημένων Λογαριασμών Νόμου του 2009.

(3) Η Κεντρική Τράπεζα δύναται να επιτρέψει σε ίδρυμα το οποίο δεν θεωρείται σημαντικό από πλευράς μεγέθους, εσωτερικής οργάνωσης και φύσεως, πεδίου εφαρμογής και πολυπλοκότητας των δραστηριοτήτων του, να συστήσει κοινή επιτροπή αποτελούμενη από την επιτροπή κινδύνου και την επιτροπή ελέγχου και / ή κοινή επιτροπή αποτελούμενη από την επιτροπή ανάδειξης υποψηφίων και την επιτροπή αποδοχών· τα μέλη κοινής επιτροπής έχουν τις γνώσεις, δεξιότητες και εξειδίκευση που απαιτούνται για τις επιτροπές που αποτελείται.

(4) Η Κεντρική Τράπεζα δύναται να επιτρέψει σε ίδρυμα που είναι θυγατρική ενός ομίλου και δεν θεωρείται σημαντικό από πλευράς μεγέθους, εσωτερικής οργάνωσης και φύσεως, πεδίου εφαρμογής και πολυπλοκότητας των δραστηριοτήτων του, να μην συστήσει επιτροπή αποδοχών ή επιτροπή διορισμών νοουμένου ότι τα σχετικά καθήκοντα ασκούνται από τις αντίστοιχες επιτροπές της μητρικής εταιρείας οι οποίες υποβάλουν τις συστάσεις και αποφάσεις τους στο διοικητικό όργανο του ιδρύματος.

(5) Τα ιδρύματα κοινοποιούν τη σύνθεση των επιτροπών του διοικητικού οργάνου στην Κεντρική Τράπεζα εντός ενός (1) μηνός από τη σύσταση ή την αλλαγή στη σύνθεση τους.

Σύνθεση και οργάνωση των επιτροπών.

36. (1) Οι επιτροπές του διοικητικού οργάνου συμμορφώνονται με τα ακόλουθα όσον αφορά τη σύνθεση τους:

(α) ο αριθμός των μελών των επιτροπών είναι επαρκής, και σε κάθε περίπτωση όχι μικρότερος από τρία (3) μέλη, για το χειρισμό του μεγέθους και της πολυπλοκότητας των καθηκόντων τους·

(β) πάνω από πενήντα τοις εκατό (50%) των μελών της επιτροπής πρέπει να είναι ανεξάρτητα μέλη·

(γ) οι επιτροπές που αναφέρονται στην παράγραφο 35(2) αποτελούνται από μέλη του διοικητικού οργάνου που δεν ασκούν εκτελεστικά καθήκοντα στο συγκεκριμένο ίδρυμα·

(δ) τα μέλη της επιτροπής δεν κατέχουν οποιεσδήποτε άλλες θέσεις ή διενεργούν συναλλαγές που θα μπορούσαν να θεωρηθούν ότι έρχονται σε σύγκρουση με τους όρους εντολής της επιτροπής·

(ε) η συμμετοχή σε περισσότερες από μία επιτροπές διασφαλίζει ότι κανένα άτομο δεν ασκεί υπερβολική επιρροή ή έλεγχο· σε κάθε περίπτωση, μέλος του διοικητικού οργάνου δεν δύναται να είναι μέλος σε περισσότερες από δύο (2) επιτροπές που αναφέρονται στην παράγραφο 35(2).

(2) Οι επιτροπές υποβάλλουν τακτικά αναφορές στο διοικητικό όργανο και κοινοποιούν τα πρακτικά τους στο διοικητικό όργανο πριν από τις συνεδριάσεις του διοικητικού οργάνου.

(3) Το διοικητικό όργανο καθορίζει διαδικασία για το συντονισμό και την επικοινωνία μεταξύ των διαφόρων επιτροπών του.

(4) Τα ιδρύματα διασφαλίζουν ότι οι επιτροπές έχουν επαρκή πρόσβαση στα τμήματα ελέγχου και σε εξωτερικούς ειδικούς συμβούλους και ότι οι επικεφαλής των τμημάτων ελέγχου καλούνται τακτικά στις συνεδριάσεις των συναφών επιτροπών.

(5) Ο πρόεδρος της κάθε επιτροπής διασφαλίζει ότι κανένα πρόσωπο δεν είναι παρόν, συμπεριλαμβανομένων και των άλλων μελών του διοικητικού οργάνου, εκτός εάν έχει κληθεί επισήμως να παραστεί για κάποιο συγκεκριμένο θέμα της ημερήσιας διάταξης· οποιοδήποτε τέτοιο πρόσωπο είναι παρόν μόνο κατά τη συζήτηση του συγκεκριμένου θέματος και αποχωρεί από την αίθουσα συσκέψεων αμέσως μετά, χωρίς καμία συμμετοχή στη διαδικασία λήψης αποφάσεων.

Όροι εντολής των επιτροπών.

37. (1) Η εξουσία, τα καθήκοντα, η συμμετοχή, η οργάνωση, οι διαδικασίες και οι δίαυλοι αναφοράς κάθε επιτροπής περιγράφονται και τεκμηριώνεται από το διοικητικό όργανο, σύμφωνα με τις διατάξεις του παρόντος Μέρους και της παραγράφου 7.

(2) Οι όροι αναφοράς επανεξετάζονται τακτικά, τουλάχιστον μία φορά ετησίως, από κάθε επιτροπή για διασφάλιση της συνεχούς διατήρησης της καταλληλότητας τους· τα σχόλια τεκμηριώνονται και περιλαμβάνουν, όπου είναι αναγκαίο, προτάσεις προς το διοικητικό όργανο για αναθεωρήσεις.

Τμήμα 2 – Επιτροπή Ελέγχου

Κριτήρια επιλεξιμότητας των μελών της επιτροπής ελέγχου.

38. (1) Η επιτροπή ελέγχου στο σύνολο της οφείλει να έχει -

(α) πρόσφατη και σχετική πρακτική εμπειρία στον τομέα των χρηματοπιστωτικών αγορών ή επαγγελματική εμπειρία που συνδέεται άμεσα με τις δραστηριότητες των χρηματοπιστωτικών αγορών·

(β) γνώση του ευρύτερου επιχειρηματικού περιβάλλοντος του ιδρύματος συμπεριλαμβανομένων των συστημάτων πληροφορικής και τεχνολογίας.

(2) Ο πρόεδρος της επιτροπής ελέγχου πρέπει να είναι ανεξάρτητος και να έχει εξειδικευμένες γνώσεις και εμπειρία στην εφαρμογή των λογιστικών αρχών και των διαδικασιών εσωτερικού ελέγχου.

(3) Ο πρόεδρος του διοικητικού οργάνου δεν δύναται να είναι μέλος της επιτροπής ελέγχου.

(4) Οι συνεδριάσεις της επιτροπής ελέγχου, ανάλογα με την περίπτωση, πρέπει να συμπίπτουν με τις σημαντικές ημερομηνίες υποβολής χρηματοοικονομικών εκθέσεων.

Καθήκοντα της επιτροπής ελέγχου.

39. Τα καθήκοντα της επιτροπής ελέγχου περιλαμβάνουν τα ακόλουθα:

(α) παρακολούθηση και αξιολόγηση, σε ετήσια βάση, της επάρκειας και αποτελεσματικότητας των συστημάτων εσωτερικού ελέγχου και των πληροφοριακών συστημάτων, με βάση τις εκθέσεις του τμήματος εσωτερικής επιθεώρησης και τις παρατηρήσεις και τα σχόλια των εξωτερικών ελεγκτών και των αρμόδιων εποπτικών αρχών, και στη συνέχεια υποβολή προτάσεων προς το διοικητικό όργανο για την αντιμετώπιση αδυναμιών που έχουν εντοπιστεί·

(β) υποβολή προτάσεων προς το διοικητικό όργανο σχετικά με το διορισμό, την αποζημίωση, τους όρους εντολής, την αντικατάσταση ή την εναλλαγή του εγκεκριμένου ελεγκτή και των άλλων εξωτερικών ελεγκτών του ιδρύματος·

(γ) διενέργεια επαφών με τους εξωτερικούς ελεγκτές ιδιαίτερα σε σχέση με τα πορίσματα του ελέγχου τους·

(δ) αξιολόγηση και παρακολούθηση της ανεξαρτησίας, επάρκειας και αποτελεσματικότητας του τμήματος εσωτερικής επιθεώρησης·

(ε) παροχή συμβουλών στο διοικητικό όργανο, στηριζόμενη στη δουλειά του τμήματος κανονιστικής συμμόρφωσης, σχετικά με την επάρκεια και αποτελεσματικότητα του πλαισίου για

επιχειρηματικής δεοντολογίας·

(στ) παροχή συμβουλών στο διοικητικό όργανο, στηριζόμενη στη δουλειά του τμήματος κανονιστικής συμμόρφωσης και των εξωτερικών ελεγκτών, σχετικά με την επάρκεια και την αποτελεσματικότητα του πλαισίου συμμόρφωσης·

(ζ) αξιολόγηση και παρακολούθηση της ανεξαρτησίας, επάρκειας και αποτελεσματικότητας του τμήματος κανονιστικής συμμόρφωσης ή στην περίπτωση που τα καθήκοντα του τμήματος κανονιστικής συμμόρφωσης διεξάγονται από ένα κοινό τμήμα ελέγχου σύμφωνα με την παράγραφο 76 (1), αξιολόγηση και παρακολούθηση της ανεξαρτησίας, επάρκειας και αποτελεσματικότητας του κοινού τμήματος ελέγχου κατά την εκτέλεση των καθηκόντων του τμήματος κανονιστικής συμμόρφωσης·

(η) σύμφωνα με την παράγραφο 41(ι) υποβολή εισηγήσεων στο διοικητικό όργανο για το διορισμό ή την απομάκρυνση των επικεφαλής των τμημάτων εσωτερικής επιθεώρησης και κανονιστικής συμμόρφωσης·

(θ) σύμφωνα με την παράγραφο 41(ια) ετήσια αξιολόγηση των επικεφαλής των τμημάτων εσωτερικής επιθεώρησης και κανονιστικής συμμόρφωσης και ακολούθως υποβολή τους στο διοικητικό όργανο·

(ι) εξέταση και έγκριση του ετήσιου προγράμματος ελέγχου του τμήματος εσωτερικής επιθεώρησης και του προγράμματος κανονιστικής συμμόρφωσης του τμήματος κανονιστικής συμμόρφωσης·

(ια) εξέταση και έγκριση των προϋπολογισμών του τμήματος εσωτερικής επιθεώρησης και κανονιστικής συμμόρφωσης, διασφαλίζοντας ότι είναι αρκετά ευέλικτοι ώστε να προσαρμόζονται σε μεταβολές ανάλογα με τις εξελίξεις·

(ιβ) εποπτεία των ανώτατων διοικητικών στελεχών ότι λαμβάνουν τα αναγκαία διορθωτικά μέτρα εγκαίρως για την αντιμετώπιση των αδυναμιών ελέγχου, τη μη συμμόρφωση με τις πολιτικές του ιδρύματος, τους νόμους και κανονισμούς και άλλες αδυναμίες που επισημάνθηκαν από τους εξωτερικούς ελεγκτές, των τμημάτων εσωτερικής επιθεώρησης και κανονιστικής συμμόρφωσης και τις εποπτικές αρχές·

(ιγ) παρακολούθηση της θέσπισης των λογιστικών πολιτικών και πρακτικών·

(ιδ) παρακολούθηση της διαδικασίας ετοιμασίας χρηματοοικονομικών αναφορών και της ακεραιότητας, ακρίβειας και αξιοπιστίας των οικονομικών καταστάσεων του ιδρύματος και κάθε επίσημη ανακοίνωση που αφορά τη χρηματοοικονομική απόδοση του ιδρύματος·

(ιε) διεξαγωγή αυτο-αξιολόγησης και υποβολής αναφορών με τα συμπεράσματα και εισηγήσεις για βελτιώσεις και αλλαγές στο διοικητικό όργανο.

Τμήμα 3 – Επιτροπή Κινδύνων

Κριτήρια επιλεξιμότητας μελών της επιτροπής κινδύνων.

40. Τα μέλη της επιτροπής κινδύνων διαθέτουν τις κατάλληλες γνώσεις, δεξιότητες και εμπειρία για να κατανοούν πλήρως και να παρακολουθούν τη στρατηγική κινδύνου και τη διάθεση ανάληψης κινδύνων του ιδρύματος.

Καθήκοντα της επιτροπής κινδύνων.

41. (1) Χωρίς επηρεασμό της πλήρης ευθύνης που φέρει το διοικητικό όργανο για τους κινδύνους, η επιτροπή κινδύνων:

(α) συμβουλεύει το διοικητικό όργανο σχετικά με τη συνολική παρούσα και μελλοντική διάθεση ανάληψης κινδύνων και στρατηγική κινδύνου του ιδρύματος, λαμβάνοντας υπόψη-

(i) τις απαιτήσεις που ορίζονται στην παρούσα Οδηγία·

(ii) το χρηματοοικονομικό προφίλ και το προφίλ κινδύνου του ιδρύματος· και

(iii) την ικανότητα του ιδρύματος για τη διαχείριση και τον έλεγχο των κινδύνων·

(β) βοηθά το διοικητικό όργανο στην επίβλεψη της υλοποίησης της στρατηγικής από τα ανώτατα διοικητικά στελέχη, συμπεριλαμβανομένων –

(i) της ανάπτυξης μηχανισμών για τη διασφάλιση της διαχείρισης των σημαντικών ανοιγμάτων που πλησιάζουν ή υπερβαίνουν τα εγκεκριμένα όρια κινδύνου και, όπου είναι αναγκαίο, του μετριασμού τους κατά τρόπο αποτελεσματικό και έγκαιρο·

(ii) του έγκαιρου προσδιορισμού και της τυχόν κλιμάκωσης των παραβιάσεων των ορίων κινδύνου και των σημαντικών ανοιγμάτων κινδύνου·

(γ) ελέγχει εάν οι τιμές των στοιχείων παθητικού και ενεργητικού που προσφέρονται στους πελάτες λαμβάνουν πλήρως υπόψη το επιχειρηματικό μοντέλο και τη στρατηγική κινδύνου του ιδρύματος· όπου οι τιμές δεν αντικατοπτρίζουν με ακρίβεια τους κινδύνους, σύμφωνα με το επιχειρηματικό μοντέλο και τη στρατηγική κινδύνου, η επιτροπή κινδύνων υποβάλλει διορθωτικό σχέδιο στο διοικητικό όργανο·

(δ) προκειμένου να συμβάλλει στη διαμόρφωση ορθών πολιτικών και πρακτικών αποδοχών και τηρουμένων των καθηκόντων της επιτροπής αποδοχών, εξετάζει κατά πόσο τα κίνητρα που προβλέπει το σύστημα αποδοχών λαμβάνουν υπόψη τον κίνδυνο, το κεφάλαιο, τη ρευστότητα και την πιθανότητα και το χρονοδιάγραμμα των εσόδων·

(ε) υποβάλλει προτάσεις στο διοικητικό όργανο και εισηγήσεις για διορθωτικές ενέργειες, όταν εντοπίζονται αδυναμίες στην εφαρμογή της στρατηγικής κινδύνου·

(στ) αξιολογεί και παρακολουθεί την ανεξαρτησία, επάρκεια και αποτελεσματικότητα του τμήματος διαχείρισης κινδύνων και του τμήματος ασφάλειας πληροφοριών·

(ζ) συμβουλεύει το διοικητικό όργανο, στηριζόμενη στη δουλειά της επιτροπής ελέγχου, του τμήματος διαχείρισης κινδύνων και των εξωτερικών ελεγκτών, σχετικά με την επάρκεια και αποτελεσματικότητα του πλαισίου διαχείρισης κινδύνων·

(η) συμβουλεύει το διοικητικό όργανο, στηριζόμενη στη δουλειά της επιτροπής ελέγχου, του τμήματος ασφάλειας των πληροφοριών και των εξωτερικών ελεγκτών, σχετικά με την επάρκεια και αποτελεσματικότητα του πλαισίου ασφάλειας των πληροφοριών·

(θ) συμβουλεύει το διοικητικό όργανο, στηριζόμενη στη δουλειά της επιτροπής ελέγχου, του τμήματος διαχείρισης κινδύνων και του τμήματος ασφάλειας πληροφοριών και των εξωτερικών ελεγκτών, σχετικά με την επάρκεια και ευρωστία των συστημάτων πληροφόρησης και επικοινωνίας έτσι ώστε –

(i) να επιτρέπουν την αναγνώριση, μέτρηση, αξιολόγηση και αναφορά των κινδύνων κατά τρόπο έγκαιρο και ακριβή·

(ii) να εξασφαλίζουν επαρκή προστασία των εμπιστευτικών και ιδιόκτητων πληροφοριών του ιδρύματος·

(ι) υποβάλλει στο διοικητικό όργανο εισηγήσεις για το διορισμό ή απομάκρυνση των επικεφαλής του τμήματος διαχείρισης κινδύνων και του τμήματος ασφάλειας πληροφοριών·

(ια) διενεργεί ετήσια αξιολόγηση των επικεφαλής των τμημάτων διαχείρισης κινδύνων, κανονιστικής συμμόρφωσης και ασφάλειας των πληροφοριών και την υποβάλλει στο διοικητικό όργανο·

Νοείται ότι, σε περίπτωση που το ίδρυμα έχει συνδυάσει το τμήμα κανονιστικής συμμόρφωσης με το τμήμα διαχείρισης κινδύνων σύμφωνα με την παράγραφο 76 (1), η επιτροπή κινδύνων εκτελεί αυτό το καθήκον με βάση την αξιολόγηση από την επιτροπή ελέγχου του ρόλου του επικεφαλής του κοινού τμήματος ελέγχου σχετικά με την επάρκεια και αποτελεσματικότητά της κατά την εκτέλεση των καθηκόντων του τμήματος κανονιστικής συμμόρφωσης·

(ιβ) διενεργεί εξέταση και έγκριση των προϋπολογισμών του τμήματος διαχείρισης κινδύνων και του τμήματος ασφάλειας των πληροφοριών, εξασφαλίζοντας ότι αυτές είναι αρκετά ευέλικτες ώστε να προσαρμόζονται σε μεταβολές ανάλογα με τις εξελίξεις.

(ιγ) συμβουλεύει το διοικητικό όργανο, στηριζόμενη στη δουλειά της επιτροπής ελέγχου, του τμήματος διαχείρισης κινδύνων και των εξωτερικών ελεγκτών, σχετικά με την επάρκεια των προβλέψεων και την αποτελεσματικότητα των στρατηγικών και πολιτικών αναφορικά με τη διατήρηση, σε συνεχή βάση, επαρκών ποσών, τύπων και διανομής εσωτερικών κεφαλαίων και ιδίων κεφαλαίων για την κάλυψη των κινδύνων του ιδρύματος·

(ιδ) διεξάγει αυτοαξιολόγηση και υποβάλλει στο διοικητικό όργανο τα συμπεράσματα και τις εισηγήσεις της για βελτιώσεις και αλλαγές.

(2) Η επιτροπή κινδύνων καθορίζει τη φύση, την ποσότητα, τη μορφή και τη συχνότητα των πληροφοριών που λαμβάνει ως προς την κατάσταση κινδύνου του ιδρύματος και για κάθε είδος κινδύνου και κάθε επιχειρηματική μονάδα· η επιτροπή κινδύνων οφείλει -

(α) να εγκρίνει μετρήσεις ή διαδικασίες για να διαβεβαιώνεται ότι οι αναφορές και πληροφορίες που λαμβάνει για θέματα κινδύνου είναι ακριβείς, πλήρεις και απεικονίζουν ορθή εικόνα για το προφίλ κινδύνου του ιδρύματος·

(β) να διασφαλίζει ότι οι παράμετροι κινδύνου και τα μοντέλα κινδύνου που αναπτύχθηκαν και χρησιμοποιούνται για την ποσοτικοποίησή τους υπόκεινται σε περιοδική ανεξάρτητη επικύρωση.

Τμήμα 4 – Επιτροπή Αποδοχών

Κριτήρια επιλεξιμότητας των μελών της επιτροπής αποδοχών.

42. Η επιτροπή αποδοχών συγκροτείται ούτως ώστε να εκφέρει αρμοδίως και ανεξαρτήτως γνώμη για τις πολιτικές και πρακτικές αποδοχών και για τα κίνητρα που δημιουργούνται για τη διαχείριση του κινδύνου, του κεφαλαίου και της ρευστότητας.

Καθήκοντα της επιτροπής αποδοχών.

43. (1) Η επιτροπή αποδοχών είναι υπεύθυνη για την προετοιμασία των αποφάσεων σχετικά με τις αποδοχές, συμπεριλαμβανομένων όσων έχουν επιπτώσεις στους κινδύνους και τη διαχείριση των κινδύνων του συγκεκριμένου ιδρύματος και οι οποίες λαμβάνονται από το διοικητικό όργανο.

(2) Κατά την προετοιμασία των αποφάσεων που αναφέρονται στην υποπαράγραφο (1), η επιτροπή αποδοχών οφείλει να λαμβάνει υπόψη τα μακροπρόθεσμα συμφέροντα των μετόχων, των επενδυτών και άλλων ενδιαφερόμενων μερών του ιδρύματος και το δημόσιο συμφέρον και να διασφαλίζει ότι:

(α) αυτά συνδέονται στενά με τους επιχειρηματικούς στόχους και τις στρατηγικές του ιδρύματος·

(β) αυτά είναι σύμφωνα με τις απαιτήσεις που καθορίζονται στο Μέρος VI·

(γ) τα μη εκτελεστικά μέλη δεν περιλαμβάνονται στους δικαιούχους των αποδοχών που συνδέονται με την απόδοση.

(3) Η επιτροπή αποδοχών διασφαλίσει ότι το τμήμα ελέγχου εμπλέκεται στο σχεδιασμό, την αναθεώρηση και την εφαρμογή της πολιτικής αποδοχών.

(4) Η επιτροπή αποδοχών διασφαλίζει ότι τα μέλη του προσωπικού που εμπλέκονται στο σχεδιασμό, την εξέταση και την εφαρμογή των πολιτικών και των πρακτικών αποδοχών έχουν σχετική εμπειρία και είναι ικανά να σχηματίζουν ανεξάρτητη γνώμη για την καταλληλότητα των πολιτικών και των πρακτικών αποδοχών, συμπεριλαμβανομένης της καταλληλότητάς τους για τη διαχείριση του κινδύνου.

(5) Η επιτροπή αποδοχών πραγματοποιεί αυτοαξιολόγηση και υποβάλλει τα συμπεράσματα και τις εισηγήσεις της για βελτιώσεις και αλλαγές στο διοικητικό όργανο.

Τμήμα 5 - Επιτροπή ανάδειξης υποψηφίων

Καθήκοντα της

44. (1) Η επιτροπή ανάδειξης υποψηφίων, ως μέρος των βασικών της καθηκόντων και

επιτροπής ανάδειξης υποψηφίων.

αρμοδιοτήτων:

(α) εντοπίζει και προτείνει, για έγκριση από το διοικητικό όργανο ή προς έγκριση κατά τη γενική συνέλευση, υποψηφίους για τις κενές θέσεις του διοικητικού οργάνου, αξιολογεί το συνδυασμό γνώσεων, δεξιοτήτων, ποικιλότητας και εμπειρίας του διοικητικού οργάνου και συντάσσει περιγραφή των ρόλων και των ικανοτήτων για συγκεκριμένη θέση διορισμού και υπολογίζει το χρόνο που αναμένεται να αφιερωθεί σε αυτή τη θέση·

(β) περιοδικά και τουλάχιστον ετησίως εκτιμά τη δομή, το μέγεθος, τη σύνθεση και την απόδοση του διοικητικού οργάνου και απευθύνει συστάσεις στο διοικητικό όργανο σχετικά με τυχόν αλλαγές·

(γ) κατά περιόδους και τουλάχιστον ετησίως εκτιμά τις γνώσεις, τις δεξιότητες και την εμπειρία μεμονωμένων μελών του διοικητικού οργάνου και του διοικητικού οργάνου ως συνόλου και υποβάλλει σχετικές αναφορές στο διοικητικό όργανο·

(δ) κατά περιόδους και τουλάχιστον ετησίως, επανεξετάζει τα σχέδια διαδοχής του διοικητικού οργάνου για να διασφαλίζει, αφενός, την ύπαρξη ομαλής διαδοχής και διατήρησης της κατάλληλης ισορροπίας της ποικιλότητας, των δεξιοτήτων και εμπειριών και αφετέρου της σταδιακής ανανέωσης του διοικητικού οργάνου, και υποβάλλει σχετικές αναφορές στο διοικητικό όργανο·

(ε) επανεξετάζει κατά περιόδους την πολιτική που εφαρμόζει το διοικητικό όργανο για την επιλογή, ανάπτυξη και το διορισμό ανώτατων διοικητικών στελεχών και των επικεφαλής του τμήματος εσωτερικού ελέγχου και κάνει συστάσεις στο διοικητικό όργανο.

(στ) επανεξετάζει κατά περιόδους την πολιτική του ιδρύματος που αφορά την πρόσληψη, εναλλαγή καθηκόντων και προαγωγή του προσωπικού και υποβάλλει σχετικές αναφορές στο διοικητικό όργανο·

(ζ) επανεξετάζει κατά περιόδους, τουλάχιστον ετησίως, σε συνεργασία με τις επιτροπές ελέγχου και κινδύνου, τη σύνθεση, εξουσία και ανεξαρτησία του τμήματος εσωτερικού ελέγχου και υποβάλλει σχετικές αναφορές στο διοικητικό όργανο·

(η) διεξάγει ετήσια αυτοαξιολόγηση και υποβάλλει αναφορές στο διοικητικό όργανο με συμπεράσματα και εισηγήσεις για βελτιώσεις και αλλαγές.

(2) Για τους σκοπούς της υποπαραγράφου (1)(α), η επιτροπή ανάδειξης υποψηφίων αποφασίζει ως προς τον καθορισμό στόχου για την εκπροσώπηση του ανεπαρκώς εκπροσωπούμενου φύλου στο διοικητικό όργανο και ετοιμάζει πολιτική για το πώς θα αυξηθεί ο αριθμός των ατόμων του ανεπαρκώς εκπροσωπούμενου φύλου στο διοικητικό όργανο, προκειμένου να υλοποιηθεί ο στόχος αυτός· ο στόχος, η πολιτική και η εφαρμογή τους δημοσιοποιούνται σύμφωνα με τις διατάξεις του Άρθρου 435 παράγραφος (2) στοιχείο (γ) του κανονισμού (ΕΕ) αριθ. 575/2013.

(3) Η επιτροπή ανάδειξης υποψηφίων, κατά την εκτέλεση των καθηκόντων της, λαμβάνει υπόψη της, στο βαθμό που είναι δυνατόν και σε διαρκή βάση, την ανάγκη να διασφαλισθεί ότι η λήψη αποφάσεων από το διοικητικό όργανο δεν κυριαρχείται από ένα άτομο ή μικρή ομάδα ατόμων κατά τρόπο που θίγει τα συμφέροντα του ιδρύματος ως συνόλου.

(4) Η επιτροπή ανάδειξης υποψηφίων πρέπει να χρησιμοποιεί οποιοδήποτε είδος πόρων κρίνει κατάλληλο, συμπεριλαμβανόμενων των εξωτερικών συμβούλων, και λαμβάνει τη δέουσα χρηματοδότηση προς τον σκοπό αυτό.

ΜΕΡΟΣ V
ΑΝΩΤΑΤΑ ΔΙΟΙΚΗΤΙΚΑ ΣΤΕΛΕΧΗ

Σύνθεση των ανώτατων διοικητικών στελεχών.

45. (1) Τηρουμένου του Άρθρου 19 του Νόμου, τα ανώτατα διοικητικά στελέχη πρέπει να είναι επαρκή σε αριθμό και να διαθέτουν την απαραίτητη τεχνογνωσία για την αποτελεσματική διαχείριση των δραστηριοτήτων του ιδρύματος.

(2) Τα ιδρύματα διασφαλίζουν ότι τα ανώτατα διοικητικά στελέχη αναλαμβάνουν τους ρόλους των επικεφαλής των τμημάτων ελέγχου, σύμφωνα με τις διατάξεις της παρούσας Οδηγίας και ότι τα άτομα αυτά δεν έχουν άμεσες αρμοδιότητες στις επιχειρηματικές μονάδες και μονάδες στήριξης τις οποίες τα τμήματα ελέγχου, στο πλαίσιο των καθηκόντων τους, παρακολουθούν και ελέγχουν.

Επιλογή, ανάπτυξη και διαδοχή των ανώτατων διοικητικών στελεχών.

46. (1) Τα ιδρύματα διαθέτουν κατάλληλες πολιτικές και διαδικασίες για την επιλογή, ανάπτυξη και, όταν χρειάζεται, την αντικατάσταση του διευθύνοντος συμβούλου ή άλλων ανώτατων διοικητικών στελεχών και κατάλληλα σχέδια διαδοχής, λαμβάνοντας δεόντως υπόψη τη σημασία και την κρισιμότητα των υποχρεώσεών τους έναντι των εργασιών και του τμήματος εσωτερικού ελέγχου του ιδρύματος και του ομίλου του· οι πολιτικές, τα σχέδια και οι διαδικασίες αυτές διασφαλίζουν:

(α) την αναγνώριση και τακτική επικαιροποίηση των απαραίτητων προσόντων, δεξιοτήτων και ακαδημαϊκών ή επαγγελματικών προσόντων για τη διασφάλιση –

(i) της αποτελεσματικότητας του διευθύνοντος συμβούλου και των άλλων ανώτατων διοικητικών στελεχών και των επικεφαλής των τμημάτων εσωτερικού ελέγχου, στην εκτέλεση των καθηκόντων και αρμοδιοτήτων τους·

(ii) της συμμόρφωσης με ρυθμιστικές απαιτήσεις ·

(β) την παρακολούθηση της ανάπτυξης και εξέλιξης πιθανών εσωτερικών υποψηφίων και της περιοδικής αξιολόγησης της καταλληλότητάς τους για θέση ανώτατου διοικητικού στελέχους σε σχέση με τις απαιτούμενες ικανότητες, δεξιότητες και προσόντα·

(γ) ότι στο σχεδιασμό της διαδοχής του διευθύνοντος συμβούλου και των άλλων ανώτατων διοικητικών στελεχών λαμβάνεται υπόψη η ημερομηνία λήξης της θητείας, ανάθεσης ή σύμβασης εργασίας του κάθε ατόμου, έτσι ώστε –

(i) να αποφευχθεί η ανάγκη ταυτόχρονης αντικατάστασης πολλών ανώτατων διοικητικών στελεχών·

(ii) να διασφαλιστεί ότι οι μεταβάσεις αυτές γίνονται ομαλά με τις ελάχιστες δυνατές επιπτώσεις στις εργασίες του ιδρύματος·

(δ) ότι έχουν θεσπιστεί σχέδια διαδοχής έκτακτης ανάγκης για απρόβλεπτα γεγονότα, όπως η αποχώρηση, ο θάνατος ή η αναπηρία του διευθύνοντος συμβούλου ή άλλων ανώτατων διοικητικών στελεχών για τη διευκόλυνση της πλήρωσης τόσο σε προσωρινή όσο και σε μακροπρόθεσμη βάση, θέσης ανώτατου διοικητικού στελέχους που κενώθηκε άκαιρα.

Ρόλοι και ευθύνες των ανώτατων διοικητικών στελεχών.

47. (1) Ο διευθύνων σύμβουλος και τα άλλα ανώτατα διοικητικά στελέχη είναι υπεύθυνα για την καθοδήγηση και επίβλεψη της αποτελεσματικής διαχείρισης του ιδρύματος στα πλαίσια των εξουσιών που τους έχουν ανατεθεί από το διοικητικό όργανο και σε συμμόρφωση με τους εφαρμοστέους νόμους και κανονισμούς.

(2) Τα ανώτατα διοικητικά στελέχη είναι υπεύθυνα για:

(α) τη διεύθυνση και επίβλεψη των καθημερινών εργασιών του ιδρύματος, τηρουμένων των επιχειρηματικών στόχων, στρατηγικών και πολιτικών που έχουν εγκριθεί από το διοικητικό όργανο, και των νομικών και ρυθμιστικών απαιτήσεων·

(β) την παροχή εισηγήσεων στο διοικητικό όργανο, προς εξέταση και έγκριση του, αναφορικά με τους επιχειρηματικούς στόχους, στρατηγικές και επιχειρηματικά σχέδια και τις μείζονες πολιτικές που διέπουν τη λειτουργία του διοικητικού οργάνου·

(γ) την παροχή ολοκληρωμένων, σχετικών και έγκαιρων πληροφοριών στο διοικητικό όργανο που θα του επιτρέψουν να επανεξετάσει τους επιχειρηματικούς στόχους, την επιχειρηματική στρατηγική και πολιτικές, και να καθιστά τα ανώτατα διοικητικά στελέχη υπόλογα για την εκτέλεση των καθηκόντων τους.

Επίβλεψη των εργασιών του ιδρύματος και καθοδήγηση σε καθημερινή βάση.

48. (1) Τα ανώτατα διοικητικά στελέχη είναι υπεύθυνα για την εφαρμογή μίας αποτελεσματικής και διαφανούς λειτουργικής δομής στο ίδρυμα ή στον όμιλο, σύμφωνα με τους επιχειρηματικούς στόχους, στρατηγικές και πολιτικές που έχουν εγκριθεί από το διοικητικό όργανο· όπου το ίδρυμα δραστηριοποιείται εκτός Δημοκρατίας ή λειτουργεί μέσω εταιρειών ειδικού σκοπού ή παρεμφερών δομών ή σε δικαιοδοσίες που παρεμποδίζουν τη διαφάνεια, τα ανώτατα διοικητικά στελέχη ασκούν επαρκή εποπτεία των εργασιών του ιδρύματος σε επίπεδο ομίλου, συμπεριλαμβανομένων των δραστηριοτήτων αυτών, και διασφαλίζουν την ύπαρξη ενδεδειγμένων δομών αναφοράς και την προσβασιμότητα του διοικητικού οργάνου και των εποπτικών αρχών σε σημαντική πληροφόρηση που αφορά μη διαφανείς ή μη τυποποιημένες δομές, υποκαταστήματα και θυγατρικές εταιρείες εκτός

της Δημοκρατίας.

(2) Τα ανώτατα διοικητικά στελέχη είναι υπεύθυνα για την ανάθεση καθηκόντων στο προσωπικό και τη θέσπιση τέτοιας διοικητικής δομής και ιεραρχίας που να προωθούν τη λογοδοσία και τη διαφάνεια, χωρίς την ύπαρξη κενών στους δίαυλους αναφοράς, και να εποπτεύουν την άσκηση των εν λόγω αρμοδιοτήτων που ανατέθηκαν.

(3) Τα ανώτατα διοικητικά στελέχη εφαρμόζουν αποτελεσματικό προγραμματισμό άντλησης κεφαλαίων και ρευστότητας και διαδικασία προϋπολογισμού κατά τρόπο συνεπή με την κατεύθυνση που δόθηκε από το διοικητικό όργανο· τα ανώτατα διοικητικά στελέχη επιβλέπουν την εφαρμογή του προϋπολογισμού και της διαδικασίας εξεύρεσης κεφαλαίων και ρευστότητας, εντοπίζουν αδυναμίες και δυνητικούς περιορισμούς και αξιολογούν τη σημαντικότητά τους, και αναπτύσσουν σχέδια αποκατάστασης σε περίπτωση που αδυναμίες επηρεάζουν την επάρκεια της ρευστότητας και των ιδίων κεφαλαίων.

(5) Τα ανώτατα διοικητικά στελέχη δίνουν το καλό παράδειγμα για την εφαρμογή του κώδικα επιχειρησιακής δεοντολογίας και των εταιρικών αξιών και προωθούν εταιρική κουλτούρα όπου οι υπάλληλοι ενθαρρύνονται να προσδιορίζουν οι ίδιοι θέματα ηθικής, κανονιστικής συμμόρφωσης ή κινδύνου, και δεν στηρίζονται στα τμήματα ελέγχου για τον προσδιορισμό των αξιών, κατά τρόπο που να συνάδει με την κατεύθυνση που δόθηκε από το διοικητικό όργανο και σύμφωνα με τις πρόνοιες της παρούσας Οδηγίας.

(6) Τα ανώτατα διοικητικά εφαρμόζουν κατάλληλο πλαίσιο συμμόρφωσης σύμφωνα με την κατεύθυνση που δόθηκε από το διοικητικό όργανο και σύμφωνα με τις διατάξεις του Μέρους VIII.

(7) Τα ανώτατα διοικητικά στελέχη εφαρμόζουν κατάλληλο πλαίσιο διαχείρισης του κινδύνου σύμφωνα με τη στρατηγική κινδύνου και τη διάθεση και κατεύθυνση που δόθηκε από το διοικητικό όργανο και τις διατάξεις του Μέρους IX· τα ανώτατα διοικητικά στελέχη διασφαλίζουν ότι έχουν αναπτυχθεί και εφαρμόζονται αποτελεσματικά διαδικασίες έγκρισης νέων προϊόντων, σύμφωνα με τις διατάξεις της παραγράφου 72.

(8) Τα ανώτατα διοικητικά στελέχη εφαρμόζουν κατάλληλο πλαίσιο εσωτερικού ελέγχου, σύμφωνα με την κατεύθυνση που δόθηκε από το διοικητικό όργανο και τις πρόνοιες του Μέρους X· τα ανώτατα διοικητικά στελέχη διασφαλίζουν ότι διατίθενται επαρκείς πόροι με κατάλληλη αρμοδιότητα και τεχνογνωσία στα τμήματα ελέγχου.

(9) Τα ανώτατα διοικητικά στελέχη διασφαλίζουν ότι το ίδρυμα αναπτύσσει κατάλληλα πληροφοριακά συστήματα και συστήματα επικοινωνίας για την υποβοήθηση του διοικητικού οργάνου να διεξάγει αποτελεσματική εποπτεία του ιδρύματος σύμφωνα με την κατεύθυνση που δόθηκε από το διοικητικό όργανο και τις διατάξεις του Μέρους XI· τα ανώτατα διοικητικά στελέχη είναι υπεύθυνα να διασφαλίζουν την τήρηση κατάλληλων αρχείων σύμφωνα με τις διατάξεις των παραγράφων 13, 62 και 105.

(10) Τα ανώτατα διοικητικά στελέχη καθορίζουν κατάλληλες πολιτικές ανθρώπινου δυναμικού, συμπεριλαμβανομένης της ανάπτυξης διοκητικών στελεχών και του προγραμματισμού της διαδοχής τους.

Παροχή εισηγήσεων στο διοικητικό όργανο.

49. (1) Τα ανώτατα διοικητικά στελέχη προβαίνουν σε εμπεριστατωμένες εισηγήσεις προς το διοικητικό όργανο σχετικά με τους επιχειρηματικούς στόχους, τη στρατηγική και διάθεση ανάληψης κινδύνων, το κεφάλαιο και τα σχεδία χρηματοδότησης και τις αποφάσεις διανομής και την πολιτική αποδοχών.

(2) Τα ανώτατα διοικητικά στελέχη διασφαλίζουν ότι οι προτεινόμενες εισηγήσεις αναλύονται επαρκώς και αντικατοπτρίζουν πλήρως τις προσδοκίες των σημαντικών ενδιαφερόμενων μερών, συμπεριλαμβανομένων των πιστωτών, των αντισυμβαλλόμενων, των επενδυτών και των εποπτικών αρχών.

(3) Τα ανώτατα διοικητικά στελέχη αναφέρουν στο διοικητικό όργανο αδυναμίες και περιορισμούς που εντοπίστηκαν στις στρατηγικές και στο σχεδιασμό, υποβάλλοντας ταυτόχρονα εισηγήσεις για αποκατάσταση.

ΜΕΡΟΣ VI
ΠΛΑΙΣΙΟ ΑΠΟΔΟΧΩΝ

Πολιτικές αποδοχών.

50. Κατά τον καθορισμό και εφαρμογή του συνόλου των πολιτικών αποδοχών, συμπεριλαμβανομένων των μισθών και των προαιρετικών συνταξιοδοτικών παροχών, για τις κατηγορίες υπαλλήλων που περιλαμβάνουν τα ανώτατα διοικητικά στελέχη, πρόσωπα τα οποία αναλαμβάνουν κινδύνους, προσωπικό που ασκεί καθήκοντα ελέγχου καθώς και κάθε εργαζόμενο οι συνολικές αποδοχές του οποίου τον εντάσσουν στο ίδιο επίπεδο αμοιβών με τα ανώτατα διοικητικά στελέχη και τα πρόσωπα που αναλαμβάνουν κινδύνους, των οποίων οι επαγγελματικές δραστηριότητες έχουν ουσιώδη αντίκτυπο στο προφίλ κινδύνου τους, τα ιδρύματα συμμορφώνονται προς τις ακόλουθες αρχές κατά τρόπο και σε βαθμό που ενδείκνυται προς το μέγεθος, την εσωτερική οργάνωση και τη φύση, το αντικείμενο και την πολυπλοκότητα των δραστηριοτήτων τους:

(α) η πολιτική αποδοχών συνάδει με και προωθεί τη συνετή και αποτελεσματική διαχείριση των κινδύνων και δεν ενθαρρύνει την ανάληψη κινδύνων που υπερβαίνουν το επίπεδο ανοχής κινδύνων του ιδρύματος·

(β) η πολιτική αποδοχών είναι σύμφωνη προς την επιχειρηματική στρατηγική, τους στόχους, τις αξίες και τα μακροπρόθεσμα συμφέροντα του ιδρύματος, και ενσωματώνει μέτρα για την αποφυγή αντικρουόμενων συμφερόντων·

(γ) το διοικητικό όργανο του ιδρύματος κατά την άσκηση της εποπτικής του αρμοδιότητας υιοθετεί και περιοδικά αναθεωρεί τις γενικές αρχές της πολιτικής αποδοχών και είναι υπεύθυνο για την επίβλεψη της υλοποίησής της·

(δ) η εφαρμογή της πολιτικής αποδοχών υπόκειται, τουλάχιστον ετησίως, σε κεντρικό και ανεξάρτητο εσωτερικό έλεγχο ως προς τη συμμόρφωση με τις πολιτικές και διαδικασίες αποδοχών που έχουν υιοθετηθεί από το διοικητικό όργανο κατά την άσκηση των εποπτικών του αρμοδιοτήτων·

(ε) το προσωπικό που έχει επιφορτισθεί με καθήκοντα ελέγχου είναι ανεξάρτητο από τις επιχειρηματικές μονάδες τις οποίες εποπτεύει, έχει τις κατάλληλες εξουσίες και αμείβεται σύμφωνα με την επίτευξη των στόχων που συνδέονται με τα καθήκοντά του, ανεξαρτήτως των επιδόσεων των επιχειρηματικών τομέων που ελέγχει·

(στ) οι αποδοχές των ανωτέρων στελεχών η του τμήματος διαχείρισης κινδύνων εποπτεύονται άμεσα από την επιτροπή αποδοχών που αναφέρεται στην υποπαράγραφο (2) της παραγράφου 35 ή, με μία συνδυασμένη επιτροπή ανάδειξης υποψηφίων και αποδοχών σύμφωνα με την υποπαράγραφο (3) της εν λόγω παραγράφου·

(ζ) στην πολιτική αποδοχών, λαμβάνοντας υπόψη εθνικά κριτήρια καθορισμού μισθών, γίνεται σαφής διάκριση μεταξύ των κριτηρίων όσον αφορά τον καθορισμό:

(i) των πάγιων βασικών αποδοχών, οι οποίες θα πρέπει πρωτίστως να αντικατοπτρίζουν τη συναφή επαγγελματική εμπειρία και την ευθύνη διαχείρισης, όπως ορίζεται στην περιγραφή καθηκόντων του υπαλλήλου ως μέρος των όρων απασχόλησης· και

(i) των μεταβλητών αποδοχών οι οποίες θα πρέπει να αντικατοπτρίζουν επιδόσεις βιώσιμες και προσαρμοσμένες στον κίνδυνο, καθώς και επιδόσεις που υπερβαίνουν τις απαιτούμενες για την εκπλήρωση των καθηκόντων του υπαλλήλου όπως αυτά ορίζονται στην περιγραφή καθηκόντων του υπαλλήλου ως μέρος των όρων απασχόλησης.

(2) Τα ιδρύματα διασφαλίζουν ότι οι μέτοχοι ενημερώνονται για το σύνολο των αποδοχών των ανώτατων διοικητικών στελεχών.

(3) Για σκοπούς της παρούσας παραγράφου, τα ιδρύματα συμμορφώνονται με τις κατευθυντήριες γραμμές της ΕΑΤ σχετικά με τις πολιτικές και πρακτικές αποδοχών του 2010, όπως εκάστοτε τροποποιούνται ή αντικαθίστανται.

Μεταβλητά στοιχεία αποδοχών.

51. Για τα μεταβλητά στοιχεία των αποδοχών ισχύουν επιπρόσθετα με, και υπό τις ίδιες συνθήκες όπως εκείνες που ορίζονται στην παράγραφο 50, οι εξής αρχές:

(α) όπου οι αποδοχές συνδέονται με την απόδοση, το συνολικό ποσό των αποδοχών βασίζεται σε ένα συνδυασμό αξιολόγησης της απόδοσης του ατόμου, και της σχετικής επιχειρηματικής μονάδας και των συνολικών αποτελεσμάτων του ιδρύματος, και, κατά την αξιολόγηση της ατομικής απόδοσης, λαμβάνονται υπόψη χρηματοοικονομικά και μη κριτήρια·

(β) η αξιολόγηση της απόδοσης εντάσσεται σε πολυετές πλαίσιο, ώστε να διασφαλίζεται ότι η διαδικασία της αξιολόγησης βασίζεται σε πιο μακροπρόθεσμες επιδόσεις και ότι η καταβολή των τμημάτων της αμοιβής που συνδέονται με την απόδοση κατανέμεται σε μια περίοδο που λαμβάνει υπόψη τον υποκείμενο κύκλο επιχειρηματικής δραστηριότητας του πιστωτικού ιδρύματος και τους επιχειρηματικούς του κινδύνους·

(γ) το σύνολο των μεταβλητών αποδοχών δεν περιορίζει τη δυνατότητα του ιδρύματος να ενισχύσει την κεφαλαιακή του βάση·

(δ) οι εγγυημένες μεταβλητές αποδοχές δεν συνάδουν με την υγιή διαχείριση κινδύνων ή την αρχή της αμοιβής της απόδοσης και δεν περιλαμβάνονται στα μελλοντικά σχέδια αποδοχών·

(ε) οι εγγυημένες μεταβλητές αποδοχές αποτελούν εξαίρεση και παρέχονται μόνο όταν προσλαμβάνεται νέο προσωπικό υπό τον όρο ότι το ίδρυμα διαθέτει υγιή και ισχυρή κεφαλαιακή βάση και περιορίζεται στο πρώτο έτος εργοδότησης·

(στ) οι σταθερές και οι μεταβλητές συνιστώσες των συνολικών αποδοχών εξισορροπούνται κατάλληλα και το σταθερό στοιχείο αντιπροσωπεύει ένα επαρκώς υψηλό ποσοστό των συνολικών αποδοχών προκειμένου να καθίσταται εφικτή η εφαρμογή μιας πλήρως ευέλικτης πολιτικής κατά το σκέλος των μεταβλητών στοιχείων των αποδοχών, συμπεριλαμβανομένης της δυνατότητας να μην καταβληθεί το μεταβλητό στοιχείο των αποδοχών·

(ζ) τα ιδρύματα καθορίζουν τη δέουσα αναλογία μεταξύ σταθερών και μεταβλητών συνιστωσών του συνόλου των αποδοχών, όπου ισχύουν οι ακόλουθες αρχές:

(i) η μεταβλητή συνιστώσα δεν υπερβαίνει το πενήντα τοις εκατό (50%) της σταθερής συνιστώσας του συνόλου των αποδοχών για κάθε άτομο·

(ii) οι μέτοχοι ή οι ιδιοκτήτες ή τα μέλη του ιδρύματος δύνανται να εγκρίνουν υψηλότερη μέγιστη αναλογία μεταξύ σταθερής και μεταβλητής συνιστώσας των αποδοχών υπό την προϋπόθεση ότι το συνολικό ύψος της μεταβλητής συνιστώσας δεν υπερβαίνει το εκατό τοις εκατό (100%) της σταθερής συνιστώσας του συνόλου των αποδοχών για κάθε άτομο· οποιαδήποτε έγκριση υψηλότερης αναλογίας, σύμφωνα με το σημείο (i) πραγματοποιείται σύμφωνα με την ακόλουθη διαδικασία:

- οι μέτοχοι ή ιδιοκτήτες ή μέλη του ιδρύματος ενεργούν δυνάμει λεπτομερούς σύστασης του ιδρύματος στην οποία αναφέρονται οι λόγοι και το πεδίο εφαρμογής της επιδιωκόμενης έγκρισης, συμπεριλαμβανομένων του αριθμού του υπηρετούντος προσωπικού που επηρεάζεται, των καθηκόντων τους και του αναμενόμενου αντίκτυπου ως προς την απαίτηση διατήρησης υγιούς κεφαλαιακής βάσης·

- οι μέτοχοι ή ιδιοκτήτες ή μέλη του ιδρύματος αποφασίζουν με πλειοψηφία τουλάχιστον εξήντα έξι τοις εκατό (66%), νοουμένου ότι εκπροσωπείται τουλάχιστον το πενήντα τοις εκατό (50%) των μετοχών ή ισοδύναμων δικαιωμάτων ιδιοκτησίας ή, ελλείψει αυτού, αποφασίζουν με πλειοψηφία εβδομήντα πέντε τοις εκατό (75%) των εκπροσωπούμενων δικαιωμάτων ιδιοκτησίας·

- το ίδρυμα κοινοποιεί σε όλους τους μετόχους ή ιδιοκτήτες ή μέλη του ιδρύματος, παρέχοντας εκ των προτέρων ένα εύλογο χρονικό διάστημα προειδοποίησης, ότι θα επιδιωχθεί έγκριση δυνάμει της πρώτης υποπαραγράφου του παρόντος σημείου·

- το ίδρυμα ενημερώνει αμελλητί την Κεντρική Τράπεζα τη σύσταση προς τους μετόχους ή ιδιοκτήτες ή μέλη του, συμπεριλαμβανομένης της προτεινόμενης υψηλότερης μέγιστης αναλογίας του σχετικού σκεπτικού, είναι δε σε θέση να αποδείξει στην Κεντρική Τράπεζα ότι η προτεινόμενη υψηλότερη αναλογία δεν αντιβαίνει στις υποχρεώσεις του ιδρύματος βάσει της παρούσας Οδηγίας και δυνάμει του Κανονισμού (ΕΕ) αριθ. 575/2013, κυρίως όσον αφορά τις υποχρεώσεις περί ιδίων κεφαλαίων του ιδρύματος·

- το ίδρυμα ενημερώνει αμελλητί την Κεντρική Τράπεζα σχετικά με τις αποφάσεις των μετόχων ή ιδιοκτητών ή μελών του, συμπεριλαμβανομένης τυχόν έγκρισης υψηλότερης αναλογίας βάσει της πρώτης υποπαραγράφου, και οι αρμόδιες αρχές χρησιμοποιούν τις λαμβανόμενες πληροφορίες για τη συγκριτική αξιολόγηση των σχετικών πρακτικών των ιδρυμάτων.

- τα μέλη του προσωπικού τα οποία αφορούν άμεσα τα αναφερόμενα στο παρόν σημείο υψηλότερα μέγιστα επίπεδα μεταβλητών αποδοχών δεν επιτρέπεται, κατά περίπτωση, να ασκούν, άμεσα ή έμμεσα, τυχόν δικαιώματα ψήφου που μπορεί να έχουν ως μέτοχοι ή ιδιοκτήτες ή μέλη του ιδρύματος·

(iii) τα ιδρύματα δύναται να εφαρμόζουν συντελεστή αναπροσαρμογής για ποσό είκοσι πέντε τοις εκατό (25%) κατ' ανώτατο όριο των συνολικών μεταβλητών αποδοχών, εφόσον αυτό πληρώνεται σε μέσα που αναβάλλονται για περίοδο η οποία δεν είναι μικρότερη των πέντε (5) ετών· τα ιδρύματα που επιλέγουν να εφαρμόσουν τις διατάξεις του παρόντος σημείου, οφείλουν να συμμορφώνονται με τις κατευθυντήριες γραμμές της ΕΑΤ σχετικά με το υποθετικό συντελεστή αναπροσαρμογής για μεταβλητές αποδοχές του 2014, όπως εκάστοτε τροποποιούνται ή αντικαθίστανται·

(η) οι πληρωμές που συνδέονται με την πρόωρη καταγγελία σύμβασης αντικατοπτρίζουν τις επιδόσεις που επιτεύχθηκαν σε βάθος χρόνου και δεν ανταμείβουν την αποτυχία ή τη διάπραξη παραπτωμάτων·

(θ) τα πακέτα αποδοχών που αφορούν αποζημίωση ή εξαγορά από συμβάσεις σε προηγούμενη απασχόληση πρέπει να ευθυγραμμίζονται με το μακροπρόθεσμο συμφέρον του ιδρύματος, περιλαμβανομένων των ρυθμίσεων περί επίσχεσης, αναστολής, επιδόσεων και ανάκτησης·

(ι) η μέτρηση των επιδόσεων που χρησιμοποιείται για τον υπολογισμό των συνιστωσών για τις μεταβλητές αποδοχές ή των ομαδοποιημένων συνιστωσών για τις μεταβλητές αποδοχές περιλαμβάνει προσαρμογή προς κάθε είδους τρεχόντων και μελλοντικών κινδύνων και λαμβάνει υπόψη το κόστος κεφαλαίου και τη ρευστότητα που απαιτείται·

(ια) η κατανομή των συνιστωσών για τις μεταβλητές αποδοχές εντός του ιδρύματος λαμβάνει επίσης υπόψη το πλήρες φάσμα των τρεχόντων και μελλοντικών κινδύνων·

(ιβ) σημαντικό μέρος, και σε κάθε περίπτωση τουλάχιστον το πενήντα τοις εκατό (50%) οιωνδήποτε μεταβλητών αποδοχών, αποτελείται από αναλογία των παρακάτω:

(i) μετοχές ή ισοδύναμα δικαιώματα ιδιοκτησίας, ανάλογα με τη νομική δομή του σχετικού ιδρύματος ή μέσα που συνδέονται με μετοχές ή ισοδύναμα μη ευχερώς ρευστοποιήσιμα μέσα, στην περίπτωση μη εισηγμένων ιδρυμάτων·

(ii) όπου είναι δυνατό, άλλα μέσα, κατά την έννοια του Άρθρου 52 ή 63 του Κανονισμού (ΕΕ) αριθ. 575/2013, ή άλλα μέσα πλήρως μετατρέψιμα σε μέσα του Κεφαλαίου Κοινών Μετοχών της Κατηγορίας 1 ή που έχουν επανεκτιμηθεί, τα οποία σε κάθε περίπτωση αντανακλούν δεόντως την πιστοληπτική ικανότητα του ιδρύματος σε συνθήκες δρώσας οικονομικής κατάστασης και είναι κατάλληλα να χρησιμοποιηθούν για τους σκοπούς των μεταβλητών αποδοχών.

Τα μέσα που αναφέρονται στο παρόν σημείο υπόκεινται σε ενδεδειγμένη πολιτική διακράτησης με σκοπό την ευθυγράμμιση των κινήτρων με τα μακροπρόθεσμα συμφέροντα του ιδρύματος. Η Κεντρική Τράπεζα δύναται να θέτει περιορισμούς στο είδος και στο σχεδιασμό αυτών των μέσων ή να απαγορεύει ορισμένα μέσα όπως αρμόζει. Το παρόν σημείο εφαρμόζεται τόσο στο μέρος του υπό αναβολή μεταβλητού στοιχείου των αποδοχών σύμφωνα με το σημείο (ιγ) όσο και στο μέρος του μεταβλητού στοιχείου των αποδοχών που δεν τελεί υπό αναβολή·

(ιγ) η καταβολή σημαντικού μέρους, και σε κάθε περίπτωση τουλάχιστον σαράντα τοις εκατό (40%) της μεταβλητής συνιστώσας των αποδοχών, αναβάλλεται για περίοδο η οποία δεν είναι μικρότερη από τρία έως πέντε έτη και ευθυγραμμίζεται ορθά με τη φύση της επιχείρησης, τους κινδύνους της και τις δραστηριότητες του εν λόγω μέλους του προσωπικού.

Οι πληρωτέες αποδοχές που υπάγονται στις ρυθμίσεις περί αναβολής κατοχυρώνονται το πολύ

κατ' αναλογία του χρόνου. Σε περίπτωση μεταβλητής συνιστώσας αποδοχών ιδιαίτερα υψηλού ποσού, αναβάλλεται η καταβολή της τουλάχιστον κατά το εξήντα τοις εκατό (60%) του ποσού. Η διάρκεια της περιόδου αναβολής ορίζεται σύμφωνα με τον επιχειρηματικό κύκλο, τη φύση της επιχειρηματικής δραστηριότητας, τους κινδύνους της και τις δραστηριότητες των εν λόγω μελών του προσωπικού·

(ιδ) η μεταβλητή αμοιβή, συμπεριλαμβανομένου του μέρους υπό αναβολή, καταβάλλεται ή κατοχυρώνεται μόνον εφόσον είναι βιώσιμη βάσει της οικονομικής κατάστασης του ιδρύματος συνολικά και δικαιολογημένη βάσει των επιδόσεων του ιδρύματος, της εν λόγω επιχειρησιακής μονάδας και του εν λόγω ατόμου.

Με την επιφύλαξη των γενικών αρχών του εθνικού εργατικού δικαίου, περιλαμβανομένων και των διατάξεων περί συμβάσεων εργασίας, το σύνολο των μεταβλητών αποδοχών θα συρρικνώνεται γενικά σημαντικά όταν το ίδρυμα παρουσιάζει υποτονικές ή αρνητικές χρηματοοικονομικές επιδόσεις, λαμβάνοντας υπόψη τόσο τις τρέχουσες αμοιβές όσο και τις μειώσεις σε αμοιβές που είχαν προηγουμένως εισπραχθεί, συμπεριλαμβανομένων μέσω ρυθμίσεων malus ή ρυθμίσεων περί επιστροφής αμοιβών.

Ποσοστό έως και 100 % του συνόλου των μεταβλητών αποδοχών υπόκειται σε ρυθμίσεις malus ή ρυθμίσεις περί επιστροφής αμοιβών. Τα ιδρύματα θεσπίζουν ειδικά κριτήρια για την εφαρμογή του malus ή της επιστροφής αμοιβών. Τα εν λόγω κριτήρια καλύπτουν ειδικότερα καταστάσεις όπου το μέλος του προσωπικού:

(i) συμμετείχε ή ήταν υπεύθυνο για συμπεριφορά η οποία προξένησε σημαντικές ζημίες στο ίδρυμα·

(ii) δεν πληρούσε τα προσήκοντα πρότυπα ικανότητας και ευπρέπειας·

(ιε) η συνταξιοδοτική πολιτική είναι σύμφωνη με την επιχειρηματική στρατηγική, τους στόχους, τις αξίες και τα μακροπρόθεσμα συμφέροντα του ιδρύματος.

Εάν ο υπάλληλος αποχωρήσει από το ίδρυμα πριν από τη συνταξιοδότηση, οι προαιρετικές συνταξιοδοτικές παροχές διατηρούνται από το ίδρυμα για διάστημα πέντε ετών, με τη μορφή των μέσων που αναφέρονται στο σημείο (ιβ). Στην περίπτωση υπαλλήλου που φθάνει στη συνταξιοδότηση, οι προαιρετικές συνταξιοδοτικές παροχές καταβάλλονται στον υπάλληλο με τη μορφή των μέσων που αναφέρονται στο σημείο (ιβ), με την επιφύλαξη πενταετούς περιόδου διακράτησης·

(ιστ) τα μέλη του προσωπικού υποχρεούνται να μην χρησιμοποιούν προσωπικές στρατηγικές αντιστάθμισης κινδύνου ή ασφάλιση συνδεδεμένη με αποδοχές ή ευθύνη για να καταστρατηγούνται οι περιλαμβανόμενοι στις ρυθμίσεις περί αποδοχών μηχανισμοί ευθυγράμμισης με τον κίνδυνο·

(ιζ) η μεταβλητή αμοιβή δεν καταβάλλεται μέσω μηχανισμών ή μεθόδων που διευκολύνουν τη μη συμμόρφωση με την παρούσα οδηγία ή τον κανονισμό (ΕΕ) αριθ. 575/2013.

Ιδρύματα που επωφελούνται από κυβερνητική παρέμβαση.

52. Στην περίπτωση των ιδρυμάτων που επωφελούνται από κατ' εξαίρεση κυβερνητική παρέμβαση, ισχύουν οι ακόλουθες αρχές επιπρόσθετα με αυτές που προνοούνται στην παράγραφο 50:

(α) οι μεταβλητές αποδοχές περιορίζονται αυστηρά ως ποσοστό επί των καθαρών εσόδων, όταν δεν συμβαδίζουν με τη διατήρηση υγιούς κεφαλαιακής βάσης και την έγκαιρη έξοδο από την κρατική στήριξη·

(β) οι αποδοχές αναδιαρθρώνονται κατά τρόπο που να ευθυγραμμίζονται με τη χρηστή διαχείριση των κινδύνων και τη μακροπρόθεσμη ανάπτυξη, συμπεριλαμβανομένης, όπου εφαρμόζεται, της θέσπισης ορίων στις αποδοχές των μελών του διοικητικού οργάνου του ιδρύματος·

(γ) δεν καταβάλλονται μεταβλητές αποδοχές στα μέλη του διοικητικού οργάνου του ιδρύματος εκτός αν αυτό είναι δικαιολογημένο.

ΜΕΡΟΣ VII
ΠΛΑΙΣΙΟ ΕΠΙΧΕΙΡΗΣΙΑΚΗΣ ΔΕΟΝΤΟΛΟΓΙΑΣ

Εταιρικές αξίες και κώδικας επιχειρησιακής δεοντολογίας.

53. (1) Τα ιδρύματα αναπτύσσουν, εγκρίνουν και προωθούν σε ολόκληρο τον οργανισμό κώδικα επιχειρησιακής δεοντολογίας και εταιρικών αξιών βάσει των γενικώς αποδεκτών αρχών.

(2) Ο κώδικας επιχειρησιακής δεοντολογίας του ιδρύματος και οι εταιρικές αξίες πρέπει να διατυπώνουν αποδεκτές και μη αποδεκτές συμπεριφορές· ο εν λόγω κώδικας και οι εν λόγω αξίες θα πρέπει ξεκάθαρα να απαγορεύουν συμπεριφορές που θα μπορούσαν να εμπλέξουν το ίδρυμα σε οποιαδήποτε ανάρμοστη, ανήθικη ή παράνομη δραστηριότητα, όπως η αναφορά εσφαλμένων οικονομικών στοιχείων, η νομιμοποίηση εσόδων από παράνομες δραστηριότητες, η απάτη, δωροδοκία ή διαφθορά και να αποθαρρύνουν την ανάληψη υπερβολικών κινδύνων, όπως ορίζονται στην εσωτερική εταιρική πολιτική.

(3) Ο κώδικας επιχειρησιακής δεοντολογίας και εταιρικών αξιών θα πρέπει να περιλαμβάνει, μεταξύ άλλων, απαιτήσεις δέουσας επιμέλειας, αποτελεσματικότητας, υπευθυνότητας, δέουσας σχέσης με το κοινό, τη μη απαίτηση ή αποδοχή ωφελημάτων τα οποία δεν έχουν συμβολική αξία και την εφαρμογή του επαγγελματικού απορρήτου.

Οι υπηρεσίες που προσφέρονται στους πελάτες.

54. Τα ιδρύματα θεσπίζουν κατάλληλες πολιτικές, πρακτικές και διαδικασίες για τη δίκαιη, έντιμη και επαγγελματική μεταχείριση των πελατών· στο πλαίσιο αυτό, τα θεσμικά όργανα πρέπει, κατ' ελάχιστο, να προβαίνουν σε:

(α) υιοθέτηση των βέλτιστων πρακτικών στην προσφορά υπηρεσιών και προϊόντων που είναι τα καταλληλότερα για τους πελάτες·

(β) παρακολούθηση και αξιολόγηση του τρόπου εξυπηρέτησης των πελατών και, ειδικότερα, των συμβατικών όρων, οι οποίοι πρέπει να είναι σύμφωνοι με τις διατάξεις των νόμων για την προστασία των καταναλωτών που ισχύουν από καιρό σε καιρό·

(γ) θέσπιση και λειτουργία κατάλληλης διαδικασίας για υποβολή παραπόνων για χρήση από τους πελάτες·

(δ) διασφάλιση των συμφερόντων των πελατών, προσφέροντας προστασία από την κατάχρηση των προσωπικών τους δεδομένων, σύμφωνα με τις διατάξεις του περί Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμου του 2001.

Σύγκρουση συμφερόντων και διαχωρισμός καθηκόντων.

55. (1) Τα ιδρύματα θεσπίζουν, εφαρμόζουν και διατηρούν αποτελεσματικές πολιτικές σύγκρουσης συμφερόντων για τον εντοπισμό, την πρόληψη και τη διαχείριση των συγκρούσεων συμφερόντων.

(2) Οι πολιτικές σύγκρουσης συμφερόντων πρέπει να προσδιορίζουν τις σχέσεις, υπηρεσίες, δραστηριότητες ή πράξεις στις οποίες μπορεί να προκύψουν συγκρούσεις συμφερόντων· οι πολιτικές αυτές θα πρέπει να καλύπτουν τις σχέσεις –

(α) μεταξύ του ιδρύματος και των ενδιαφερόμενων μερών, συμπεριλαμβανομένων:

(i) των πελατών του·

(ii) των μετόχων του·

(iii) των μελών του διοικητικού οργάνου·

(iv) του προσωπικού·

(v) σημαντικών προμηθευτών ή επιχειρηματικών εταίρων· και

(vi) άλλων συνδεδεμένων μερών, όπως η μητρική εταιρεία ή οι θυγατρικές του ιδρύματος· και

(β) μεταξύ διαφόρων πελατών του ιδρύματος.

(3) Οι πολιτικές σύγκρουσης συμφερόντων καθορίζουν τα μέτρα που πρέπει να υιοθετούνται για την πρόληψη ή τη διαχείριση των συγκρούσεων συμφερόντων· τέτοιες διαδικασίες και μέτρα πρέπει να περιλαμβάνουν:

(α) επαρκή διαχωρισμό καθηκόντων, αναθέτοντας συγκρουόμενες δραστηριότητες κατά μήκος της αλυσίδας συναλλαγών ή υπηρεσιών σε διαφορετικά πρόσωπα ή αναθέτοντας εποπτικές αρμοδιότητες και αρμοδιότητες αναφοράς επί συγκρουόμενων δραστηριοτήτων σε διαφορετικά πρόσωπα·

(β) την επιβολή φραγμών στην ενημέρωση όπως ο φυσικός διαχωρισμός ορισμένων τμημάτων·

(γ) την παρεμπόδιση ατόμων που δραστηριοποιούνται και εκτός του ιδρύματος από το να αποκτούν ανάρμοστη επιρροή εντός του ιδρύματος σχετικά με συγκρουόμενες δραστηριότητες·

(δ) στην περίπτωση όπου το ίδρυμα είναι μητρική εταιρεία, την εξισορρόπηση των συμφερόντων όλων των θυγατρικών του, λαμβάνοντας υπόψη το πώς τα συμφέροντα αυτά συμβάλλουν μακροπρόθεσμα στο κοινό σκοπό και συμφέροντα του ομίλου ως σύνολο.

(4) Οι συγκρούσεις συμφερόντων που έχουν γνωστοποιηθεί και έχουν εγκριθεί από το διοικητικό όργανο πρέπει να τυγχάνουν της δέουσας διαχείρισης.

Μη τυποποιημένες ή μη διαφανείς δραστηριότητες.

56. Τα Ιδρύματα οφείλουν να θεσπίζουν και να εφαρμόζουν αποτελεσματικές πολιτικές και διαδικασίες σύμφωνα με την παράγραφο 73 για -

(α) την έγκριση και λειτουργία μέσω δομών ειδικού σκοπού ή σχετιζόμενες με ή σε δικαιοδοσίες που εμποδίζουν τη διαφάνεια ή δεν πληρούν τα διεθνή τραπεζικά πρότυπα·

(β) την έγκριση και την εκτέλεση των μη τυποποιημένων ή μη διαφανών δραστηριοτήτων για τους πελάτες.

Διαδικασίες προειδοποίησης.

57. (1) Τα ιδρύματα υιοθετούν κατάλληλες διαδικασίες έγκαιρης προειδοποίησης, προκειμένου οι εργαζόμενοι να κοινοποιούν εσωτερικά μέσω ενός ειδικού, ανεξάρτητου και αυτόνομου δίαυλου αναφοράς, ή να γνωστοποιούν στην Κεντρική Τράπεζα -

(α) πιθανές ή πραγματικές παραβάσεις –

(i) των νόμων ή κανονισμών·

(ii) των εσωτερικών πολιτικών, προτύπων και διαδικασιών·

(β) προβληματισμούς ή/και ανησυχίες για ανήθικες και αμφισβητήσιμες πρακτικές,

(γ) σοβαρές παρατυπίες και παραλείψεις·

(2) Οι διαδικασίες που αναφέρονται στην υποπαράγραφο (1) περιλαμβάνουν τουλάχιστον:

(α) κατάλληλη προστασία των εργαζομένων που αναφέρουν παραβιάσεις λόγω αντίποινων, διακρίσεων ή άλλων ειδών άδικης μεταχείρισης·

(β) προστασία προσωπικών δεδομένων που αφορούν τόσο τον εργαζόμενο ο οποίος αναφέρει παραβάσεις ή/και εγείρει ανησυχίες όσο και το πρόσωπο που φέρεται ως υπεύθυνος για διάπραξη παραβάσεως, σύμφωνα με τις διατάξεις του περί Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμου του 2001·

(γ) σαφείς κανόνες που διασφαλίζουν σε κάθε περίπτωση το απόρρητο των εργαζομένων που αναφέρουν παραβιάσεις ή/και εγείρουν ανησυχίες, παρέχοντας την ευκαιρία σε εργαζόμενο να εγείρει τις ανησυχίες αυτές εκτός των συνήθων δίαυλων αναφοράς·

(δ) τη δυνατότητα να εγείρουν οι εργαζόμενοι τις ανησυχίες ή/και τους ανώνυμα·

(ε) αυτόνομο δίαυλο γνωστοποίησης σημαντικών παραβιάσεων ή προβληματισμών απευθείας στο διοικητικό όργανο, ή στην Κεντρική Τράπεζα.

ΜΕΡΟΣ VIII
ΡΥΘΜΙΣΕΙΣ ΚΑΝΟΝΙΣΤΙΚΗΣ ΣΥΜΜΟΡΦΩΣΗΣ

Κουλτούρα κανονιστικής συμμόρφωσης.

58. (1) Τα ιδρύματα αναπτύσσουν μια ολοκληρωμένη κουλτούρα κανονιστικής συμμόρφωσης, -

(α) η οποία βασίζεται –

(i) στην πλήρη κατανόηση των κανονισμών, εθνικών και διεθνών προτύπων και βέλτιστων πρακτικών που τους αφορούν· και

(ii) στους κινδύνους συμμόρφωσης που αντιμετωπίζουν και τον τρόπο διαχείρισης των κινδύνων αυτών· και

(β) είναι σύμφωνη με τον κώδικα επιχειρηματικής δεοντολογίας και τις εταιρικές αξίες τους· τα ιδρύματα αναπτύσσουν την κουλτούρα κανονιστικής συμμόρφωσης τους μέσω πολιτικών, παραδειγμάτων επικοινωνίας, και εκπαίδευσης του προσωπικού σχετικά με τις ευθύνες τους για κανονιστική συμμόρφωση.

(2) Τα ιδρύματα διασφαλίζουν ότι η κουλτούρα κανονιστικής συμμόρφωσης διαχέεται σε όλα τα επίπεδα ιεραρχίας, με στόχο την ευαισθητοποίηση και τη διασφάλιση ότι κάθε μέλος του προσωπικού –

(α) κατανοεί τους κανονισμούς, τα πρότυπα και τις βέλτιστες πρακτικές που συνδέονται με την εκπλήρωση των επιχειρησιακών ή εποπτικών καθηκόντων του·

(β) κατανοεί τους συναφείς κινδύνους κανονιστικής συμμόρφωσης και την ανάγκη και ευθύνη του για τη διαχείριση των κινδύνων αυτών · και

(γ) κατανοεί τη σημασία των τμημάτων ελέγχου στη διαχείριση των κινδύνων κανονιστικής συμμόρφωσης και διευκολύνει τις εργασίες τους.

Απαιτήσεις για τη δημιουργία πλαισίου κανονιστικής συμμόρφωσης.

59. (1) Τα ιδρύματα σχεδιάζουν, αναπτύσσουν και εφαρμόζουν ένα ολοκληρωμένο, πλαίσιο κανονιστικής συμμόρφωσης το οποίο βασίζεται στην πολιτική κανονιστικής συμμόρφωσης και υποστηρίζεται από σχεδιασμούς, διαδικασίες και διασφαλίσεις κανονιστικής συμμόρφωσης.

(2) Τα ιδρύματα διασφαλίζουν ότι το πλαίσιο κανονιστικής συμμόρφωσής τους περιλαμβάνει τουλάχιστον τις ακόλουθες πτυχές:

(α) πολιτική κανονιστικής συμμόρφωσης ή οποία προσδιορίζει το επιχειρηματικό και νομικό περιβάλλον που ισχύει για το ίδρυμα και καθορίζει τους στόχους, τις αρχές και την κατανομή ευθυνών κανονιστικής συμμόρφωσης· σε περίπτωση ομίλου, η πολιτική κανονιστικής συμμόρφωσης αναφέρει τον τρόπο που οι ευθύνες συμμόρφωσης κατανέμονται και διεκπεραιώνεται σε επίπεδο ομίλου και επίπεδο ιδρύματος·

(β) μέθοδοι και διαδικασίες για τη δημιουργία και τη διατήρηση ενός ενημερωμένου μητρώου εσωτερικών, ρυθμιστικών και επιχειρησιακών απαιτήσεων, τις υποχρεώσεις που επιβάλλει κάθε σύνολο απαιτήσεων και τους συνδέσμους προς τις πολιτικές και τις διαδικασίες που έχουν αναπτυχθεί από το ίδρυμα για την εκπλήρωση των υποχρεώσεων αυτών·

(γ) μέθοδοι και διαδικασίες για τον εντοπισμό, αξιολόγηση, διαχείριση και παρακολούθηση των κινδύνων μη συμμόρφωσης με τις σχετικές υποχρεώσεις·

(δ) μηχανισμός για την υποβολή αναφορών και το χειρισμό παραβάσεων και περιστατικών·

(ε) υπεύθυνο προσωπικό για το συντονισμό και την παρακολούθηση της συμμόρφωσης με τις σχετικές υποχρεώσεις·

(στ) καθοδήγηση, υποστήριξη, και κατάρτιση για υποβοήθηση του προσωπικού στην εκπλήρωση των υποχρεώσεών του.

(3) Τα ιδρύματα διασφαλίζουν ότι η διαδικασία προσδιορισμού των απαιτήσεων συμμόρφωσης καλύπτει τους ακόλουθους τομείς κανονιστικών, επιχειρηματικών και εσωτερικών απαιτήσεων:

(α) τον κώδικα επιχειρησιακής δεοντολογίας του ιδρύματος και των εταιρικών αξιών·

(β) τους νόμους και κανονισμούς προληπτικής εποπτείας·

(γ) τις ρυθμίσεις παρεμπόδισης της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και χρηματοδότησης της τρομοκρατίας·

(δ) τις ρυθμίσεις που αφορούν την παροχή επενδυτικών υπηρεσιών και δραστηριοτήτων·

(ε) τους φορολογικούς νόμους που αφορούν τη δομή τραπεζικών προϊόντων ή παροχή συμβουλών στους πελάτες·

(στ) άλλους κανονισμούς που εφαρμόζονται στα ιδρύματα όπως οι κανονισμοί σχετικά με τα δικαιώματα των καταναλωτών, την προστασία των δεδομένων και τον ανταγωνισμό·

(ζ) απαιτήσεις λογιστικής και ελέγχου·

(η) επιχειρηματικά πρότυπα και βέλτιστες πρακτικές όπως –

(i) τη συμπεριφορά στην αγορά·

(ii) τη διαχείριση συγκρούσεων συμφερόντων·

(iii) τη δίκαιη αντιμετώπιση των πελατών και τη διασφάλιση της καταλληλότητας των συμβουλών που παρέχονται προς τους πελάτες·

(iv) την τεχνολογία πληροφοριών και ηλεκτρονική τραπεζική.

(4) Τα ιδρύματα διασφαλίζουν ότι οι διεργασίες και διαδικασίες τους για παρακολούθηση της κανονιστικής συμμόρφωσης υποβάλλονται τακτικά προς το προσωπικό που διορίζεται ως λειτουργοί κανονιστικής συμμόρφωσης σε μεγάλες επιχειρηματικές μονάδες, υποκαταστήματα και θυγατρικές στη Δημοκρατία και το εξωτερικό για την εκτέλεση καθηκόντων κανονιστικής συμμόρφωσης, ώστε να βοηθείται το εν λόγω προσωπικό στην εκτέλεση των καθηκόντων του που αφορά το τμήμα της κανονιστικής συμμόρφωσης.

ΜΕΡΟΣ IX
ΠΛΑΙΣΙΟ ΓΙΑ ΤΗΝ ΑΝΤΙΜΕΤΩΠΙΣΗ ΤΩΝ ΚΙΝΔΥΝΩΝ

Τμήμα 1 –Κουλτούρα διαχείρισης κινδύνων και διάθεση ανάληψης κινδύνων

Κουλτούρα διαχείρισης κινδύνων.

60. (1) Τα ιδρύματα αναπτύσσουν ολοκληρωμένη κουλτούρα διαχείρισης κινδύνου, που βασίζεται στην πλήρη κατανόηση των κινδύνων που αντιμετωπίζουν και τον τρόπο διαχείρισής τους, σύμφωνα με τη διάθεση ανάληψης κινδύνων τους· τα ιδρύματα αναπτύσσουν την κουλτούρα διαχείρισης κινδύνων τους μέσω πολιτικών, παραδειγμάτων, επικοινωνία και εκπαίδευση του προσωπικού σχετικά με τις ευθύνες του προς τον κίνδυνο.

(2) Τα ιδρύματα διασφαλίζουν ότι η κουλτούρα διαχείρισης κινδύνων διαχέεται σε όλα τα επίπεδα ιεραρχίας, με στόχο την ευαισθητοποίηση και τη διασφάλιση ότι κάθε μέλος του προσωπικού –

(α) κατανοεί τη φύση κάθε κινδύνου που σχετίζεται με την εκπλήρωση των επιχειρησιακών ή εποπτικών καθηκόντων του και την ανάγκη και ευθύνη για τη διαχείριση των κινδύνων αυτών· και

(β) κατανοεί τη σημασία των τμημάτων ελέγχου στη διαχείριση κινδύνων και διευκολύνει την εφαρμογή των λειτουργιών τους.

Πλαίσιο διάθεσης ανάληψης κινδύνων.

61. (1) Τα ιδρύματα διασφαλίζουν ότι διαθέτουν ένα αποτελεσματικό πλαίσιο διάθεσης ανάληψης κινδύνων μέσω κατάλληλων πολιτικών, διαδικασιών, ελέγχων, συστημάτων για την επικοινωνία μεταξύ των ανώτατων διοικητικών στελεχών και του διοικητικού οργάνου, κατανοούν και αξιολογούν το συνολικό επίπεδο κινδύνου και τους τύπους των κινδύνων τους οποίους το ίδρυμα είναι διατεθειμένο να αναλάβει στα πλαίσια των δυνατοτήτων του για ανάληψη κινδύνων ούτως ώστε να επιτύχει τους στρατηγικούς του στόχους και το επιχειρηματικό του σχέδιο.

(2) Ένα αποτελεσματικό πλαίσιο διάθεσης ανάληψης κινδύνων απαιτεί κατ' ελάχιστο:

(α) αξιολόγηση της δυνατότητας ανάληψης κινδύνων του ιδρύματος·

(β) καθορισμό της διάθεσης ανάληψης κινδύνων του ιδρύματος, μέσω της διατύπωσης σε γραπτή μορφή δήλωσης της διάθεσης για ανάληψη κινδύνων·

(γ) εξαγωγή της δήλωσης της διάθεσης για ανάληψη κινδύνων του ιδρύματος στους επιχειρηματικούς τομείς, επιχειρηματικές μονάδες, σε συγκεκριμένες κατηγορίες κινδύνων, συγκεντρώσεις και άλλα σχετικά επίπεδα υπό τη μορφή ορίων κινδύνου·

(δ) αξιολόγηση του προφίλ κινδύνου του ιδρύματος σε σχέση με τη διάθεσή του για ανάληψη κινδύνων·

(ε) περιγραφή των ρόλων και ευθυνών του προσωπικού που επιβλέπει την εφαρμογή και παρακολούθηση του πλαισίου διάθεσης για ανάληψη κινδύνων

(3) Τα ιδρύματα διασφαλίζουν ότι η δήλωση της διάθεσης ανάληψης κινδύνων:

(α) συνδέεται με το στρατηγικό σχεδιασμό και το σχεδιασμό άντλησης κεφαλαίων και ρευστότητας, καθώς και με τα προγράμματα αποδοχών·

(β) καθορίζει το ύψος του κινδύνου τον οποίο το ίδρυμα είναι διατεθειμένο να αποδεχτεί για την επίτευξη των στρατηγικών του στόχων και του επιχειρηματικού του σχεδίου, λαμβάνοντας υπόψη τα συμφέροντα των ενδιαφερομένων μερών, καθώς και τις κεφαλαιακές και άλλες ρυθμιστικές απαιτήσεις·

(γ) καθορίζει για κάθε σημαντική δραστηριότητα το ανώτατο επίπεδο κινδύνου μέσα στο οποίο το ίδρυμα είναι διατεθειμένο να λειτουργήσει, βάσει της διάθεσής του για ανάληψη κινδύνων, δυνατότητας ανάληψης κινδύνου και του προφίλ κινδύνου·

(δ) περιλαμβάνει ποσοτικές μετρήσεις οι οποίες μπορούν να μεταφραστούν σε όρια κινδύνου που ισχύουν για επιχειρησιακούς τομείς και μονάδες τα οποία με τη σειρά τους μπορούν να συγκεντρώνονται και να αποσυγκεντρώνονται έτσι ώστε να επιτρέπουν τη μέτρηση του προφίλ κινδύνου σε σχέση με τη διάθεση του για ανάληψη κινδύνων και τη δυνατότητα ανάληψης κινδύνου·

(ε) περιλαμβάνει ποιοτικές δηλώσεις για κινδύνους που δεν είναι εύκολο να μετρηθούν, συμπεριλαμβανομένων των κινδύνων φήμης και οικονομικών συνεπειών από τη πλημμελή διαχείριση των κινδύνων δραστηριοποίησης στις αγορές λιανικής και χονδρικής τραπεζικής, και του καθορισμού κάποιας μορφή ορίων ή δεικτών που να επιτρέπουν την παρακολούθηση των κινδύνων αυτών·

(στ) διασφαλίζει ότι η στρατηγική και τα όρια κινδύνου για κάθε επιχειρηματικό τομέα του ιδρύματος και νομική οντότητα ευθυγραμμίζονται με τη δήλωση της διάθεσης για ανάληψη κινδύνων από το ίδρυμα ανάλογα με την περίπτωση· και

(ζ) είναι προσανατολισμένη στο μέλλον και υπόκειται σε σενάρια και δοκιμές προσομοίωσης ακραίων καταστάσεων για να διασφαλίζεται ότι το ίδρυμα αντιλαμβάνεται το είδος των περιστατικών που θα μπορούσαν να το θέσουν εκτός της διάθεσής του για ανάληψη κινδύνων και της δυνατότητάς του για ανάληψη κινδύνων.

(4) Τα ιδρύματα διασφαλίζουν ότι τα όρια κινδύνου:

(α) καθορίζονται σε επίπεδο που περιορίζει την ανάληψη κινδύνων εντός της διάθεσης ανάληψης κινδύνου στη βάση εκτίμησης των επιπτώσεων στα συμφέροντα των ενδιαφερόμενων μερών, καθώς επίσης και στη συμμόρφωση με τις κεφαλαιακές και λοιπές κανονιστικές απαιτήσεις, σε περίπτωση παραβίασης ορίου κινδύνου και της πιθανότητας πραγματοποίησης κάθε σημαντικού κινδύνου·

(β) καλύπτουν συγκεντρώσεις σημαντικών κινδύνων και όλων των επιχειρηματικών τομέων και μονάδων του ιδρύματος, όπως κίνδυνος αντισυμβαλλομένου, κλάδου, περιφέρειας, τύπου εξασφάλισης, συναλλάγματος και προϊόντος·

(γ) παρακολουθούνται τακτικά.

(5) Τα ιδρύματα διασφαλίζουν ότι διαθέτουν τους απαραίτητους μηχανισμούς για την προσαρμογή του πλαισίου διάθεσης ανάληψης κινδύνων στις μεταβαλλόμενες επιχειρηματικές συνθήκες και συνθήκες της αγοράς.

(6) Τα ιδρύματα διασφαλίζουν ότι οι παραβιάσεις των ορίων κινδύνου παραπέμπονται στο αρμόδιο επίπεδο αναφοράς και αντιμετωπίζονται με τη δέουσα παρακολούθηση.

Τμήμα 2 – Πλαίσιο διαχείρισης κινδύνων

Υποτμήμα 2.1 – Γενικές απαιτήσεις

Γενικές απαιτήσεις για τη διαχείριση κινδύνων.

62. (1) Τα ιδρύματα διασφαλίσουν ότι διαθέτουν ένα κατάλληλο και ολιστικό πλαίσιο διαχείρισης κινδύνων που να τους επιτρέπει να λαμβάνουν αποφάσεις έχοντας επίγνωση των συνεπαγόμενων κινδύνων και το οποίο –

(α) επεκτείνεται σε όλες τις επιχειρηματικές δραστηριότητες, τις λειτουργίες στήριξης και τμήματα ελέγχου,

(β) αναγνωρίζει πλήρως την οικονομική υπόσταση των ανοιγμάτων κινδύνου τους, και

(γ) καλύπτει όλους τους σχετικούς κινδύνους, χρηματοοικονομικούς και μη χρηματοοικονομικούς, εντός και εκτός ισολογισμού, και είτε προκύπτουν από σύμβαση είτε όχι.

(2) Το πλαίσιο διαχείρισης κινδύνων διασφαλίζει ότι όλοι οι σημαντικοί κίνδυνοι αναγνωρίζονται και τυγχάνουν διαχείρισης, περιλαμβανομένων των κινδύνων που αναφέρονται στις παραγράφους 63 μέχρι 71· τα ιδρύματα διασφαλίζουν ότι διαθέτουν τις κατάλληλες, επαρκείς και αποτελεσματικές πολιτικές, συστήματα, διεργασίες και διαδικασίες για:

(α) τον εντοπισμό όλων των σχετικών κινδύνων του ιδρύματος, σε συνεχή βάση, υφιστάμενων και αναδυόμενων, σε επίπεδο συναλλαγών και χαρτοφυλακίου·

(β) την αξιολόγηση των κινδύνων αυτών και μέτρηση των ανοιγμάτων του ιδρύματος σε αυτά, σε επίπεδο συναλλαγών και χαρτοφυλακίου, σε ατομική βάση και ενοποιημένη βάση, αναγνωρίζοντας τις αλληλεπιδράσεις μεταξύ των κινδύνων αυτών, έγκαιρα και με ακρίβεια·

(γ) την παρακολούθηση των κινδύνων των ανοιγμάτων και τον προσδιορισμό των αντίστοιχων αναγκών για κεφάλαια σε συνεχή βάση·

(δ) την παρακολούθηση και αξιολόγηση των αποφάσεων για αποδοχή συγκεκριμένων κινδύνων, μέτρων μετριασμού των κινδύνων και κατά πόσο οι αποφάσεις που αφορούν τους κινδύνους είναι σύμφωνες με τη διάθεση ανάληψης κινδύνων και των ορίων κινδύνου·

(ε) την υποβολή αναφορών προς τα ανώτατα διοικητικά στελέχη και το διοικητικό όργανο ανάλογα με την περίπτωση, για όλα τα προαναφερθέντα·

(στ) την τήρηση των κατάλληλων αρχείων.

(3) Τα ιδρύματα διασφαλίζουν ότι κάθε σημαντικός κίνδυνος συνδέεται με μία πολιτική, διαδικασία ή μέτρο, καθώς και σχετικό έλεγχο που να διασφαλίζει ότι κάθε τέτοια πολιτική, διαδικασία ή άλλο μέτρο εφαρμόζεται και λειτουργεί όπως προβλέπεται.

(4) Η αξιολόγηση των κινδύνων δεν πρέπει να στηρίζεται αποκλειστικά ή μηχανιστικά σε εξωτερικές αξιολογήσεις, όπως οι εξωτερικές διαβαθμίσεις πιστοληπτικής ικανότητας ή τα μοντέλα κινδύνου που αγοράζονται από τρίτους, αλλά τα ιδρύματα επιδιώκουν να αναπτύσσουν εσωτερική ικανότητα αξιολόγησης ανάλογη με το μέγεθος, τη φύση και την κλίμακα των δραστηριοτήτων τους· τα ιδρύματα διασφαλίζουν ότι τα μοντέλα κινδύνου που αγοράζονται από τρίτους επικυρώνονται και προσαρμόζονται στις συνθήκες του ιδρύματος για να διασφαλιστεί η ακριβής και πλήρης κάλυψη και ανάλυση του προφίλ κινδύνου και της δυνατότητας ανάληψης κινδύνου του ιδρύματος.

(5) Οι κίνδυνοι αξιολογούνται από τη βάση προς την κορυφή και από την κορυφή προς τη βάση, σε

επίπεδο ιδρύματος, επιχειρηματικής δραστηριότητας και επιχειρησιακών μονάδων, χρησιμοποιώντας συνεπή ορολογία και συμβατές τόσο σε επίπεδο ιδρύματος όσο και ομίλου, μεθοδολογίες.

(6) Τα ιδρύματα χρησιμοποιούν εργαλεία ανάλυσης μελλοντικών εξελίξεων, όπως είναι η ανάλυση σεναρίων και οι προσομοιώσεις ακραίων καταστάσεων, ως μέρος των διαδικασιών αναγνώρισης και μέτρησης των κινδύνων προκειμένου να προσδιοριστούν ενδεχόμενα ανοίγματα κινδύνου σε μια σειρά δυσμενών συνθηκών· για τους σκοπούς της παρούσας υποπαραγράφου, τα ιδρύματα οφείλουν να:

(α) αναγνωρίζουν μία σειρά δυσμενών συνθηκών ποικίλης φύσης, σοβαρότητας και διάρκειας σχετικών με τις δραστηριότητες και το προφίλ κινδύνου τους και εξετάζουν τα ανοίγματά τους σε αυτές τις συνθήκες, συμπεριλαμβανομένων:

(i) συνθηκών και γεγονότων που συμβαίνουν κατά τη διάρκεια μιας παρατεταμένης χρονικής περιόδου·

(ii) ξαφνικών και σοβαρών γεγονότων, όπως οι κρίσεις της αγοράς ή άλλα παρόμοια γεγονότα· και

(iii) συνδυασμού των συνθηκών και γεγονότων που περιγράφονται στο (i), και (ii), τα οποία μπορεί να περιλαμβάνουν κάποιο αιφνίδιο και σοβαρό περιστατικό της αγοράς ως επακόλουθο της οικονομικής ύφεσης·

(β) αξιολογούν τους χρηματοοικονομικούς πόρους που θα χρειαστούν, προκειμένου να συνεχίσουν να τηρούν τις κεφαλαιακές απαιτήσεις που καθορίζονται στον Κανονισμό (ΕΕ) 575/2013 υπό δυσμενείς συνθήκες·

(γ) αξιολογούν το πώς οι κίνδυνοι, σε ενοποιημένη βάση, που αφορούν στους επιχειρησιακούς τομείς ή μονάδες, ή οποιουσδήποτε σημαντικούς έκτακτους ή ενδεχόμενους κινδύνους και πώς οι συσχετισμοί των εν λόω κινδύνων μπορεί να αυξηθούν σε ακραίες συνθήκες·

(δ) τεκμηριώνουν και εξετάζουν τις υποθέσεις και τους περιορισμούς των εργαλείων ανάλυσης μελλοντικών κινδύνων.

(7) Το πλαίσιο διαχείρισης κινδύνων διασφαλίζει ότι οι αποφάσεις που καθορίζουν το επίπεδο κινδύνου που αναλαμβάνει το ίδρυμα δεν βασίζονται αποκλειστικά σε ποσοτικές πληροφορίες ή αποτελέσματα που λαμβάνονται από τη χρήση μοντέλων, αλλά λαμβάνονται υπόψη πρακτικοί και υποθετικοί περιορισμοί των κριτηρίων και μοντέλων χρησιμοποιώντας μια ποιοτική προσέγγιση, όπως η γνώμη των εμπειρογνωμόνων και η κριτική ανάλυση· τα ιδρύματα διασφαλίζουν ότι η αξιολόγηση των επιπτώσεων των τάσεων του σχετικού μακροοικονομικού περιβάλλοντος και των δεδομένων που αφορά τα ανοίγματα και τα χαρτοφυλάκια ενσωματώνονται επισήμως στις σημαντικές αποφάσεις κινδύνου.

(8) Τα ιδρύματα διασφαλίζουν ότι χρησιμοποιούνται εργαλεία που βασίζονται σε παρελθοντικές πληροφορίες για την εξέταση του πραγματικού τους προφίλ κινδύνου, σε σχέση με τη διάθεση για ανάληψη κινδύνων και των ορίων κινδύνου του ιδρύματος και παρέχουν στοιχεία για οποιαδήποτε αναπροσαρμογή.

(9) Τα ιδρύματα θεσπίζουν δίαυλους αναφορών προς το διοικητικό όργανο που καλύπτουν όλους τους σημαντικούς κινδύνους και τις πολιτικές διαχείρισης κινδύνου και τις σχετικές μεταβολές τους.

(10) Τα ιδρύματα διασφαλίζουν την υιοθέτηση τακτικών και διαφανών μηχανισμών υποβολής αναφορών, έτσι ώστε το διοικητικό όργανο και όλα τα σχετικά τμήματα να –

(α) λαμβάνουν έγκαιρες, ακριβής, περιεκτικές, κατανοητές και ουσιαστικές αναφορές· και

(β) μπορούν να μοιραστούν τις σχετικές πληροφορίες για τον εντοπισμό, τη μέτρηση ή την αξιολόγηση και την παρακολούθηση κινδύνων.

(11) Τα ιδρύματα προβαίνουν σε έγγραφη καταχώριση σε ατομική και σε ενοποιημένη βάση των:

(α) κύριων πηγών κινδύνου που ενοπίζονται·

(β) αξιολογήσεων που διεξάγονται για τους κινδύνους αυτούς καθώς και λεπτομέρειες των προσομοιώσεων ακραίων καταστάσεων και ανάλυση σεναρίων που εκτελείται·

(γ) πώς σκοπεύουν να αντιμετωπίσουν τους κινδύνους αυτούς· και

(δ) τελικών χρηματοοικονομικών πόρων που εκτιμάται ότι θα χρειαστούν ως μέρος της εσωτερικής διαδικασίας κεφαλαιακής επάρκειας.

Υποτμήμα 2.2 – Αντιμετώπιση συγκεκριμένων κινδύνων

Πιστωτικός κίνδυνος και κίνδυνος αντισυμβαλλομένου

63. (1) Τα ιδρύματα θεσπίζουν υγιή και σαφώς καθορισμένα κριτήρια για τη χορήγηση πιστώσεων και καθορίζουν με σαφήνεια τη διαδικασία έγκρισης, τροποποίησης, ανανέωσης και αναχρηματοδότησης των πιστώσεων σύμφωνα με τις πρόνοιες της Οδηγίας περί των Διαδικασιών Χορήγησης Νέων Πιστωτικών Διευκολύνσεων και των Διαδικασιών Αναθεώρησης Υφιστάμενων Πιστωτικών Διευκολύνσεων του 2013 και της Οδηγίας για τη Διαχείριση των Καθυστερήσεων του 2013-2014.

(2) Τα ιδρύματα οφείλουν να έχουν εσωτερικές μεθοδολογίες που:

(α) να τους επιτρέπουν να αξιολογούν τον πιστωτικό κίνδυνο των ανοιγμάτων σε μεμονωμένους οφειλέτες, σε χρεόγραφα ή θέσεις τιτλοποίησης και του πιστωτικού κινδύνου σε επίπεδο χαρτοφυλακίου·

(β) δεν στηρίζονται αποκλειστικά ή μηχανιστικά σε εξωτερικές αξιολογήσεις πιστοληπτικής ικανότητας· και

(γ) όπου οι απαιτήσεις ιδίων κεφαλαίων βασίζονται σε διαβάθμιση από Εξωτερικό Οργανισμό Πιστοληπτικών Αξιολογήσεων (ΕΟΠΑ) ή στο γεγονός ότι ένα άνοιγμα είναι χωρίς διαβάθμιση, δεν απαλλάσσει τα ιδρύματα από την πρόσθετη εξέταση άλλων σχετικών πληροφοριών για την εκτίμηση της κατανομής των εσωτερικών κεφαλαίων.

(3) Τα ιδρύματα θεσπίσουν αποτελεσματικά συστήματα για τη διαρκής διαχείριση και παρακολούθηση των διαφόρων χαρτοφυλακίων και ανοιγμάτων που ενέχουν πιστωτικό κίνδυνο των ιδρυμάτων, συμπεριλαμβανομένων του εντοπισμού και της διαχείρισης προβληματικών πιστώσεων και της διενέργειας επαρκών προσαρμογών και προβλέψεων αξίας.

(4) Τα ιδρύματα θεσπίζουν κατάλληλα συστήματα για την αποτελεσματική διαχείριση των πιστωτικών διευκολύνσεων σε καθυστέρηση και τη διεξαγωγή των εφικτής και βιώσιμης αναδιάρθρωσης του χρέους, σύμφωνα με τις διατάξεις της Οδηγίας για τη Διαχείριση των Καθυστερήσεων του 2013-2014.

(5) Τα ιδρύματα διαφοροποιούν επαρκώς τα πιστωτικά χαρτοφυλάκια σύμφωνα με τις αγορές-στόχους και τη συνολική στρατηγική πιστώσεων του ιδρύματος.

Υπολειπόμενος κίνδυνος.

64. Τα Ιδρύματα αντιμετωπίζουν και ελέγχουν, μεταξύ άλλων και μέσω γραπτών πολιτικών και διαδικασιών, τον κίνδυνο οι αναγνωρισμένες τεχνικές μείωσης του πιστωτικού κινδύνου που χρησιμοποιούνται από αυτούς να αποδειχθούν λιγότερο αποτελεσματικές από ότι αναμενόταν.

Κίνδυνος συγκέντρωσης.

65. Τα Ιδρύματα αντιμετωπίζουν και ελέγχουν, μεταξύ άλλων και μέσω γραπτών πολιτικών και διαδικασιών, τον κίνδυνο συγκέντρωσης από:

(α) ανοίγματα έναντι κάθε αντισυμβαλλομένου περιλαμβανομένων και των κεντρικών αντισυμβαλλομένων, ομάδων συνδεδεμένων αντισυμβαλλομένων και αντισυμβαλλόμενων στον ίδιο οικονομικό τομέα ή γεωγραφική περιοχή, ή από την ίδια δραστηριότητα ή βασικό εμπόρευμα·

(β) την εφαρμογή τεχνικών μείωσης του πιστωτικού κινδύνου· και

(γ) τους κινδύνους που συνδέονται με μεγάλα έμμεσα πιστωτικά ανοίγματα, όπως ενός μόνο εκδότη εξασφαλίσεων.

Κίνδυνος τιτλοποίησης.

66. (1) Τα ιδρύματα αξιολογούν και αντιμετωπίζουν μέσω κατάλληλων πολιτικών και διαδικασιών, τους κινδύνους που προκύπτουν από συναλλαγές τιτλοποίησης στις οποίες το πιστωτικό ίδρυμα είναι επενδυτής, μεταβιβάζων ή χρηματοδότης, συμπεριλαμβανομένων των κινδύνων φήμης, όπως προκύπτουν σε σχέση με πολύπλοκες δομές ή προϊόντα, ώστε να διασφαλίζεται ότι η οικονομική σημασία της συναλλαγής λαμβάνεται πλήρως υπόψη στις αποφάσεις αξιολόγησης και διαχείρισης των κινδύνων.

(2) Ίδρυμα που είναι το μεταβιβάζον ίδρυμα ανακυκλούμενων συναλλαγών τιτλοποίησης με ρήτρα πρόωρης εξόφλησης πρέπει να διαθέτει σχεδιασμό σχετικά με τη ρευστότητα για την αντιμετώπιση των επιπτώσεων τόσο των προγραμματισμένων όσο και των πρόωρων εξοφλήσεων.

Κίνδυνος αγοράς.

67. (1) Τα ιδρύματα εφαρμόζουν πολιτικές και διαδικασίες για τον εντοπισμό, τη μέτρηση και τη διαχείριση όλων των σημαντικών πηγών και επιπτώσεων των κινδύνων της αγοράς, σύμφωνα με τις κατευθυντήριες γραμμές της Κεντρικής Τράπεζας για τη διαχείρισης του κινδύνου αγοράς.

(2) Τα ιδρύματα εφαρμόζουν πολιτικές και διαδικασίες, έτσι ώστε όταν η θέση πώλησης (short position) καθίσταται ληξιπρόθεσμη πριν από τη θέση αγοράς, λάβουν επίσης μέτρα έναντι του κινδύνου ανεπαρκούς ρευστότητας.

(3) Τα ιδρύματα εφαρμόζουν πολιτικές και διαδικασίες για να διασφαλίζεται ότι το εσωτερικό κεφάλαιο είναι επαρκές για σημαντικούς κινδύνους της αγοράς που δεν υπόκεινται σε απαιτήσεις ιδίων κεφαλαίων.

(4) Τα ιδρύματα που έχουν, κατά τον υπολογισμό των απαιτήσεων ιδίων κεφαλαίων για τον κίνδυνο θέσης, σύμφωνα με το Τρίτο Μέρος, Τίτλος IV Κεφάλαιο 2 του Κανονισμού (ΕΕ) αριθ. 575/2013, συμψηφίσει τις θέσεις που έχουν σε μία ή περισσότερες από τις μετοχές που συναποτελούν ένα δείκτη μετοχών με θέση ή θέσεις στο συμβόλαιο μελλοντικής εκπλήρωσης σε δείκτη μετοχών ή σε άλλο προϊόν συνδεδεμένο με δείκτη μετοχών, οφείλουν να διαθέτουν επαρκή εσωτερικά κεφάλαια για την κάλυψη του κινδύνου βάσης για ζημιά που προκαλείται από το ενδεχόμενο να μην ακολουθεί πλήρως η τιμή του συμβολαίου μελλοντικής εκπλήρωσης ή του άλλου προϊόντος τις τιμές των μετοχών που το συναποτελούν· τα ιδρύματα έχουν επίσης τέτοια επαρκή εσωτερικά κεφάλαια που όταν αυτά κατέχουν αντίθετες θέσεις σε συμβόλαιο μελλοντικής εκπλήρωσης σε δείκτη μετοχών των οποίων η λήξη προθεσμίας, η σύνθεση ή και τα δύο δεν είναι πανομοιότυπες.

(5) Τα ιδρύματα διασφαλίζουν ότι, όταν χρησιμοποιούν τη μεταχείριση του άρθρου 345 του Κανονισμού (ΕΕ) αριθ. 575/2013, διαθέτουν επαρκή εσωτερικά κεφάλαια για την κάλυψη του κινδύνου ζημίας που υφίσταται μεταξύ του χρόνου της αρχικής δέσμευσης και της επόμενης εργάσιμης ημέρας.

Κίνδυνος επιτοκίου από δραστηριότητες εκτός χαρτοφυλακίου.

68. Τα ιδρύματα εφαρμόζουν συστήματα για τον εντοπισμό, την αξιολόγηση και τη διαχείριση του κινδύνου από δυνητικές μεταβολές επιτοκίων κατά το μέτρο που επηρεάζουν τις δραστηριότητες του ιδρύματος που δεν σχετίζονται με το χαρτοφυλάκιο συναλλαγών.

Κίνδυνος υπερβολικής μόχλευσης.

69. (1) Τα ιδρύματα θεσπίζουν πολιτικές και διαδικασίες για τον προσδιορισμό, τη διαχείριση και την παρακολούθηση του κινδύνου υπερβολικής μόχλευσης· οι δείκτες κινδύνου υπερβολικής μόχλευσης περιλαμβάνουν το δείκτη μόχλευσης που καθορίζεται σύμφωνα με το άρθρο 429 του Κανονισμού (ΕΕ) αριθ. 575/2013 και τις ασυμφωνίες μεταξύ του ενεργητικού και των υποχρεώσεων.

(2) Τα ιδρύματα αντιμετωπίζουν τον κίνδυνο υπερβολικής μόχλευσης με προνοητικό τρόπο λαμβάνοντας υπόψη τις δυνητικές αυξήσεις του κινδύνου υπερβολικής μόχλευσης λόγω μειώσεων των ιδίων κεφαλαίων του ιδρύματος συνεπεία αναμενόμενων ή πραγματοποιηθεισών ζημιών, ανάλογα με τους ισχύοντες λογιστικούς κανόνες· για αυτόν τον σκοπό, τα ιδρύματα πρέπει να είναι ικανά να αντέξουν σε μια σειρά διαφορετικών περιπτώσεων πίεσης όσον αφορά τον κίνδυνο υπερβολικής μόχλευσης.

Λειτουργικός κίνδυνος.

70.(1) Τα ιδρύματα εφαρμόζουν πολιτικές και διαδικασίες για την αξιολόγηση και τη διαχείριση της έκθεσης σε λειτουργικό κίνδυνο, περιλαμβανομένου του κινδύνου υποδείγματος, και την κάλυψη του κινδύνου που απορρέει από γεγονότα με χαμηλή συχνότητα και σοβαρές επιπτώσεις· τα ιδρύματα διατυπώνουν με σαφήνεια τι συνιστά λειτουργικό κίνδυνο για τους σκοπούς αυτών των πολιτικών και διαδικασιών.

(2) Τα ιδρύματα διασφαλίζουν ότι καταρτίζονται εναλλακτικά σχέδια αντιμετώπισης εκτάκτων περιστατικών και συνέχειας εργασιών για τη διασφάλιση, σε συνεχή βάση, της δυνατότητας λειτουργίας τους και τον περιορισμό των ζημιών σε περίπτωση σοβαρής διαταραχής των επιχειρησιακών λειτουργιών τους.

Κίνδυνος ρευστότητας.

71.(1) Τα ιδρύματα διαθέτουν άρτιες στρατηγικές, πολιτικές, διαδικασίες και συστήματα για τον εντοπισμό, τη μέτρηση, τη διαχείριση και την παρακολούθηση του κινδύνου ρευστότητας εντός κατάλληλου συνόλου χρονικών οριζόντων, μεταξύ άλλων εντός της ίδιας ημέρας, προκειμένου να εξασφαλιστεί ότι τα διατηρούνται επαρκή επίπεδα αποθεμάτων ρευστότητας· αυτές οι στρατηγικές, πολιτικές, διαδικασίες και συστήματα θα είναι σχεδιασμένα με βάση τους επιχειρηματικούς τομείς, τα νομίσματα, τους κλάδους και τις νομικές οντότητες και θα περιλαμβάνουν επαρκείς μηχανισμούς κατανομής κόστους ρευστότητας, ωφελειών και κινδύνων.

(2) Οι στρατηγικές, πολιτικές, διαδικασίες και τα συστήματα που αναφέρονται στην παράγραφο (1) είναι αναλογικά προς την πολυπλοκότητα, το προφίλ κινδύνου, το πεδίο λειτουργίας των ιδρυμάτων και το επίπεδο ανοχής κινδύνων που έχει οριστεί από το διοικητικό όργανο και απηχούν τη σημασία του ιδρύματος στη Δημοκρατία και σε κάθε άλλο Κράτος Μέλος στο οποίο δραστηριοποιείται επιχειρηματικά. Τα ιδρύματα κοινοποιούν την ανοχή κινδύνων σε όλους τους σχετικούς επιχειρηματικούς φορείς.

(3) Τα ιδρύματα, λαμβανομένων υπόψη της φύσης, της κλίμακας και της πολυπλοκότητας των δραστηριοτήτων τους, έχουν χαρακτηριστικά κινδύνου ρευστότητας που συνάδουν με, χωρίς να υπερβαίνουν, τα απαιτούμενα για ένα εύρυθμο και άρτιο σύστημα.

(4) Τα ιδρύματα αναπτύσσουν μεθόδους για τον προσδιορισμό, τη μέτρηση, τη διαχείριση και την παρακολούθηση χρηματοδοτικών θέσεων· αυτές οι μέθοδοι περιλαμβάνουν τωρινές και προβλεπόμενες σημαντικές χρηματορροές που προκύπτουν από στοιχεία του ενεργητικού, του παθητικού, στοιχεία εκτός ισολογισμού, συμπεριλαμβανομένων ενδεχόμενων υποχρεώσεων και πιθανών επιπτώσεων του κινδύνου φήμης.

(5) Τα ιδρύματα διακρίνουν μεταξύ δεσμευμένων και μη βεβαρημένων στοιχείων του ενεργητικού τα οποία είναι πάντοτε διαθέσιμα, ιδιαίτερα σε επείγουσες καταστάσεις· τα ιδρύματα λαμβάνουν υπόψη τη νομική οντότητα στην οποία ανήκουν τα στοιχεία του ενεργητικού, τη χώρα όπου τα στοιχεία είναι εγγεγραμμένα σε μητρώο ή σε λογαριασμό και την επιλεξιμότητα τους, και παρακολουθούν πώς μπορούν να κινητοποιούνται εγκαίρως τα στοιχεία του ενεργητικού.

(6) Τα ιδρύματα λαμβάνουν υπόψη τους υφιστάμενους νομικούς, κανονιστικούς και λειτουργικούς περιορισμούς σε ενδεχόμενες μεταφορές ρευστότητας και μη βεβαρημένων στοιχείων του ενεργητικού μεταξύ νομικών οντοτήτων, εντός και εκτός του Ευρωπαϊκού Οικονομικού Χώρου.

(7) Τα ιδρύματα εξετάζουν διάφορα μέσα μείωσης του κινδύνου ρευστότητας, συμπεριλαμβανομένου ενός συστήματος ορίων και αποθεμάτων ρευστότητας, προκειμένου να είναι σε θέση να αντέξουν ποικίλες περιπτώσεις πίεσης, καθώς και μίας επαρκώς διαφοροποιημένης χρηματοδοτικής διάρθρωσης και πρόσβασης σε πηγές χρηματοδότησης· τα ιδρύματα διασφαλίζουν ότι οι ρυθμίσεις αυτές επανεξετάζονται τακτικά.

(8) Τα ιδρύματα εξετάζουν εναλλακτικά σενάρια σχετικά με τις θέσεις ρευστότητας και τους παράγοντες μείωσης του κινδύνου και επανεξετάζουν τουλάχιστον ετησίως τις παραδοχές στις οποίες στηρίζονται οι αποφάσεις σχετικά με τη χρηματοδοτική θέση· για τους σκοπούς αυτούς, τα εναλλακτικά σενάρια αντιμετωπίζουν ιδιαίτερα τα στοιχεία εκτός ισολογισμού και άλλες ενδεχόμενες υποχρεώσεις, συμπεριλαμβανομένων εκείνων των οντοτήτων ειδικού σκοπού τιτλοποίησης (SSPE) ή άλλων οντοτήτων ειδικού σκοπού, όπως ορίζονται στον Κανονισμό (ΕΕ) αριθ. 575/2013, σε σχέση με τις οποίες το ίδρυμα ενεργεί ως ανάδοχος ή παρέχει σημαντική υποστήριξη ρευστότητας.

(9) Τα ιδρύματα εξετάζουν τις πιθανές επιπτώσεις συνδυασμένων εναλλακτικών σεναρίων ανάλογα με το ίδρυμα, σε όλο το εύρος της αγοράς και με συνδυασμένα εναλλακτικά σενάρια· εξετάζονται διαφορετικές χρονικές περίοδοι και διάφοροι βαθμοί συνθηκών πίεσης.

(10) Τα ιδρύματα προσαρμόζουν τις στρατηγικές, τις εσωτερικές πολιτικές και τα όρια κινδύνου ρευστότητας και αναπτύσσουν αποτελεσματικά σχέδια έκτακτης ανάγκης, λαμβάνοντας υπόψη το αποτέλεσμα των εναλλακτικών σεναρίων που αναφέρονται στην παράγραφο 8.

(11) Τα ιδρύματα θεσπίζουν σχέδια ανάκτησης ρευστότητας, τα οποία καθορίζουν επαρκείς

στρατηγικές και κατάλληλα μέτρα εφαρμογής προκειμένου να αντιμετωπίσουν πιθανά ελλείμματα ρευστότητας, συμπεριλαμβανομένων ελλειμμάτων που αφορούν υποκαταστήματα σε άλλα κράτη μέλη· τα σχέδια ελέγχονται από τα ιδρύματα τουλάχιστον ετησίως, ενημερώνονται βάσει του αποτελέσματος των εναλλακτικών σεναρίων που ορίζονται στην παράγραφο 8, υποβάλλονται με τη μορφή έκθεσης στα ανώτατα διοικητικά στελέχη και λαμβάνουν την έγκρισή τους, ώστε οι εσωτερικές πολιτικές και διαδικασίες να μπορούν να προσαρμοστούν ανάλογα· τα ιδρύματα προβαίνουν στις απαραίτητες λειτουργικές ενέργειες εκ των προτέρων για να διασφαλίσουν ότι τα σχέδια ανάκτησης ρευστότητας μπορούν να υλοποιηθούν άμεσα.

(12) Οι λειτουργικές ενέργειες που αναφέρονται στην υποπαράγραφο (11) περιλαμβάνουν την τήρηση ενεχύρων που είναι άμεσα διαθέσιμα για τη χρηματοδότηση της κεντρικής τράπεζας· αυτό περιλαμβάνει την τήρηση ενεχύρων, όπου απαιτείται, στο νόμισμα άλλου κράτους μέλους ή στο νόμισμα τρίτης χώρας στην οποία είναι εκτεθειμένα τα πιστωτικά ιδρύματα και, όπου απαιτείται για λειτουργικούς λόγους, εντός της επικράτειας ενός κράτους μέλους υποδοχής ή τρίτης χώρας στο νόμισμα της οποίας είναι εκτεθειμένα.

Υποτμήμα 2.3 – Νέα προϊόντα και αγορές και μη τυποποιημένες ή μη διαφανείς δραστηριότητες

Νέα προϊόντα και αγορές.

72. (1) Τα ιδρύματα διαθέτουν μία καλά τεκμηριωμένη πολιτική έγκρισης νέων προϊόντων, που εγκρίνεται από το διοικητικό όργανο, η οποία αφορά την ανάπτυξη νέων αγορών, προϊόντων και υπηρεσιών και σημαντικές αλλαγές στις υπάρχουσες αγορές, προϊόντα και υπηρεσίες.

(2) Η πολιτική έγκρισης νέων προϊόντων των ιδρυμάτων καλύπτει όλες τις παραμέτρους που πρέπει να λαμβάνονται υπόψη πριν ληφθεί η απόφαση να εισέλθουν σε νέες αγορές, να ασχοληθούν με νέα προϊόντα, να εισάγουν μια νέα υπηρεσία ή να κάνουν σημαντικές αλλαγές σε υπάρχοντα προϊόντα ή υπηρεσίες· η πολιτική έγκρισης νέων προϊόντων θα πρέπει επίσης να περιλαμβάνει ορισμούς για το «νέο προϊόν», τη «νέα αγορά» και τη «νέα δραστηριότητα» που θα χρησιμοποιούνται από τον οργανισμό και από τα τμήματα που θα συμμετέχουν στη διαδικασία λήψης αποφάσεων.

(3) Η πολιτική έγκρισης νέων προϊόντων καθορίζει τα κύρια θέματα που πρέπει να αντιμετωπιστούν προτού ληφθεί μια απόφαση· αυτά θα πρέπει να περιλαμβάνουν θέματα κανονιστικής συμμόρφωσης, μοντέλων τιμολόγησης, επιπτώσεων στο προφίλ κινδύνου, κεφαλαιακής επάρκειας και κερδοφορίας, διαθεσιμότητας επαρκών πόρων των υπηρεσιών εξυπηρέτησης κοινού (front office), των υπηρεσιών οργανωτικής υποστήριξης πράξεων αγοράς και διαχείρισης κινδύνων (middle office), και των υπηρεσιών οργανωτικής υποστήριξης (back office) και επαρκών εσωτερικών εργαλείων και εμπειριών για την κατανόηση και παρακολούθηση των συναφών κινδύνων.

(4) Η πολιτική έγκρισης νέων προϊόντων διασφαλίζει ότι η απόφαση για την προώθηση μιας νέας δραστηριότητας αναφέρει με σαφήνεια την επιχειρηματική μονάδα και τα άτομα που ευθύνονται γι' αυτήν· δεν πρέπει να προωθείται μια νέα δραστηριότητα έως ότου υπάρχουν διαθέσιμοι επαρκείς πόροι για τη διαχείριση και παρακολούθηση των συναφών κινδύνων.

(5) Τα ιδρύματα διασφαλίζουν ότι το τμήμα διαχείρισης κινδύνων και το τμήμα κανονιστικής συμμόρφωσης εκφέρουν γνώμη πριν από την απόφαση να εισέλθει το ίδρυμα σε νέες αγορές, την εισαγωγή νέων προϊόντων και υπηρεσιών και για οποιαδήποτε σημαντική αλλαγή σε υφιστάμενες αγορές ή προϊόντα.

Μη τυποποιημένες ή μη διαφανείς δραστηριότητες.

73. (1) Τα ιδρύματα αναπτύσσουν και εφαρμόζουν αποτελεσματικά κατάλληλες πολιτικές και διαδικασίες και τεκμηριωμένες διεργασίες για την έγκριση και δημιουργία εταιρειών ειδικού σκοπού ή παρεμφερών δομών ή δραστηριοποίηση σε δικαιοδοσίες που παρεμποδίζουν τη διαφάνεια ή δεν πληρούν τα διεθνή τραπεζικά πρότυπα, με σκοπό να διασφαλιστεί ότι –

(α) οι σχετικοί κίνδυνοι αναγνωρίζονται και διαχειρίζονται κατάλληλα· και

(β) η συνεχιζόμενη ανάγκη για την εκτέλεση τέτοιων δραστηριοτήτων αξιολογείται περιοδικά για να διασφαλιστεί ότι τέτοιες δομές και δραστηριότητες παραμένουν συνεπείς με τους επιδιωκόμενους στόχους τους.

(2) Τα ιδρύματα αναπτύσσουν και εφαρμόζουν αποτελεσματικά παρόμοιες πολιτικές, διαδικασίες και διεργασίες κατά την εκτέλεση μη τυποποιημένων ή μη διαφανών δραστηριοτήτων για πελάτες, σύμφωνα με τις διατάξεις του περί της Πρόληψης και Καταστολής της Νομιμοποίησης Εσόδων από

Παράνομες Δραστηριότητες Νόμου του 2007 και των Οδηγιών της Κεντρικής Τράπεζας και εγκύκλιων για την παρεμπόδιση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και χρηματοδότησης της τρομοκρατίας που εκδίδονται σύμφωνα με το άρθρο 59 (4) του εν λόγω Νόμου.

ΜΕΡΟΣ Χ
ΠΛΑΙΣΙΟ ΕΣΩΤΕΡΙΚΟΥ ΕΛΕΓΧΟΥ

Τμήμα 1 – Γενικές απαιτήσεις

Απαιτήσεις για τη θέσπιση πλαισίου εσωτερικού ελέγχου.

74. (1) Τα ιδρύματα σχεδιάζουν, αναπτύσσουν και διατηρούν ένα ισχυρό και ολοκληρωμένο πλαίσιο εσωτερικού ελέγχου, συμπεριλαμβανομένων συστημάτων ελέγχου και ανεξάρτητων τμημάτων ελέγχου με την κατάλληλη υπόσταση για την εκπλήρωση της αποστολής τους.

(2) Ο σχεδιασμός του πλαισίου εσωτερικού ελέγχου θα πρέπει να διασφαλίζει –

(α) την αποτελεσματικότητα και αποδοτικότητα των δραστηριοτήτων του ιδρύματος·

(β) τον επαρκή έλεγχο των κινδύνων·

(γ) τη συνετή διεξαγωγή των εργασιών·

(δ) τον αποτελεσματικό διαχωρισμό μεταξύ των εποπτικών και των επιχειρησιακών λειτουργιών·

(ε) την αξιοπιστία των χρηματοοικονομικών και μη χρηματοοικονομικών πληροφοριών που αναφέρονται, τόσο εσωτερικά όσο και εκτός του ιδρύματος· και

(στ) τη συμμόρφωση με τους νόμους, κανονισμούς, εποπτικές απαιτήσεις, πρότυπα και εσωτερικούς κανόνες και αποφάσεις του ιδρύματος.

(3) Το πλαίσιο εσωτερικού ελέγχου θα πρέπει να –

(α) καλύπτει τον οργανισμό στο σύνολο του, συμπεριλαμβανομένων των δραστηριοτήτων όλων των τμημάτων ελέγχου, των επιχειρησιακών μονάδων και μονάδων στήριξης·

(β) είναι κατάλληλο για τις εργασίες του ιδρύματος, με υγιής διοικητικές και λογιστικές διαδικασίες.

(4) Κατά την ανάπτυξη του πλαισίου εσωτερικού ελέγχου, το ίδρυμα διασφαλίζει την ύπαρξη σαφών, διάφανων και τεκμηριωμένων διαδικασιών λήψης αποφάσεων και τη σαφή κατανομή αρμοδιοτήτων και εξουσιών για διασφάλιση της συμμόρφωσης με τους εσωτερικούς κανόνες και αποφάσεις· οι επιχειρησιακές και μονάδες και μονάδες στήριξης πρέπει να έχουν την πρωταρχική ευθύνη για τη δημιουργία και διατήρηση επαρκών πολιτικών και διαδικασιών εσωτερικού ελέγχου με ενδεχόμενη συμμετοχή των τμημάτων ελέγχου υπό συμβουλευτική ιδιότητα.

(5) Ένα κατάλληλο πλαίσιο εσωτερικού ελέγχου απαιτεί επαλήθευση από ανεξάρτητες λειτουργίες εσωτερικού ελέγχου για τη συμμόρφωση του με τις εν λόγω πολιτικές και διαδικασίες.

Τμήμα 2 – Συστήματα εσωτερικού ελέγχου

Απαιτήσεις για τη δημιουργία συστημάτων ελέγχου.

75. Τα ιδρύματα σχεδιάζουν και εφαρμόζουν αποτελεσματικά συστήματα εσωτερικού ελέγχου τα οποία είναι κατάλληλα με τη φύση, την κλίμακα και την πολυπλοκότητα των δραστηριοτήτων και του προφίλ κινδύνου τους ιδρύματος· τα ιδρύματα διασφαλίζουν ότι τα σύστημα εσωτερικού ελέγχου περιλαμβάνουν τουλάχιστον τα ακόλουθα:

(α) κατάλληλους ελέγχους που διασφαλίζουν ότι όλες οι συναλλαγές –

(i) είναι δεόντως εξουσιοδοτημένες και νόμιμες·

(ii) εκτελούνται σύμφωνα με όλους τους σχετικούς διαδικαστικούς κανόνες κάθε

επιχειρησιακής μονάδας·

(iii) έχουν αξιολογηθεί ως προς τον εγγενή τους κίνδυνο·

(iv) διεξάγονται από δεόντως εξουσιοδοτημένα και άμεσα αναγνωρίσιμα πρόσωπα·

(v) καταγράφονται δεόντως στα σχετικά βιβλία και αρχεία·

(vi) εισάγονται δεόντως στο σύστημα διαχείρισης πληροφοριών·

(β) κατάλληλους ελέγχους προκειμένου να παρέχουν εύλογη βεβαιότητα για την αμεροληψία, ακρίβεια και πληρότητα των βιβλίων, αρχείων και λογαριασμών του ιδρύματος, καθώς και για την οικονομική ενοποίηση και υποβολή οικονομικών καταστάσεων·

(γ) κατάλληλους ελέγχους για άλλες βασικές επιχειρηματικές διαδικασίες και πολιτικές, συμπεριλαμβανομένων των σημαντικών επιχειρηματικών αποφάσεων και συναλλαγών, των σημαντικών λειτουργιών του συστήματος πληροφόρησης, της πρόσβασης σε βάσεις δεδομένων και πληροφόρησης των υπαλλήλων, και των σημαντικών νομικών και ρυθμιστικών υποχρεώσεων·

(δ) κατάλληλους ελέγχους για την ορθή και αποτελεσματική λειτουργία των συστημάτων πληροφόρησης·

(ε) κατάλληλο διαχωρισμό των καθηκόντων, όπου είναι απαραίτητο, και ελέγχους για τη διασφάλιση της τήρησης του εν λόγω διαχωρισμού·

(στ) ελέγχους στα κατάλληλα επίπεδα, ώστε να είναι αποτελεσματικοί, περιλαμβανομένων των ελέγχων σε επίπεδο διαδικασιών ή συναλλαγών και σε επίπεδο επιχειρηματικού τομέα/μονάδας·

(ζ) ελάχιστο όριο απουσίας δύο συνεχόμενων εβδομάδων το χρόνο για τους υπαλλήλους σε ευαίσθητες θέσεις, όπως οι εργασίες εμβασμάτων· κατά την απουσία τους –

(i) δεν πρέπει να επιτρέπεται η απομακρυσμένη ηλεκτρονική τους πρόσβαση στα συστήματα ή τα αρχεία·

(ii) η καθημερινή τους εργασία θα πρέπει να διεκπεραιώνεται από άλλον υπάλληλο·

(η) κεντρική απογραφή των σημαντικών διαδικασιών και πολιτικών ολόκληρου του ιδρύματος, και των ελέγχων που έχουν τεθεί σε σχέση με αυτές τις διαδικασίες και πολιτικές·

(θ) εκπαίδευση σε σχέση με τους ελέγχους, ιδιαίτερα για τους υπαλλήλους σε θέσεις υψηλής ευθύνης ή που διεξάγουν εργασίες υψηλού κινδύνου·

(ι) διαδικασίες για να ελέγχεται σε τακτική βάση ότι οι έλεγχοι αποτελούν ένα συνεκτικό σύστημα και ότι το σύστημα αυτό λειτουργεί με βάση το σκοπό του, εντάσσεται κατάλληλα στο όλο πλαίσιο της δομής διακυβέρνησης του ιδρύματος, και παρέχει στοιχείο του ελέγχου κινδύνων που συμπληρώνει τις δραστηριότητες αναγνώρισης, αξιολόγησης, και διαχείρισης των κινδύνων του ιδρύματος·

(ια) περιοδική εξέταση και αξιολόγηση για τον προσδιορισμό της επάρκειας, πληρότητας και αποτελεσματικότητας του συστήματος εσωτερικού ελέγχου και της χρησιμότητάς του στο διοικητικό όργανο και τα ανώτατα διοικητικά στελέχη για τον έλεγχο των δραστηριοτήτων του ιδρύματος.

Τμήμα 3- Τμήματα Ελέγχου

Υποτμήμα 3.1- Γενικές απαιτήσεις των τμημάτων ελέγχου

Απαιτήσεις για τη θέσπιση τμήματος ελέγχου.

76. (1) Τα ιδρύματα συστήνουν τμήμα διαχείρισης κινδύνων, τμήμα κανονιστικής συμμόρφωσης, τμήμα ασφάλειας των πληροφοριών και τμήμα εσωτερικής επιθεώρησης τα οποία είναι ανεξάρτητα από τα επιχειρησιακά τμήματα και τα οποία θα πρέπει να έχουν επαρκείς εξουσίες, κύρος, πόρους και πρόσβαση στο διοικητικό όργανο· λιγότερο πολύπλοκα ή μικρότερα ιδρύματα δύνανται, με την έγκριση της Κεντρικής Τράπεζας, να συνδυάζουν τα καθήκοντα των τμημάτων κανονιστικής συμμόρφωσης και/ή ασφάλειας των πληροφοριών με τα καθήκοντα του τμήματος διαχείρισης κινδύνων.

(2) Τα τμήματα ελέγχου έχουν το δικαίωμα με δική τους πρωτοβουλία να επικοινωνούν με οποιοδήποτε μέλος του προσωπικού και να αποκτούν πρόσβαση σε οποιαδήποτε αρχεία ή φακέλους ή οποιαδήποτε άλλη μορφή πληροφοριών όπως είναι απαραίτητο για την εκτέλεση των καθηκόντων τους.

(3) Το τμήμα εσωτερικής επιθεώρησης αναφέρεται στο διοικητικό όργανο μέσω της επιτροπής ελέγχου και ενημερώνει τα ανώτατα διοικητικά στελέχη σχετικά με τα ευρήματά του, σύμφωνα με τις πρόνοιες της παρούσας Οδηγίας.

(4) Το τμήμα διαχείρισης κινδύνων, το τμήμα κανονιστικής συμμόρφωσης και ασφάλειας των πληροφοριών έχουν το δικαίωμα να αναφέρουν τα πορίσματα και τις αξιολογήσεις τους απευθείας στο διοικητικό όργανο και τις αρμόδιες επιτροπές, ανεξάρτητα από τα ανώτατα διοικητικά στελέχη μέσω σαφών διαύλων αναφοράς.

(5) Τα τμήματα ελέγχου διασφαλίζουν ότι η επικοινωνία με τα ανώτατα διοικητικά στελέχη, το διοικητικό όργανο και τις σχετικές επιτροπές είναι επαρκώς τεκμηριωμένη.

Ανεξαρτησία τμημάτων ελέγχου.

77. (1) Τα τμήματα ελέγχου είναι ανεξάρτητα από τις επιχειρησιακές μονάδες και μονάδες στήριξης που παρακολουθούν και ελέγχουν, καθώς και οργανικά ανεξάρτητα το ένα από το άλλο.

(2) Τμήμα ελέγχου θεωρείται ανεξάρτητο εάν πληρούνται οι ακόλουθες προϋποθέσεις:

(α) το προσωπικό του δεν εκτελεί οποιαδήποτε καθήκοντα που εμπίπτουν στο πεδίο των δραστηριοτήτων τις οποίες προορίζεται να παρακολουθεί και να ελέγχει και δεν προκύπτουν ενδεχόμενες συγκρούσεις αρμοδιοτήτων·

(β) είναι οργανικά ξεχωριστό από τις δραστηριότητες τις οποίες του ανατέθηκε να παρακολουθεί και να ελέγχει·

(γ) οι αποδοχές του προσωπικού της τμήματος ελέγχου δεν –

(i) συνδέονται με την απόδοση των δραστηριοτήτων τις οποίες παρακολουθεί και ελέγχει το τμήμα ελέγχου·

(ii) είναι δομημένες κατά τρόπο που θα μπορούσε να υπονομεύει την αντικειμενικότητά του προσωπικού.

Επικεφαλής τμημάτων ελέγχου.

78. (1) Τα ιδρύματα διασφαλίζουν ότι ο επικεφαλής τμήματος ελέγχου είναι ανεξάρτητο ανώτατο διοικητικό στέλεχος με διακριτή αρμοδιότητα για το εν λόγω τμήμα ελέγχου.

(2) Ο επικεφαλής τμήματος ελέγχου δεν απομακρύνεται από τη θέση του χωρίς την προηγούμενη έγκριση του διοικητικού οργάνου στα πλαίσια των εποπτικών του αρμοδιοτήτων και να είναι σε θέση να έχει άμεση πρόσβαση στο διοικητικό όργανο όποτε αυτό απαιτείται.

(3) Ο επικεφαλής τμήματος ελέγχου έχει ηγετικές ικανότητες και είναι υπεύθυνος για την –

(α) διασφάλιση της αντικειμενικότητας και ανεξαρτησίας του εν λόγω τμήματος ελέγχου·

(β) απόκτηση ανθρώπινου δυναμικού με επαρκή προσόντα και δεξιότητες για τη διασφάλιση της ικανότητας του εν λόγω τμήματος ελέγχου να εκτελεί τα καθήκοντα και τις ευθύνες του σύμφωνα με το παρόν Μέρος·

(γ) συνεχή αξιολόγηση και παρακολούθηση των δεξιοτήτων που είναι απαραίτητες για την εκτέλεση των καθηκόντων του εν λόγω τμήματος στο απαιτούμενο επίπεδο·

(δ) εξασφάλιση της κατάλληλης συνεχούς εκπαίδευσης του προσωπικού του εν λόγω τμήματος ελέγχου, προκειμένου να διεξάγει την αυξανόμενη ποικιλομορφία των εργασιών που πρέπει να αναληφθούν ως αποτέλεσμα της εισαγωγής νέων προϊόντων και διαδικασιών εντός του ιδρύματος, των αλλαγών σε κανονισμούς ή επαγγελματικά πρότυπα καθώς και άλλες εξελίξεις στο χρηματοπιστωτικό τομέα·

(ε) άμεση ενημέρωση προς τους επικεφαλείς των άλλων τμημάτων για τυχόν ευρήματα που τους αφορούν·

(στ) υποβολή αναφορών προς στο διοικητικό όργανο και τις σχετικές επιτροπές και συμμετοχή στις συνεδριάσεις τους για παρουσίαση των εν λόγω αναφορών και την παροχή επιπρόσθετων πληροφοριών ή/και διευκρινίσεων ή στήριξη για τη διαχείριση των θεμάτων που προκύπτουν·

(ζ) προετοιμασία και παράδοση στα νεοδιορισθέντα μέλη του διοικητικού οργάνου, σε συντονισμό με τον γραμματέα του διοικητικού οργάνου, ενός εισαγωγικού σεμιναρίου που να καλύπτει επαρκώς τους σχετικούς τομείς αρμοδιοτήτων του εν λόγω τμήματος ελέγχου με αναφορές στις ευθύνες του διοικητικού οργάνου και στις απαιτήσεις του ρυθμιστικού πλαισίου·

(η) έκφραση γνώμης, στην περίπτωση κατά την οποία το ίδρυμα είναι η μητρική εταιρεία ενός ομίλου, για την επιλογή και την καταλληλότητα των προσώπων που είναι υπεύθυνα για τα αντίστοιχα τμήματα ελέγχου των θυγατρικών εταιρειών στην Κύπρο και το εξωτερικό, καθώς και αυτών που εργοδοτούνται σε υποκαταστήματα του εξωτερικού·

(θ) ενημέρωση προς την Κεντρική Τράπεζα όσον αφορά σημαντικά ευρήματα ή εξελίξεις τα οποία έχουν σημαντική επίπτωση στο προφίλ κινδύνου του ιδρύματος και για οποιεσδήποτε σημαντικές αλλαγές στη δομή και τις εργασίες του εν λόγω τμήματος ελέγχου·

(ι) πραγματοποίηση συναντήσεων με την Κεντρική Τράπεζα τουλάχιστον σε ετήσια βάση ή κατά οποιονδήποτε άλλο χρόνο απαιτήσει η Κεντρική Τράπεζα με σκοπό να συζητηθεί το πεδίο εφαρμογής και η έκταση των εργασιών των τμημάτων ελέγχου, καθώς και της ανάλυσης κινδύνων, των ευρημάτων και εισηγήσεων του.

Προσόντα υπαλλήλων τμήματος ελέγχου.

79. (1) Τα τμήματα ελέγχου έχουν επαρκή αριθμό προσοντούχου προσωπικού, και σε περίπτωση ομίλου, τόσο σε επίπεδο μητρικής όσο και σε επίπεδο θυγατρικής.

(2) Το προσωπικό των τμημάτων ελέγχου πρέπει να λαμβάνει την κατάλληλη εκπαίδευση.

(3) Τα ιδρύματα διασφαλίζουν ότι το προσωπικό των τμημάτων ελέγχου έχει στη διάθεσή του τα κατάλληλα συστήματα πληροφόρησης καθώς και υποστήριξη, με πρόσβαση σε εσωτερικές και εξωτερικές πληροφορίες που θεωρούνται απαραίτητες ώστε να ανταποκριθεί στις υποχρεώσεις του.

Εναλλαγή προσωπικού τμημάτων ελέγχου.

80. Τηρουμένης της υποπαραγράφου (2), τα ιδρύματα θα πρέπει, όποτε αυτό είναι εφικτό και χωρίς να τίθεται σε κίνδυνο η ικανότητα και τεχνογνωσία των τμημάτων ελέγχου, να εναλλάσσουν περιοδικά το προσωπικό κάθε τμήματος ελέγχου ή να μεταθέτουν προσωπικό από ένα τμήμα ελέγχου προς άλλο τμήμα του ιδρύματος, ούτως ώστε να διασφαλίζεται ότι η ικανότητα ευθυκρισίας των υπαλλήλων ενός τμήματος ελέγχου, δεν τίθεται υπό αμφισβήτηση λόγω πιθανής απώλειας της αντικειμενικότητας από τη συνεχή εκτέλεση παρόμοιων εργασιών ή εργασιών ρουτίνας.

(2) Η εναλλαγή ρόλων και θέσεων προσωπικού εντός ενός τμήματος ελέγχου και οι μεταθέσεις προσωπικού προς και από ένα τμήμα ελέγχου θα πρέπει να διέπονται και να διεξάγονται σύμφωνα με μία ορθή και καταγεγραμμένη πολιτική· η πολιτική αυτή πρέπει να σχεδιάζεται κατά τρόπο που να αποφεύγονται οι συγκρούσεις συμφερόντων και να διασφαλίζεται ότι:

(α) έχει παρέλθει ικανοποιητικός χρόνος προσαρμοσμένος στο μέγεθος και την πολυπλοκότητα του ιδρύματος, προτού ανατεθούν σε προσωπικό που έχει μετακινηθεί σε τμήμα ελέγχου από άλλους λειτουργικούς τομείς του ιδρύματος, αρμοδιότητες επίβλεψης που σχετίζονται με το τμήμα ελέγχου στο οποίο εργαζόταν πριν την μετακίνηση του·

(β) δημιουργείται η ελάχιστη δυνατή διατάραξη των εργασιών του τμήματος ελέγχου από τη διαδικασία των μετακινήσεων.

Σχέσεις μεταξύ τμημάτων ελέγχου.

81. (1) Ενόψει της στενής σχέσης μεταξύ των δραστηριοτήτων των τμημάτων ελέγχου, τα ιδρύματα διασφαλίζουν ότι υπάρχει σαφώς προσδιορισμένη κατανομή και διαχωρισμός των αρμοδιοτήτων, ιδίως όσον αφορά την ευθύνη για μέτρηση των κινδύνων, καθώς και τον εντοπισμό, επαλήθευση και αξιολόγηση της επάρκειας των σχετικών διαδικασιών και κανονισμών εσωτερικής επιθεώρησης.

(2) Ένα τμήμα ελέγχου οφείλει να κοινοποιεί σε άλλα τμήματα ελέγχου οποιαδήποτε ευρήματα τα αφορά· τα ευρήματα αυτά λειτουργούν ως ένας μηχανισμός ανατροφοδότησης για αξιολόγηση των τομέων που βρίσκονται υπό την ευθύνη τμημάτων ελέγχου στις συναφείς πολιτικές και διαδικασίες ελέγχου.

Καταστατικό τμημάτων ελέγχου.

82. (1) Ο σκοπός, η υπόσταση και οι εξουσίες κάθε τμήματος ελέγχου θα πρέπει να διέπονται από καταστατικό που επανεξετάζεται περιοδικά από τον επικεφαλής του εν λόγω τμήματος ελέγχου και εγκρίνεται από το διοικητικό όργανο.

(2) Το καταστατικό καθορίζει, κατ' ελάχιστον, τα ακόλουθα:

(α) την υπόσταση του τμήματος ελέγχου εντός του ιδρύματος, τις εξουσίες του, το σκοπό και το πεδίο εφαρμογής του, τα κύρια χαρακτηριστικά και τις ευθύνες του, τους δίαυλους επικοινωνίας και τις σχέσεις του με άλλα τμήματα ελέγχου, κατά τρόπο που να προωθεί την αποτελεσματικότητά του·

(β) μέτρα για διασφάλιση της ανεξαρτησίας του·

(γ) το δικαίωμά του για ιδία έναρξη επικοινωνίας με οποιοδήποτε μέλος του προσωπικού, για να λάβει πλήρη και άνευ όρων πρόσβαση σε όλα τα αρχεία και φακέλους του ιδρύματος, καθώς και κάθε άλλη πληροφορία που απαιτείται για την εκτέλεση των καθηκόντων του·

(δ) το δικαίωμα της ελεύθερης έκφρασης και αναφοράς των ευρημάτων του στο διοικητικό όργανο και στις σχετικές επιτροπές του χωρίς την παρουσία των εκτελεστικών μελών του διοικητικού οργάνου·

(ε) τους όρους και προϋποθέσεις βάσει των οποίων το τμήμα ελέγχου μπορεί να κληθεί να παράσχει υποστήριξη ή συμβουλευτικές υπηρεσίες ή να διεκπεραιώσει άλλα ειδικά καθήκοντα·

(στ) το ρόλο του στην έγκριση νέων προϊόντων και υπηρεσιών, την ανάπτυξη νέων αγορών και σημαντικών αλλαγών στις υφιστάμενες·

(ζ) την ευθύνη και την υποχρέωση λογοδοσίας του επικεφαλή του τμήματος ελέγχου·

(η) απαίτηση για συμμόρφωση με επαγγελματικά πρότυπα.

Ο ρόλος των τμημάτων ελέγχου σε ομίλους.

83. (1) Σε περίπτωση όπου το ίδρυμα είναι η μητρική εταιρεία ενός ομίλου, τα τμήματα ελέγχου του ιδρύματος διασφαλίζουν ότι τα αντίστοιχα τμήματα ελέγχου των θυγατρικών προβαίνουν σε αναφορές, σε τακτική βάση, σχετικά με τις δραστηριότητες και τα ευρήματά τους. Τα τμήματα ελέγχου του ιδρύματος οφείλουν, με βάση τις δραστηριότητες και τα ευρήματα των τμημάτων ελέγχου των θυγατρικών, να διενεργούν, σε περιοδική βάση, τόσο εκ του γραφείου όσο και επιτόπιους ελέγχους των μονάδων, υποκαταστημάτων, θυγατρικών εταιρειών στην Κύπρο και το εξωτερικό για την αξιολόγηση της συμμόρφωσης τους με τις πολιτικές και διαδικασίες του ομίλου.

(2) Σε περίπτωση όπου το ίδρυμα είναι η θυγατρική εταιρεία ενός ομίλου, τα τμήματα ελέγχου του ιδρύματος οφείλουν να προβαίνουν σε αναφορές, σε τακτική βάση, στον επικεφαλής τμήματος ελέγχου του ομιλου, σχετικά με τις δραστηριότητες και τα ευρήματα τους σε τομείς, λειτουργίες και δραστηριότητες του ιδρύματος.

Υποτμήμα 3.1 – Τμήμα διαχείρισης κινδύνων

Γενικές απαιτήσεις του τμήματος διαχείρισης κινδύνων.

84. (1) Το τμήμα διαχείρισης κινδύνων διασφαλίζει τον εντοπισμό, τη μέτρηση και τη δέουσα αναφορά όλων των σημαντικών κινδύνων.

(2) Το τμήμα διαχείρισης κινδύνων εμπλέκεται ενεργά στην λεπτομερή επεξεργασία της στρατηγικής κινδύνου του ιδρύματος και σε όλες τις σημαντικές αποφάσεις διαχείρισης κινδύνων και θα πρέπει να είναι σε θέση να αποδώσει μία ολοκληρωμένη εικόνα ολόκληρου του φάσματος των κινδύνων που αντιμετωπίζει το ίδρυμα.

(3) Τα ιδρύματα διασφαλίζουν ότι το τμήμα διαχείρισης κινδύνων είναι σε θέση να αναφέρεται απευθείας στο διοικητικό όργανο, κατά την άσκηση της εποπτικής του δραστηριότητας, ανεξάρτητα από τα ανώτατα διοικητικά στελέχη, και να εγείρει ανησυχίες και να προειδοποιεί το εν λόγω όργανο, όταν κρίνεται σκόπιμο, σε περίπτωση εξελίξεων ειδικού κινδύνου που πλήττουν ή ενδέχεται να πλήξουν το ίδρυμα, ανεξάρτητα από τις αρμοδιότητες του διοικητικού οργάνου κατά την άσκηση της

εποπτικής και/ή διοικητικής του αρμοδιότητας δυνάμει της παρούσας Οδηγίας και του Κανονισμού (ΕΕ) αριθ. 575/2013.

Ο ρόλος του τμήματος διαχείρισης κινδύνων στη διαμόρφωση στρατηγικής, διάθεσης ανάληψης κινδύνων και λήψης αποφάσεων.

85. (1) Το τμήμα διαχείρισης κινδύνων προβαίνει σε αναλύσεις και κρίσεις εμπειρικές αναφορικά με την έκθεση σε κινδύνους, προκειμένου να διευκολύνει το διοικητικό όργανο να καθορίσει τη στρατηγική του ιδρύματος και το πλαίσιο διάθεσης ανάληψης κινδύνων.

(2) Το τμήμα διαχείρισης κινδύνων αξιολογεί τη στρατηγική κινδύνων και τη διάθεση ανάληψης κινδύνων, συμπεριλαμβανομένων των στόχων που προτείνονται από τις επιχειρηματικές μονάδες και συμβουλεύει το διοικητικό όργανο προτού ληφθεί απόφαση· οι στόχοι, οι οποίοι περιλαμβάνουν αξιολογήσεις πιστοληπτικής ικανότητας και δείκτες απόδοσης των ιδίων κεφαλαίων, θα πρέπει να είναι αληθοφανείς και συνεπείς.

(3) Το τμήμα διαχείρισης κινδύνων συμμετέχει επαρκώς σε τυχόν αλλαγές στη στρατηγική του ιδρύματος, στο πλαίσιο διάθεσης για ανάληψη κινδύνων και στα όρια κινδύνου.

(4) Το τμήμα διαχείρισης κινδύνων συμμετέχει ενεργά σε αρχικό στάδιο στην αξιολόγηση των επιπτώσεων των σημαντικών αλλαγών στη δομή του ιδρύματος και των ασυνήθιστων συναλλαγών στο συνολικό κίνδυνο του ιδρύματος και του ομίλου, πριν ληφθεί οποιαδήποτε απόφαση σχετικά με αυτές τις αλλαγές.

(5) Η συμμετοχή του τμήματος διαχείρισης κινδύνων στις διαδικασίες λήψης αποφάσεων διασφαλίζει ότι:

(α) η συνεχής αξιολόγηση των δραστηριοτήτων ανάληψης κινδύνων παραμένει αντικειμενική και ανεξάρτητη·

(β) η λογοδοσία για τις αποφάσεις που λαμβάνονται παραμένει στην εταιρεία και τις μονάδες στήριξης και, τελικά, στο διοικητικό όργανο.

(6) Το τμήμα διαχείρισης κινδύνων διαδραματίζει κύριο ρόλο προκειμένου να διασφαλίζεται ότι η απόφαση σχετικά με τις εισηγήσεις της λαμβάνεται στο κατάλληλο επίπεδο, τυγχάνει συμμόρφωσης απο τις αρμόδιες υπηρεσιακές μονάδες και αναφέρεται κατάλληλα στο διοικητικό όργανο, στην επιτροπή κινδύνων και στην μονάδα στήριξης.

(7) Οι απαιτήσεις που καθορίζονται στην παρούσα παράγραφο ισχύουν για το τμήμα διαχείρισης κινδύνων του μητρικού ιδρύματος αναφορικά με ολόκληρο τον όμιλο.

Ο ρόλος του τμήματος διαχείρισης κινδύνων στη διαχείριση κινδύνων.

86. (1) Το τμήμα διαχείρισης κινδύνων είναι υπεύθυνο για τον κατάλληλο σχεδιασμό, ανάπτυξη παρακολούθηση και υποβολή αναφορών σχετικά με το πλαίσιο διαχείρισης κινδύνων όπως προβλέπεται στο Μέρος ΙΧ.

(2) Το τμήμα διαχείρισης κινδύνων διασφαλίζει ότι το πλαίσιο διαχείρισης κινδύνων εντοπίζει, ενοποιεί και ιεραρχεί τους κινδύνους που αντιμετωπίζει το ίδρυμα.

(3) Το τμήμα διαχείρισης κινδύνων διασφαλίζει ότι η διαδικασία εντοπισμού των κινδύνων του ιδρύματος δεν επικεντρώνεται μόνο στους κινδύνους που προβλέπονται στο Μέρος ΙΧ ή σε χρηματοπιστωτικούς κινδύνους που είναι εύκολο να μετρηθούν, αλλά εξετάζει όλες τις διαστάσεις των κινδύνων που αντιμετωπίζει το ίδρυμα, συμπεριλαμβανομένων των μη χρηματοπιστωτικών κινδύνων, όπως είναι ο νομικός κίνδυνος και ο κίνδυνος φήμης· το τμήμα διαχείρισης κινδύνων είναι υπεύθυνο για τον εντοπισμό των κινδύνων που απορρέουν από την πολυπλοκότητα της νομικής δομής του ιδρύματος και για την αναγνώριση νέων ή αναδυόμενων κινδύνων που προκύπτουν από τις μεταβαλλόμενες καταστάσεις και συνθήκες.

(4) Το τμήμα διαχείρισης κινδύνων διασφαλίζει ότι οι κύριες πηγές των κινδύνων που εντοπίζονται αναγνωρίζονται με συνεπή τρόπο ώστε να καταστεί δυνατή η αξιολόγηση των αλληλεπιδράσεων μεταξύ των κινδύνων αυτών.

(5) Το τμήμα διαχείρισης κινδύνου επικυρώνει τακτικά την ακρίβεια και αποτελεσματικότητα της διαδικασίας διαχείρισης κινδύνων· τέτοιες ασκήσεις επικύρωσης περιλαμβάνουν τουλάχιστον την εξέταση των πραγματικών αποτελεσμάτων, έναντι των παλαιότερων εκτιμήσεων.

(6) Το τμήμα διαχείρισης κινδύνων αξιολογεί ανεξάρτητα τυχόν παράβαση ή παραβίαση των ορίων

ανάληψης κινδύνων, συμπεριλαμβανομένης της αιτίας για την παράβαση ή παραβίαση και προβαίνει σε νομική και οικονομική ανάλυση του πραγματικού κόστους εξάλειψης, μείωσης ή αντιστάθμισης του ανοίγματος σε σχέση με το δυνητικό κόστος διατήρησης του· το τμήμα διαχείρισης κινδύνων ενημερώνει, ανάλογα, τις εμπλεκόμενες επιχειρησιακές μονάδες και προτείνει πιθανά διορθωτικά μέτρα.

(7) Στην περίπτωση κατά την οποία το ίδρυμα είναι η μητρική εταιρεία ενός ομίλου, το τμήμα διαχείρισης κινδύνων παρακολουθεί τους κινδύνους που αναλαμβάνονται από τις θυγατρικές του και αναφέρει στο διοικητικό όργανο τυχόν ασυνέπειες με την εγκεκριμένη στρατηγική του ομίλου.

Ο ρόλος του τμήματος διαχείρισης κινδύνων στην ανάπτυξη και έγκριση νέων προϊόντων.

87. (1) Το τμήμα διαχείρισης κινδύνων συμμετέχει ενεργά στη διαδικασία έγκρισης της ανάπτυξης νέων αγορών, προϊόντων και υπηρεσιών καθώς και των σημαντικών αλλαγών στις υφιστάμενες, έχοντας σαφή εικόνα του σχεδίου εφαρμογής στις διάφορες επιχειρησιακές δραστηριότητες και χαρτοφυλάκια, και έχει την εξουσία να απαιτεί όπως οι αλλαγές σε υφιστάμενα προϊόντα ακολουθούν την τυπική διαδικασία έγκρισης νέων προϊόντων σύμφωνα με την παράγραφο 72· η συμβολή του τμήματος διαχείρισης κινδύνων περιλαμβάνει μια πλήρη και αντικειμενική αξιολόγηση -

(α) των κινδύνων που προκύπτουν από τις νέες δραστηριότητες υπό το πλαίσιο ποικίλων σεναρίων·

(β) των ενδεχόμενων αδυναμιών των πλαισίων διαχείρισης κινδύνων και εσωτερικού ελέγχου του ιδρύματος· και

(γ) της ικανότητας του ιδρύματος να κατανοήσει και να διαχειριστεί τυχόν συναφείς κινδύνους.

Συγκεκριμένες απαιτήσεις του επικεφαλής του τμήματος διαχείρισης κινδύνων.

88. Ο επικεφαλής του τμήματος διαχείρισης κινδύνων πρέπει να έχει επαρκή τεχνογνωσία και πρακτική εμπειρία που να του επιτρέπει να αμφισβητεί τις αποφάσεις που επηρεάζουν την έκθεση του ιδρύματος σε κίνδυνο.

Απαιτήσεις για υποβολή αναφορών του τμήματος διαχείρισης κινδύνων.

89. (1) Ο επικεφαλής του τμήματος διαχείρισης κινδύνων υποβάλλει, σε τριμηνιαία βάση, έκθεση στην επιτροπή κινδύνων, αντίγραφο της οποίας κοινοποιείται στον διευθύνοντα εκτελεστικό σύμβουλο· η έκθεση θα πρέπει να καλύπτει, τουλάχιστον, τα ακόλουθα:

(α) εσωτερική αξιολόγηση και μέτρηση των κινδύνων που αντιμετωπίζει το ίδρυμα·

(β) αποτελέσματα και παραδοχές των προσομοιώσεων ακραίων καταστάσεων ή των αναλύσεων σεναρίου·

(γ) υπολογισμό των κεφαλαιακών απαιτήσεων και του δείκτη κεφαλαιακής επάρκειας· και

(δ) πληροφορίες για το εξωτερικό περιβάλλον με σκοπό τον προσδιορισμό των συνθηκών της αγοράς και των τάσεων που ενδέχεται να έχουν σχέση με το παρόν και μελλοντικό προφίλ κινδύνου του ιδρύματος.

(2) Ο επικεφαλής του τμήματος διαχείρισης κινδύνων υποβάλλει ετήσια έκθεση προς το διοικητικό όργανο εντός δύο μηνών από το τέλος κάθε έτους, μέσω της επιτροπής κινδύνων, αντίγραφο της οποίας κοινοποιείται στον διευθύνοντα εκτελεστικό σύμβουλο και περιλαμβάνει, τουλάχιστον, τις ακόλουθες πληροφορίες:

(α) επισκόπηση των βασικών χρηματοοικονομικών εξελίξεων κατά τη διάρκεια του έτους, οι οποίες είχαν σημαντική επίδραση στις εργασίες του ιδρύματος και το προφίλ κινδύνου·

(β) περιγραφή του πλαισίου διαχείρισης κινδύνων, συμπεριλαμβανομένης της οργάνωσης και λειτουργίας του τμήματος διαχείρισης κινδύνων, και της υφιστάμενης διαδικασίας διαχείρισης κινδύνων·

(γ) τις παραδοχές και τα αποτελέσματα των προσομοιώσεων ακραίων καταστάσεων και των αναλύσεων σεναρίου που διεξάγονται κατά τη διάρκεια του υπό επισκόπηση έτους·

(δ) λεπτομερείς πληροφορίες για το προφίλ κινδύνου του ιδρύματος και της διαδικασίας κατανομής κεφαλαίων·

(ε) περίληψη των αποτελεσμάτων της άσκησης αυτοαξιολόγησης κινδύνων και ελέγχου που διεξήχθη κατά τη διάρκεια του υπό επισκόπηση έτους, μαζί με εισηγήσεις για την ελαχιστοποίηση τυχόν αυξημένων λειτουργικών κινδύνων που έχουν εντοπιστεί·

(στ) πληροφορίες για λειτουργικές ζημίες κατά τη διάρκεια του υπό επισκόπηση έτους·

(ζ) πληροφορίες σχετικά με τους σημαντικούς δείκτες κινδύνου και τους σημαντικούς δείκτες απόδοσης των μη-εξυπηρετούμενων δανείων που παρακολουθούνται από το ίδρυμα·

(η) υπολογισμό των κεφαλαιακών απαιτήσεων του ιδρύματος και του δείκτη κεφαλαιακής επάρκειας·

(θ) εισηγήσεις και συγκεκριμένα μέτρα που πρέπει να ληφθούν για την αντιμετώπιση τυχόν αδυναμιών που εντοπίζονται στο πλαίσιο διαχείρισης κινδύνων του ιδρύματος· και

(ι) ολοκληρωμένη ανάλυση χάσματος όπου το τμήμα διαχείρισης κινδύνων θα σχολιάζει τις εισηγήσεις που διατυπώθηκαν στην έκθεση του προηγούμενου έτους συμπεριλαμβανομένης αξιολόγησης της προόδου που έχει επιτευχθεί και της υφιστάμενης κατάστασης.

Υποτμήμα 3.2 – Τμήμα Κανονιστικής Συμμόρφωσης

Ρόλος και ευθύνες του τμήματος κανονιστικής συμμόρφωσης.

90. (1) Το τμήμα κανονιστικής συμμόρφωσης θεσπίζει, εφαρμόζει και διατηρεί κατάλληλους μηχανισμούς και δραστηριότητες για –

(α) την προώθηση και διατήρηση μιας εταιρικής κουλτούρας κανονιστικής συμμόρφωσης και ακεραιότητας εντός του ιδρύματος·

(β) να επικουρεί τα ανώτατα διοικητικά στελέχη στο σχεδιασμό, ανάπτυξη και εφαρμογή ενός κατάλληλου και αποτελεσματικού πλαισίου κανονιστικής συμμόρφωσης σύμφωνα με τις διατάξεις του Μέρους VIII για:

(i) την έγκαιρη και συνεχή συμμόρφωση του ιδρύματος και των θυγατρικών του εταιρειών στην Κύπρο και το εξωτερικό και των ξένων υποκαταστημάτων του με τις νομικές, ρυθμιστικές και επιχειρησιακές υποχρεώσεις τους·

(ii) την αποτελεσματική διαχείριση των κινδύνων μη συμμόρφωσης με τις υποχρεώσεις αυτές.

(2) Οι δραστηριότητες κανονιστικής συμμόρφωσης καθορίζονται σε ένα πρόγραμμα κανονιστικής συμμόρφωσης που ετοιμάζεται και παρακολουθείται από τον επικεφαλής του τμήματος κανονιστικής συμμόρφωσης ο οποίος διασφαλίζει ότι όλοι οι σχετικοί τομείς του ιδρύματος, των θυγατρικών του στην Κύπρο και το εξωτερικό καθώς και των υποκαταστημάτων καλύπτονται κατάλληλα, λαμβάνοντας υπόψη την ευαισθησία τους στον κίνδυνο συμμόρφωσης· οι δραστηριότητες κανονιστικής συμμόρφωσης περιλαμβάνουν τουλάχιστον τα ακόλουθα:

(α) αναγνώριση, σε συνεχή βάση, με τη βοήθεια της μονάδας νομικών υπηρεσιών και των άλλων αρμόδιων μονάδων του ιδρύματος, των νομικών, ρυθμιστικών και επιχειρησιακών απαιτήσεων που διέπουν και/ή επηρεάζουν τις δραστηριότητες του ιδρύματος·

(β) διασφάλιση της διατήρησης ενός ολοκληρωμένου και ενημερωμένου μητρώου των νομικών, ρυθμιστικών και επιχειρησιακών απαιτήσεων και εγγραφή των απορρέουσων υποχρεώσεων συμμόρφωσης·

(γ) ενημέρωση προς τις επιχειρησιακές μονάδες, υποκαταστήματα και θυγατρικές όσον αφορά τις ισχύουσες νομικές, ρυθμιστικές και επιχειρησιακές απαιτήσεις για –

(i) τον προσδιορισμό των υποχρεώσεων συμμόρφωσης που απορρέουν από τις απαιτήσεις

αυτές·

(ii) τη μέτρηση και αξιολόγηση των επιπτώσεων των υποχρεώσεων αυτών στις διεργασίες, διαδικασίες και δραστηριότητες του ιδρύματος·

(iii) την αξιολόγηση της καταλληλότητας των πολιτικών και διαδικασιών κανονιστικής συμμόρφωσης του ιδρύματος, της παρακολούθησης των ελλείψεων και, όπου είναι απαραίτητο, της διατύπωσης εισηγήσεων για τροποποιήσεις·

(δ) αναγνώριση και εγγραφή των κινδύνων κανονιστικής συμμόρφωσης που σχετίζονται με τις επιχειρηματικές δραστηριότητες του ιδρύματος, σε προληπτική βάση·

(ε) ανάπτυξη κατάλληλων πρακτικών και μεθοδολογιών για τη μέτρηση του κινδύνου κανονιστικής συμμόρφωσης, όπως δείκτες κινδύνου, με τη βοήθεια, αν καταστεί αναγκαία, των εμπειρογνωμόνων του τμήματος διαχείρισης κινδύνων και τη χρήση τέτοιων μετρήσεων για τη βελτίωση της ικανότητας αξιολόγησης του κινδύνου κανονιστικής συμμόρφωσης· το τμήμα κανονιστικής συμμόρφωσης διασφαλίζει ότι οι μεθοδολογίες αυτές επιτρέπουν τη συνάθροιση ή φιλτράρισμα των δεδομένων τα οποία δύναται να είναι ενδεικτικά πιθανών προβλημάτων κανονιστικής συμμόρφωσης·

(στ) διατύπωση προτάσεων για οργανωτικές και διαδικαστικές αλλαγές για τη διασφάλιση της κατάλληλης διαχείρισης των αναγνωρισμένων κίνδυνων κανονιστικής συμμόρφωσης·

(ζ) διασφάλιση της χρήσης κατάλληλων εργαλείων και μεθοδολογιών για την παρακολούθηση των δραστηριοτήτων οι οποίες, μεταξύ άλλων, περιλαμβάνουν:

(i) αξιολόγηση των περιοδικών εκθέσεων που υποβάλλονται από τους υπεύθυνους λειτουργούς συμμόρφωσης σύμφωνα με την παράγραφο 59(4)·

(ii) τη χρήση συγκεντρωτικών μετρήσεων κινδύνου, όπως οι δείκτες κινδύνου·

(ii) τη χρήση αναφορών άξιων προσοχής της διοίκησης, εγγραφή σημαντικών αποκλίσεων μεταξύ των πραγματικών περιστατικών και των προσδοκιών (κατ' εξαίρεση έκθεση) ή καταστάσεων που απαιτούν εξυγίανση (καταγραφή θεμάτων)·

(iv) στοχευόμενη επιχειρηματική παρακολούθηση του χαρτοφυλακίου συναλλαγών, την παρατήρηση των διαδικασιών, έλεγχο εγγράφων και/ή συνεντεύξεις του εμπλεκόμενου προσωπικού·

(v) εξακρίβωση του τρόπου πρακτικής εφαρμογής των πολιτικών και διαδικασιών κανονιστικής συμμόρφωσης μέσω επιτόπιων ελέγχων· και

(vi) διερεύνηση πιθανών παραβάσεων της πολιτικής συμμόρφωσης και του κανονιστικού πλαισίου με τη βοήθεια, εάν καταστεί αναγκαίο, εμπειρογνωμόνων εντός του ιδρύματος όπως εμπειρογνώμονες του τμήματος εσωτερικού ελέγχου επιθεώρησης ή της μονάδας νομικών υπηρεσιών·

(η) διασφάλιση της ύπαρξης εσωτερικής διαδικασίας έγκαιρης προειδοποίησης για διευκόλυνση της εμπιστευτικής υποβολής αναφορών από υπαλλήλους σχετικά με ανησυχίες, ελλείψεις, ή πιθανές παραβιάσεις των πολιτικών του ιδρύματος, των νομικών, ρυθμιστικών ή επιχειρησιακών υποχρεώσεων, ή ηθικών θεμάτων, σύμφωνα με τις διατάξεις της παραγράφου 57·

(θ) επίβλεψη της διαδικασίας παραπόνων και αξιοποίηση των παραπόνων των πελατών ως πηγή άντλησης χρήσιμων πληροφοριών στο πλαίσιο των γενικών αρμοδιοτήτων παρακολούθησης·

(ι) περιοδική επαναξιολόγηση και επανεξέταση του πεδίου εφαρμογής των ελέγχων κανονιστικής συμμόρφωσης που πρέπει να διεξάγονται·

(ια) συνεργασία και ανταλλαγή πληροφοριών με άλλα τμήματα ελέγχου και διαχείρισης κινδύνων για θέματα συμμόρφωσης·

(ιβ) έγκαιρη υποβολή εκθέσεων στα ανώτατα διοικητικά στελέχη και το διοικητικό όργανο σχετικά με σημαντικές ελλείψεις και αδυναμίες της πολιτικής κανονιστικής συμμόρφωσης και των διαδικασιών εσωτερικού ελέγχου, καθώς και παραβάσεις του ρυθμιστικού πλαισίου που αποκαλύπτονται από τις δραστηριότητες παρακολούθησης της συμμόρφωσης του ιδρύματος, τους επιτόπιους ελέγχους και έρευνες·

(ιγ) οργάνωση τακτικών προγραμμάτων κατάρτισης και εκπαίδευσης της διεύθυνσης και του προσωπικού σε θέματα κανονιστικής συμμόρφωσης και ρύθμισης·

(ιδ) παροχή συμβουλών και ανταπόκριση σε ερωτήματα σχετικά με θέματα συμμόρφωσης από το προσωπικό·

(ιε) έκδοση γραπτών οδηγιών και εγκυκλίων προς το προσωπικό, τις επιχειρηματικές μονάδες και τα αρμόδια τμήματα του ιδρύματος και του ομίλου για την έγκαιρη προσαρμογή των εσωτερικών διαδικασιών και κανονισμών στις αλλαγές του ρυθμιστικού πλαισίου·

(ιστ) εξακρίβωση ότι τα νέα προϊόντα και διαδικασίες είναι σύμφωνες με το ισχύον νομικό πλαίσιο και τα επαγγελματικά πρότυπα και με κάθε γνωστή αλλαγή στη νομοθεσία, τους κανονισμούς, τις εποπτικές απαιτήσεις και τα επαγγελματικά πρότυπα.

Ρόλος του τμήματος κανονιστικής συμμόρφωσης στην παρεμπόδιση νομιμοποίησης εσόδων από παράνομες δραστηριότητες.

91. Το τμήμα κανονιστικής συμμόρφωσης διασφαλίζει τη συμμόρφωση του ιδρύματος με τον περί Πρόληψης και Καταστολής της Νομιμοποίησης Εσόδων από Παράνομες Δραστηριότητες Νόμο του 2007 όπως εκάστοτε τροποποιείται ή αντικαθίσταται και των Οδηγιών της Κεντρικής Τράπεζας και εγκυκλίων που αφορούν την παρεμπόδιση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και χρηματοδότησης της τρομοκρατίας που εκδίδονται δυνάμει του άρθρου 59 (4) του εν λόγω Νόμου· ο επικεφαλής του τμήματος κανονιστικής συμμόρφωσης ή άλλο μέλος του τμήματος κανονιστικής συμμόρφωσης που κατέχει διευθυντική θέση θα πρέπει να διοριστεί στη θέση του Λειτουργού Συμμόρφωσης δυνάμει του άρθρου 69 του εν λόγω Νόμου.

Ρόλος του τμήματος κανονιστικής συμμόρφωσης στην παροχή επενδυτικών υπηρεσιών και δραστηριοτήτων.

92. Τα ιδρύματα που παρέχουν επενδυτικές υπηρεσίες και δραστηριότητες και επικουρικές υπηρεσίες, σύμφωνα με τον περί Επενδυτικών Υπηρεσιών και Δραστηριοτήτων και Ρυθμιζόμενων Αγορών Νόμο του 2007, διασφαλίζουν ότι το τμήμα κανονιστικής συμμόρφωσης συμμετέχει στη διαμόρφωση των σχετικών πολιτικών και διαδικασιών εντός του ιδρύματος· το τμήμα κανονιστικής συμμόρφωσης αξιολογεί περιοδικά τη συμμόρφωση του ιδρύματος με τις διατάξεις του προαναφερθέντος Νόμου, συμπεριλαμβανομένης της αξιολόγησης κατά πόσο το προσωπικό στον τομέα των επενδυτικών υπηρεσιών και δραστηριοτήτων διαθέτει την απαραίτητη ενημέρωση και εφαρμόζει ορθά τις πολιτικές και διαδικασίες του ιδρύματος.

Καταστατικό του τμήματος κανονιστικής συμμόρφωσης.

93. Σε περίπτωση που οι αρμοδιότητες κανονιστικής συμμόρφωσης διενεργούνται από προσωπικό με διαφορετικές αρμοδιότητες, το καταστατικό κανονιστικής συμμόρφωσης θα πρέπει να καθορίζει τον τρόπο κατανομής των καθηκόντων αυτών μεταξύ των τμημάτων.

Απαιτήσεις για υποβολή αναφορών.

94. (1) Ο επικεφαλής του τμήματος κανονιστικής συμμόρφωσης υποβάλλει, σε τριμηνιαία βάση, έκθεση στην επιτροπή ελέγχου, αντίγραφο της οποίας κοινοποιείται στον διευθύνοντα εκτελεστικό σύμβουλο· η έκθεση καλύπτει, τουλάχιστον, τα ακόλουθα:

(α) πληροφορίες σχετικά με τους κύριους δείκτες κινδύνου συμμόρφωσης που παρακολουθούνται από το ίδρυμα·

(β) σημαντικούς τομείς συμμόρφωσης και την πορεία σχετικών ερευνών που έχουν διεξαχθεί ή άλλων ενεργειών που έχουν αναληφθεί·

(γ) επικαιροποιημένες πληροφορίες σχετικά με το επιχειρησιακό και ρυθμιστικό πλαίσιο του ιδρύματος για τον προσδιορισμό των εξελίξεων που δύναται να επηρεάσουν τις τρέχουσες και μελλοντικές υποχρεώσεις συμμόρφωσης του ιδρύματος·

(δ) σύντομη ενημέρωση σχετικά με τα πιο πάνω για κάθε θυγατρική στην Κύπρο και το εξωτερικό καθώς και για τα υποκαταστήματα·

(ε) σημαντικές ποινές ή άλλα πειθαρχικά μέτρα που λαμβάνονται από τις εποπτικές αρχές και

αφορούν το ίδρυμα ή οποιονδήποτε υπάλληλο.

(2) Ο επικεφαλής του τμήματος κανονιστικής συμμόρφωσης υποβάλλει ετήσια έκθεση προς το διοικητικό όργανο εντός δύο μηνών από τη λήξη κάθε έτους, μέσω της επιτροπής ελέγχου, αντίγραφο της οποίας κοινοποιείται στον διευθύνοντα σύμβουλο, με τις ακόλουθες ελάχιστες πληροφορίες:

(α) περιγραφή του πλαισίου κανονιστικής συμμόρφωσης, συμπεριλαμβανομένης της οργάνωσης και λειτουργίας του τμήματος κανονιστικής συμμόρφωσης, και της υφιστάμενης διαδικασίας διαχείρισης της κανονιστικής συμμόρφωσης·

(β) το πρόγραμμα κανονιστικής συμμόρφωσης για το υπό επισκόπηση έτος·

(γ) τις εργασίες κανονιστικής συμμόρφωσης που διεκπεραιώθηκαν κατά τη διάρκεια του έτους·

(δ) συνοπτική περιγραφή, σε συνδυασμό με εκτενείς παρατηρήσεις, των σημαντικότερων ευρημάτων και αδυναμιών που εντοπίστηκαν από την εξέταση της πολιτικής και των διαδικασιών κανονιστικής συμμόρφωσης που διεξήχθη κατά το υπό επισκόπηση έτος, και υποβολή εισηγήσεων για λήψη διορθωτικών μέτρων·

(ε) επικαιροποιημένη σύνοψη της προόδου που επιτεύχθηκε και εφαρμογή των διορθωτικών μέτρων που λήφθηκαν για την αντιμετώπιση οποιωνδήποτε αδυναμιών συμμόρφωσης και ευρημάτων που εντοπίστηκαν στα πορίσματα των διαφόρων εκθέσεων των τμημάτων ελέγχου, των εξωτερικών ελεγκτών και συμβούλων, καθώς και των εκθέσεων των εποπτικών αρχών·

(στ) αξιολόγηση των σημαντικότερων κίνδυνων συμμόρφωσης που αντιμετωπίζει το ίδρυμα με βάση τους δείκτες κινδύνου και τα μέτρα που λαμβάνονται για αντιμετώπισή τους·

(ζ) επικαιροποιημένη σύνοψη των αλλαγών και εξελίξεων στις νομικές, ρυθμιστικές και επιχειρησιακές απαιτήσεις που πραγματοποιήθηκαν κατά τη διάρκεια του έτους και που αναμένεται να πραγματοποιηθούν στο εγγύς μέλλον και τα μέτρα που λαμβάνονται ή πρόκειται να ληφθούν για διασφάλιση της συμμόρφωσης με τις τροποποιημένες απαιτήσεις·

(η) λεπτομέρειες σχετικά με τα πιο πάνω για κάθε θυγατρική στην Κύπρο και το εξωτερικό καθώς και για τα υποκαταστήματα·

(θ) επικαιροποιημένη σύνοψη της σημαντικότερης αλληλογραφίας με τις αρμόδιες αρχές·

(ι) το πρόγραμμα κανονιστικής συμμόρφωσης και το σχέδιο δράσης του τμήματος κανονιστικής συμμόρφωσης για το επόμενο έτος.

Υποτμήμα 3.4 – Τμήμα ασφάλειας πληροφοριών

Ρόλος και ευθύνες του τμήματος ασφάλειας πληροφοριών.

95. (1) Το τμήμα ασφάλειας πληροφοριών είναι υπεύθυνο και υπόλογο για την ανάπτυξη και την υλοποίηση του πλαισίου ασφάλειας των πληροφοριών· κατ' ελάχιστο το τμήμα οφείλει να–

(α) παρέχει συμβουλές και εισηγήσεις προς το διοικητικό όργανο για την ανάπτυξη πολιτικής ασφάλειας πληροφοριών, που να συμβαδίζει με το μέγεθος του ιδρύματος και την πολυπλοκότητα των δραστηριοτήτων και των δικτύων διανομής πληροφοριών του·

(β) παρέχει συμβουλές και εισηγήσεις προς τα ανώτατα διοικητικά στελέχη για την ανάπτυξη και εφαρμογή του προγράμματος ασφάλειας πληροφοριών του ιδρύματος, υπό τη μορφή πολιτικών ασφάλειας, προτύπων, κατευθυντήριων γραμμών, διαδικασιών και διεργασιών· οφείλει να διασφαλίζει, μεταξύ άλλων, την ανάπτυξη, τεκμηρίωση και εφαρμογή:

(i) πολιτικών ταξινόμησης πληροφοριών και προτύπων που σχεδιάστηκαν για να παρέχουν στους ιδιοκτήτες των πληροφοριών οδηγίες για τον τρόπο κατάλληλης διαβάθμισης των πληροφοριών που έχει στην κατοχή του το ίδρυμα και καθορισμού του κατάλληλου επιπέδου προστασίας και των διαδικασιών για την κατάλληλη δημοσιοποίηση, τροποποίηση, αφαίρεση ή καταστροφή πληροφοριών που έχει στην κατοχή του το ίδρυμα·

(ii) πολιτικών και διαδικασιών για τη διασφάλιση της συμμόρφωσης των υπό προμήθεια, υπό

ανάπτυξη και υπό συντήρηση πληροφοριακών συστημάτων , με την πολιτική ασφάλειας πληροφοριών του ιδρύματος·

(iii) πολιτικών και διαδικασιών για τη διαχείριση των δικαιωμάτων πρόσβασης στα πληροφορικά συστήματα του ιδρύματος·

(iv) διαδικασιών αντιμετώπισης περιστατικών ασφάλειας, εντοπισμού και παραπομπής σε ανώτερο επίπεδο και μίας επίσημης διαδικασίας για την ανάπτυξη, τεκμηρίωση και εφαρμογή σχεδίων για λήψη διορθωτικών μέτρων για την αποφυγή επανάληψης παρόμοιων θεμάτων·

(v) κατάλληλων δικλείδων ασφαλείας σε υφιστάμενες και νέες λειτουργικές διαδικασίες, συμπεριλαμβανομένου του κατάλληλου διαχωρισμού καθηκόντων·

(vi) διαδικασιών για την προστασία των πληροφοριών του ιδρύματος κατά τη διάρκεια και μετά τη διακοπή των συμβάσεων με προμηθευτές και τρίτα μέρη, αλλά και με τη λήξη εργοδότησης, μακροχρόνιας άδειας απουσίας, μετακίνησης ή αλλαγής καθηκόντων·

(vii) πολιτικών και διαδικασιών που αποσκοπούν στην πρόληψη της μη εξουσιοδοτημένης φυσικής πρόσβασης σε πληροφορίες που έχει στην κατοχή του το ίδρυμα και των ζημιών από ανθρώπινα ή φυσικά αίτια.

(γ) επιβλέπει τη διάδοση και εφαρμογή του προγράμματος ασφάλειας πληροφοριών εντός του ιδρύματος·

(δ) συνεργάζεται με τις επιχειρησιακές μονάδες στήριξης του ιδρύματος καθώς και με άλλες μονάδες ελέγχου για την αποτελεσματική εφαρμογή των αρχών ασφάλειας στην ανάπτυξη των πολιτικών και διαδικασιών τους· η αλληλεπίδραση μεταξύ των επιχειρησιακών μονάδων και μονάδων στήριξης και των άλλων μονάδων ελέγχου και του τμήματος ασφάλειας πληροφοριών διευκολύνει την επίτευξη του στόχου που θέλει όλο το προσωπικό του ιδρύματος να φέρει ευθύνη για την προστασία των εμπιστευτικών και ιδιόκτητων πληροφοριών του ιδρύματος·

(ε) αναπτύσσει και εφαρμόζει, σε συνεργασία με τη λειτουργία διαχείρισης κινδύνων, πρόγραμμα αξιολόγησης και διαχείρισης κινδύνων της ασφάλειας πληροφοριών ·

(στ) συμμετέχει στις δραστηριότητες που απαιτούνται για την εφαρμογή αποτελεσματικών δικλείδων ασφαλείας στις υποδομές πληροφορικής του ιδρύματος και παρέχει κατευθυντήριες γραμμές στη μονάδα πληροφορικής που είναι αρμόδια για τη λειτουργία των συστημάτων πληροφορικής και δικτύων του ιδρύματος

(ζ) σχεδιάζει, οργανώνει και συντονίζει τις δραστηριότητες αξιολόγησης της ασφάλειας πληροφοριών σε ολόκληρο το ίδρυμα·

(η) παρακολουθεί τη συμμόρφωση με τις πολιτικές ασφάλειας των πληροφοριών, τα πρότυπα, τις κατευθυντήριες γραμμές, διεργασίες και διαδικασίες.

(2) Το τμήμα ασφάλειας πληροφοριών συμμετέχει ενεργά στην ανάπτυξη και εφαρμογή ενός προγράμματος εκπαίδευσης και κατάρτισης για θέματα που σχετίζονται με την ασφάλεια των πληροφοριών και του ιδιωτικού απορρήτου για όλους τους εργαζόμενους του ιδρύματος, συμπεριλαμβανομένων των ανώτατων διοικητικών στελεχών.

Απαιτήσεις για υποβολή εκθέσεων.

96. Ο επικεφαλής του τμήματος ασφάλειας πληροφοριών υποβάλλει ετήσια έκθεση προς το διοικητικό όργανο, εντός προθεσμίας δύο μηνών από το τέλος κάθε έτους, μέσω της επιτροπής κινδύνου, αντίγραφο της οποίας κοινοποιείται στον διευθύνοντα σύμβουλο· η έκθεση καλύπτει, τουλάχιστον, τα ακόλουθα:

(α) σύνοψη των σημαντικότερων κινδύνων ασφάλειας των πληροφοριών που αντιμετωπίζει το ίδρυμα κατά το χρόνο υποβολής των εκθέσεων·

(β) κατάλογο όλων των σημαντικών περιστατικών ασφάλειας των πληροφοριών που έλαβαν χώρα κατά τη διάρκεια του έτους και των διορθωτικών μέτρων που λαμβάνονται για πρόληψη της επανάληψης παρόμοιων περιστατικών·

(γ) τυχόν σημαντικές ενέργειες που λήφθηκαν το προηγούμενο έτος για βελτίωση των αδυναμιών

στο περιβάλλον ασφάλειας πληροφοριών· και

(δ) τυχόν εκκρεμή θέματα που θέτουν σε κίνδυνο την ασφάλεια πληροφοριών του ιδρύματος.

Υποτμήμα 3.5 – Τμήμα εσωτερικής επιθεώρησης

Ρόλος και ευθύνες του τμήματος εσωτερικής επιθεώρησης.

97. (1) Το τμήμα εσωτερικής επιθεώρησης εκτελεί τις αποστολές ελέγχου σύμφωνα με την παράγραφο 99 με δική του πρωτοβουλία σε όλους τους τομείς και τις λειτουργίες του ιδρύματος, συμπεριλαμβανομένων των εργασιών του ιδρύματος που ανατέθηκαν σε τρίτους, σύμφωνα με το πλάνο ελέγχου που ετοιμάζεται από τον επικεφαλής του τμήματος και εγκρίνεται από το διοικητικό όργανο σύμφωνα με την παράγραφο 101, για την παροχή ανεξάρτητης διαβεβαίωσης προς το διοικητικό όργανο σε σχέση με θέματα όπως:

(α) η καταλληλότητα, επάρκεια και αποτελεσματικότητα του πλαισίου διακυβέρνησης·

(β) τα συνολικά μέσα με τα οποία το ίδρυμα διαχειρίζεται και μετριάζει τους κινδύνους για διαφύλαξη των περιουσιακών του στοιχείων, και επιδιώκει να αποτρέψει την απάτη, υπεξαίρεση, ή την εσφαλμένη χρήση των εν λόγω περιουσιακών στοιχείων·

(γ) την αξιοπιστία, ακεραιότητα και πληρότητα των λογιστικών εκθέσεων, των χρηματοοικονομικών εκθέσεων και διαχείρισης πληροφοριών και των πληροφοριακών συστημάτων·

(δ) το σχεδιασμό και την επιχειρησιακή αποτελεσματικότητα των μεμονομένων ελέγχων και των τμημάτων ελέγχου του ιδρύματος σε σχέση με τα προαναφερθέντα θέματα, καθώς και επι του συνόλου των εν λόγω ελέγχων·

(ε) άλλα θέματα που δύναται να ζητηθούν από το διοικητικό όργανο, τα ανώτατα διοικητικά στελέχη ή την Κεντρική Τράπεζα· και

(στ) άλλα θέματα τα οποία το τμήμα εσωτερικής επιθεώρησης απαιτεί επανεξέταση για εκπλήρωση της αποστολής του, σύμφωνα με το καταστατικό εσωτερικού ελέγχου.

(2) Το τμήμα εσωτερικής επιθεώρησης συμμετέχει στο σχεδιασμό, επιλογή, εφαρμογή ή λειτουργία συγκεκριμένων μέτρων ελέγχου· το τμήμα εσωτερικής επιθεώρησης δύναται να παρέχει στοιχεία για θέματα σχετικά με κινδύνους και εσωτερικούς ελέγχους κατόπιν αιτήματος των ανώτατων διοικητικών στελεχών νοουμένου ότι η ανεξαρτησία της αποστολής του τμήματος δεν τίθεται υπό αμφισβήτηση.

Καταστατικό εσωτερικής επιθεώρησης

98. (1) Τηρουμένων των προνοιών της παραγράφου 82, το καταστατικό εσωτερικής επιθεώρησης εξουσιοδοτεί το τμήμα εσωτερικής επιθεώρησης, όπου σχετίζεται με την εκτέλεση των αποστολών του, να προβαίνει σε άμεση επικοινωνία με οποιοδήποτε μέλος του προσωπικού, να εξετάζει οποιαδήποτε δραστηριότητα ή οντότητα του ιδρύματος συμπεριλαμβανομένων άλλων τμημάτων ελέγχου, και να έχει πλήρη και άνευ όρων πρόσβαση σε οποιαδήποτε αρχεία, φακέλους, δεδομένα και φυσικές εγκαταστάσεις του ιδρύματος, συμπεριλαμβανομένης της πρόσβασης σε πληροφοριακά συστήματα διοίκησης και αρχεία και πρακτικά των συναντήσεων όλων των συμβουλευτικών οργάνων και οργάνων λήψης αποφάσεων.

(2) Το καταστατικό εσωτερικής επιθεώρησης καθορίζει επίσης διαδικασίες για το συντονισμό του τμήματος εσωτερικής επιθεώρησης με τους εξωτερικούς ελεγκτές.

Αποστολές ελέγχου.

99. (1) Το τμήμα εσωτερικής επιθεώρησης διεξάγει τις αποστολές που απαιτείται για εκπλήρωση των καθηκόντων του για την παροχή διαβεβαίωσης σύμφωνα με την παράγραφο 97, μέσω τακτικών και ειδικών ελέγχων, τόσο αυτών που ανακοινώνονται όσο και αυτών που διεξάγονται αιφνιδιαστικά.

(2) Οι ακόλουθες δραστηριότητες ελέγχου περιλαμβάνονται, τουλάχιστον, στο πεδίο εφαρμογής των αποστολών εσωτερικής επιθεώρησης:

(α) αξιολόγηση της καταλληλότητας και επάρκειας της οργανωτικής δομής και της διαχείρισης των ανθρώπινων πόρων και του βαθμού στον οποίο το ίδρυμα έχει θεσπίσει κατάλληλες πολιτικές και διαδικασίες εταιρικής διακυβέρνησης·

(β) αξιολόγηση του βαθμού αποτελεσματικής αξιοποίησης από τα συλλογικά όργανα του

ιδρύματος, καθώς και από τις επιχειρησιακές μονάδες και τμήματα ελέγχου, των μέσων και των πόρων που διαθέτουν, συμμόρφωσης με τις οδηγίες και διαδικασίες που έχουν οριστεί επίσημα, κατά πόσο δόθηκε η δέουσα προσοχή για διασφάλιση της πληρότητας και ακρίβειας των πληροφοριών και κατά πόσο προβλέπεται η ενσωμάτωση σε όλες τις διαδικασίες και συναλλαγές που διεξάγονται των κατάλληλων μηχανισμών πρόληψης και ελέγχου κινδύνων·

(γ) αξιολόγηση της αποτελεσματικότητας, επάρκειας και τήρησης των διαδικασιών διαχείρισης και συμμόρφωσης κινδύνων·

(δ) αξιολόγηση της ακεραιότητας των πληροφοριακών συστημάτων, συμπεριλαμβανομένων των συστημάτων διαχείρισης κινδύνων και λογιστικών πληροφοριών, καθώς και η ακρίβεια, αξιοπιστία και η πληρότητα των πληροφοριακών στοιχείων που χρησιμοποιούνται ή εξάγονται σύμφωνα με τις αρχές που αναφέρονται στο Παράρτημα 3·

(ε) αξιολόγηση των συστημάτων και διαδικασιών που διέπουν την εξαγωγή αξιόπιστων, ολοκληρωμένων και επικαιροποιημένων οικονομικών, διοικητικών και κανονιστικών πληροφοριών·

(στ) αξιολόγηση της ασφάλειας πληροφοριών κάθε είδους, που βρίσκονται σε οποιοδήποτε μέσο συμπεριλαμβανομένων των πληροφοριών σε έντυπη μορφή·

(ζ) αξιολόγηση των διαδικασιών προμηθειών/προσφορών και των πραγματοποιηθείσεων προσφορών·

(η) αξιολόγηση της πληρότητας και αποτελεσματικότητας της πολιτικής ανάθεσης εργασιών σε τρίτους·

(θ) αξιολόγηση της πληρότητας και επάρκειας των σχεδίων συνέχειας εργασιών του ιδρύματος και ανάκαμψης από καταστροφή των πληροφοριακών συστημάτων·

(ι) αξιολόγηση της πληρότητας και της επάρκειας της πολιτικής ασφάλειας πληροφοριών του ιδρύματος, συμπεριλαμβανομένης της ασφάλειας Πληροφοριακών Συστημάτων·

(ια) αξιολόγηση της διαδικασίας εκτίμησης της Εσωτερικής Διαδικασίας Αξιολόγησης της Κεφαλαιακής Επάρκειας (ΕΔΑΚΕ) του ιδρύματος σε σχέση με το προφίλ κινδύνου, των παραμέτρων στις οποίες το ίδρυμα έχει βασίσει τους υπολογισμούς του αναφορικά με την κεφαλαιακή επάρκεια και την εξέταση της διαδικασίας των ασκήσεων προσομοίωσης ακραίων καταστάσεων αναφορικά με την κεφαλαιακή βάση του ιδρύματος, λαμβάνοντας υπόψη τη συχνότητα διεξαγωγής των εν λόγω ασκήσεων, το σκοπό τους, τη λογική των σεναρίων, τις υποκείμενες παραδοχές και την αξιοπιστία των διαδικασιών που χρησιμοποιούνται·

(ιβ) αξιολόγηση σε ποιο βαθμό εφαρμόζονται οι διαδικασίες για την έγκριση νέων προϊόντων εφαρμόζονται σύμφωνα με τις διαδικασίες έγκρισης νέου προϊόντος και κατά πόσο οι διαδικασίες αυτές είναι επαρκείς και αποτελεσματικές·

(ιγ) αξιολόγηση της καταλληλότητας της πολιτικής αποδοχών σε σχέση με τους προκαθορισμένους στόχους που τίθενται από το νομικό και ρυθμιστικό πλαίσιο, καθώς και τις πιθανές συνέπειες της πολιτικής στην ανάληψη και διαχείριση των κινδύνων·

(ιδ) αξιολόγηση της επάρκειας και της δυνατότητας εφαρμογής των διαδικασιών επανάκτησης (claw back arrangements), καθώς και της δομής των πρόσθετων φιλοδορημάτων σε σχέση με το αναβαλλόμενου στοιχείο πληρωμής και της σύνδεσής του με μελλοντικές αποδόσεις εντός ενός εύλογου χρονικού ορίζοντα.

(ιε) αξιολόγηση της επάρκειας και αποτελεσματικότητας των τμημάτων κανονιστικής συμμόρφωσης, διαχείρισης κινδύνων και ασφάλειας πληροφοριών.

Σχέδιο ελέγχου.

100. (1) Το πρόγραμμα ελέγχου θα πρέπει να έχει ως βάση την αξιολόγηση των κινδύνων, να δυναμική και στόχο να διασφαλίζει ότι όλες οι οντότητες και όλες οι δραστηριότητες του ιδρύματος ελέγχονται τουλάχιστο μία φορά εντός μίας κατάλληλα καθορισμένης χρονικής περιόδου. Το πρόγραμμα ελέγχου θα πρέπει να είναι ένα μέσο για την αξιολόγηση της επάρκειας και

αποτελεσματικότητας του πλαισίου εσωτερικού ελέγχου.

(2) Το πρόγραμμα ελέγχου διασφαλίζει τουλάχιστον:

(α) τη διεξαγωγή ελέγχων της επιθεώρησης της πιστοληπτικής ικανότητας σε κατάλληλη κλίμακα σε ετήσια βάση ως μέσο για αξιολόγηση:

(i) της επάρκειας και αποτελεσματικότητας, και τήρησης των διαδικασιών και της πολιτικής χορήγησης πιστώσεων, συμπεριλαμβανομένων των διαδικασιών αξιολόγησης των αιτήσεων για την παροχή πιστώσεων και έγκρισης των πιστωτικών διευκολύνσεων, καθώς και της διαχείρισης και παρακολούθησης του μηχανισμού των εξασφαλίσεων και διασφάλισης της συμμόρφωσης με τις ρήτρες πιστώσεων, σύμφωνα με την Οδηγία της Κεντρικής Τράπεζας περί των Διαδικασιών Χορήγησης Νέων Πιστωτικών Διευκολύνσεων και των Διαδικασιών Αναθεώρησης Υφιστάμενων Πιστωτικών Διευκολύνσεων·

(ii) της ορθής εφαρμογής του συστήματος εσωτερικής αξιολόγησης της πιστοληπτικής ικανότητας που αναπτύχθηκε από το ίδρυμα σύμφωνα με τις οδηγίες της Κεντρικής Τράπεζας σε σχέση με τη διαχείριση πιστωτικού κινδύνου·

(iii) της καταλληλότητας, επάρκειας και ορθής εφαρμογής της πολιτικής για τη δημιουργία προβλέψεων για επισφαλείς απαιτήσεις καθώς και της επάρκειας των προβλέψεων και πληρότητας της μεθοδολογίας και διαδικασίας για τον υπολογισμό των απομειώσεων των δανείων, συμπεριλαμβανομένων των κριτηρίων επιλογής των δανείων για σκοπούς ελέγχου της απομείωσης·

(iv) της πληρότητας της μεθοδολογίας και διαδικασίας για τον υπολογισμό της απομείωσης λοιπών στοιχείων ενεργητικού, καθώς και της επάρκειας των σχετικών προβλέψεων για επισφαλείς απαιτήσεις και διαγραφές απομειώσης·

(v) της επάρκειας των διαδικασιών παρακολούθησης και χειρισμού των μη εξυπηρετούμενων και προβληματικών δανείων·

(vi) της επάρκειας και αποτελεσματικότητας των εσωτερικών επιθεωρήσεων·

(β) την επάρκεια και τήρηση των διαδικασιών χορήγησης πιστωτικών διευκολύνσεων σε μέλη του διοικητικού οργάνου και των συνδεδεμένων με αυτούς προσώπων, σε μεγαλομετόχους και των συνδεδεμένων με αυτούς προσώπων, αξιολογείται σε ετήσια βάση·

(γ) τη διεξαγωγή σε ετήσια βάση ειδικών επιθεωρήσεων κατάλληλης κλίμακας, ως μέσο για την αξιολόγηση της επάρκειας και αποτελεσματικότητας:

(i) του πλαισίου διαχείρισης κινδύνων·

(ii) των πληροφοριακών συστημάτων· και

(iii) της ασφάλειας των πληροφοριών·

(δ) την αποτελεσματικότητα και επάρκεια της πολιτικής, των διαδικασιών και ελέγχων για την παρεμπόδιση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και χρηματοδότησης της τρομοκρατίας, καθώς και το επίπεδο συμμόρφωσης με τις διατάξεις του περί της Παρεμπόδισης και Καταπολέμησης της Νομιμοποίησης Εσόδων από Παράνομες Δραστηριότητες Νόμου του 2007 όπως εκάστοτε τροποποιείται ή αντικαθίσταται, και της Οδηγίας για την Παρεμπόδιση Ξεπλύματος Παράνομου Χρήματος και Χρηματοδότησης της Τρομοκρατίας του 2013 αξιολογείται σε ετήσια βάση, σύμφωνα με τις διατάξεις της εν λόγω Οδηγίας.

(ε) την αξιολόγηση τουλάχιστον κάθε τρία χρόνια της επάρκειας και πληρότητας της πολιτικής ανάθεσης εργασιών σε τρίτους και λήψης διορθωτικών μέτρων παρακολούθησης σε ετήσια βάση· επίσης το τμήμα εσωτερικής επιθεώρησης διεξάγει ετήσιες αξιολογήσεις της ανάθεσης εργασιών σε τρίτους ή δραστηριοτήτων σε κατάλληλη κλίμακα, ως μέσο για την αξιολόγηση της τήρησης της πολιτικής ανάθεσης εργασιών σε τρίτους δίνοντας προτεραιότητα στην ανάθεση σημαντικών υπηρεσιών ή δραστηριοτήτων σε τρίτους·

(στ) την αξιολόγηση τουλάχιστον σε ετήσια βάση της εφαρμογής της πολιτικής αποδοχών από τα ανώτατα διοικητικά στελέχη και τη συμμόρφωσή της με τις σχετικές πολιτικές και διαδικασίες που υιοθετούνται από το διοικητικό όργανο .

Υποβολή εκθέσεων στο διοικητικό όργανο.

101. (1) Ο επικεφαλής του τμήματος εσωτερικής επιθεώρησης υποβάλλει στο διοικητικό όργανο μέσω της επιτροπής ελέγχου, τουλάχιστον σε τριμηνιαία βάση, έκθεση των σημαντικότερων παρατηρήσεων που απορρέουν από τους ελέγχους που πραγματοποιήθηκαν μετά την τελευταία έκθεση προς το διοικητικό όργανο, καθώς και εισηγήσεων για αντιμετώπιση τυχόν αδυναμιών που εντοπίστηκαν· όταν εντοπίζονται σημαντικές αδυναμίες, ο επικεφαλής του τμήματος εσωτερικής επιθεώρησης έχει την ευθύνη να ενημερώνει το συντομότερο πρακτικά δυνατόν το διοικητικό όργανο.

(2) Ο επικεφαλής του τμήματος εσωτερικής επιθεώρησης υποβάλλει ετήσια έκθεση προς το διοικητικό όργανο, εντός δύο μηνών από τη λήξη κάθε έτους, μέσω της επιτροπής ελέγχου, αντίγραφο της οποίας κοινοποιείται στον διευθύνοντα σύμβουλο, με τις ακόλουθες ελάχιστες πληροφορίες:

(α) πρόγραμμα ελέγχου εγκεκριμένο από το διοικητικό όργανο για το υπό ανασκόπηση έτος και το σκεπτικό για τυχόν αποκλίσεις στην εφαρμογή του·

(β) περίληψη, σε συνδυασμό με εκτεταμένες παρατηρήσεις, των σημαντικότερων ευρημάτων και αδυναμιών που εντοπίστηκαν από τις επιθεωρήσεις ρουτίνας και τους ειδικούς ελέγχους που διεξήχθηκαν κατά το υπό επισκόπηση έτος για κάθε τομέα που ελέγχθηκε·

(γ) επικαιροποιημένη σύνοψη της προόδου που επιτεύχθηκε στην εκτέλεση και εφαρμογή των διορθωτικών μέτρων που λαμβάνονται για την αντιμετώπιση οποιωνδήποτε αδυναμιών και των ευρημάτων που εντοπίστηκαν σε διάφορες εκθέσεις επιθεώρησης των εσωτερικών επιθεωρητών και των εξωτερικών ελεγκτών, καθώς και των εποπτικών αρχών·

(δ) επαλήθευση σε δειγματοληπτική βάση της ακρίβειας των αναφορών που υποβάλλονται στην Κεντρική Τράπεζα, ειδικά του Κοινού Πλαισίου Πληροφόρησης (COREP), της Χρηματοοικονομικής Πληροφόρησης (FINREP), των μεγάλων χρηματοδοτικών ανοιγμάτων, της προληπτικής ρευστότητας και των πιστωτικών διευκολύνσεων σε μέλη του διοικητικού οργάνου, μεγαλομετόχους και συνδεδεμένα τους πρόσωπα·

(ε) έλεγχος και σχέδιο δράσης για το επόμενο έτος.

Συνεργασία του τμήματος εσωτερικής επιθεώρησης με την Κεντρική Τράπεζα.

102. Η συνεργασία του επικεφαλής του τμήματος εσωτερικής επιθεώρησης με την Κεντρική Τράπεζα οφείλει να καλύπτει τα ακόλουθα για σκοπούς της παραγράφου 78(3)(α)-(ι), με βάση τα αποτελέσματα των αξιολογήσεων που διενεργήθηκαν:

(α) επάρκεια και αποτελεσματικότητα των διεργασιών του ιδρύματος για τον καθορισμό στόχων και στρατηγικών αποφάσεων·

(β) ποιότητα και σημασία των δομών και διαδικασιών διαχείρισης και διακυβέρνησης·

(γ) την κεφαλαιακή βάση και την κατάσταση ρευστότητας του ιδρύματος και τις διαδικασίες και μεθόδους του για αναγνώριση, παρακολούθηση, έλεγχο και υποβολή εκθέσεων για τους σημαντικούς κινδύνους συμπεριλαμβανομένων των κινδύνων που αναφέρονται στις παραγράφους 63 έως 71·

(δ) του επιχειρηματικού μοντέλου του ιδρύματος, συμπεριλαμβανομένων των κινδύνων στις επιχειρηματικές δραστηριότητες του ιδρύματος, διαδικασίες και λειτουργίες και την επάρκεια της παρακολούθησης και εποπτείας των κινδύνων αυτών όπως:

(i) εκτέλεση και εφαρμογή της διαχείρισης κινδύνων και των μεθόδων αξιολόγησης των κινδύνων όπως εφαρμόζεται για σημαντικούς κινδύνους, συμπεριλαμβανομένων των κινδύνων που αναφέρονται στις παραγράφους 63 έως 71·

(ii) καταλληλότητα και επάρκεια της πολιτικής των προβλέψεων για επισφαλείς απαιτήσεις καθώς και της επάρκειας των προβλέψεων·

(iii) πληρότητα της μεθοδολογίας απομείωσης/ διαγραφής·

(iv) σημαντικές συναλλαγές·

(v) χειρισμός μη εξυπηρετούμενων και προβληματικών δανείων·

(vi) απάτες·

(vii) διευθετήσεις της ανάθεσης εργασιών σε τρίτους·

(ε) θέματα δεοντολογίας όπως:

(i) διαχείριση της σύγκρουσης συμφερόντων·

(ii) τήρηση των κανόνων στην παροχή υπηρεσιών προς τους πελάτες·

(iii) διαδικασίες και έλεγχοι καταπολέμησης της νομιμοποίησης εσόδων από παράνομες δραστηριότητες·

(στ) θέματα που σχετίζονται με εσωτερικούς ελέγχους και επάρκεια και αποτελεσματικότητα των άλλων τμημάτων ελέγχου.

Προσόντα και δεξιότητες και επαγγελματική επιμέλεια του προσωπικού εσωτερικής επιθεώρησης.

103. (1) Πρόσωπο που διορίζεται ως εσωτερικός επιθεωρητής πρέπει να διαθέτει την απαραίτητη επαγγελματική ικανότητα και τη δέουσα επαγγελματική επιμέλεια για την αποτελεσματική εκτέλεση των καθηκόντων του/της.

(2) Ο εσωτερικός επιθεωρητής πρέπει, τουλάχιστον, να διαθέτει γνώση, εμπειρία και ικανότητα για την –

(α) εφαρμογή των κατάλληλων μεθοδολογιών ελέγχου, εργαλείων και τεχνικών για:
(i) τη συλλογή και επεξεργασία πληροφοριών· και
(ii) την εξέταση και αξιολόγηση των τεκμηρίων των ελέγχων· και

(β) επικοινωνία κατά σαφή και αποτελεσματικό τρόπο με τα ενδιαφερόμενα μέρη του τμήματος εσωτερικής επιθεώρησης.

(3) Ο εσωτερικός επιθεωρητής οφείλει να –

(α) ενεργεί με ακεραιότητα, διεκπεραιώνει τα καθήκοντα του/της κατά τρόπο ειλικρινή και επαγγελματικό και ενημερώνει τον επικεφαλής του τμήματος εσωτερικής επιθεώρησης, εάν η ικανότητα του/της να διεξάγει μια αποστολή ελέγχου τεθεί υπό αμφισβήτηση·

(β) να επιδεικνύει επιμέλεια αναφορικά με την προστασία των πληροφοριών που αποκτώνται κατά την εκτέλεση των καθηκόντων του/της·

(γ) διασφαλίζει ότι η επαγγελματική του/της άποψη δεν επηρεάζεται από οποιαδήποτε προσωπικά ή επαγγελματικά συμφέροντα· οι εσωτερικοί επιθεωρητές που εργοδοτούνται εσωτερικά δεν πρέπει να εμπλέκονται σε επιθεώρηση δραστηριοτήτων για τις οποίες είχαν προηγουμένως την ευθύνη ως ότου παρέλθει μία επαρκώς μακρά χρονική περίοδος.

Υποτμήμα 4 – Εξωτερική αξιολόγηση της επάρκειας του πλαισίου εσωτερικού ελέγχου

Εξωτερική αξιολόγηση της επάρκειας του πλαισίου εσωτερικού ελέγχου.

104. (1) Τα ιδρύματα αναθέτουν τουλάχιστον μία φορά κάθε τρία χρόνια, την αξιολόγηση της επάρκειας και αποτελεσματικότητας του πλαισίου εσωτερικού ελέγχου σε εξωτερικό ελεγκτή, άλλο από τον εγκεκριμένο ελεγκτή του ιδρύματος, ο οποίος διαθέτει την απαραίτητη τεχνογνωσία για τη διεξαγωγή της απαιτούμενης αξιολόγησης σύμφωνα με τις πρόνοιες του Παραρτήματος 1.

(2) Η αξιολόγηση που αναφέρεται στην υποπαράγραφο (1) διεξάγεται τόσο σε ενοποιημένη βάση όσο και σε ατομική βάση.

(3) Τα ιδρύματα αλλάζουν τους εξωτερικούς ελεγκτές που αναφέρονται στην υποπαράγραφο (1), μετά από δύο διαδοχικές αξιολογήσεις.

ΜΕΡΟΣ XI

ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΕΠΙΧΕΙΡΗΣΙΑΚΗ ΣΥΝΕΧΕΙΑ

Πληροφοριακά συστήματα.

105. (1) Τα ιδρύματα διαθέτουν αποτελεσματικά και αξιόπιστα συστήματα πληροφορικής και επικοινωνιών που να καλύπτουν όλες τις σημαντικές δραστηριότητες τους.

(2) Τα ιδρύματα διασφαλίζουν ότι τα πληροφοριακά συστήματα εξάγουν έγκαιρες, ακριβής, συνεπής, πλήρης και σχετικές πληροφορία, ώστε να καθίσταται δυνατή –

(α) η κατάρτιση ετήσιων ή περιοδικών χρηματοοικονομικών ή μη χρηματοοικονομικών καταστάσεων για το οικονομικό προφίλ και το προφίλ κινδύνου του ιδρύματος, για εσωτερικούς ή εξωτερικούς σκοπούς·

(β) η αποτελεσματική διαχείριση της λήψης αποφάσεων και της εποπτείας·

(γ) η δημιουργία εμπεριστατωμένων απόψεων σχετικά με την αποτελεσματικότητα –

(i) του διοικητικού οργάνου, των ανώτατων διοικητικών στελεχών και των τμημάτων ελέγχου·

(ii) των πλαισίων διαχείρισης κινδύνων, συμμόρφωσης και εσωτερικού ελέγχου.

(3) Τα πληροφοριακά συστήματα, συμπεριλαμβανομένων εκείνων που φυλάσσουν και επεξεργάζονται δεδομένα σε ηλεκτρονική μορφή, θα πρέπει να είναι ασφαλή, να παρακολουθούνται ανεξάρτητα και να στηρίζονται από τις κατάλληλες ρυθμίσεις έκτακτης ανάγκης· τα ιδρύματα εφαρμόζουν το πλαίσιο αρχών για την ασφαλή και αποτελεσματική λειτουργία των πληροφοριακών και τεχνολογικών συστημάτων που περιγράφεται στο Παράρτημα 3.

(4) Τα ιδρύματα διασφαλίζουν ότι οι εγγραφές των συναλλαγών διατηρούνται κατά τρόπο συστηματικό και ασφαλή, για χρονικό διάστημα όχι μικρότερο των δέκα (10) ετών και κατά τρόπο που να διευκολύνεται η παραγωγή ελεγκτικών αρχείων καταγραφής και η ανασυγκρότηση όλων των συναλλαγών κατά χρονολογική σειρά, την επαλήθευση κάθε καταγραμμένης συναλλαγής σε σχέση με τα αρχικά τιμολόγια και την επικύρωση τυχόν αλλαγών στα υπόλοιπα των λογαριασμών σε σχέση με τα δικαιολογητικά στοιχεία που καλύπτουν όλες τις συναλλαγές που οδηγούν στις προαναφερθείσες αλλαγές.

Σχέδια έκτακτης ανάγκης και επιχειρησιακής συνέχειας.

106. (1) Τα ιδρύματα διαθέτουν επαρκή σχέδια έκτακτης ανάγκης και επιχειρησιακής συνέχειας που αποσκοπούν στη διασφάλιση ότι, σε περίπτωση σοβαρής διαταραχής των δραστηριοτήτων, θα είναι σε θέση να λειτουργήσουν σε συνεχή βάση και ότι οι ενδεχόμενες ζημιές θα είναι περιορισμένες· τα σχέδια έκτακτης ανάγκης και επιχειρησιακής συνέχειας θα πρέπει να υλοποιούνται σύμφωνα με το πλαίσιο αρχών για την ασφαλή και αποτελεσματική λειτουργία των πληροφοριακών και τεχνολογικών συστημάτων που περιγράφεται στο Παράρτημα 3.

(2) Τα ιδρύματα διασφαλίζουν ότι τα τμήματα ελέγχου συμμετέχουν ενεργά στην καθιέρωση, παρακολούθηση και εποπτεία των σχεδίων έκτακτης ανάγκης και επιχειρησιακής συνέχειας.

ΜΕΡΟΣ XII

ΔΙΑΦΑΝΕΙΑ

Ενδυνάμωση προσωπικού.

107. Τα ιδρύματα διασφαλίζουν ότι οι στρατηγικές και πολιτικές διαβιβάζονται σε όλο το αρμόδιο προσωπικό σε ολόκληρο το ίδρυμα κατά τρόπο σαφή και συνεπή, τουλάχιστον στο επίπεδο που απαιτείται για εκτέλεση των συγκεκριμένων καθηκόντων τους, μέσω γραπτών κατευθυντηρίων γραμμών, εγχειριδίων ή άλλων μέσων.

Δημοσιοποιήσεις.

108. (1) Τα ιδρύματα διασφαλίζουν ότι διαθέτουν τις κατάλληλες και επαρκείς πολιτικές, διαδικασίες και συστήματα για την έγκαιρη και ακριβής δημοσιοποίηση πληροφοριών στα ενδιαφερόμενα μέρη σχετικά με την υφιστάμενη κατάσταση τους και τις μελλοντικές προοπτικές.

(2) Οι πληροφορίες που δημοσιοποιούνται σχετικά με την υφιστάμενη οικονομική κατάσταση των ιδρυμάτων θα πρέπει να συμμορφώνονται με τις νομικές, ρυθμιστικές απαιτήσεις ή απαιτήσεις γνωστοποίησης του χρηματιστηρίου και θα πρέπει να είναι σαφείς, ακριβείς, σχετικές, έγκαιρες και προσβάσιμες.

(3) Απαιτείται όπως τα ιδρύματα δημοσιοποιούν στην ιστοσελίδα τους και ενημερώνουν άμεσα τις ακόλουθες πληροφορίες σχετικά με την εταιρική τους δομή και την εσωτερική διακυβέρνηση κατά τρόπο σαφή και ευδιάκριτο:

(α) την ιδιοκτησιακή δομή, τους μετόχους, το μερίδιο ιδιοκτησίας και τα δικαιώματα ψήφου, τους δικαιούχους μετόχους σε περίπτωση νομικών προσώπων, τη συμμετοχή των μετόχων στο διοικητικό όργανο ή σε ανώτατες διοικητικές θέσεις, τις βασικές δραστηριότητες·

(β) όταν ένα ίδρυμα δραστηριοποιείται σε δικαιοδοσίες που εμποδίζουν τη διαφάνεια ή μέσω πολύπλοκων δομών, τις πληροφορίες σχετικά με το σκοπό, τις στρατηγικές, τις δομές, τους κινδύνους και τους ελέγχους των δραστηριοτήτων αυτών·

(γ) τις δομές και πολιτικές διακυβέρνησης, συμπεριλαμβανομένων των στόχων του ιδρύματος, την οργανωτική δομή, τις ρυθμίσεις εσωτερικής διακυβέρνησης, τους δίαυλους αναφοράς.

(δ) τη δομή του διοικητικού οργάνου, το καταστατικό, τη σύνθεση, τη διαδικασία επιλογής, τα προσόντα μελών, τις διευθυντικές θέσεις μελών σε άλλους οργανισμούς, τις συμμετοχές σε συνεδριάσεις, τα κριτήρια ανεξαρτησίας, τη σύνθεση των μελών των επιτροπών, τις αρμοδιότητες και τους όρους εντολής των επιτροπών·

(ε) τη δομή των ανώτατων διοικητικών στελεχών, τις ευθύνες, τα προσόντα και την εμπειρία τους·

(στ) τις πληροφορίες σχετικά με το σχέδιο κινήτρων του ιδρύματος, τις πολιτικές αποδοχών, μισθών, ειδικών αποζημιώσεων, πρόσθετων αμοιβών, δικαιωμάτων προαιρετικής αγοράς μετοχών·

(ζ) τον κώδικα δεοντολογίας και εταιρικών αξιών και τη διαδικασία με την οποία εφαρμόζονται πρακτικά στον οργανισμό·

(η) τη φύση, έκταση, σκοπό και οικονομική υπόσταση των σημαντικών συναλλαγών με τα μέλη του διοικητικού οργάνου και των συνδεδεμένων μερών· οι πράξεις αυτές δημοσιεύονται εντός πέντε (5) εργάσιμων ημερών·

(θ) μια περιγραφή του πλαισίου εσωτερικού ελέγχου, του τρόπου οργάνωσης των τμημάτων ελέγχου, των κυριότερων εργασιών που επιτελούν·

(ι) όταν ένα ίδρυμα είναι κρατικό, τους γενικούς στόχους της κρατικής ιδιοκτησίας, συμπεριλαμβανομένων οποιονδήποτε ειδικών υποχρεώσεων του ιδρύματος σχετικά με την κοινωνική πολιτική του κράτους, το πώς χρηματοδοτούνται οι υποχρεώσεις αυτές καθώς και την πολιτική και το ρόλο του κράτους στην εσωτερική διακυβέρνηση του ιδρύματος.

(4) Τα ιδρύματα επεξηγούν στην ιστοσελίδα τους τον τρόπο συμμόρφωσης τους με τις απαιτήσεις των παραγράφων 5, 6 (α), 7 (3) - (4), 9, 9, 15 (2), 20 (1) - (2), 22 (1) - (2), 23 (3), 24 (1), 25 (1) (γ), 25 (5), 34 (2), 35, 42, 43, 44 και 49 έως 52 και του Παραρτήματος ΙΙΙ της περί της Αξιολόγησης για την Ικανότητα και Καταλληλότητα των Μελών Διοικητικού Οργάνου και των Διευθυντών των ΑΠΙ Οδηγία του 2014.

(5) Στις περιπτώσεις κατά τις οποίες ο υψηλός βαθμός ακρίβειας θα μπορούσε να καθυστερήσει την ανακοίνωση πληροφοριών ευαίσθητων στο χρόνο, το ίδρυμα θα πρέπει να λάβει μια απόφαση σχετικά με την εξεύρεση της κατάλληλης ισορροπίας μεταξύ χρονοδιαγράμματος και ακρίβειας, έχοντας υπόψη την απαίτηση για παρουσίαση αληθινής και δίκαιης εικόνας της κατάστασης του και παροχής μιας ικανοποιητικής εξήγησης για τυχόν καθυστέρηση· η εξήγηση αυτή δεν πρέπει να χρησιμοποιείται για να καθυστερεί η υποβολή των τακτικών απαιτούμενων αναφορών.

ΜΕΡΟΣ XIII

ΑΝΑΦΟΡΑ ΣΤΗΝ ΚΕΝΤΡΙΚΗ ΤΡΑΠΕΖΑ

Υποβολή αναφορών στην Κεντρική Τράπεζα.

109. (1) Τα ιδρύματα υποβάλουν στην Κεντρική Τράπεζα τα τελικά πρακτικά των συνεδριάσεων της επιτροπής ελέγχου και της επιτροπής κινδύνου, όπως προβλέπεται στην παράγραφο 7(4) εντός ενός (1) μηνός από την ημερομηνία της συνεδρίας.

(2) Τα ιδρύματα υποβάλλουν στην Κεντρική Τράπεζα, εντός τριών (3) μηνών από το τέλος κάθε έτους, τις ακόλουθες αναφορές και πληροφορίες, συνοδευόμενες με τις αντίστοιχες αξιολογήσεις των αρμόδιων επιτροπών του διοικητικού οργάνου και των σχετικών αποσπασμάτων από τα πρακτικά των συναντήσεων του διοικητικού οργάνου:

(α) ετήσια έκθεση για το πλαίσιο εσωτερικού ελέγχου που ετοιμάζεται από τον επικεφαλής του τμήματος εσωτερικής επιθεώρησης·

(β) ετήσια έκθεση για τη διαχείριση κινδύνων, η οποία ετοιμάζεται από τον επικεφαλής του τμήματος διαχείρισης κινδύνων·

(γ) ετήσια έκθεση για την κανονιστική συμμόρφωση, η οποία ετοιμάζεται από τον επικεφαλής του τμήματος κανονιστικής συμμόρφωσης·

(δ) ετήσια έκθεση για την ασφάλεια πληροφοριών, η οποία ετοιμάζεται από τον επικεφαλής του τμήματος ασφάλειας πληροφοριών·

(ε) έκθεση αξιολόγησης της απόδοσης του διοικητικού οργάνου στο σύνολό του, των επιτροπών και των επιμέρους μελών, η οποία ετοιμάζεται από το διοικητικό όργανο σύμφωνα με τις διατάξεις της παραγράφου 10 συμπεριλαμβανομένης της αξιολόγησης του προέδρου του διοικητικού οργάνου·

(3) Τα ιδρύματα υποβάλουν στην Κεντρική Τράπεζα την εξαμηνιαία έκθεση του λειτουργού ανάθεσης εργασιών σε τρίτους που φαίνεται στο Παράρτημα 2, εντός ενός (1) μηνός από τη λήξη της υπό αναφοράς περιόδου.

(4) Τα ιδρύματα υποβάλουν στην Κεντρική Τράπεζα σε ετήσια βάση μέχρι τις 30 Ιουνίου κάθε έτους –

(α) τις πληροφορίες που δημοσιοποιούνται σύμφωνα με τα κριτήρια για δημοσιοποίηση που ορίζονται στα σημεία (ζ), (η) και (θ) του άρθρου 450 (1) του Κανονισμού (ΕΕ) αριθ. 575/2013· για τους σκοπούς του παρόντος σημείου, τα ιδρύματα πρέπει να συμπληρώσουν και να υποβάλουν τα πρότυπα που προβλέπονται στα Παραρτήματα 1-3 στις κατευθυντήριες γραμμές της ΕΑΤ σχετικά με την άσκηση συγκριτικής αξιολόγησης των αποδοχών του 2014, όπως εκάστοτε τροποποιούνται ή αντικαθίστανται, σύμφωνα με τις απαιτήσεις που καθορίζονται στους Τίτλους ΙΙΙ και IV των εν λόγω κατευθυντήριες γραμμών της ΕΑΤ·

(β) τις πληροφορίες για τον αριθμό των φυσικών προσώπων ανά ίδρυμα που αμείβονται με 1 εκατομμύριο ευρώ ή περισσότερο ανά οικονομικό έτος, σε διαστήματα αμοιβών του 1 εκατομμυρίου ευρώ, συμπεριλαμβανομένων των αρμοδιοτήτων τους, της περιοχής των εργασιών που συμμετέχουν και τα κύρια στοιχεία του μισθού, φιλοδωρήματος, μακροπρόθεσμων επιβραβεύσεων και συνταξιοδοτικών εισφορών· για τους σκοπούς του παρόντος σημείου, τα ιδρύματα πρέπει να συμπληρώσουν και να υποβάλουν τα πρότυπα που προβλέπονται στο Παράρτημα 1 των κατευθυντήριων γραμμών ΕΑΤ για την άσκηση συλλογής δεδομένων σχετικά με τα υψηλά εισοδήματα του 2014, όπως εκάστοτε τροποποιείται ή αντικαθίσταται, σύμφωνα με τις απαιτήσεις που καθορίζονται στους Τίτλους ΙΙ και ΙΙΙ των εν λόγω κατευθυντήριων γραμμών·

(γ) την πολιτική πολυμορφίας όσον αφορά την επιλογή των μελών του διοικητικού οργάνου κατά τα προβλεπόμενα στη παράγραφο 9(1) που δημοσιοποιούνται σύμφωνα με το άρθρο 435(2)(γ) του Κανονισμού (ΕΕ) αριθ. 575/2013.

(5) Τα ιδρύματα υποβάλουν στην Κεντρική Τράπεζα εκθέσεις αξιολόγησης σχετικά με την επάρκεια και αποτελεσματικότητα του πλαισίου εσωτερικού ελέγχου σε ατομική και ενοποιημένη βάση οι οποίες συντάσσονται από τους εξωτερικούς ελεγκτές σύμφωνα με τις διατάξεις της παραγράφου 104.

(6) Τα ιδρύματα υποβάλουν στην Κεντρική Τράπεζα εκθέσεις αξιολόγησης σχετικά με τη σύνθεση και τις αρμοδιότητες του διοικητικού οργάνου και των επιτροπών του, οι οποίες ετοιμάζονται από εξωτερικό σύμβουλο σύμφωνα με τις διατάξεις της παραγράφου 10· η επόμενη έκθεση θα πρέπει να ετοιμαστεί και να υποβληθεί στην Κεντρική Τράπεζα μέχρι την 31η Δεκεμβρίου 2014 και οι επόμενες εκθέσεις θα πρέπει να υποβάλλονται μαζί με τις εκθέσεις που υποβάλλονται σύμφωνα με την υποπαράγραφο (1).

ΜΕΡΟΣ XIV
ΠΟΙΚΙΛΕΣ ΔΙΑΤΑΞΕΙΣ

Ημερομηνία έναρξης ισχύος.

110. Οι διατάξεις της παρούσας Οδηγίας τίθενται σε άμεση ισχύ.

Παράταση προθεσμίας για συμμόρφωση με τις διατάξεις της παρούσας Οδηγίας.

111. Τα Ιδρύματα εντός ενός (1) μηνός από την ημερομηνία έναρξης ισχύος της παρούσας Οδηγίας, ενημερώνουν την Κεντρική Τράπεζα, εάν δεν συμμορφώνονται με τις διατάξεις των παραγράφων 6(α), 9(3)-(4), 35(2) και 76(1) και υποβάλλουν στην Κεντρική Τράπεζα χρονοδιάγραμμα συμμόρφωσης το οποίο δεν υπερβαίνει το ένα έτος από την ημερομηνία έναρξης ισχύος της παρούσας Οδηγίας.

Συμμόρφωση με τις αρχές αποδοχών.

112. Τα ιδρύματα υποχρεούνται να εφαρμόζουν τις αρχές που καθορίζονται στο Μέρος VI για τις αποδοχές που παραχωρούνται για την παροχή υπηρεσιών ή για την απόδοση από το έτος 2014 και μετά, βάσει των συμβάσεων που έχουν συναφθεί είτε πριν ή μετά την ημερομηνία έναρξης ισχύος της παρούσας Οδηγίας.

Κατάργηση.

113. Η Οδηγία που εκδόθηκε από την Κεντρική Τράπεζα προς τις τράπεζες αναφορικά με το Πλαίσιο Αρχών Λειτουργίας και Κριτηρίων Αξιολόγησης της Οργανωτικής Δομής των τραπεζών, της Εσωτερικής Διακυβέρνησης και των Συστημάτων Εσωτερικού Ελέγχου του 2006 έως το 2012, καταργείται.

ΠΑΡΑΡΤΗΜΑ 1

(Παράγραφος 104)

ΠΕΡΙΕΧΟΜΕΝΟ ΤΗΣ ΕΚΘΕΣΗΣ

ΑΞΙΟΛΟΓΗΣΗΣ ΤΗΣ ΕΠΑΡΚΕΙΑΣ ΤΟΥ ΠΛΑΙΣΙΟΥ ΕΣΩΤΕΡΙΚΟΥ ΕΛΕΓΧΟΥ

ΠΟΥ ΕΤΟΙΜΑΖΕΤΑΙ ΑΠΟ ΤΟΥΣ ΕΞΩΤΕΡΙΚΟΥΣ ΕΛΕΓΚΤΕΣ

ΜΕΡΟΣ Ι

ΕΙΣΑΓΩΓΗ

1. (1) Η αξιολόγηση πρέπει να πραγματοποιείται σύμφωνα με τις βέλτιστες διεθνείς πρακτικές, προκειμένου να διασφαλιστεί ότι το σύστημα εσωτερικού ελέγχου πληροί τα πρότυπα που απαιτούνται από την παρούσα Οδηγία.

(2) Η αξιολόγηση της επάρκειας του πλαισίου εσωτερικού ελέγχου πρέπει να καλύπτει επιθεώρηση:

(α) του περιβάλλοντος ελέγχου·

(β) της διαδικασίας αξιολόγησης κινδύνων·

(γ) των μηχανισμών και δικλείδων ασφάλειας και ελέγχου·

(δ) των δικτύων επικοινωνίας και πληροφοριακών συστημάτων·

(ε) του ρόλου, των καθηκόντων και των αρμοδιοτήτων του διοικητικού οργάνου και των τμημάτων ελέγχου· και

(στ) της λειτουργίας, στελέχωσης των βασικών τμημάτων / διευθύνσεων / μονάδων του ιδρύματος, τους όρους εντολής τους, των διαδικασιών και των πληροφοριακών συστημάτων που χρησιμοποιούνται.

2. Πριν από την έναρξη των εργασιών, η επιτροπή ελέγχου του ιδρύματος πρέπει να καθορίζει τις μονάδες και τις θυγατρικές που θα συμπεριληφθούν στο πεδίο εφαρμογής της αξιολόγησης. Αυτό θα πρέπει να βασίζεται στην αρχή της αναλογικότητας, καθώς και σε άλλα ποιοτικά κριτήρια. Το πεδίο εφαρμογής της αξιολόγησης θα πρέπει να υποβληθεί εκ των προτέρων στην Κεντρική Τράπεζα.

3. Μετά την ολοκλήρωση της αξιολόγησης, οι εξωτερικοί ελεγκτές εκδίδουν έκθεση στην οποία εκφράζουν τις απόψεις τους σχετικά με την επάρκεια του Συστήματος Εσωτερικού Ελέγχου και ετοιμάζουν μία αναλυτική έκθεση με τις παρατηρήσεις / αδυναμίες που έχουν εντοπιστεί και τις εισηγήσεις τους για διορθωτικές ενέργειες. Η εν λόγω έκθεση πρέπει να επανεξεταστεί από την επιτροπή ελέγχου του ιδρύματος.

ΜΕΡΟΣ ΙΙ

ΕΛΑΧΙΣΤΕΣ ΠΤΥΧΕΣ ΤΗΣ ΑΞΙΟΛΟΓΗΣΗΣ

4. Η έκθεση πρέπει να καλύπτει, τουλάχιστον, την αξιολόγηση/εξέταση των ακόλουθων:

(α) Οργανωτική δομή

(i) Οργανωτική δομή (οργανόγραμμα και γραμμές αναφοράς, τη σύνθεση, τους όρους εντολής και τη λειτουργία του διοικητικού οργάνου και των επιτροπών του)·

(ii) Αξιολόγηση κατά πόσο το γενικό πλαίσιο εταιρικής διακυβέρνησης συμμορφώνεται με τις διατάξεις της Οδηγίας και διασφαλίζει την έγκαιρη και ακριβή επικοινωνία όλων των σημαντικών θεμάτων που αφορούν το ίδρυμα·

(iii) Επάρκεια των συστημάτων που χρησιμοποιούνται για την παραγωγή των πληροφοριών σύμφωνα με το σχετικό νομικό / ρυθμιστικό πλαίσιο·

(iv) Ο ρόλος του διοικητικού οργάνου σε σχέση με τη διασφάλιση της επάρκειας του πλαισίου εσωτερικού ελέγχου·

(v) Σύγκρουση συμφερόντων, αρχή της ύπαρξης δύο διοικητικών στελεχών (four eyes principle) και διαχωρισμός καθηκόντων· και

(vi) Διαδικασία για την κατάρτιση του ετήσιου προϋπολογισμού, σύμφωνα με τη στρατηγική και τις διαδικασίες του ιδρύματος που πρέπει να ακολουθείται σε περιπτώσεις αποκλίσεων από την εν λόγω στρατηγική.

(β) Λογιστικό σύστημα

Κατά την εξέταση του λογιστικού συστήματος πρέπει να αξιολογείται η επάρκεια του συστήματος εσωτερικού ελέγχου σχετικά με την κατάρτιση αξιόπιστων οικονομικών καταστάσεων. Η αξιολόγηση θα πρέπει να καλύπτει την ικανότητα του συστήματος για διαχείριση των πληροφοριών το οποίο να διευκολύνει την έγκαιρη και αξιόπιστη ροή των απαιτούμενων πληροφοριών σε κάθε λειτουργό ή διοικητική μονάδα, για εκπλήρωση των καθηκόντων τους.

(γ) Πληροφοριακά συστήματα

(i) Οργάνωση και διακυβέρνηση των πληροφοριακών συστημάτων·

(ii) ανάπτυξη και έναρξη λειτουργίας των συστημάτων·

(iii) λειτουργία και υποστήριξη των συστημάτων·

(iv) φυσική και λογική ασφάλεια·

(v) ηλεκτρονική και μέσω κινητής τηλεφωνίας τραπεζική· και

(vi) σχέδια επιχειρησιακής συνέχειας και σχέδια αποκατάστασης.

(δ) Επιτροπή ελέγχου και τμήμα εσωτερικής επιθεώρησης

(i) Η επιτροπή ελέγχου ως προς τα μέλη της, τα καθήκοντά της, τη συμμετοχή στη διαδικασία ελέγχου, την ετήσια έκθεση για το σύστημα εσωτερικού ελέγχου που ετοιμάζεται από τον επικεφαλή του τμήματος εσωτερικής επιθεώρησης και την ενημέρωση του διοικητικού οργάνου. Αναφορικά με το τμήμα εσωτερικής επιθεώρησης, θα πρέπει να εξετάζεται η ανεξαρτησία του, η θέση του στο οργανόγραμμα και η σύνδεση του με το διοικητικό όργανο και την επιτροπή ελέγχου·

(ii) πρακτικές και μεθοδολογία εσωτερικής επιθεώρησης που πρέπει να συγκριθούν με τις βέλτιστες πρακτικές·

(iii) σύστημα εσωτερικής επιθεώρησης (για την αποθήκευση των προγραμμάτων ελέγχου, των σχεδίων, πορισμάτων, εισηγήσεων και για την δημιουργία εκθέσεων διαχείρισης) και τεχνικές επιθεώρησης με τη βοήθεια υπολογιστή, εάν υπάρχουν, που χρησιμοποιούνται από το ίδρυμα·

(iv) σε δειγματοληπτική βάση, την επάρκεια των εκθέσεων ελέγχου για το ίδρυμα και τις θυγατρικές του, που ετοιμάζονται από το τμήμα εσωτερικής επιθεώρησης·

(v) διαδικασία παρακολούθησης της συμμόρφωσης των μονάδων που έχουν επιθεωρηθεί με τις εισηγήσεις του επικεφαλής του τμήματος εσωτερικής επιθεώρησης· και

(vi) εξωτερική αξιολόγηση της ποιότητας του τμήματος εσωτερικής επιθεώρησης.

(ε) Επιτροπή κινδύνων και τμήμα διαχείρισης κινδύνων

(i) Σύνθεση και ρόλος της επιτροπής κινδύνων·

(ii) πλαίσιο για διαχείριση των κινδύνων και, πιο συγκεκριμένα, κατά πόσο υπάρχουν επαρκείς μηχανισμοί για τον εντοπισμό, την παρακολούθηση και τη διαχείριση όλων των τύπων κινδύνων που αναλαμβάνονται από το ίδρυμα·

(iii) μέτρα που πρέπει να ληφθούν όταν προκύπτουν προβλήματα ρευστότητας έκτακτης ανάγκης·

(iv) ανεξαρτησία, ρόλοι και αρμοδιότητες και το έργο που εκτελείται από το τμήμα διαχείρισης κινδύνων και τον επικεφαλής του εν λόγω τμήματος·

(v) επάρκεια και αποτελεσματικότητα των πολιτικών και διαδικασιών διαχείρισης κινδύνων (συμπεριλαμβανομένης της μεθοδολογία προβλέψεων για επισφαλής απαιτήσεις)·

(vi) δυνατότητα διαφορετικών διαδικασιών διαχείρισης κινδύνων σε άλλες χώρες στις οποίες το ίδρυμα έχει παρουσία·

(vii) διαδικασία αξιολόγησης των κινδύνων που συνδέονται με το σχεδιασμό νέων προϊόντων / προώθησης νέας υπηρεσίας·

(viii) αντικειμενικότητα των διαδικασιών αξιολόγησης των αιτήσεων για χορήγηση πιστώσεων και της έγκρισης πιστωτικών διευκολύνσεων, εργαλεία που χρησιμοποιούνται για την εσωτερική πιστωτική διαβάθμιση των χορηγήσεων, διαχείριση και παρακολούθηση του μηχανισμού των εξασφαλίσεων και συμμόρφωση με τις πιστωτικές ρήτρες, μέτρα που λαμβάνονται για την αντιμετώπιση των μη εξυπηρετούμενων δανείων και η δυνατότητα παρακολούθησης των κινδύνων στο σύνολο του χαρτοφυλακίου δανείων του ιδρύματος· και

(ix) επάρκεια και τήρηση των διαδικασιών για τη χορήγηση πιστωτικών διευκολύνσεων προς τα μέλη του διοικητικού οργάνου και τα συνδεδεμένα τους πρόσωπα, καθώς και σε άλλα πρόσωπα που διατηρούν ειδική σχέση με το ίδρυμα και για τη διασφάλιση μη προτιμησιακής μεταχείρισης.

(στ) Τμήμα κανονιστικής συμμόρφωσης

(i) Το τμήμα κανονιστικής συμμόρφωσης ως προς την ανεξαρτησία, τους ρόλους και τις ευθύνες της, την πρόσβασή της σε όλες τις πηγές πληροφοριών, την άμεση και αξιόπιστη επικοινωνία των ευρημάτων της και την αποτελεσματική υιοθέτηση των αλλαγών στο ρυθμιστικό πλαίσιο·

(ii) επάρκεια και αποτελεσματικότητα των πολιτικών και διαδικασιών, καθώς και των ευθυνών των ανώτατων διοικητικών στελεχών και του διοικητικού οργάνου για τη διαχείριση του κινδύνου κανονιστικής συμμόρφωσης· και

(iii) επάρκεια των διαδικασιών που υπάρχουν για την πρόληψη και καταστολή του ξεπλύματος παράνομου χρήματος και χρηματοδότησης της τρομοκρατίας και της διαδικασίας για την ταξινόμηση των συναλλαγών και των αντισυμβαλλομένων στις διάφορες κατηγορίες κινδύνου.

(ζ) Τμήμα Ασφάλειας Πληροφοριών

(i) Το τμήμα ασφάλειας πληροφοριών ως προς την ανεξαρτησία, τους ρόλους και τις ευθύνες της, την πρόσβασή της σε όλες τις πηγές πληροφοριών, την άμεση και αξιόπιστη επικοινωνία των ευρημάτων της και την αποτελεσματική υιοθέτηση των αλλαγών στο πλαίσιο της ασφάλειας πληροφοριών·

(ii) επάρκεια και αποτελεσματικότητα του πλαισίου ασφάλειας πληροφοριών, καθώς και της ευθύνης του διοικητικού οργάνου και των ανώτατων διοικητικών στελεχών για επίβλεψη του κινδύνου των πληροφοριών ·

(iii) επάρκεια των πολιτικών και διαδικασιών για την αποτελεσματική διαχείριση της ασφάλειας των πληροφοριών, καθώς και την αποτελεσματική αντιμετώπιση του κινδύνου ασφάλειας των πληροφοριών του ιδρύματος·

(iv) ύπαρξη επαρκούς παρακολούθησης και επιθεώρησης των διαδικασιών για σκοπούς συνεχούς βελτίωσης της ασφάλειας των πληροφοριών στο ίδρυμα.

5. Η αξιολόγηση του συστήματος εσωτερικού ελέγχου του ιδρύματος συμμετοχών και των θυγατρικών του θα πρέπει να διεξάγεται κατά τον ίδιο τρόπο.

ΠΑΡΑΡΤΗΜΑ 2
(Παράγραφος 21)
ΑΝΑΘΕΣΗ ΕΡΓΑΣΙΩΝ ΣΕ ΤΡΙΤΟΥΣ
ΜΕΡΟΣ Ι
ΕΙΣΑΓΩΓΗ ΚΑΙ ΟΡΙΣΜΟΙ

1. Για σκοπούς του παρόντος παραρτήματος:

«Πάροχος υπηρεσιών» σημαίνει τον πάροχο υπηρεσιών ή δραστηριοτήτων, ο οποίος δύναται να είναι ξεχωριστή νομική οντότητα μέσα στον όμιλο ή οντότητα εκτός του ομίλου·

«ουσιώδης ή σημαντική υπηρεσία ή δραστηριότητα» σημαίνει την υπηρεσία ή την δραστηριότητα της οποίας η ενδεχόμενη πλημμελής ή μη κατάλληλη ή τυχόν παράλειψη εκτέλεσής της, θα επηρέαζε αρνητικά τη διαρκή συμμόρφωση του ιδρύματος με τους όρους και τις προϋποθέσεις που υπέχει βάσει της άδειας λειτουργίας του, ή την ικανότητα του ιδρύματος να συμμορφωθεί με τις λοιπές υποχρεώσεις του που απορρέουν από τη νομοθεσία που διέπει τη λειτουργία των πιστωτικών ιδρυμάτων ή θα έθιγε τα οικονομικά του αποτελέσματα, την ευρωστία ή τη συνέχιση των εργασιών του ιδρύματος·

Αναφέρονται πιο κάτω ενδεικτικά, χωρίς αυτές να εξαντλούν όλες τις περιπτώσεις, υπηρεσίες ή δραστηριότητες οι οποίες θεωρούνται ουσιώδεις ή σημαντικές:

(i). Εργασίες οι οποίες είναι αναπόσπαστα συνδεδεμένες με εργασίες πιστωτικού ιδρύματος ή σχετίζονται στενά με αυτές, όπως ορίζονται στα άρθρα 3 και 13(3) του Νόμου

(ii). Τα τμήματα εσωτερικού ελέγχου

(iii). Η διαχείριση των κυρίως τραπεζικών συστημάτων του ιδρύματος καθώς και άλλων συστημάτων τα οποία είναι η πηγή πληροφοριών για τις λογιστικές και εποπτικές αναφορές

(iv). Η διαχείριση της υποδομής των πληροφοριακών συστημάτων και του δικτύου επικοινωνίας του ιδρύματος.

Ουσιώδεις ή σημαντικές υπηρεσίες ή δραστηριότητες

2. Η ανάθεση υπηρεσιών ή δραστηριοτήτων οι οποίες θεωρούνται ως ουσιώδεις ή σημαντικές, συμπεριλαμβανομένων και της ανάθεσης ουσιωδών ή σημαντικών υπηρεσιών και δραστηριοτήτων εντός του Ομίλου, δεν επιτρέπεται χωρίς την προηγούμενη γραπτή έγκριση της Κεντρικής Τράπεζας. Το αίτημα το οποίο υποβάλλεται στην Κεντρική Τράπεζα ζητώντας έγκριση για ανάθεση υπηρεσιών και δραστηριοτήτων οι οποίες θεωρούνται ως ουσιώδεις ή σημαντικές, θα πρέπει να περιλαμβάνει τουλάχιστον τις ακόλουθες πληροφορίες:

(α) το τμήμα / μονάδα του ιδρύματος το οποίο είναι ο ιδιοκτήτης της εργασίας που θα ανατεθεί·

(β) περιγραφή της υπηρεσίας ή δραστηριότητας η οποία θα ανατεθεί·

(γ) πληροφορίες για τον πάροχο υπηρεσιών. Σε περίπτωση κατά την οποία ο πάροχος υπηρεσιών εποπτεύεται από άλλη αρμόδια εποπτική αρχή θα πρέπει να δοθούν πληροφορίες για την άλλη αρμόδια εποπτική αρχή·

(δ) βεβαίωση ότι η διαδικασία ανάθεσης εργασιών συνάδει με τις πρόνοιες του παρόντος Παραρτήματος, στην οποία περιλαμβάνεται και βεβαίωση ότι διενεργήθηκε αξιολόγηση των κινδύνων από το Τμήμα Διαχείρισης Κινδύνων και ότι έχει ληφθεί νομική γνωμάτευση·

(ε) βεβαίωση ότι έχει ληφθεί επίσημη έγκριση για την ανάθεση εργασιών από το αρμόδιο εγκριτικό κλιμάκιο·

(στ) βεβαίωση ότι, με την επιφύλαξη της έγκρισης της Κεντρικής Τράπεζας, θα ετοιμαστεί και υπογραφεί επίσημη συμφωνία μεταξύ του ιδρύματος και του πάροχου υπηρεσιών, η οποία θα συνάδει με τις πρόνοιες του παρόντος Παραρτήματος.

Υπηρεσίες ή δραστηριότητες οι οποίες δεν θεωρούνται ουσιώδεις ή σημαντικές

3. Σε περίπτωση κατά την οποία ανατίθενται υπηρεσίες ή δραστηριότητες οι οποίες δεν θεωρούνται ουσιώδεις ή σημαντικές, τα ιδρύματα καλούνται να ενημερώνουν γραπτώς την Κεντρική Τράπεζα, υποβάλλοντας εξαμηνιαία κατάσταση με όλες τις υπηρεσίες ή δραστηριότητες οι οποίες ανατέθηκαν σε τρίτους και δεν θεωρούνται ουσιώδεις ή σημαντικές. Η πιο πάνω κατάσταση θα πρέπει να υποβάλλεται από το Λειτουργό ο οποίος είναι ο αρμόδιος για θέματα ανάθεσης εργασιών όχι αργότερα από την 31^{ην} Ιουλίου για τους πρώτους έξι μήνες του χρόνου και την 31^{η} Ιανουαρίου για τους υπόλοιπους έξι μήνες του χρόνου αναφοράς. Η κατάσταση θα πρέπει, μεταξύ άλλων, να περιλαμβάνει τα ακόλουθα:

(α) το τμήμα / μονάδα του ιδρύματος το οποίο είναι ο ιδιοκτήτης της εργασίας που θα ανατεθεί·

(β) σύντομη περιγραφή της υπηρεσίας ή δραστηριότητας η οποία θα ανατεθεί·

(γ) πληροφορίες για τον πάροχο υπηρεσιών·

(δ) ημερομηνία έναρξης και η διάρκεια της συμφωνίας ανάθεσης εργασιών·

(ε) βεβαίωση ότι η ανάθεση των εργασιών δεν θεωρείται ουσιώδης ή σημαντική και βεβαίωση ότι λήφθηκε και νομική γνωμάτευση για το θέμα αυτό·

(στ) βεβαίωση ότι διενεργήθηκε κατάλληλη αξιολόγηση των κινδύνων βάσει της σημαντικότητας της υπηρεσίας ή δραστηριότητας ή οποία έχει ανατεθεί· και

(ζ) βεβαίωση ότι έχει ληφθεί επίσημη έγκριση για την ανάθεση εργασιών από το αρμόδιο εγκριτικό κλιμάκιο.

ΜΕΡΟΣ ΙΙ

ΕΥΘΥΝΕΣ ΤΟΥ ΑΡΜΟΔΙΟΥ ΛΕΙΤΟΥΡΓΟΥ ΓΙΑ ΘΕΜΑΤΑ ΑΝΑΘΕΣΗΣ ΕΡΓΑΣΙΩΝ (ΛΕΙΤΟΥΡΓΟΣ ΑΝΑΘΕΣΗΣ ΕΡΓΑΣΙΩΝ)

4. Τα ιδρύματα καλούνται να διορίσουν Λειτουργό ο οποίος θα είναι ο αρμόδιος για την ανάθεση εργασιών (Λειτουργός Ανάθεσης Εργασιών) και την επικοινωνία με την Κεντρική Τράπεζα για θέματα ανάθεσης εργασιών. Ωστόσο, επισημαίνεται ότι, τα αρμόδια τμήματα και / ή μονάδες του ιδρύματος φέρουν πλήρη ευθύνη για την εξωτερική ανάθεση και τη συμμόρφωση.

5. Ο Λειτουργός Ανάθεσης Εργασιών, είναι υπεύθυνος, μεταξύ άλλων, για τα πιο κάτω:

(α) διασφαλίζει ότι η διαδικασία ανάθεσης εργασιών διεξάγεται από το κάθε τμήμα/μονάδα βάσει της πολιτικής και των διαδικασιών του ιδρύματος και συνάδει με τις απαιτήσεις του παρόντος παραρτήματος·

(β) διασφαλίζει ότι λαμβάνεται νομική γνωμάτευση για το κατά πόσο μία υπηρεσία ή δραστηριότητα η οποία ανατέθηκε θεωρείται ότι είναι ή δεν είναι ουσιώδης ή σημαντική·

(γ) διασφαλίζει ότι διενεργήθηκε περιεκτική διαδικασία διαχείρισης των κινδύνων από το τμήμα διαχείρισης κινδύνων στις περιπτώσεις κατά τις οποίες απαιτείται·

(δ) διασφαλίζει ότι διενεργήθηκε κατάλληλη αξιολόγηση των κινδύνων για κάθε εργασία η οποία ανατέθηκε·

(ε) ενεργεί ως πρόσωπο επαφής με την Κεντρική Τράπεζα για θέματα ανάθεσης εργασιών και παρέχει όλες τις απαραίτητες πληροφορίες οι οποίες απαιτούνται από την Κεντρική Τράπεζα·

(στ) διατηρεί αναλυτικό και επικαιροποιημένο κατάλογο όλων των υπηρεσιών ή δραστηριοτήτων οι οποίες ανατέθηκαν σε τρίτους·

(ζ) ετοιμάζει την ετήσια έκθεση, η οποία περιλαμβάνει τις υπηρεσίες ή δραστηριότητες οι οποίες ανατέθηκαν κατά τη διάρκεια του χρόνου με ιδιαίτερη έμφαση στις υπηρεσίες ή δραστηριότητες οι οποίες θεωρούνται ουσιώδεις ή σημαντικές. Η έκθεση υποβάλλεται στα ανώτατα διοικητικά στελέχη του ιδρύματος.

ΜΕΡΟΣ ΙΙΙ

ΒΑΣΙΚΕΣ ΑΡΧΕΣ ΓΙΑ ΑΝΑΘΕΣΗ ΕΡΓΑΣΙΩΝ ΣΕ ΤΡΙΤΟΥΣ

6. Κατά τη διαδικασία λήψης απόφασης για ανάθεση εργασιών σε τρίτους, το ίδρυμα θα πρέπει να καθοδηγείται και να εφαρμόζει τις πιο κάτω βασικές αρχές:

(1) Το ίδρυμα οφείλει να διασφαλίζει ότι έχει διενεργηθεί κατάλληλη αξιολόγηση των κινδύνων που απορρέουν από την κάθε ανάθεση εργασιών.

Στην περίπτωση ανάθεσης υπηρεσιών ή δραστηριοτήτων οι οποίες θεωρούνται ως ουσιώδεις ή σημαντικές ή οποιανδήποτε άλλη υπηρεσία ή δραστηριότητα που θα αποφασίσει το ίδρυμα, θα πρέπει να διεξαχθεί αξιολόγηση κινδύνων από το τμήμα διαχείρισης κινδύνων του ιδρύματος.

Στην περίπτωση ανάθεσης υπηρεσιών ή δραστηριοτήτων οι οποίες δεν θεωρούνται ως ουσιώδεις ή σημαντικές, θα πρέπει να διεξαχθεί κατάλληλη αξιολόγηση των κινδύνων, βάσει της σημαντικότητας της υπηρεσίας ή δραστηριότητας ή οποία έχει ανατεθεί.

(2) Κατά τον καθορισμό του προγράμματος αξιολόγησης κινδύνων, θα πρέπει να λαμβάνονται υπόψη διάφοροι παράγοντες, όπως το είδος της εργασίας ή δραστηριότητας που ανατίθεται, η ικανότητα του ιδρύματος να εντοπίζει, παρακολουθεί, διαχειρίζεται και ελέγχει τους κινδύνους που προκύπτουν από την ανάθεση και η ικανότητα του παρόχου υπηρεσιών να διαχειρίζεται και να ελέγχει τους πιθανούς κινδύνους της ανάθεσης. Οι ακόλουθοι παράγοντες θα πρέπει επίσης να λαμβάνονται υπόψη:

(α) ο οικονομικός και λειτουργικός αντίκτυπος στο ίδρυμα καθώς και ο αντίκτυπος από δυσφήμιση λόγω αποτυχίας του παρόχου υπηρεσιών να εκτελεί επαρκώς την υπηρεσία ή δραστηριότητα·

(β) το κόστος·

(γ) πιθανές ζημιές για τους πελάτες του ιδρύματος και για τους συνεργάτες τους σε περίπτωση αποτυχίας του παρόχου υπηρεσιών·

(δ) συνέπειες από την ανάθεση της υπηρεσίας ή δραστηριότητας στη δυνατότητα και την ικανότητα του ιδρύματος να προσαρμόζεται σε εποπτικές/ ρυθμιστικές απαιτήσεις καθώς και σε αλλαγές στις εποπτικές/ ρυθμιστικές απαιτήσεις·

(ε) αλληλεξαρτήσεις και αλληλεπιδράσεις της ανατιθέμενης υπηρεσίας ή δραστηριότητας με άλλες υπηρεσίες ή δραστηριότητες εντός του ιδρύματος·

(στ) επαγγελματική ή άλλου είδους σχέση ανάμεσα στο ίδρυμα και τον πάροχο υπηρεσιών·

(ζ) την καταλληλότητα και ικανότητα του πάροχου υπηρεσιών, καθώς και κατά πόσο υπόκειται σε οποιαδήποτε εποπτεία ή ρύθμιση·

(η) ο βαθμός δυσκολίας και ο χρόνος που απαιτείται είτε για την επιλογή ενός εναλλακτικού παρόχου υπηρεσιών είτε

για την επαναφορά και διεκπεραίωση της υπηρεσίας ή δραστηριότητας στο ίδρυμα αν αυτό είναι απαραίτητο·

(θ) η πολυπλοκότητα των διευθετήσεων για ανάθεση εργασιών. Για παράδειγμα, η δυνατότητα να ελεγχθούν οι κίνδυνοι στην περίπτωση όπου συνεργάζονται περισσότεροι από ένα πάροχο υπηρεσιών για να παραδώσουν μια ολοκληρωμένη λύση για μια ανάθεση που έγινε·

(ι) το ενδεχόμενο συγκέντρωσης κινδύνων, δηλαδή κίνδυνοι που προκύπτουν από την ανάθεση πολλαπλών υπηρεσιών ή δραστηριοτήτων στον ίδιο πάροχο υπηρεσιών·

(ια) τα αποδεκτά όρια όσον αφορά το σύνολο των υπηρεσιών ή δραστηριοτήτων που ενδείκνυται να ανατεθούν·

(ιβ) η πιθανότητα να ασφαλιστούν, εξολοκλήρου ή εν μέρει, οι κίνδυνοι που αναλήφθηκαν.

Επιπρόσθετα με τα πιο πάνω, το ίδρυμα θα πρέπει επίσης να λάβει υπόψη την προστασία δεδομένων και την ασφάλεια τους καθώς επίσης και άλλους κίνδυνους οι οποίοι μπορούν να επηρεασθούν αρνητικά από την γεωγραφική τοποθεσία του παρόχου υπηρεσιών. Για το λόγο αυτό πιθανόν να χρειάζεται εξειδίκευση και πείρα για την αξιολόγηση του κινδύνου χώρας (δηλαδή τους κίνδυνους που σχετίζονται με τις πολιτικές, οικονομικές και νομικές συνθήκες) κατά τη σύναψη και εφαρμογή συμφωνιών με παρόχους υπηρεσιών που βρίσκονται εκτός της Δημοκρατίας.

Γενικά, ένα πλήρες πρόγραμμα αξιολόγησης κινδύνων θα πρέπει να προνοεί συνεχή παρακολούθηση και έλεγχο όλων των σχετικών πτυχών των σχετικών ρυθμίσεων που διέπουν την ανάθεση, συμπεριλαμβανομένης και της καθοδήγησης ως προς τη λήψη διορθωτικών ενεργειών όταν παρουσιάζονται συγκεκριμένα περιστατικά.

(3) Το ίδρυμα θα πρέπει να διασφαλίζει ότι η ανάθεση εργασιών δεν μειώνει την ικανότητα του να εκπληρώνει τις υποχρεώσεις του προς τους πελάτες του και επομένως δεν επηρεάζει τα δικαιώματα του πελάτη έναντι του ιδρύματος, συμπεριλαμβανομένης και της δυνατότητα του πελάτη για αποζημίωση.

(4) Το ίδρυμα θα πρέπει να διασφαλίζει ότι ο πάροχος υπηρεσιών συμμορφώνεται με τις νομικές και ρυθμιστικές απαιτήσεις.

(5) Το ίδρυμα θα πρέπει να διασφαλίζει ότι η ανάθεση εργασιών δεν μειώνει τη δυνατότητα της Κεντρικής Τράπεζας να ασκήσει τις ρυθμιστικές της εξουσίες όπως είναι η αποτελεσματική εποπτεία και ρύθμιση των εργασιών του ιδρύματος. Καμία υπηρεσία ή δραστηριότητα δεν πρέπει να ανατίθενται εάν αυτό θα επηρεάσει την ικανότητα της Κεντρικής Τράπεζας να αξιολογεί ή να εποπτεύει αποτελεσματικά τις εργασίες του ιδρύματος.

(6) Το ίδρυμα θα πρέπει να ασκήσει τη δέουσα επιμέλεια κατά την επιλογή των παρόχων υπηρεσιών. Τα ιδρύματα θα πρέπει να καθορίσουν κριτήρια τα οποία θα τους επιτρέψουν να αξιολογούν, πριν από την επιλογή, τη δυνατότητα και την ικανότητα του παρόχου υπηρεσιών να εκτελεί τις υπηρεσίες ή δραστηριότητες που του ανατίθενται αποτελεσματικά, με σοβαρότητα και σε υψηλά επίπεδα ποιότητας, σε συνάρτηση με τυχόν κινδύνους που συνδέονται με την επιλογή ενός συγκεκριμένου παρόχου υπηρεσιών. Δεν θα πρέπει να ανατίθενται υπηρεσίες ή δραστηριότητες σε πάροχο υπηρεσιών ο οποίος δεν ικανοποιεί τα κριτήρια του ιδρύματος. Η δέουσα επιμέλεια θα πρέπει να περιλαμβάνει:

(α) Την αναγνώριση οποιασδήποτε σύγκρουσης συμφερόντων ή ενδεχόμενης σύγκρουσης συμφερόντων που προκύπτει λόγω του ότι ο πάροχος υπηρεσιών αποτελεί συνδεδεμένο πρόσωπο με:

(ι) οποιοδήποτε ανώτατο διοικητικό στέλεχος ή μέλος του διοικητικού οργάνου του ιδρύματος ή του ομίλου·

(ιι) τους εξωτερικούς ελεγκτές του ιδρύματος·

(ιιι) τους εξωτερικούς νομικούς σύμβουλους του ιδρύματος·

(β) την επιλογή παρόχων υπηρεσιών που είναι ειδικευμένοι και διαθέτουν επαρκείς πόρους για την εκτέλεση των εργασιών που τους ανατίθενται·

(γ) τη διασφάλιση ότι ο πάροχος υπηρεσιών κατανοεί και είναι σε θέση να επιτύχει τους στόχους του ιδρύματος σε σχέση με τη συγκεκριμένη υπηρεσία ή δραστηριότητα·

(δ) εξακρίβωση της οικονομικής ευρωστίας του παρόχου υπηρεσιών η οποία θα του επιτρέψει να εκπληρώσει τις υποχρεώσεις του. Οποιεσδήποτε ειδικές ανάγκες, όπως η εξυπηρέτηση γεωγραφικά διασκορπισμένων υπηρεσιών ή δραστηριοτήτων, θα πρέπει να καθοριστούν και να ικανοποιηθούν με την επιλογή παρόχων υπηρεσιών με ανάλογες ικανότητες και προσβάσεις·

(ε) τομείς ανησυχίας:

(ι) εάν ένας πάροχος υπηρεσιών αποτύχει ή με οποιονδήποτε τρόπο δεν είναι σε θέση να εκτελέσει την ανατιθέμενη υπηρεσία ή δραστηριότητα, πιθανόν να είναι δαπανηρή ή/και προβληματική η διαδικασία εξεύρεσης έγκαιρα εναλλακτικών λύσεων·

(ιι) οι δαπάνες κατά το μεταβατικό στάδιο, οι πιθανές διαταραχές στη διεξαγωγή εργασιών και η πιθανή απώλεια υφιστάμενων εργασιών ή νέων επιχειρηματικών ευκαιριών είναι παράγοντες που θα πρέπει να λαμβάνονται

υπόψη, και

(iii) πρόσθετες ανησυχίες εγείρονται σε περίπτωση κατά την οποία μια υπηρεσία ή δραστηριότητα ανατίθεται στο εξωτερικό. Για παράδειγμα, σε μια έκτακτη κατάσταση, το ίδρυμα ενδεχομένως να διαπιστώσει ότι είναι δυσκολότερο να ανταποκριθεί έγκαιρα. Σε μια τέτοια περίπτωση τα ανώτατα διοικητικά στελέχη του ιδρύματος μπορεί να χρειασθεί να αξιολογήσουν τις οικονομικές, νομικές και πολιτικές συνθήκες οι οποίες πιθανόν να έχουν αρνητική επίδραση στη δυνατότητα του παρόχου υπηρεσιών να λειτουργήσει αποτελεσματικά για το ίδρυμα.

(7) Γενικά, η Κεντρική Τράπεζα απαιτεί όπως τα ιδρύματα διασφαλίζουν ότι διατηρούν τον πλήρη έλεγχο των εργασιών τους, ότι έχουν υπό τον έλεγχο τους τους υφιστάμενους επιχειρησιακούς τους κινδύνους καθώς επίσης και τους νέους κινδύνους που προκύπτουν με την ανάθεση εργασιών και, τέλος, συμμορφώνονται πλήρως με τις ρυθμιστικές υποχρεώσεις και τις υποχρεώσεις τους προς τους πελάτες τους.

Συμβάσεις και Συμφωνίες Διασφάλισης Ποιότητας Υπηρεσιών (SLA)

7. Το ίδρυμα θα πρέπει να διασφαλίζει ότι στις περιπτώσεις ανάθεσης εργασιών, οι σχέσεις ανάμεσα στα συμβαλλόμενα μέρη θα πρέπει να ρυθμίζονται με γραπτές συμβάσεις και συμφωνίες διασφάλισης ποιότητας υπηρεσιών μέσα από τις οποίες θα περιγράφονται με σαφήνεια και λεπτομέρεια όλες οι πτυχές της συνεργασίας, συμπεριλαμβανομένων των δικαιωμάτων, ευθυνών και προσδοκιών όλων των συμβαλλόμενων μερών. Το είδος και οι λεπτομέρειες τέτοιων συμβάσεων θα πρέπει να είναι τέτοια που να συνάδουν με την σημαντικότητα που έχει η υπηρεσία ή δραστηριότητα που ανατίθεται σε σχέση με τις εργασίες του ιδρύματος. Οι κατάλληλες πρόνοιες στις συμβάσεις μπορούν να μειώσουν τον κίνδυνο μη εκτέλεσης των υπηρεσιών ή εμφάνισης διαφωνιών σχετικά με την έκταση, τη φύση και την ποιότητα της υπηρεσίας που θα παρέχεται. Μερικές κύριες διατάξεις μιας τέτοιας σύμβασης είναι οι ακόλουθες:

(α) σαφής καθορισμός των υπηρεσιών ή δραστηριότητων που πρόκειται να ανατεθούν, συμπεριλαμβανομένων και των επιθυμητών επιπέδων εξυπηρέτησης και απόδοσης. Θα πρέπει να αξιολογηθεί εκ των προτέρων η ικανότητα του παρόχου υπηρεσιών να ανταποκριθεί στις απαιτούμενες επιδόσεις, τόσο σε ποσοτικό όσο και σε ποιοτικό επίπεδο, καθώς επίσης και η ικανότητα και προθυμία του να συμμορφωθεί με τις απαιτήσεις του παρόντος παραρτήματος·

(β) η σύμβαση θα πρέπει να καθορίζει με σαφήνεια τα αντίστοιχα δικαιώματα και υποχρεώσεις του ιδρύματος και του παρόχου υπηρεσιών·

(γ) η σύμβαση δεν θα πρέπει να αποτρέπει ούτε να εμποδίζει το ίδρυμα από την εκπλήρωση των εποπτικών/ρυθμιστικών υποχρεώσεων του, ή την Κεντρική Τράπεζα από την άσκηση των εποπτικών/ ρυθμιστικών εξουσιών της·

(δ) η σύμβαση θα πρέπει να προϋποθέτει ξεκάθαρα ότι η Κεντρική Τράπεζα έχει το δικαίωμα, οποτεδήποτε κριθεί αναγκαίο να:

(i) έχει πρόσβαση σε όλα τα βιβλία, αρχεία, πληροφορίες, άτομα και εγκαταστάσεις του παρόχου υπηρεσιών, σχετικά με την υπηρεσία ή δραστηριότητα που ανατέθηκε·

(ii) ζητά απευθείας από τον πάροχο υπηρεσιών οποιαδήποτε πληροφορία σε μορφή έκτακτων ή περιοδικών εκθέσεων·

(iii) επικοινωνεί απευθείας με τον πάροχο υπηρεσιών με σκοπό τη διεξαγωγή επιτόπιων ελέγχων, οι οποίοι να είναι αντίστοιχοι με τους ελέγχους που θα διενεργούσε στην περίπτωση που το ίδιο το ίδρυμα εκτελούσε την ανατιθέμενη υπηρεσία ή δραστηριότητα·

(ε) η σύμβαση θα πρέπει να διασφαλίζει ότι το ίδρυμα έχει τη δυνατότητα πρόσβασης σε όλα τα βιβλία, αρχεία, πληροφορίες, μέλη του προσωπικού και εγκαταστάσεις σχετικά με την υπηρεσία, δραστηριότητα που ανατίθεται·

(στ) η σύμβαση θα πρέπει να προνοεί για το συνεχή έλεγχο και αξιολόγηση του παρόχου υπηρεσιών από το ίδρυμα ώστε να μπορούν να ληφθούν έγκαιρα οποιαδήποτε αναγκαία διορθωτικά μέτρα·

(ζ) η σύμβαση θα πρέπει να περιγράφει με σαφήνεια και λεπτομέρεια όλες τις πτυχές διακοπής της συνεργασίας, λόγω ομαλού ή μη, τερματισμού της σύμβασης. Η σύμβαση θα πρέπει να περιέχει ρήτρα τερματισμού της σύμβασης καθώς επίσης και να καθορίζει τον ελάχιστο χρόνο εφαρμογής της. Ο όρος αυτός θα δίνει την δυνατότητα ανάθεσης των εργασιών σε κάποιο άλλο πάροχο υπηρεσιών ή την ενσωμάτωση τους πίσω στο ίδρυμα. Ο όρος αυτός θα πρέπει να περιλαμβάνει διατάξεις σχετικά με περιπτώσεις αφερεγγυότητας ή άλλων σημαντικών αλλαγών στην εταιρική μορφή του παρόχου υπηρεσιών, καθώς επίσης και το σαφή καθορισμό του ιδιοκτησιακού καθεστώτος οποιασδήποτε πνευματικής ιδιοκτησίας μετά τον τερματισμό, συμπεριλαμβανομένης της μεταφοράς πληροφοριών, στοιχείων ή/και όλων των μορφών τεχνογνωσίας πίσω στο ίδρυμα·

(η) ουσιώδη ζητήματα τα οποία αποτελούν ιδιαίτερα χαρακτηριστικά της συμφωνίας για ανάθεση θα πρέπει να διευκρινιστούν. Για παράδειγμα, όταν ο πάροχος υπηρεσιών βρίσκεται στο εξωτερικό, η σύμβαση θα πρέπει να περιλαμβάνει διατάξεις που να διευκρινίζουν ποιοι νόμοι εφαρμόζονται. Επίσης, θα πρέπει να υπάρχουν μηχανισμοί για τη διευθέτηση και επίλυση τυχόν διαφορών μεταξύ των συμβαλλομένων μερών με βάσει τη νομοθεσία που συμφωνήθηκε να εφαρμόζεται·

(θ) η σύμβαση θα πρέπει να περιλαμβάνει, όπου είναι απαραίτητο, όρους που να ρυθμίζουν την ανάθεση εκ μέρους του παρόχου υπηρεσιών της εκτέλεσης του συνόλου ή μέρους της εργασίας που του ανατέθηκε σε υπεργολάβους. Σε

περιπτώσεις όπου κρίνεται σκόπιμο, ο πάροχος υπηρεσιών, θα πρέπει να ζητεί την έγκριση του ιδρύματος πριν τη χρήση τέτοιων υπεργολάβων για το σύνολο ή μέρος της υπηρεσίας ή δραστηριότητας που ανατίθεται. Επιπρόσθετα, σε περιπτώσεις υπεργολαβίας σημαντικού μέρους υπηρεσίας ή δραστηριότητας που θεωρείται ουσιώδης ή σημαντική, απαιτείται η προηγούμενη έγκριση της Κεντρικής Τράπεζας. Γενικά, η σύμβαση θα πρέπει να εξασφαλίζει τη δυνατότητα στο ίδρυμα να διατηρεί το ίδιο επίπεδο ελέγχου των κινδύνων ως αυτό προνοείται στην αρχική σύμβαση στην περίπτωση που ο πάροχος υπηρεσιών αναθέτει εργασίες σε υπεργολάβους. Νοείται ότι ο τρίτος πάροχος υπηρεσιών θα πρέπει να συμμορφώνεται πλήρως με τις υφιστάμενες υποχρεώσεις μεταξύ του ιδρύματος και του παρόχου υπηρεσιών·

(ι) η σύμβαση θα πρέπει να περιλαμβάνει όρο που να υποχρεώνει τον πάροχο υπηρεσιών να ειδοποιεί άμεσα το ίδρυμα ή απευθείας την Κεντρική Τράπεζα για οποιεσδήποτε σημαντικές αλλαγές σε συνθήκες οι οποίες θα μπορούσαν να επηρεάσουν σημαντικά την συνέχιση της παροχής υπηρεσιών·

(κ) η σύμβαση θα πρέπει να περιλαμβάνει ρήτρα εμπιστευτικότητας και

(λ) κατά την προετοιμασία, διαπραγμάτευση, ανανέωση ή τροποποίηση μιας σύμβασης ανάθεσης εργασιών, το ίδρυμα θα πρέπει συμβουλεύεται τους νομικούς του συμβούλους.

Συνέχεια εργασιών και ανάκαμψη από καταστροφή

8. Το ίδρυμα θα πρέπει να διασφαλίζει ότι, σε περίπτωση που η ανάθεση υπηρεσιών ή δραστηριοτήτων που θεωρούνται ουσιώδεις ή σημαντικές ή οποιωνδήποτε άλλων υπηρεσιών ή δραστηριοτήτων που το ίδρυμα αποφασίσει, οι πάροχοι υπηρεσιών θα καταρτίσουν και θα διατηρούν σχέδιο αντιμετώπισης έκτακτων περιστατικών, συμπεριλαμβανομένου σχεδίου ανάκαμψης από καταστροφή και τα οποία θα ελέγχουν επαρκώς σε περιοδική βάση. Τα εν λόγω σχέδια θα πρέπει να συμμορφώνονται με τις ρυθμιστικές υποχρεώσεις του ιδρύματος και θα πρέπει να ελέγχονται ότι είναι από λειτουργικής άποψης πλήρως έτοιμα πριν από την έναρξη της διεκπεραίωσης της ανατιθέμενης υπηρεσίας ή δραστηριότητας. Συγκεκριμένα,

(α) το ίδρυμα θα πρέπει να λάβει τα απαραίτητα μέτρα έτσι ώστε να αξιολογήσει και να είναι σε θέση να αντιμετωπίσει πιθανές συνέπειες λόγω οποιονδήποτε διαταραχών στις εργασίες ή άλλων προβλημάτων από την πλευρά του παρόχου υπηρεσιών. Θα πρέπει επίσης να απαιτεί από αυτόν την ετοιμασία κατάλληλων σχεδίων αντιμετώπισης έκτακτων περιστατικών και να διασφαλίζει το συντονισμό των σχεδίων αντιμετώπισης έκτακτων υπηρεσιών του ιδρύματος και αυτών του παρόχου υπηρεσιών·

(β) το ίδρυμα θα πρέπει επίσης να έχει σχέδιο δράσης σε περίπτωση αδυναμίας του παρόχου υπηρεσιών να ανταποκριθεί στις υποχρεώσεις του. Τα σχέδια δράσης θα πρέπει να λαμβάνουν υπόψη το κόστος για υιοθέτηση εναλλακτικών επιλογών σε περίπτωση όπου θα παρατηρηθεί επιδείνωση της επίδοσης.

Συστήματα πληροφορικής και ασφάλεια δεδομένων

9. (1) Το ίδρυμα θα πρέπει να λαμβάνει τα κατάλληλα μέτρα για να διασφαλίζει ότι οι πάροχοι υπηρεσιών διατηρούν την ασφάλεια των πληροφοριακών συστημάτων στο ίδιο επίπεδο, όπως ορίζεται στο Παράρτημα 3, για προστασία των εμπιστευτικών πληροφοριών και των πληροφοριών που αποτελούν ιδιοκτησία του ιδρύματος, συμπεριλαμβανομένων των πληροφοριών πελατών. Για το σκοπό αυτό, θα μπορούσαν να περιλαμβάνονται πρόνοιες στην σύμβαση που να απαγορεύουν στον πάροχο υπηρεσιών και τους υπεργολάβους του τη χρησιμοποίηση ή την αποκάλυψη πληροφοριών που αποτελούν ιδιοκτησία του ιδρύματος ή των πελατών του, εκτός στις περιπτώσεις όπου κρίνεται απαραίτητο για την παροχή των υπηρεσιών και για να ικανοποιούν ρυθμιστικές και νομικές υποχρεώσεις.

(2) Το ίδρυμα, λαμβάνοντας υπόψη τις υφιστάμενες νομικές διατάξεις ή κανονισμούς θα πρέπει να εξετάζει κατά πόσον θα πρέπει να ενημερωθούν οι πελάτες του ότι οι πληροφορίες που σχετίζονται με αυτούς πιθανόν να διαβιβαστούν σε ένα πάροχο υπηρεσιών.

ΜΕΡΟΣ IV
ΥΠΟΧΡΕΩΣΕΙΣ ΔΙΟΙΚΗΤΙΚΟΥ ΟΡΓΑΝΟΥ

10. Το διοικητικό όργανο του ιδρύματος έχει την συνολική ευθύνη των υπηρεσιών ή δραστηριοτήτων οι οποίες ανατέθηκαν, συμπεριλαμβανομένων των ακολούθων:

(α) να καθορίζει, εγκρίνει και επιβλέπει συστηματικά την πολιτική ανάθεσης εργασιών του ιδρύματος. Η πολιτική ανάθεσης εργασιών θα πρέπει να καλύπτει όλες τις πτυχές της ανάθεσης εργασιών, συμπεριλαμβανομένων και της ανάθεσης εργασιών οι οποίες δεν θεωρούνται ουσιώδεις ή σημαντικές ή/και γίνεται εντός ή εκτός του ομίλου. Η πολιτική ανάθεσης εργασιών θα πρέπει να καθοδηγεί τη διαδικασία αξιολόγησης όσον αφορά το κατά πόσον και με ποιο τρόπο ενδείκνυται να γίνει ανάθεση εργασιών σε πάροχο υπηρεσιών και θα πρέπει να περιλαμβάνει, μεταξύ άλλων, τα ακόλουθα:

(i) σαφή ορισμό των υπηρεσιών και των δραστηριοτήτων που μπορούν να ανατεθούν καθώς επίσης και των αναγκών και στόχων που θα πρέπει να εξυπηρετούνται από την ανάθεση εργασιών·

(ii) πρόνοιες που να διασφαλίζουν ότι πριν οποιαδήποτε ανάθεση εργασιών, το ίδρυμα έχει πλήρη αντίληψη των σχετικών ωφελημάτων, δαπανών και των κινδύνων που συνεπάγονται. Αυτό απαιτεί ανάλυση και αξιολόγηση των κύριων δραστηριοτήτων του ιδρύματος, των δυνατών και αδύνατων σημείων του καθώς επίσης και των μελλοντικών σχεδίων και στόχων του πριν οποιαδήποτε ανάθεση εργασιών·

(iii) πρόνοιες που να διασφαλίζουν ότι οι υπηρεσίες ή δραστηριότητες οι οποίες ανατέθηκαν θα πρέπει να συνεχίζουν να ικανοποιούν το επίπεδο απόδοσης και ποιότητας που θα ίσχυαν σε περίπτωση που το ίδρυμα εκτελούσε εσωτερικά αυτές τις υπηρεσίες ή δραστηριότητες·

(iv) πρόνοιες για οποιεσδήποτε αναθέσεις εργασιών εντός του ομίλου (π.χ. σε ξεχωριστή νομική οντότητα εντός του ομίλου)·

(v) πρόνοιες που να διασφαλίζουν την ικανότητα του ιδρύματος να συμμορφώνεται με τις νομικές και ρυθμιστικές απαιτήσεις·

(iv) πρόνοιες που να διασφαλίζουν ότι μια υπηρεσία ή δραστηριότητα δεν θα πρέπει να ανατίθεται σε περίπτωση που θίγεται το δικαίωμα της Κεντρικής Τράπεζας να έχει πρόσβαση ή να εποπτεύει τις εργασίες του ιδρύματος·

(vii) πρόνοιες που να διασφαλίζουν ότι το ίδρυμα διαθέτει διαδικασίες για να επιβλέπει αποτελεσματικά τις υπηρεσίες ή δραστηριότητες που ανατίθενται·

(β) να επιβλέπει και αξιολογεί την αποτελεσματικότητα της εφαρμογής της πολιτικής ανάθεσης εργασιών και να διασφαλίζει τη βελτίωσή της.

ΜΕΡΟΣ V

ΕΥΘΥΝΕΣ ΤΩΝ ΑΝΩΤΑΤΩΝ ΔΙΟΙΚΗΤΙΚΩΝ ΣΤΕΛΕΧΩΝ

11. Τα ανώτατα διοικητικά στελέχη έχουν την ευθύνη για τα εξής:

(α) την εφαρμογή της πολιτικής ανάθεσης εργασιών όπως εγκρίνεται από το διοικητικό όργανο και τη θέσπιση διαδικασιών οι οποίες να ακολουθούνται σε περίπτωση ανάθεσης υπηρεσίας ή δραστηριότητας·

(β) τη θέσπιση διαδικασιών για επιλογή του παρόχου υπηρεσιών σύμφωνα με τις απαιτήσεις της παρούσας Οδηγίας·

(γ) τον καθορισμό των κύριων προνοιών που θα μπορούσαν να περιληφθούν στη σύμβαση ανάθεσης εργασιών, σύμφωνα με τις απαιτήσεις της παρούσας Οδηγίας·

(δ) την αξιολόγηση της πληρότητας και αποτελεσματικότητας της εφαρμογής της πολιτικής και των διαδικασιών ανάθεσης εργασιών και τον καθορισμό τρόπων για την αντιμετώπιση και βελτίωση οποιωνδήποτε θεμάτων προκύπτουν, βάσει της ετήσιας έκθεσης που υποβάλλεται από το Λειτουργό Ανάθεσης Εργασιών καθώς επίσης και των παρατηρήσεων του τμήματος Εσωτερικής Επιθεώρησης που υποβάλλονται στην Επιτροπή Ελέγχου·

(ε) το διορισμό διευθυντή ή ατόμου που έχει την τεχνογνωσία και εξουσία να χειριστεί αυτό το θέμα ως Λειτουργός Ανάθεσης Εργασιών και την κοινοποίηση προς την Κεντρική Τράπεζα του ονόματος, θέσης και στοιχεία επικοινωνίας του Λειτουργού Ανάθεσης Εργασιών όταν αυτός διοριστεί ή αντικατασταθεί.

ΠΑΡΑΡΤΗΜΑ 3

(Παράγραφος 105)

ΑΡΧΕΣ ΑΣΦΑΛΟΥΣ ΚΑΙ ΑΠΟΤΕΛΕΣΜΑΤΙΚΗΣ ΛΕΙΤΟΥΡΓΙΑΣ ΤΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΣΤΑ ΠΛΑΙΣΙΑ ΤΗΣ ΔΙΑΧΕΙΡΙΣΗΣ ΤΟΥ ΛΕΙΤΟΥΡΓΙΚΟΥ ΚΙΝΔΥΝΟΥ

ΜΕΡΟΣ 1

ΕΙΣΑΓΩΓΗ

1. (1) Το παρόν Παράρτημα παρουσιάζει ένα πλαίσιο γενικών αρχών και κριτηρίων για την ασφαλή και αποτελεσματική λειτουργία των Πληροφοριακών Συστημάτων, λαμβάνοντας παράλληλα υπόψη τις πρόσφατες εξελίξεις της πληροφορικής στο βαθμό που επηρεάζουν τη λειτουργία των τραπεζών.

(2) Το πλαίσιο αυτό αποτελεί τη βάση αξιολόγησης των τραπεζών στο συγκεκριμένο τομέα και η εφαρμογή των αρχών του αναμένεται να συμβάλει σημαντικά στην αποτελεσματική διαχείριση του λειτουργικού κινδύνου που σχετίζεται με τα Πληροφοριακά Συστήματα.

(3) Οι αρχές αυτές ομαδοποιούνται σε τέσσερις ενότητες και συγκεκριμένα στις εξής:

(α) Οργάνωση και διοίκηση πληροφορικής, όπου γίνεται αναφορά στην διακυβέρνηση της πληροφορικής, στην οργάνωση της Υπηρεσιακής Μονάδας της Πληροφορικής και στις σχέσεις με τους εξωτερικούς συνεργάτες.

(β) Ανάπτυξη και προμήθεια συστημάτων, όπου γίνεται αναφορά στις μεθοδολογίες, πρότυπα και διαδικασίες ανάπτυξης και προμήθειας Πληροφοριακών Συστημάτων.

(γ) Λειτουργία και υποστήριξη, όπου γίνεται αναφορά στις διαδικασίες λειτουργίας των συστημάτων, στη φυσική και λογική τους ασφάλεια, καθώς και στη διασφάλιση της συνέχειας των εργασιών του ιδρύματος.

(δ) Έλεγχος συστημάτων πληροφορικής, όπου γίνεται αναφορά σε κανόνες και βασικές απαιτήσεις για την επαρκή και αποτελεσματική λειτουργία του τμήματος Εσωτερικής Επιθεώρησης αναφορικά με τα Πληροφοριακά Συστήματα.

ΜΕΡΟΣ ΙΙ.

ΟΡΓΑΝΩΣΗ ΚΑΙ ΔΙΟΙΚΗΣΗ ΤΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

Διακυβέρνηση Πληροφορικής

2. (1) Η διακυβέρνηση της πληροφορικής είναι ευθύνη των ανώτατων διοικητικών στελεχών του ιδρύματος. Περιλαμβάνει το σύνολο των κατάλληλων επιχειρησιακών δομών και διαδικασιών μέσω των οποίων διασφαλίζεται ότι η πληροφορική υποστηρίζει τη στρατηγική και τους στόχους του ιδρύματος, διαχειρίζεται αποτελεσματικά τους πόρους που της διατίθενται, αξιολογεί και διαχειρίζεται αποτελεσματικά τους κινδύνους που απορρέουν από τη λειτουργία των Πληροφοριακών Συστημάτων, εφαρμόζει πιστά την πολιτική ασφάλειας πληροφοριών, είναι σε θέση να μετρήσει την αποτελεσματικότητα και αποδοτικότητά της και, τέλος, υλοποιεί ένα σύνολο μηχανισμών ελέγχου στα πλαίσια ενός γενικότερου ελεγκτικού πλαισίου.

(2) Για την επίτευξη των προαναφερθέντων, τα ιδρύματα θα πρέπει:

(α) να διαθέτουν καταγεγραμμένη και επίσημα εγκεκριμένη από το διοικητικό όργανο στρατηγική για την πληροφορική, συμβατή με τις γενικότερες επιχειρησιακές στρατηγικές τους. Ένα αναλυτικό και ακριβές στρατηγικό πλάνο θα πρέπει να υπάρχει βραχυπρόθεσμα (σε ετήσια βάση) και ένα στοχευμένο στρατηγικό πλάνο θα πρέπει να υπάρχει μεσοπρόθεσμα (σε τριετή βάση). Το ίδρυμα θα πρέπει επίσης να διαθέτει μια στρατηγική άποψη ως προς τη μακροπρόθεσμη (σε βάση πενταετίας και άνω) διαμόρφωση του τοπίου των πληροφοριακών συστημάτων της. Η στρατηγική της πληροφορικής οφείλει, αφενός μεν να υλοποιεί τους επιχειρησιακούς στόχους που έχουν τεθεί από τα ανώτατα διοικητικά στελέχη του ιδρύματος, αφετέρου δε να διαμορφώνει έγκαιρα την απαραίτητη τεχνολογική υποδομή για τις μελλοντικές ανάγκες του ιδρύματος,

(β) να διαθέτουν Ειδική Συντονιστική Επιτροπή για την Πληροφορική. Επικεφαλής της Επιτροπής συνιστάται να είναι ανώτατο διοικητικό στέλεχος του ιδρύματος με επαρκή γνώση των θεμάτων πληροφορικής. Τα μέλη της Επιτροπής θα πρέπει να αποτελούνται από διοικητικά στελέχη του ιδρύματος και σχετικα τμήματα ελέγχου. Ο ρόλος, τα καθήκοντα και η ελάχιστη σύνθεση της Επιτροπής θα πρέπει να ορίζονται στους επίσημους κανονισμούς αναφοράς της. Ως ελάχιστη απαίτηση, η επιτροπή θα πρέπει να καθορίσει την ιεράρχηση των επενδύσεων στην πληροφορική και σε συναφή έργα, σύμφωνα με τους στρατηγικούς στόχους του ιδρύματος, να παρακολουθεί την πρόοδο των έργων και να μεριμνά για την επίλυση διαφορών. Η Επιτροπή, τέλος, θα πρέπει να λαμβάνει γνώση των πορισμάτων των ελέγχων που διενεργούνται στα Πληροφοριακά Συστήματα,

(γ) να αξιολογούν, να κατηγοριοποιούν και να διαχειρίζονται τους κινδύνους που απορρέουν από την ανάπτυξη, ενσωμάτωση και λειτουργία των Πληροφοριακών Συστημάτων. Οι κίνδυνοι αυτοί θα πρέπει να συνεκτιμούνται με τους υπόλοιπους κινδύνους στους οποίους είναι εκτεθειμένο το ίδρυμα,

(δ) να μεριμνούν ώστε οι υπάρχουσες πολιτικές, πρότυπα, διαδικασίες και μεθοδολογίες να είναι επίσημα καταγεγραμμένες και εγκεκριμένες από τα αρμόδια υπηρεσιακά όργανα,

(ε) να διαθέτουν πρότυπα και μεθοδολογίες για το σχεδιασμό και την ανάπτυξη των Πληροφοριακών Συστημάτων, καθώς και διαδικασίες για την καθημερινή τους λειτουργία, υποστήριξη και παρακολούθηση,

(στ) να διαθέτουν πρότυπα και διαδικασίες για τη διαχείριση και την αποτελεσματική έκβαση των έργων πληροφορικής.

Στην πρόταση για την υλοποίηση κάθε μεγάλου έργου πληροφορικής πρέπει να προσδιορίζεται ο επιχειρησιακός στόχος, καθώς και τα ποιοτικά και ποσοτικά οφέλη που θα αποφέρει η υλοποίησή του,

(ζ) να εγγυούνται την ποιότητα των παρεχόμενων υπηρεσιών πληροφορικής μέσω της ύπαρξης διαδικασιών διασφάλισης ποιότητας και εναρμόνισης, σε όλα τα στάδια του κύκλου ζωής των συστημάτων, με πρότυπα ποιότητας στη βάση μετρήσιμων κριτηρίων,

(η) να διαθέτουν τις κατάλληλες διαδικασίες για τον έγκαιρο εντοπισμό και την αποτελεσματική αντιμετώπιση των προβλημάτων που προκύπτουν στα Πληροφοριακά Συστήματα,

(θ) να διαθέτουν διαδικασίες για την αναλυτική κατηγοριοποίηση, καταγραφή και παρακολούθηση των γεγονότων που δημιουργούν λειτουργικό κίνδυνο, συμπεριλαμβανομένων των οικονομικών ζημιών που προέρχονται από προβλήματα στα Πληροφοριακά Συστήματα (π.χ. μη εξουσιοδοτημένη πρόσβαση, κλοπή μηχανογραφικού εξοπλισμού, απάτη, παραβίαση ασφάλειας, μη διαθεσιμότητα συστημάτων, καταστροφή μηχανογραφικού εξοπλισμού, κακόβουλη χρήση, κτλ) και ενημέρωσης των αρμόδιων εσωτερικών τμημάτων ελέγχου (Ασφάλειας Πληροφοριών, Διαχείρισης Κινδύνων και Εσωτερικής Επιθεώρησης), για την αποτελεσματικότερη καταγραφή και αντιμετώπιση του λειτουργικού κινδύνου,

(ι) να διαθέτουν σύστημα διοικητικών πληροφοριών (“Management Information System”), κατάλληλο για την αποτελεσματική πληροφόρηση των ανώτατων διοικητικών στελεχών του ιδρύματος. Ένα τέτοιο σύστημα θα πρέπει να χαρακτηρίζεται από την ομοιόμορφη και βάσει καταγεγραμμένων διαδικασιών συλλογή και επεξεργασία, έγκαιρη διάθεση, ακρίβεια, αξιοπιστία, και πληρότητα πληροφοριών,

(ια) να γνωρίζουν και να συμμορφώνονται με το νομικό, εποπτικό και κανονιστικό πλαίσιο σε ότι αφορά θέματα πληροφορικής,

(ιβ) να μελετούν, να αξιολογούν και να εφαρμόζουν, όπου κριθεί κατάλληλο, τα διεθνή πρότυπα και μεθοδολογίες διαχείρισης και ασφάλειας των Πληροφοριακών Συστημάτων. Τα ιδρύματα θα πρέπει επίσης να είναι ενήμερα και να λαμβάνουν υπόψη όλες τις διεθνείς εξελίξεις στους συγκεκριμένους τομείς.

Οργάνωση της Υπηρεσιακής Μονάδας Πληροφορικής

3. Τα ιδρύματα θα πρέπει να θεσπίσουν εξειδικευμένη Υπηρεσιακή Μονάδα Πληροφορικής, λειτουργικά και διοικητικά ανεξάρτητη από τους τελικούς χρήστες των υπηρεσιών πληροφορικής, η οποία θα πρέπει:

(α) να διαθέτει οργανόγραμμα στο οποίο:

i. να απεικονίζονται οι επιχειρησιακές και οργανωτικές ανάγκες της μονάδας και να περιγράφονται με σαφήνεια οι αρμοδιότητες των επί μέρους υπηρεσιακών μονάδων που το αποτελούν,

ii. να απεικονίζεται ο διαχωρισμός των καθηκόντων προκειμένου να αποκλείεται η ύπαρξη ασυμβίβαστων ρόλων, να παρέχεται η δυνατότητα καταλογισμού των ευθυνών και να αξιοποιούνται με τον καταλληλότερο τρόπο οι δυνατότητες του προσωπικού. Ειδικότερα, θα πρέπει να διασφαλίζεται ότι διαχωρίζονται πλήρως οι λειτουργίες που σχετίζονται με το σχεδιασμό και την ανάπτυξη των συστημάτων από τις λειτουργίες που αφορούν την καθημερινή λειτουργία τους,

iii. προσωπικό για την ασφάλεια των Πληροφοριακών Συστημάτων να ανατίθεται, αναλόγως αναγκών, για να λειτουργεί ως σύνδεσμος με τον Υπεύθυνο Ασφάλειας Πληροφοριών και να διασφαλίζει ότι η πολιτική ασφάλειας πληροφοριών εφαρμόζεται αποτελεσματικά στα πληροφοριακά συστήματα και υποδομή δικτύου του ιδρύματος,

iv. να εξασφαλίζεται η αναπλήρωση του προσωπικού, τουλάχιστον στις κρίσιμες μηχανογραφικές λειτουργίες.

(β) να διαθέτει καταγεγραμμένες και επίσημα εγκεκριμένες περιγραφές θέσεων εργασίας στις οποίες θα περιλαμβάνονται οι αρμοδιότητες, οι υπευθυνότητες και οι δεξιότητες που απαιτούνται για κάθε θέση.

Σχέσεις με Εξωτερικούς Συνεργάτες

4. Η χρήση εξωτερικών συνεργατών, ενώ μπορεί να επιλύει σημαντικά προβλήματα, δημιουργεί πεδίο πρόσθετων κινδύνων για το ίδρυμα, οι οποίοι πρέπει να εντοπισθούν, να εκτιμηθούν και να αντιμετωπισθούν αποτελεσματικά. Στους κινδύνους αυτούς περιλαμβάνονται η πιθανή έλλειψη ουσιαστικού ελέγχου στις προσφερόμενες υπηρεσίες, η εξάρτηση από τρίτους, η απώλεια εσωτερικής τεχνογνωσίας, η ενδεχόμενη αδυναμία άμεσης προσαρμογής στις απαιτήσεις των πελατών και του οικονομικού περιβάλλοντος, η αδιαφανής κοστολόγηση των προσφερόμενων υπηρεσιών και η διαφορά νοοτροπίας μεταξύ ιδρύματος και παρόχου υπηρεσιών,

(α) σε περίπτωση που ίδρυμα αποφασίσει να αναθέσει οποιαδήποτε από τις υπηρεσίες πληροφορικής, συμπεριλαμβανομένων της υποδομής, πλατφόρμας, λογισμικού, ή δεδομένων, σε εξωτερικούς συνεργάτες, συμπεριλαμβανομένων και παρόχων υπηρεσιών «cloud computing», τότε η ανάθεση πρέπει να γίνεται συνειδητά και να τηρούνται αυστηρά οι αρχές του “Παραρτήματος 2” της παρούσας Οδηγίας,

(β) η ανάθεση υλοποίησης σημαντικών για το ίδρυμα συστημάτων σε τρίτους, θα πρέπει να αιτιολογείται από την Ειδική Συντονιστική Επιτροπή για την Πληροφορική εγγράφως προς τα ανώτατα διοικητικά στελέχη, τα οποία και παρέχουν την τελική έγκριση.

ΜΕΡΟΣ ΙΙΙ
ΑΝΑΠΤΥΞΗ ΚΑΙ ΠΡΟΜΗΘΕΙΑ ΣΥΣΤΗΜΑΤΩΝ

5. (1) Ο κύκλος ζωής ενός συστήματος πρέπει να χαρακτηρίζεται από διακριτές φάσεις, οι οποίες θα υλοποιούν πρότυπα, μεθοδολογίες και διαδικασίες επίσημα καταγεγραμμένες και εγκεκριμένες. Η εποπτεία του έργου της ανάπτυξης κάθε σημαντικού συστήματος πρέπει να ανατίθεται στην Ειδική Συντονιστική Επιτροπή για την Πληροφορική. Με την ολοκλήρωση της ανάπτυξης του συστήματος, η λειτουργική και τεχνική παρακολούθηση θα πρέπει να ανατίθεται στις αρμόδιες υπηρεσιακές μονάδες ή στελέχη.

(2) Πριν την ανάπτυξη ή προμήθεια ενός σημαντικού συστήματος πρέπει να γίνεται μελέτη σκοπιμότητας

Ανάπτυξη Συστημάτων

Στις περιπτώσεις που ένα ίδρυμα επιλέγει την ανάπτυξη ενός νέου συστήματος, ή την υλοποίηση σημαντικών αλλαγών σε υφιστάμενο σύστημα, θα πρέπει:

(α) πριν την έναρξη της ανάπτυξης, να ορισθεί Ομάδα Έργου που θα αναλάβει τη διαχείριση του έργου και την κατάρτιση ενός χρονοδιαγράμματος υλοποίησης,

(β) το χρονοδιάγραμμα υλοποίησης να προσδιορίζει, μεταξύ άλλων, τις φάσεις, τη διάρκεια τους, και τους υπεύθυνους για την υλοποίηση της κάθε φάσης, καθώς και τα παραδοτέα,

(γ) να ορίζεται ένα σχέδιο επικοινωνίας, στο οποίο θα καθορίζονται οι διαδικασίες ενημέρωσης των εμπλεκομένων μερών για την πρόοδο του έργου,

(δ) να λαμβάνονται υπόψη θέματα αποδοχής και αποτελεσματικής λειτουργίας του νέου Πληροφοριακού Συστήματος από τους χρήστες,

(ε) να γίνει λεπτομερής σχεδιασμός για τη διαχείριση των δεδομένων του προϋπάρχοντος συστήματος, μηχανογραφημένου ή μη, και να περιλαμβάνει θέματα εκκαθάρισης παλαιών δεδομένων (“data cleansing”), μετατροπής δεδομένων στη μορφή του νέου συστήματος (“data conversion”) και μετάπτωσης δεδομένων (“data migration”),

(στ) στις φάσεις της τεχνικής ανάλυσης και του σχεδιασμού, να καθορίζονται με λεπτομέρεια οι απαιτήσεις ασφαλούς λειτουργίας του συστήματος σύμφωνα με όσα προβλέπονται στην ισχύουσα πολιτική ασφάλειας πληροφοριών του ιδρύματος και να διεκπεραιώνεται ανάλυση κινδύνων για το σκοπό αυτό,

(ζ) η ανάπτυξη του συστήματος να υλοποιείται ακολουθώντας τα ισχύοντα πρότυπα, σε ξεχωριστό μηχανογραφικό περιβάλλον από αυτό της παραγωγής,

(η) οι δοκιμές του συστήματος να διενεργούνται σε πρώτη φάση από το προσωπικό της Υπηρεσιακής Μονάδας Πληροφορικής σε ξεχωριστό περιβάλλον. Στην τελική φάση θα πρέπει να γίνονται επαρκώς τεκμηριωμένες και ολοκληρωμένες και είναι απαραίτητο να συμμετέχουν, πέραν των υπηρεσιών πληροφορικής, οι τελικοί χρήστες και η Μονάδα Διασφάλισης Ποιότητας (όπου υπάρχει). Οι Εσωτερικές Λειτουργίες Ελέγχου και οι τελικοί χρήστες θα πρέπει να διασφαλίσουν και να επιβεβαιώσουν, πριν από τη μεταφορά στην παραγωγή, ότι οι απαιτήσεις που έχουν καθοριστεί από τους ίδιους έχουν διευθετηθεί,

(θ) η μεταφορά του νέου συστήματος στην παραγωγή να πραγματοποιείται από εξειδικευμένο προσωπικό, όπως για παράδειγμα βιβλιοθηκάριων (librarians) βάσει καταγεγραμμένων οδηγιών,

(ι) το σύστημα, πριν ακόμη τεθεί σε λειτουργία, να διαθέτει πλήρη τεκμηρίωση με βάση τα πρότυπα που έχουν τεθεί από το ίδιο το ίδρυμα,

(ια) να πραγματοποιείται εκπαίδευση των χρηστών του συστήματος σε ξεχωριστό περιβάλλον, το οποίο δε θα επηρεάζεται από τα περιβάλλοντα ανάπτυξης και παραγωγής,

(ιβ) η λειτουργία και υποστήριξη του συστήματος να περιλαμβάνει διαδικασίες ελέγχου των αλλαγών , ελέγχου των εκδόσεων του συστήματος , ελέγχου ενημερώσεων του συστήματος για την αντιμετώπιση προβλημάτων που εντοπίστηκαν (“patching”), ελέγχου της απόδοσης του συστήματος, λήψης και φύλαξης εφεδρικών αρχείων, συνέχειας των εργασιών, ενημέρωσης του “Help Desk” για την υποστήριξη των χρηστών του συστήματος, κτλ,

(ιγ) η φάση απόσυρσης του συστήματος να περιλαμβάνει διαδικασίες για τη διατήρηση των πληροφοριών σύμφωνα με τις νομικές και εποπτικές απαιτήσεις. Πριν την απόσυρση του υλικού και λογισμικού, οι πληροφορίες θα πρέπει να καταστρέφονται χωρίς δυνατότητα ανάκτησης.

Προμήθεια Συστημάτων

7. Στις περιπτώσεις που ίδρυμα αποφασίζει την προμήθεια Πληροφοριακών Συστημάτων θα πρέπει, επιπλέον των προαναφερθέντων απαιτήσεων για την «Ανάπτυξη Συστημάτων», να λαμβάνει υπόψη και τα ακόλουθα:

(α) η όλη διαδικασία προμήθειας να χαρακτηρίζεται από διακριτές φάσεις, οι οποίες θα υλοποιούν πρότυπα, μεθοδολογίες και διαδικασίες επίσημα καταγεγραμμένες και εγκεκριμένες. Τέτοιες φάσεις, είναι αυτές της πρόσκλησης για υποβολή προτάσεων (“Request for proposal”) με αναλυτική περιγραφή των αναγκών που θα καλύπτει το σύστημα, της επιλογής του εξωτερικού συνεργάτη, της σύναψης της συμφωνίας και της υπογραφής του συμβολαίου, της ένταξης και λειτουργίας των συστημάτων στην παραγωγή και, τέλος, της εποπτείας και του ελέγχου τους,

(β) η επιλογή του συστήματος να γίνεται με βάση τις αναλυτικές λειτουργικές και τεχνικές προδιαγραφές που οφείλει να θέτει το ίδρυμα,

(γ) μέσω μιας επαρκούς αναγνώρισης και αξιολόγησης κινδύνων, ότι η εισαγωγή νέων μορφών τεχνολογίας στην υποδομή τεχνολογίας πληροφοριών και δικτύου, δε δημιουργεί επιπρόσθετους κινδύνους που το ίδρυμα δεν είναι διατεθειμένο να αποδεχθεί,

(δ) το είδος παρέμβασης του ιδρύματος στο σύστημα να είναι εκ των προτέρων αυστηρά καθορισμένο. Οι όποιες παρεμβάσεις θα πρέπει να ακολουθούν εγκεκριμένες και καταγεγραμμένες διαδικασίες, να υλοποιούνται από εξειδικευμένο προσωπικό και να διατηρούνται στο ελάχιστο δυνατό επίπεδο έτσι ώστε να μην αλλοιώνεται η φυσιογνωμία του συστήματος και να είναι εύκολη η αναβάθμιση και συντήρησή του. Σημειώνεται ότι, σε περίπτωση σημαντικής απόκλισης των λειτουργικών διαδικασιών του ιδρύματος από εκείνες που υποστηρίζει το αγορασθέν σύστημα, το ίδρυμα είναι αυτό που συνήθως θα πρέπει να προσαρμόσει τις λειτουργικές του διαδικασίες στα χαρακτηριστικά του συστήματος και όχι το αντίστροφο,

(ε) στα κεντρικά συστήματα τραπεζικών εργασιών, η ανάπτυξη περιφερειακών εφαρμογών που θα αντλούν πληροφορίες από το κεντρικό σύστημα και θα υλοποιούν τοπικές αλλά και επιχειρησιακές ιδιαιτερότητες να γίνεται με βάση τα ισχύοντα στο ίδρυμα πρότυπα για την ανάπτυξη εφαρμογών, έτσι ώστε να διατηρείται η μηχανογραφική ομοιογένεια,

(στ) ο τρόπος υποστήριξης των συστημάτων να είναι αυστηρά προδιαγεγραμμένος, με σαφή καθορισμό των περιπτώσεων στις οποίες απαιτείται υποστήριξη από τον προμηθευτή αλλά και των χρονικών περιθωρίων ανταπόκρισής του,

(ζ) να είναι απαραίτητη η απόκτηση τεχνογνωσίας, όχι μόνο μέσω της κατάλληλης εκπαίδευσης του εμπλεκόμενου προσωπικού στη λειτουργία τέτοιων συστημάτων, αλλά κυρίως μέσω της συμμετοχής του σε όλες τις φάσεις υλοποίησης των συστημάτων, έτσι ώστε η εξάρτηση του ιδρύματος από τον προμηθευτή βαθμιαία να ελαττώνεται,

(η) εφόσον έχουν υλοποιηθεί οι απαιτήσεις του ιδρύματος - όπως αυτές αναφέρονται στο συμβόλαιο - και μετά το πέρας των απαραίτητων δοκιμών εκ μέρους του παρόχου, να υφίσταται διαδικασία επίσημης αποδοχής και παραλαβής του συστήματος εκ μέρους του ιδρύματος με τη συμμετοχή όλων των εμπλεκομένων μερών

ΜΕΡΟΣ IV
ΛΕΙΤΟΥΡΓΙΑ ΚΑΙ ΥΠΟΣΤΗΡΙΞΗ

8. (1) Η απρόσκοπτη λειτουργία των Πληροφοριακών Συστημάτων και η αποτελεσματική υποστήριξή τους είναι παράγοντες κρίσιμοι τόσο για την εύρυθμη λειτουργία του ιδρύματος και τη δημιουργία σχέσεων εμπιστοσύνης με τους πελάτες, όσο και για την αποτελεσματική αντιμετώπιση του λειτουργικού κινδύνου. Η απρόσκοπτη λειτουργία και η αποτελεσματική υποστήριξη των Πληροφοριακών Συστημάτων προϋποθέτουν την τήρηση των πολιτικών, προτύπων και διαδικασιών του ιδρύματος από όλες τις εμπλεκόμενες υπηρεσιακές μονάδες, αλλά και τους παρόχους υπηρεσιών πληροφορικής.

Λειτουργία Συστημάτων

(2) Ο όρος «λειτουργία συστημάτων» αναφέρεται στο σύνολο των διαδικασιών που απαιτούνται για την καθημερινή λειτουργία των Πληροφοριακών Συστημάτων σε ένα ίδρυμα. Για ένα αποδεκτό επίπεδο ασφαλούς και αποτελεσματικής λειτουργίας τους θα πρέπει να υφίστανται:

(α) πλήρης και λεπτομερής καταγραφή του μηχανογραφικού εξοπλισμού (κεντρικά συστήματα, εξυπηρετητές, προσωπικοί υπολογιστές, περιφερειακά, δίκτυα και τηλεπικοινωνίες), του αρχιτεκτονικού σχεδιασμού, του χρησιμοποιούμενου λογισμικού, καθώς και του ιστορικού των εκδόσεων, των ενημερώσεων, και των αδειών χρήσης. Αρχείο πρέπει να τηρείται επίσης για τα μέσα που αποθηκεύουν και διακινούν ευαίσθητα δεδομένα του οργανισμού,

(β) πλήρης και ενημερωμένη τεκμηρίωση για κάθε σύστημα με τα επίσημα εγχειρίδια των προμηθευτών εξοπλισμού και λογισμικών συστημάτων, ως επίσης και τα εγχειρίδια που συντάσσονται από το προσωπικό του ιδρύματος,

(γ) επαρκής συντήρηση και τεχνική υποστήριξη των συστημάτων,

(δ) υποστήριξη των χρηστών εντός, αλλά και των χρηστών (πελατών) εκτός του οργανισμού, η οποία και θα πρέπει να ανατίθεται σε κατάλληλα οργανωμένες και στελεχωμένες υπηρεσιακές μονάδες (“Help Desk"),

(ε) διαδικασίες διαχείρισης των παραμέτρων λειτουργίας των συστημάτων,

(στ) διαδικασίες αποτροπής και ανίχνευσης τυχόν εγκατάστασης και χρήσης μη εγκεκριμένου από το ίδρυμα λογισμικού, καθώς επίσης και λογισμικού χωρίς την κατάλληλη αδειοδότηση,

(ζ) προγραμματισμός των εργασιών προς εκτέλεση, καταγραφή των προβλημάτων που προκύπτουν και των ενεργειών που πρέπει να γίνονται στις έκτακτες περιπτώσεις. Η επιτυχής ή μη εκτέλεση των προγραμματισμένων αλλά και έκτακτων εργασιών θα πρέπει να καταχωρείται σε ειδικό ημερολόγιο, το οποίο και θα φέρει τις υπογραφές του προσωπικού που τις εκτέλεσε. Η εκτέλεση έκτακτων εργασιών θα πρέπει να γίνεται κατόπιν ειδικής έγκρισης.

(η) έλεγχος των δεδομένων, για εξασφάλιση της ακεραιότητας, ορθότητας και εμπιστευτικότητας τους, σε όλες τις φάσεις επεξεργασίας τους. Οι κάθε είδους ασυνέπειες θα πρέπει να διαπιστώνονται και να αντιμετωπίζονται βάσει καταγεγραμμένων διαδικασιών,

(θ) διαδικασίες διαχείρισης της χωρητικότητας, του φόρτου και της απόδοσης των συστημάτων και δικτύων,

(ι) συνεχής παρακολούθηση της διαθεσιμότητας των συστημάτων και των δικτύων. Ειδικότερα για τα κρίσιμα συστήματα, το ίδρυμα πρέπει να είναι σε θέση να υπολογίζει το ποσοστό διαθεσιμότητάς τους σε ετήσια βάση και να το συγκρίνει με προκαθορισμένους στόχους,

(ια) επαρκείς διαδικασίες διαχείρισης αντιγράφων ασφαλείας.

(ιβ) ειδικότερα, για τα συστήματα και τις υπηρεσίες που προσφέρονται μέσω του διαδικτύου θα πρέπει να υφίστανται:

i. επαρκής πληροφόρηση στο διαδικτυακό τόπο (“web-site”) του ιδρύματος, έτσι ώστε να μπορούν οι εν δυνάμει πελάτες του να έχουν μια επαρκή γνώση για την ταυτότητα του ιδρύματος και την εποπτεύουσα αρχή που παρέχει την άδεια λειτουργίας, πριν πραγματοποιήσουν τις ηλεκτρονικές τους συναλλαγές. Επίσης, γνωστοποίηση του τρόπου με τον οποίο μπορούν να επικοινωνήσουν οι πελάτες με το σχετικό κέντρο υποστήριξης σε περίπτωση πάσης φύσεως προβλήματος, το ψηφιακό πιστοποιητικό του διαδικτυακού τόπου, το οποίο θα πρέπει να έχει εκδοθεί από επίσημη αρχή πιστοποίησης, πληροφορίες για την ασφαλή χρήση των παρεχομένων υπηρεσιών και άλλες σχετικές πληροφορίες,

ii. ενημέρωση των πελατών για την πολιτική εμπιστευτικότητας που εφαρμόζει το ίδρυμα σε σχέση με τα προσωπικά τους δεδομένα. Η πληροφόρηση αυτή συνιστάται να παρέχεται και μέσα από το διαδικτυακό τόπο του ιδρύματος. Παροχή επίσης στους πελάτες του δικαιώματος να αρνηθούν τη διάθεση – εκχώρηση σε τρίτους δεδομένων που τους αφορούν, για προώθηση προϊόντων ή άλλο λόγο. Τα δεδομένα των πελατών θα πρέπει να χρησιμοποιούνται μόνο για τους σκοπούς για τους οποίους οι πελάτες γνωρίζουν ότι τα διαθέτουν και σύμφωνα με τη σχετική νομοθεσία,

iii. σαφής σήμανση στο διαδικτυακό τόπο του ιδρύματος των συνδέσεων (“links”) με διαδικτυακούς τόπους άλλων εταιρειών ή οργανισμών. Πρέπει να φαίνεται έκδηλα στον πελάτη ότι, όταν εγκαταλείπει το διαδικτυακό τόπο του ιδρύματος, συνδέεται με μια εντελώς ξεχωριστή επιχειρηματική μονάδα ή άλλη νομική οντότητα,

iv. αυτοματοποιημένα συστήματα παρακολούθησης των συναλλαγών, τα οποία και θα βασίζουν την αποτελεσματική λειτουργία τους στη δημιουργία εκ μέρους του ιδρύματος στατιστικών προτύπων κίνησης λογαριασμού για κάθε πελάτη. Τα συστήματα αυτά, με βάση τα διαμορφωμένα χαρακτηριστικά κίνησης των λογαριασμών των πελατών (“profiles”), θα πρέπει να εντοπίζουν και να καταγράφουν ασυνήθιστες συναλλακτικές συμπεριφορές και να παράγουν, σε πραγματικό χρόνο, προειδοποιητικά μηνύματα (“alerts”) για τη διερεύνηση ενδεχόμενων περιπτώσεων απάτης,

v. αποτελεσματική αντιμετώπιση των κινδύνων νομιμοποίησης εσόδων από το ξέπλυμα παράνομου χρήματος και τη χρηματοδότηση της τρομοκρατίας. Οι συγκεκριμένοι κίνδυνοι στις ηλεκτρονικές συναλλαγές είναι ιδιαίτερα αυξημένοι λόγω της ευκολίας χρήσης των υπηρεσιών από οπουδήποτε και οποιαδήποτε χρονική στιγμή, της απρόσωπης φύσης των συναλλαγών και της αυτόματης διεκπεραίωσής τους. Ως εκ τούτου, τα ιδρύματα θα πρέπει να μεριμνούν για την εγκατάσταση αυτοματοποιημένων συστημάτων και εργαλείων διαχείρισης των συναλλαγών, τα οποία κατ’ ελάχιστο θα θέτουν όρια σε συγκεκριμένες ομάδες ή κατηγορίες συναλλαγών, και θα παρέχουν τη δυνατότητα καθυστέρησης εκτέλεσης της συναλλαγής μέχρι την εξακρίβωση συγκεκριμένων στοιχείων (“filters & monitoring tools/systems”),

vi. δυνατότητα εύκολης προσπέλασης και επεξεργασίας στοιχείων παλαιότερων συναλλαγών, έτσι ώστε να γίνεται εφικτός ο εντοπισμός συναλλακτικών ιδιαιτεροτήτων και ανωμαλιών, για να διευκολύνεται η στοιχειοθέτηση αποδεικτικών στοιχείων και η επαρκής πληροφόρηση των εποπτικών αρχών, ειδικά στις περιπτώσεις απάτης και νομιμοποίησης εσόδων από το ξέπλυμα παράνομου χρήματος και τη χρηματοδότηση της τρομοκρατίας, παροχής επενδυτικών υπηρεσιών και άλλων συναλλαγών,

vii. εγχειρίδια σε ηλεκτρονική ή έντυπη μορφή, τα οποία θα ενημερώνουν τους πελάτες για τον τρόπο χρήσης των συστημάτων με έμφαση σε θέματα ασφάλειας. Επιπλέον, τα ιδρύματα θα πρέπει να εφοδιάζουν τους χρήστες με πρακτικές ασφαλούς χρήσης των προσωπικών υπολογιστών μέσω των οποίων αποκτούν πρόσβαση στα συστήματα ηλεκτρονικής τραπεζικής και ηλεκτρονικών πληρωμών του ιδρύματος. Στις πρακτικές αυτές θα πρέπει να γίνεται αναφορά, μεταξύ άλλων, σε θέματα προστασίας από ιούς και άλλο κακόβουλο λογισμικό, απόπειρας υποκλοπής (“phishing”) και άλλων κακοήθων τακτικών, ασφαλούς αποθήκευσης και χρήσης προσωπικών κλειδιών (“tokens”) και κωδικών (ειδικά σε υπολογιστές κοινής χρήσης των οποίων τέτοια χρήση, ως θέμα αρχής, θα πρέπει να αποθαρρύνεται και να αποφεύγεται στο

βαθμό που είναι δυνατό),

viii. επαρκείς διαδικασίες ασφάλειας με έμφαση στη πιστοποίηση των συναλλασσόμενων μερών (ψηφιακό πιστοποιητικό διαδικτυακού τόπου του ιδρύματος, πιστοποίηση δύο επιπέδων για τον πελάτη, με χρήση ψηφιακών πιστοποιητικών ή άλλης μεθόδου), τη μη αποποίηση των συναλλαγών, την κρυπτογράφηση της επικοινωνίας, την ασφάλεια των συναλλαγών (αποδεικτικά στοιχεία επιτυχούς ολοκλήρωσης, αποσύνδεση σε περίπτωση ανενεργού χρήστη, εντοπισμός ύποπτων συναλλαγών κλπ), και τέλος τη λειτουργία των συστημάτων που υποστηρίζουν τις εν λόγω υπηρεσίες σε ειδικές περιοχές του δικτύου που παρέχουν υψηλή προστασία από κακόβουλες ενέργειες εσωτερικών ή εξωτερικών χρηστών.

Φυσική Ασφάλεια

(3) Ο όρος «φυσική ασφάλεια» αναφέρεται στα μέτρα που πρέπει να λαμβάνονται για την προστασία των συστημάτων και της υποδομής που τα υποστηρίζει, από κινδύνους που προέρχονται από μη εξουσιοδοτημένα ή κακοήθη πρόσωπα και περιβαλλοντικές καταστροφές. Είναι απαραίτητο η ανάλυση κινδύνων να προηγείται της λήψης μέτρων, αφού οι απαιτήσεις φυσικής ασφάλειας δεν είναι δυνατόν να είναι οι ίδιες για όλες τις περιοχές και χώρους που στεγάζουν συστήματα.Στα μέτρα φυσικής ασφάλειας πρέπει, τουλάχιστον, να περιλαμβάνονται:

(α) μηχανισμοί ελέγχου φυσικής πρόσβασης. Τέτοιοι μηχανισμοί πρέπει να περιορίζουν, να ελέγχουν και να καταγράφουν, αφ' ενός μεν την είσοδο και την έξοδο του προσωπικού και των επισκεπτών, αφ' ετέρου δε τη διακίνηση μηχανογραφικού εξοπλισμού και αποθηκευτικών μέσων. Το είδος των μηχανισμών ελέγχου που υλοποιούνται θα πρέπει να καθορίζεται από την κρισιμότητα των συστημάτων που καλούνται να προστατεύσουν. Για παράδειγμα, στα μηχανογραφικά κέντρα θα πρέπει να παρέχεται το υψηλότερο επίπεδο προστασίας.

(β) μηχανισμοί πρόληψης και αντιμετώπισης καταστροφών από φυσικά αίτια.

(γ) μηχανισμοί πρόληψης και αντιμετώπισης κακόβουλων ενεργειών (διάρρηξης / κλοπής, βανδαλισμού, τρομοκρατικής ενέργειας κτλ.). Οι συγκεκριμένοι κίνδυνοι, όπως και οι κίνδυνοι από φυσικά αίτια, εκτός του ότι μπορεί να προκαλέσουν ολοσχερή καταστροφή των συστημάτων και των δικτύων, είναι δυνατό να διακυβεύσουν τις ζωές του προσωπικού.

(δ) μηχανισμοί πρόληψης και αντιμετώπισης προβλημάτων από διακοπή λειτουργίας και παροχής υπηρεσιών, ή βλάβη υποστηρικτικών συσκευών. Τα συστήματα είναι απαραίτητο να λειτουργούν σε κατάλληλες περιβαλλοντικές συνθήκες και σε τεχνικό περιβάλλον που υποστηρίζεται αποτελεσματικά.

(ε) η αποτελεσματική διαχείριση της τηλεπικοινωνιακής και δικτυακής καλωδίωσης για την αντιμετώπιση προβλημάτων, όπως φυσικής φθοράς, παρεμβολών και έλλειψης κατάλληλης σήμανσης.

(στ) μηχανισμοί για την ασφάλεια των φορητών συστημάτων. Η χρήση φορητών υπολογιστών και οποιωνδήποτε άλλων φορητών συσκευών θα πρέπει να λαμβάνεται σοβαρά υπόψη στην ανάλυση κινδύνων. Φορητοί υπολογιστές και συσκευές που αποθηκεύουν ευαίσθητα εταιρικά δεδομένα θα πρέπει, αφενός μεν να φυλάσσονται σε ασφαλή σημεία όταν δεν είναι σε χρήση, αφετέρου δε να αποθηκεύουν τα ευαίσθητα δεδομένα σε κρυπτογραφημένη μορφή.

(ζ) η ασφαλής μεταφορά και αποθήκευση των εγγράφων και φορητών μέσων τα οποία φυλάσσουν ευαίσθητες πληροφορίες. Στην πρώτη κατηγορία ανήκουν ανάμεσα σε άλλα οι διαβαθμισμένες αναφορές, οι εφεδρικοί κωδικοί εισόδου των διαχειριστών συστημάτων, τα συνθηματικά των πελατών μέχρι να τους αποσταλούν, η τεκμηρίωση των συστημάτων και εφαρμογών, η Πολιτική Ασφάλειας Πληροφοριών και τα Σχέδια Συνέχειας Εργασιών και Ανάκαμψης από Καταστροφή. Στη δεύτερη ανήκουν, ανάμεσα σε άλλα, τα εφεδρικά αντίγραφα αρχείων και το πλαστικό υλικό των καρτών συναλλαγών.

(η) η επιλογή και κατάλληλη διαμόρφωση των χώρων με σκοπό την ελαχιστοποίηση των προαναφερθέντων κινδύνων, σε σχέση πάντοτε με τη χρήση για την οποία προορίζονται και την κρισιμότητα των συστημάτων που στεγάζουν.

Λογική ασφάλεια

(4) Ο όρος «λογική ασφάλεια» αναφέρεται στο σύνολο των μέτρων που λαμβάνονται για τον περιορισμό της πρόσβασης στους πόρους των συστημάτων ("system resources"). Ως πόροι των συστημάτων θεωρούνται ο μηχανογραφικός εξοπλισμός και τα δίκτυα, πραγματικά ή εικονικά ("virtual"), το λογισμικό και τα δεδομένα. Τα μέτρα που υλοποιούν την λογική ασφάλεια καθορίζουν όχι μόνον το «ποιος» ή «τι», ποιο πρόγραμμα για παράδειγμα, θα έχει πρόσβαση σε συγκεκριμένους πόρους του συστήματος, αλλά και το είδος της πρόσβασης που επιτρέπεται να έχει. Τα μέτρα αυτά μπορεί να είναι ενσωματωμένα στα λειτουργικά συστήματα, να υλοποιούνται σε προγράμματα εφαρμογών, σε συστήματα διαχείρισης βάσεων δεδομένων, σε συστήματα επικοινωνιών ή ακόμη να υλοποιούνται μέσω πρόσθετων αυτόνομων πακέτων ασφάλειας. Για τη διατήρηση ενός αποδεκτού επιπέδου λογικής ασφαλείας, κρίνεται σκόπιμο:

(α) Για την ασφάλεια των προσβάσεων στα συστήματα:

i. να έχουν όλοι οι χρήστες ένα μοναδικό ατομικό λογαριασμό πρόσβασης σε κάθε σύστημα και μόνο για τους πόρους εκείνους που δικαιούνται πρόσβαση, ώστε κάθε ενέργεια να χρεώνεται μονοσήμαντα. Ως εκ τούτου, κοινοί – ομαδικοί λογαριασμοί πρόσβασης δεν θα πρέπει να χρησιμοποιούνται και, όπου αυτό δεν είναι εφικτό,

θα πρέπει οι ενέργειες των κατόχων των λογαριασμών αυτών να καταγράφονται και να ελέγχονται σχολαστικά,

ii. όπου είναι αναγκαία η χρήση λογαριασμών πρόσβασης συστημάτων/υπηρεσιών (“system/service accounts”), ο σκοπός χρήσης θα πρέπει να είναι επαρκώς τεκμηριωμένος και θα πρέπει να εφαρμόζονται αυστηρά μέτρα ασφαλείας για την πρόσβαση στους λογαριασμούς αυτούς,

iii. να υπάρχουν καταγεγραμμένες και εγκεκριμένες διαδικασίες για τη διαχείριση των λογαριασμών πρόσβασης, τον καθορισμό και την αναθεώρηση των δικαιωμάτων που παρέχονται στον κάθε λογαριασμό. Να υπάρχει διαχωρισμός αρμοδιοτήτων στην έγκριση, υλοποίηση και έλεγχο των προσβάσεων,

iv. να καταγράφονται και να ελέγχονται συστηματικά οι ενέργειες που γίνονται με χρήση λογαριασμών πρόσβασης με προνομιακά δικαιώματα, όπως λογαριασμών διαχειριστών συστημάτων και γενικά χρηστών με αυξημένα δικαιώματα,

v. οι λογαριασμοί πρόσβασης να απενεργοποιούνται άμεσα μόλις παύουν να είναι απαραίτητοι ή σε περίπτωση σημαντικής παραβίασης των κανόνων ασφάλειας,

vi. να υπάρχει συγκεκριμένη διαδικασία που να προβλέπει τη δημιουργία προσωρινών λογαριασμών πρόσβασης, με καθορισμένο επίπεδο εξουσιοδότησης, για συγκεκριμένες εργασίες ή σε περιπτώσεις ανάγκης. Η χρήση των λογαριασμών αυτών θα πρέπει να ελέγχεται σχολαστικά και μόλις εκλείψει η ανάγκη για την οποία δημιουργήθηκαν θα πρέπει να απενεργοποιούνται,

vii. να πιστοποιείται ο ιδιοκτήτης ενός λογαριασμού πρόσβασης, κατά τη διαδικασία εισόδου του στο σύστημα μέσω ασφαλούς διαδικασίας, βασισμένη σε σύγχρονες μεθόδους βέλτιστης πρακτικής,

viii. να αλλάζονται άμεσα οι κωδικοί πρόσβασης που έχουν τεθεί από κατασκευαστές/προμηθευτές σε κάθε νέο σύστημα ή εξοπλισμό μετά την παραλαβή του,

ix. οι κωδικοί πρόσβασης, ανάλογοι της κρισιμότητας των πληροφοριών που προστατεύουν, θα πρέπει:

1. να δημιουργούνται βάσει σύγχρονων προτύπων και βέλτιστων πρακτικών,
2. να διαχειρίζονται βάσει πολιτικών και διαδικασιών,
3. να τηρούνται εμπιστευτικοί με ευθύνη των κατόχων τους,
4. να αλλάζουν σε περιοδική βάση και οπωσδήποτε την πρώτη φορά εισόδου του κατόχου τους στο σύστημα,

x. οι εφεδρικοί κωδικοί των διαχειριστών συστημάτων ή λογαριασμών ειδικών προνομίων θα πρέπει να βρίσκονται αποθηκευμένοι σε ασφαλές σημείο, ώστε να μπορούν να χρησιμοποιηθούν βάσει ειδικής διαδικασίας σε περίπτωση έκτακτης ανάγκης,

xi. όπου κρίνεται αναγκαίο, οι κωδικοί πρόσβασης λογαριασμών ειδικών προνομίων θα πρέπει να μη φυλάσσονται ενιαίοι, αλλά σε τμήματα με ευθύνη διαφορετικών ατόμων,

xii. να χρησιμοποιείται – όπου είναι εφικτό – ειδικό λογισμικό διαχείρισης και ελέγχου των προσβάσεων.

(β) Για την προστασία των δεδομένων

i. να υπάρχουν επαρκείς ενσωματωμένοι μηχανισμοί ελέγχου (“controls”) των δεδομένων στα διάφορα συστήματα, και ειδικότερα, στην προετοιμασία, εισαγωγή, και επεξεργασία τους.

ii. να υπάρχει καταγεγραμμένη και εγκεκριμένη διαβάθμιση των δεδομένων σύμφωνα με το βαθμό ευαισθησίας τους. Για τα ευαίσθητα δεδομένα, να προβλέπονται διαδικασίες χειρισμού και επεξεργασίας βάσει αυξημένων προδιαγραφών ασφαλείας, όπως τεχνικών κρυπτογράφησης ή άλλων μεθόδων προστασίας.

iii. για την κρυπτογράφηση:

1. να καθορίζεται σαφώς το πότε και σε ποιο επίπεδο γίνεται κρυπτογράφηση,
2. να χρησιμοποιείται υψηλής ασφάλειας κλειδί κρυπτογράφησης σε όλο το λογισμικό,
3. να χρησιμοποιείται κατάλληλος αλγόριθμος κρυπτογράφησης, με βάση το είδος, την ανθεκτικότητα και την ποιότητα του,
4. να εφαρμόζεται στρατηγική υποδομής δημόσιου κλειδιού (“public key infrastructure”) για τη διαχείριση των ψηφιακών πιστοποιητικών, κυρίως για την επικοινωνία του ιδρύματος με τους πελάτες του για παροχή υπηρεσιών ηλεκτρονικής τραπεζικής,
5. να επιδιώκεται η συμμόρφωση με τους εγχώριους και διεθνείς κανονισμούς και πρακτικές κρυπτογράφησης.

iv. να γίνονται οι απαραίτητες ενέργειες για τη συμμόρφωση με τη σχετική νομοθεσία και κανονισμούς προστασίας δεδομένων,

v. να υπάρχει πολιτική σχετικά με την ενημέρωση των πελατών στην περίπτωση διαρροής εμπιστευτικών και προσωπικών δεδομένων τους, λόγω παραβίασης της ασφάλειας των συστημάτων.

vi. για τις βάσεις δεδομένων:

1. να υπάρχει ολοκληρωμένη και ακριβής τεκμηρίωση της βάσης που να περιλαμβάνει τουλάχιστον το λογικό σχεδιασμό, το φυσικό σχεδιασμό και το λεξικό δεδομένων,
2. να γίνεται αναδιοργάνωση της βάσης σε τακτά χρονικά διαστήματα,

3. να εξασφαλίζεται η καταχώρηση μόνο ολοκληρωμένων συναλλαγών (“commit / rollback”).

(γ) Για την προστασία των συστημάτων

i. να υπάρχει εγκατεστημένο ειδικό λογισμικό προστασίας από ιούς ή άλλο «κακόβουλο» λογισμικό,

ii. να παρέχεται αποτελεσματική προστασία σε ευαίσθητους πόρους των συστημάτων, όπως τα αρχεία συστήματος και εφαρμογών,

iii. να συντηρείται αρχείο με το εγκεκριμένο από το ίδρυμα λογισμικό,

iv. να απεγκαθίσταται ή να απενεργοποιείται σε κάθε σύστημα, κάθε λογισμικό ή λειτουργία που δεν κρίνεται απαραίτητη,

v. να ενεργοποιούνται τουλάχιστον οι βασικές λειτουργίες ελέγχου και καταγραφής (“auditing & logging functions”) σε κάθε σύστημα και να παραμετροποιούνται κατάλληλα σε συνεργασία με την εσωτερική επιθεώρηση,

vi. να εξασφαλίζεται όπου αυτό είναι αναγκαίο, κατόπιν σχετικής εγκριτικής διαδικασίας, η συνεχής ενημέρωση των συστημάτων με τις τελευταίες εκδόσεις λογισμικού και ενημερώσεων σε θέματα ασφάλειας, ώστε να ελαχιστοποιούνται οι αδυναμίες και τα τρωτά τους σημεία,

vii. να υπάρχουν καταγεγραμμένες διαδικασίες αποκατάστασης της ασφαλούς λειτουργίας ενός συστήματος σε περίπτωση που παραβιαστεί η ασφάλειά του,

viii. να προστατεύεται, όσο αυτό είναι εφικτό, το ηλεκτρονικό ταχυδρομείο από πιθανούς κινδύνους αναξιόπιστης γνησιότητας του αποστολέα, υποκλοπής ή/και παραποίησης του περιεχομένου, επικίνδυνων προσαρτημάτων και ανεπιθύμητων μηνυμάτων,

ix. να υπάρχουν περιορισμοί στις ενέργειες των χρηστών του διαδικτύου, για παράδειγμα στις προσβάσεις σε συγκεκριμένους διαδικτυακούς τόπους, στη διακίνηση αρχείων και σε άλλες σχετικές ενέργειες,

x. να γίνεται συνεχής εκπαίδευση και ενημέρωση των χρηστών σε θέματα ασφαλούς λειτουργίας των συστημάτων,

xi. να προστατεύονται αποτελεσματικά τα κρίσιμα συστήματα από κακόβουλες ενέργειες εξωτερικών ή εσωτερικών χρηστών. Προς αυτή την κατεύθυνση θα πρέπει να υλοποιούνται διάφορες τεχνικές, όπως:

1. η χρήση ειδικών συστημάτων (“firewalls”, “filtering routers” κλπ), τα οποία, ως σημεία ελέγχου των προσβάσεων, θα ρυθμίζουν και θα ελέγχουν την επικοινωνία από και προς περιοχές του δικτύου οι οποίες είναι συνήθως εκτεθειμένες σε αυξημένους κινδύνους,

2. η δημιουργία στο δίκτυο ειδικών περιοχών (“Demilitarized zones”), ανάμεσα σε σημεία ελέγχου προσβάσεων, οι οποίες να λειτουργούν σαν απομονωμένο δίκτυο για τα προσβάσιμα από εσωτερικούς ή εξωτερικούς χρήστες συστήματα του ιδρύματος, προστατεύοντας έτσι αποτελεσματικά το υπόλοιπο δίκτυο από κακόβουλες ενέργειες.

(δ) Για την ασφάλεια της δικτυακής υποδομής και των επικοινωνιών:

i. να είναι σαφώς καθορισμένες, καταγεγραμμένες και ελεγχόμενες οι δίοδοι επικοινωνίας (“gateways”) με εξωτερικά δίκτυα,

ii. να εκτιμάται η δυνατότητα κατάτμησης (“segmentation”) του δικτύου σε ελεγχόμενα επί μέρους υποδίκτυα για τον καλύτερο έλεγχο των προσβάσεων,

iii. να μην παραμένουν ανοιχτές λογικές θύρες επικοινωνίας (“ports”) σε οποιαδήποτε συσκευή του δικτύου, εκτός όσων έχουν καθοριστεί σαφώς ως αναγκαίες για τις υπηρεσίες που υποστηρίζουν και αφού έχει συνεκτιμηθεί ο συνεπαγόμενος κίνδυνος από τη λειτουργία τους,

iv. να περιορίζεται και να ελέγχεται επαρκώς η πρόσβαση στις ειδικές λειτουργίες διαχείρισης και ελέγχου του δικτύου,

v. να υπάρχει αποτελεσματική διαχείριση των παραμετροποιήσεων των συσκευών του δικτύου,

vi. να υπάρχει η δυνατότητα εντοπισμού λειτουργίας μη εξουσιοδοτημένων συσκευών, από το διαχειριστή του δικτύου,

vii. να περιορίζονται στα απολύτως απαραίτητα τα σημεία πρόσβασης στο δίκτυο, τα οποία βρίσκονται σε χώρους μη ελεγχόμενης φυσικής πρόσβασης. Ενόσω δε χρησιμοποιούνται, να παραμένουν ανενεργά,

viii. να περιορίζεται και να ελέγχεται συστηματικά η δυνατότητα ασύρματης σύνδεσης χρηστών στο δίκτυο, ώστε να αποτρέπεται η παρείσφρηση μη εξουσιοδοτημένων χρηστών σε αυτό,

ix. να μην παρέχεται η δυνατότητα απομεμακρυσμένης πρόσβασης στο δίκτυο και, όπου κρίνεται αναγκαία τέτοια πρόσβαση, να καταγράφεται και να ελέγχεται συστηματικά,

x. να χρησιμοποιούνται τα κατάλληλα πρωτόκολλα επικοινωνίας ανάλογα με το είδος των δεδομένων που μεταδίδονται, αντιμετωπίζοντας αποτελεσματικά θέματα διαχείρισης και ασφάλειάς τους,

xi. να εξασφαλίζεται η εμπιστευτικότητα και η ακεραιότητα των δεδομένων που μεταδίδονται μέσω του δικτύου καθ’ όλη τη διαδρομή τους σε αυτό,

xii. να γίνεται χρήση ειδικών εργαλείων λογισμικού για τον εντοπισμό κενών ασφαλείας ή σημείων μειωμένης ασφάλειας στο δίκτυο (“vulnerability tests”),

xiii. να υπάρχουν διαδικασίες και συστήματα παρακολούθησης, αποτροπής και αντιμετώπισης προσπαθειών παρείσφρησης στο δίκτυο ή γενικότερα προσπαθειών παραβίασης της ασφάλειας του δικτύου (“intrusion

detection/prevention systems"),

xiv. να διενεργούνται σε τακτική βάση, από ειδικευμένες εταιρίες, εξωτερικές και εσωτερικές δοκιμαστικές απόπειρες παραβίασης της ασφάλειας του δικτύου ("penetration tests"), βάσει καθορισμένων σεναρίων, με στόχο την αξιολόγηση της επάρκειας της ασφάλειας του δικτύου.

Οποιεσδήποτε τεχνικές απειλές και τρωτά σημεία θα πρέπει να εντοπίζονται, να αξιολογούνται και να αντιμετωπίζονται έγκαιρα, μέσω της θέσπισης ενός κατάλληλου προγράμματος διαχείρισης ευπαθειών ("vulnerability management programme").

Σχέδια Συνέχειας Εργασιών και Ανάκαμψης από Καταστροφή

(5) Τα ιδρύματα θα πρέπει να εφαρμόσουν κατάλληλο πρόγραμμα διαχείρισης επιχειρησιακής συνέχειας για τη διασφάλιση, σε συνεχή βάση, της δυνατότητας λειτουργίας τους και τον περιορισμό των ζημιών σε περίπτωση σοβαρής διαταραχής των επιχειρησιακών λειτουργιών τους. Στο πλαίσιο αυτό, τα ιδρύματα θα πρέπει να εφαρμόζουν Σχέδιο Συνέχειας Εργασιών, το οποίο να είναι εγκεκριμένο από τα ανώτατα διοικητικά στελέχη, έτσι ώστε να εξασφαλίζεται η συνέχεια των κρισιμότερων λειτουργιών και πληροφοριακών συστημάτων τους. Επιπλέον, τα ιδρύματα πρέπει να διαθέτουν αποτελεσματικό Σχέδιο Ανάκαμψης από Καταστροφή που θα εφαρμόζεται στις περιπτώσεις καταστροφικών συμβάντων που μπορεί να προκαλέσουν παρατεταμένη διακοπή της λειτουργίας ενός κρίσιμου συστήματος, ολόκληρου του μηχανογραφικού κέντρου, ή ακόμη και ολόκληρης της τεχνολογικής υποδομής. Για την εφαρμογή κατάλληλων Σχεδίων Συνέχειας Εργασιών και Ανάκαμψης από Καταστροφή, τα ιδρύματα θα πρέπει να αναλύσουν προσεκτικά την έκθεσή τους σε παράγοντες που δύνανται να επιφέρουν σοβαρές διαταραχές στη λειτουργία τους και να αξιολογούν (ποσοτικά και ποιοτικά) τις πιθανές επιπτώσεις, χρησιμοποιώντας εσωτερική ή/και εξωτερική πληροφόρηση για την ανάλυση δεδομένων και σεναρίων. Η ανάλυση αυτή θα πρέπει να καλύπτει όλες τις μονάδες του ιδρύματος, λαμβάνοντας υπόψη την αλληλεξάρτηση τους. Βάσει αυτών:

(α) θα προσδιορίζονται όλες οι κρίσιμες λειτουργίες καθώς και τα συστήματα και οι πόροι που χρησιμοποιούν,

(β) θα καθορίζονται με σαφήνεια οι προτεραιότητες και οι στόχοι ανάκαμψης,

(γ) θα προσδιορίζονται όλοι οι κίνδυνοι που απειλούν τις κρίσιμες λειτουργίες και θα κατατάσσονται σύμφωνα με την πιθανότητα εμφάνισής τους και τις πιθανές επιπτώσεις τους στα συστήματα και τις λειτουργίες,

(δ) θα σταθμίζεται το λειτουργικό κόστος από ενδεχόμενη διακοπή των κρίσιμων λειτουργιών και το κόστος ενεργοποίησης του Σχεδίου Συνέχειας Εργασιών και Σχεδίου Ανάκαμψης από Καταστροφή για να προσδιορίζονται οι συνθήκες που θα θέτουν σε εφαρμογή το αντίστοιχο σχέδιο

(ε) θα προσδιορίζεται ο χρόνος ανάκαμψης των κρίσιμων πληροφοριακών συστημάτων ("recovery time") αλλά και το σημείο ανάκαμψης ("recovery point"), δηλαδή σε πόσο χρόνο και σε ποια εικόνα χρονικά θα επανέλθουν μετά την ανάκαμψη.

(6) Πρώτο επίπεδο εξασφάλισης συνέχειας εργασιών θεωρείται η ύπαρξη σχεδίου λήψης και διαχείρισης αντιγράφων ασφαλείας του λογισμικού, των παραμέτρων λειτουργίας και των δεδομένων, καθώς και η ύπαρξη του αναγκαίου εφεδρικού εξοπλισμού, όπως συσκευών παροχής αδιάλειπτης τάσης και ηλεκτρογεννητριών στους χώρους λειτουργίας των συστημάτων. Με στόχο την εξασφάλιση της γρήγορης και επιτυχούς ανάκτησης των δεδομένων και του λογισμικού, θα πρέπει για τα αντίγραφα ασφαλείας να υφίστανται οι ακόλουθες διαδικασίες:

(α) δημιουργία αντιγράφων με συχνότητα που υπαγορεύεται από την κρισιμότητα των πληροφοριών.

(β) ασφαλούς φύλαξη στο χώρο των συστημάτων.

(γ) ασφαλούς μεταφορά και φύλαξη σε απομακρυσμένο χώρο των επιπλέον αντιγράφων.

(δ) δοκιμές για τη διασφάλιση της ακεραιότητας των δεδομένων.

(ε) αρχειοθέτηση με αναγραφή στα μέσα αποθήκευσης του περιεχομένου και του χρόνου αποθήκευσης των δεδομένων.

(7) Σε δεύτερο επίπεδο, ένα ολοκληρωμένο και αποτελεσματικό Σχέδιο Συνέχειας Εργασιών και Ανάκαμψης από Καταστροφή, συνίσταται να είναι γραμμένο σε απλή και κατανοητή γλώσσα και να κοινοποιείται επίσημα σε όλο το εμπλεκόμενο προσωπικό. Τυχόν διαβαθμισμένες πληροφορίες του σχεδίου, όπως για παράδειγμα κωδικοί, κλειδιά ασφαλείας, διαγράμματα δικτύου και άλλες συναφείς πληροφορίες θα πρέπει να γνωστοποιούνται μόνο σε εξουσιοδοτημένο προσωπικό. Αντίγραφο του σχεδίου να φυλάσσεται εκτυπωμένο σε ασφαλείς χώρους και σε συστήματα τα οποία είναι σε ασφαλή απόσταση από το μηχανογραφικό κέντρο. Επιπλέον, θα πρέπει να είναι άμεσα προσβάσιμο από το εμπλεκόμενο προσωπικό σε περίπτωση ανάγκης. Ένα τέτοιο σχέδιο θα πρέπει να περιλαμβάνει:

(α) κατάταξη των συστημάτων βάσει λειτουργικής ανάγκης. Στην κατάταξη αυτή θα πρέπει, μεταξύ άλλων, να αναφέρεται ο χρόνος που απαιτείται για την ανάκτηση του κάθε συστήματος καθώς και η ελάχιστη εκτιμώμενη απόδοσή του μετά την ανάκτηση.

(β) τη σαφή ιεραρχική δομή των στελεχών που συμμετέχουν στην εφαρμογή του, τις αρμοδιότητές τους, καθώς και τους υπεύθυνους λήψης αποφάσεων σε κάθε ομάδα έκτακτης ανάγκης.

(γ) τις διαδικασίες εκτίμησης του εύρους της καταστροφής, με βάση τις οποίες προσδιορίζονται επακριβώς τα

τμήματα του σχεδίου τα οποία θα πρέπει να ενεργοποιηθούν.

(δ) τις διαδικασίες ενεργοποίησης του σχεδίου, ειδοποίησης των στελεχών και κινητοποίησης των ομάδων έκτακτης ανάγκης.

(ε) τις ενέργειες που θα εκτελούνται σε συγκεκριμένες επείγουσες καταστάσεις, οι οποίες μεταξύ άλλων θα πρέπει να διασφαλίζουν το προσωπικό σε περίπτωση κινδύνου / καταστροφής όπως για παράδειγμα σε περίπτωση φωτιάς, σεισμού και άλλων καταστροφών.

(στ) τους εναλλακτικούς χώρους εργασίας των χρηστών, τον εξοπλισμό που θα χρησιμοποιηθεί, καθώς και τις απαιτούμενες προδιαγραφές τους.

(ζ) τις διαδικασίες προετοιμασίας και ενεργοποίησης του εναλλακτικού μηχανογραφικού κέντρου.

(η) τα συστήματα του εναλλακτικού κέντρου, την υποδομή τους καθώς και την τοπολογία δικτύου.

(θ) λίστα προμηθευτών με τους οποίους υπάρχουν συμβάσεις, τις υπηρεσίες που αυτοί προσφέρουν και τους αναμενόμενους χρόνους ανταπόκρισης τους σε περίπτωση έκτακτης ανάγκης.

(ι) τις διαδικασίες που εξασφαλίζουν ότι τα σχέδια συντηρούνται, προσαρμόζονται και ενημερώνονται σε κάθε αλλαγή στις διαδικασίες λειτουργίας του ιδρύματος.

(ια) τις διαδικασίες εκπαίδευσης του προσωπικού, σύμφωνα με τις αρμοδιότητες που αναλαμβάνουν κατά την υλοποίηση του σχεδίου.

(ιβ) τις διαδικασίες εκτέλεσης δοκιμών, σύμφωνα με τις οποίες:

i. θα προσδιορίζεται η συχνότητά τους (κατ' ελάχιστον μία φορά το χρόνο).

ii. θα υπάρχουν σαφείς στόχοι εκ των προτέρων, είτε για την εξέταση συγκεκριμένων υποσυστημάτων, είτε για την εξέταση του συστήματος στο σύνολό του. Η εκτέλεση δοκιμών της τελευταίας κατηγορίας συνιστάται να περιλαμβάνει την πλήρη κάλυψη όλων των κρίσιμων λειτουργιών όπως αναγράφονται στο σχέδιο και να κάνει αποκλειστική χρήση του εναλλακτικού χώρου, του εξοπλισμού και των εφεδρικών αντιγράφων.

iii. θα διεξάγονται υπό συνθήκες που θα προσομοιώνουν περιπτώσεις έκτακτης ανάγκης.

iv. θα εξασφαλίζεται η συμμετοχή της Μονάδας Εσωτερικής Επιθεώρησης.

v. θα συντάσσεται έκθεση των αποτελεσμάτων μετά την ολοκλήρωση των δοκιμών.

vi. θα γίνονται οι απαραίτητες αναθεωρήσεις και διορθώσεις στα σχέδια για την αντιμετώπιση όλων των δυσκολιών και προβλημάτων που διαπιστώνονται σε κάθε δοκιμή.

vii. θα λαμβάνουν γνώση των αποτελεσμάτων τα ανώτατα διοικητικά στελέχη και η Επιτροπή Ελέγχου.

(8) Τέλος, θα πρέπει:

(α) να εξασφαλίζει την ύπαρξη κατάλληλων σχεδίων επαναφοράς για τους κρίσιμους πόρους, έτσι ώστε να μπορέσει το ίδρυμα να επιστρέψει στην ομαλή διεξαγωγή των εργασιών του εντός κατάλληλου χρονικού διαστήματος,

(β) να εξασφαλίζει την αποτελεσματική λειτουργία εναλλακτικού μηχανογραφικού κέντρου, το οποίο θα πρέπει να βρίσκεται σε κατάλληλη απόσταση, ώστε να μην επηρεάζεται από τους ίδιους κινδύνους που μπορεί να πλήξουν το κύριο μηχανογραφικό κέντρο. Το εναλλακτικό κέντρο θα πρέπει να διαθέτει κατάλληλο (εφεδρικό) εξοπλισμό που να παρέχει όλες τις κρίσιμες υπηρεσίες στους χρόνους που έχουν προκαθοριστεί, καθώς και τα εγχειρίδια των διαδικασιών και χρήσης των συστημάτων. Επιπλέον, θα πρέπει να επιτρέπει την απρόσκοπτη χρήση των εναλλακτικών μέσων μέχρι τη στιγμή της επαναφοράς των λειτουργιών στο κύριο μηχανογραφικό κέντρο.

(γ) να διασφαλίζει τη φυσική ασφάλεια του εναλλακτικού κέντρου, καθώς και ένα αποδεκτό επίπεδο λογικής ασφάλειας κατά την εφαρμογή του σχεδίου.

(δ) να φροντίζει για την ασφαλιστική κάλυψη του ιδρύματος έναντι κινδύνων που είναι δυνατόν να προκαλέσουν διακοπή της λειτουργίας των Πληροφοριακών Συστημάτων.

(ε) σε περίπτωση που οι χώροι λειτουργίας του εναλλακτικού κέντρου, ο εξοπλισμός ή οι υπηρεσίες παρέχονται από τρίτους:

i. να προνοεί, μέσω κατάλληλων συμβάσεων, για την αποτελεσματική συνέχεια των εργασιών σε περίπτωση καταστροφής που θα πλήξει ταυτόχρονα πολλούς οργανισμούς οι οποίοι εξυπηρετούνται από τον ίδιο πάροχο

ii. να φροντίζει για την ενημέρωση του παρόχου για τυχόν αλλαγές στα συστήματα που πιθανό να απαιτήσουν αντίστοιχες προσαρμογές-ενημερώσεις στα Σχέδια Ανάκαμψης από Καταστροφή.

ΜΕΡΟΣ V
ΕΛΕΓΧΟΣ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ

9. (1) Μια αποτελεσματική λειτουργία ελέγχου για τα Πληροφοριακά Συστήματα θα πρέπει να εστιάζεται στους κινδύνους που απορρέουν από την ανάπτυξη, ενσωμάτωση και λειτουργία τους, να εξετάζει την επάρκεια των ελεγκτικών μηχανισμών ("controls") και διαδικασιών, και να προτείνει, όπου χρειάζεται, τις κατάλληλες τροποποιήσεις. Επιπλέον, θα πρέπει να αξιολογεί το βαθμό συμμόρφωσης με την επιχειρηματική στρατηγική και τις καταγεγραμμένες πολιτικές, τα

πρότυπα και τις διαδικασίες, και να παρακολουθεί το βαθμό συμμόρφωσης με τις διαπιστώσεις των πορισμάτων των ελέγχων. Τέλος, θα πρέπει να διαμορφώνει ολοκληρωμένη εικόνα για τη λειτουργία των Πληροφοριακών Συστημάτων ώστε να δίνεται η δυνατότητα επαρκούς ενημέρωσης σε ετήσια βάση της Επιτροπής Ελέγχου.

(2) Για τους λόγους αυτούς, η Λειτουργία Εσωτερικής Επιθεώρησης θα πρέπει:

(α) να διαθέτει την τεχνογνωσία, την ποιοτική και ποσοτική επάρκεια προσωπικού, μέσων και διαδικασιών για τη διενέργεια εξειδικευμένων ελέγχων στα Πληροφοριακά Συστήματα. Η τεχνογνωσία και η εκπαίδευση του προσωπικού θα πρέπει να είναι τέτοιες ώστε να καλύπτονται ελεγκτικά οι τρέχουσες και οι μελλοντικές μηχανογραφικές λειτουργίες του ιδρύματος.

(β) να καταρτίζει και να υλοποιεί ελεγκτικό πρόγραμμα, το οποίο θα βασίζεται σε ανάλυση κινδύνων που έχει διενεργηθεί στα Πληροφοριακά Συστήματα αλλά και σε ευρήματα προγενέστερων ελέγχων.

(γ) να ακολουθεί καταγεγραμμένες διαδικασίες σχεδιασμού, οργάνωσης και διενέργειας των ελέγχων, συγγραφής των πορισμάτων καθώς και διαδικασίες επανελέγχου ("follow-up"). Οι διαδικασίες αυτές, τα κάθε είδους προγράμματα ελέγχου που χρησιμοποιούνται στους εξειδικευμένους ελέγχους, καθώς και η χρησιμοποιούμενη μεθοδολογία ανάλυσης μηχανογραφικών κινδύνων, θα πρέπει να αποτελούν την επίσημη τεκμηρίωση της λειτουργίας του ελέγχου των Πληροφοριακών Συστημάτων.

(δ) να παρακολουθεί τα θέματα που αφορούν τα Πληροφοριακά Συστήματα του ιδρύματος, ώστε να διαμορφώνει εικόνα για τους κινδύνους που υπάρχουν ή ενδέχεται να ανακύψουν. Για τη διαμόρφωση όσο το δυνατόν πληρέστερης εικόνας, συνίσταται η παρακολούθηση της λειτουργίας των Πληροφοριακών Συστημάτων μέσω ειδικών προσβάσεων χωρίς δυνατότητα εκτέλεσης συναλλαγών, η συμμετοχή στις διάφορες επιτροπές έργων και η ύπαρξη διαδικασιών και μηχανισμών άμεσης ενημέρωσης της Λειτουργίας Εσωτερικής Επιθεώρησης στις περιπτώσεις εμφάνισης σημαντικών προβλημάτων και εκτάκτων περιστατικών.

(ε) να κάνει χρήση – ανάλογα με την περίπτωση - ειδικού ελεγκτικού λογισμικού για τον αποτελεσματικότερο έλεγχο της ασφάλειας των συστημάτων και της ακεραιότητας των δεδομένων τους.

(στ) να συμμετέχει στη φάση σχεδιασμού των συστημάτων για τη διαμόρφωση κατάλληλων δικλείδων ασφαλείας για τον έλεγχο των πληροφοριακών συστημάτων, των ελεγκτικών αρχείων καταγραφής και αναφορών που παράγονται για τη διευκόλυνση του ελέγχου, καθώς και στη φάση των δοκιμών.

(ζ) να ελέγχει και να αξιολογεί τις διαδικασίες παραγωγής των στοιχείων που υποβάλλονται στα Ανώτατα Διοικητικά Στελέχη του ιδρύματος και τις Εποπτικές Αρχές ώστε να διασφαλίζεται η πληρότητα και ακρίβειά τους.

(η) να μεριμνά για την άμεση και πλήρη ενημέρωση προς την Κεντρική Τράπεζα της Κύπρου, στις περιπτώσεις σοβαρών προβλημάτων και έκτακτων περιστατικών στα Πληροφοριακά Συστήματα (περιπτώσεις απάτης, παραβίασης της ασφάλειας σημαντικών συστημάτων, μη διαθεσιμότητας ή δυσλειτουργίας κρίσιμων συστημάτων, ενεργοποίησης Σχεδίων Ανάκαμψης από Καταστροφή), ή στην περίπτωση ενεργοποίησης του Σχεδίου Συνέχειας Εργασιών κατόπιν καταστροφής.

(θ) να ελέγχει και να αξιολογεί την επάρκεια και συμμόρφωση με τις διαδικασίες που διέπουν τις φάσεις συνεργασίας του ιδρύματος με προμηθευτές και παρόχους μηχανογραφικών υπηρεσιών, για παράδειγμα την επιλογή συνεργάτη, τη σύναψη και τήρηση συμβολαίου, την ποιότητα των παρεχόμενων υπηρεσιών βάσει των προαναφερθέντων στο Μέρος ΙΙΙ του παρόντος Παραρτήματος.

(ι) να επιβλέπει το ελεγκτικό έργο στα συστήματα πληροφορικής σε επίπεδο ομίλου. Για το σκοπό αυτό οφείλει να διατηρεί διαύλους επικοινωνίας με στόχο την αποτελεσματική συνεργασία με τις διοικήσεις και τον εσωτερικό έλεγχο των θυγατρικών και του δικτύου υποκαταστημάτων εξωτερικού. Να αξιολογεί την επάρκεια του ελεγκτικού έργου μέσω περιοδικών αναφορών ή και συμμετοχής του στις Επιτροπές Ελέγχου των θυγατρικών, ειδικά σε αυτές που το μέγεθος και η πολυπλοκότητα των συστημάτων το καθιστούν αναγκαίο. Να αξιολογεί την επάρκεια των διενεργούμενων εξειδικευμένων ελέγχων από εσωτερικούς και εξωτερικούς ελεγκτές. Να προβαίνει σε γενικούς ή ειδικούς ελέγχους ανά περίπτωση, για την κάλυψη των ελεγκτικών αναγκών που είτε δεν καλύπτονται επαρκώς από τον εσωτερικό έλεγχο των εν λόγω μονάδων, είτε κρίνονται απαραίτητοι από τη σχετική ανάλυση κινδύνων.

(ια) να μελετά, αξιολογεί και εφαρμόζει, όπου κρίνει πρόσφορο, τα διεθνή πρότυπα και μεθοδολογίες ελέγχου Πληροφοριακών Συστημάτων.

(3) Σε ότι αφορά στους ελέγχους που ανατίθενται σε εξωτερικούς ελεγκτές, τα ιδρύματα θα πρέπει να διαθέτουν πολιτική για το εύρος και το ρόλο του εξωτερικού ελέγχου στα Πληροφοριακά Συστήματα, καθώς και διαδικασίες αξιολόγησης των προσφερομένων υπηρεσιών. Η πολιτική θα πρέπει να τεκμηριώνει τις περιπτώσεις που ο εξωτερικός έλεγχος δρα είτε παράλληλα με τον εσωτερικό προσφέροντας μια επιπλέον εξειδικευμένη άποψη, είτε συμπληρωματικά προκειμένου να καλύψει εξειδικευμένες ελεγκτικές απαιτήσεις όπου δεν υπάρχει η δυνατότητα να καλυφθούν εσωτερικά, ή και με τους δύο τρόπους.