

Κατευθυντήριες γραμμές

σχετικά με τους εσωτερικούς ελέγχους για τους διαχειριστές δεικτών αναφοράς, τους οργανισμούς αξιολόγησης της πιστοληπτικής ικανότητας και τις υποδομές διαφάνειας της αγοράς

Πίνακας περιεχομένων

1	Πεδίο εφαρμογής	4
2	Νομοθετικές παραπομπές, συντομογραφίες και ορισμοί	6
2.1	Νομοθετικές παραπομπές	6
2.2	Συντομογραφίες	7
2.3	Ορισμοί	8
3	Σκοπός	9
4	Υποχρεώσεις συμμόρφωσης και υποβολής στοιχείων και αναφορών	9
4.1	Καθεστώς των κατευθυντήριων γραμμών	9
4.2	Απαιτήσεις υποβολής στοιχείων και αναφορών	9
5	Κατευθυντήριες γραμμές σχετικά με τους εσωτερικούς ελέγχους	11
5.1	Πλαίσιο εσωτερικού ελέγχου	11
	Συνιστώσα 1.1 Περιβάλλον ελέγχου	11
	Συνιστώσα 1.2 Διαχείριση κινδύνων	12
	Συνιστώσα 1.3 Δραστηριότητες δικλίδων ελέγχου	13
	Συνιστώσα 1.4 Ενημέρωση και επικοινωνία	16
	Συνιστώσα 1.5 Δραστηριότητες παρακολούθησης	16
5.2	Λειτουργίες εσωτερικού ελέγχου	17
	Αναλογικότητα – Λειτουργίες εσωτερικού ελέγχου	19
	Συνιστώσα 2.1 Λειτουργία συμμόρφωσης	20
	Συνιστώσα 2.2 Λειτουργία διαχείρισης κινδύνων	21
	Συνιστώσα 2.3 Λειτουργία διαχείρισης της ασφάλειας των πληροφοριών (μόνο για εποπτευόμενες οντότητες που δεν υπόκεινται στον κανονισμό DORA)	22
	Συνιστώσα 2.4 Λειτουργία εσωτερικής επιθεώρησης	23
	Συνιστώσα 2.5 Λειτουργία επανεξέτασης (μόνο για τους ΟΑΠΙ)	24
	Συνιστώσα 2.6 Λειτουργία εποπτείας (μόνο για τους ΒΜΑ)	25

1 Πεδίο εφαρμογής

Ποιος;

1. Οι παρούσες κατευθυντήριες γραμμές εφαρμόζονται σε:

(i) διαχειριστές δεικτών αναφοράς, οι οποίοι έχουν άδεια, είναι εγγεγραμμένοι στο μητρώο ή είναι αναγνωρισμένοι από την ESMA (εφεξής αναφέρονται συλλήβδην ως «BMA») σύμφωνα με τον κανονισμό για τους δείκτες αναφοράς·

(ii) οργανισμούς αξιολόγησης πιστοληπτικής ικανότητας εγκατεστημένους στην Ένωση και εγγεγραμμένους στην ESMA (ΟΑΠΙ) σύμφωνα με τον κανονισμό ΟΑΠΙ·

(iii) παρόχους υπηρεσιών αναφοράς δεδομένων (ΠΥΑΔ) [εξαιρουμένων των παρόχων ενοποιημένου δελτίου συναλλαγών (Π.Ε.ΔΕ.ΣΥ.)] που είναι εγκατεστημένοι στην Ένωση και έχουν λάβει άδεια από την ESMA σύμφωνα με τον κανονισμό MiFIR·

(iv) αρχεία καταγραφής τιτλοποιήσεων που είναι εγκατεστημένα στην Ένωση και καταχωρισμένα στην ESMA (Securitisations Repositories-SR) σύμφωνα με τον κανονισμό για την τιτλοποίηση (SecR)·

(v) αρχεία καταγραφής συναλλαγών (ΑΚΣ) εγκατεστημένα στην Ένωση και καταχωρισμένα στην ESMA σύμφωνα με τον κανονισμό EMIR

(vi) αρχεία καταγραφής συναλλαγών εγκατεστημένα στην Ένωση και καταχωρισμένα στην ESMA σύμφωνα με τον κανονισμό για τις συναλλαγές χρηματοδότησης τίτλων (SFTR) (εφεξής αναφέρονται συλλήβδην ως «επιοπτευόμενες οντότητες»).

Τι;

2. Οι παρούσες κατευθυντήριες γραμμές αφορούν ζητήματα που σχετίζονται με τη δομή και τους μηχανισμούς εσωτερικού ελέγχου που απαιτούνται για τη διασφάλιση i) της αποτελεσματικής συμμόρφωσης των BMA με τα άρθρα 4 έως 10 του κανονισμού BMR ii) της αποτελεσματικής συμμόρφωσης των ΟΑΠΙ με το άρθρο 6 παράγραφοι 1, 2 και 4, το άρθρο 9 και το παράρτημα I ενότητα A του κανονισμού ΟΑΠΙ· iii) της αποτελεσματικής συμμόρφωσης των ΠΥΑΔ με τα άρθρα 27στ, 27ζ, 27θ του κανονισμού MiFIR· και iv) της αποτελεσματικής συμμόρφωσης των TR ή των SR με τα άρθρα 78 και 79 του κανονισμού EMIR.

Πότε;

3. Οι παρούσες κατευθυντήριες γραμμές εφαρμόζονται από την 1η Οκτωβρίου 2026.
4. Από την ημερομηνία που αναφέρεται στην παράγραφο 3, οι κατευθυντήριες γραμμές για τον εσωτερικό έλεγχο των ΟΑΠΙ (ESMA33-9-371) καταργούνται.

2 Νομοθετικές παραπομπές, συντομογραφίες και ορισμοί

2.1 Νομοθετικές παραπομπές

DORA	Κανονισμός (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014, (ΕΕ) αριθ. 909/2014 και (ΕΕ) 2016/1011. ¹
Κανονισμός EMIR	Κανονισμός (ΕΕ) αριθ. 648/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 4ης Ιουλίου 2012, για τα εξωχρηματιστηριακά παράγωγα, τους κεντρικούς αντισυμβαλλομένους και τα αρχεία καταγραφής συναλλαγών ²
Κανονισμός για την τιτλοποίηση (SecR)	Κανονισμός (ΕΕ) 2017/2402 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Δεκεμβρίου 2017, σχετικά με τη θέσπιση γενικού πλαισίου για την τιτλοποίηση και σχετικά με τη δημιουργία ειδικού πλαισίου για απλή, διαφανή και τυποποιημένη τιτλοποίηση και σχετικά με την τροποποίηση των οδηγιών 2009/65/ΕΚ, 2009/138/ΕΚ και 2011/61/ΕΕ και των κανονισμών (ΕΚ) αριθ. 1060/2009 και (ΕΕ) αριθ. 648/2012 ³
Κανονισμός για τις αγορές χρηματοπιστωτικών μέσων (MiFIR)	Κανονισμός (ΕΕ) αριθ. 600/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 15ης Μαΐου 2014, για τις αγορές χρηματοπιστωτικών μέσων και για την τροποποίηση του κανονισμού (ΕΕ) αριθ. 648/2012 ⁴
Κανονισμός για τις συναλλαγές χρηματοδότησης τίτλων (SFTR)	Κανονισμός (ΕΕ) 2015/2365 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Νοεμβρίου 2015, περί διαφάνειας των συναλλαγών χρηματοδότησης τίτλων και επαναχρησιμοποίησης, και περί τροποποιήσεως του κανονισμού (ΕΕ) αριθ. 648/2012 ⁵
Κανονισμός για τους δείκτες αναφοράς (BMR)	Κανονισμός (ΕΕ) 2016/1011 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 8ης Ιουνίου 2016, σχετικά με τους δείκτες που χρησιμοποιούνται ως δείκτες αναφοράς σε χρηματοπιστωτικά μέσα και χρηματοπιστωτικές συμβάσεις ή για τη μέτρηση της απόδοσης επενδυτικών κεφαλαίων, και για την τροποποίηση των

¹ ΕΕ L 333 της 27.12.2022, σ. 1.

² ΕΕ L 201 της 27.7.2012, σ. 1

³ ΕΕ L 347 της 28.12.2017, σ. 35.

⁴ ΕΕ L 173 της 12.6.2014, σ. 84.

⁵ ΕΕ L 337 της 23.12.2015, σ. 1.

οδηγιών 2008/48/ΕΚ και 2014/17/ΕΕ και του κανονισμού (ΕΕ) αριθ. 596/2014⁶

Κανονισμός ΟΑΠΙ

Κανονισμός (ΕΚ) αριθ. 1060/2009 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 16ης Σεπτεμβρίου 2009, για τους οργανισμούς αξιολόγησης πιστοληπτικής ικανότητας⁷

2.2 Συντομογραφίες

DORA	Πράξη σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα
ESMA	Ευρωπαϊκή Αρχή Κινητών Αξιών και Αγορών
INED	Ανεξάρτητο μη εκτελεστικό στέλεχος
SR	Αρχείο καταγραφής τιτλοποιήσεων
TN	Τεχνητή νοημοσύνη
ΑΚΣ	Αρχείο καταγραφής συναλλαγών
BMA	Διαχειριστής δείκτη αναφοράς
Ε.ΜΗ.ΓΝΩ.ΣΥ.	Εγκεκριμένος μηχανισμός γνωστοποίησης συναλλαγών
Ε.ΜΗ.ΔΗ.ΣΥ.	Εγκεκριμένος μηχανισμός δημοσιοποίησης συναλλαγών
ΕΔ	Έγγραφο διαβούλευσης
ΕΕ	Ευρωπαϊκή Ένωση
Λειτουργίες ΕΕ	Λειτουργίες εσωτερικού ελέγχου
ΜΙ	Πληροφορίες σχετικά με τη διαχείριση
ΟΑΠΙ	Οργανισμός αξιολόγησης πιστοληπτικής ικανότητας
Πλαίσιο ΕΕ	Πλαίσιο εσωτερικού ελέγχου
ΠΥΑΔ	Πάροχος υπηρεσιών αναφοράς δεδομένων
ΡΤΠ	Ρυθμιστικά τεχνικά πρότυπα

⁶ ΕΕ L 171 της 29.6.2016, σ. 1

⁷ ΕΕ L 302 της 17.11.2009, σ. 1.

ΤΠΕ

Τεχνολογία πληροφοριών και επικοινωνιών

2.3 Ορισμοί

<p>Διοικητικό όργανο</p>	<p>Το όργανο ή τα όργανα, τα οποία είναι διορισμένα σύμφωνα με την εθνική νομοθεσία, έχουν την εξουσία να καθορίζουν τη στρατηγική, τους στόχους και τη συνολική κατεύθυνση της οντότητας, επιβλέπουν και παρακολουθούν τη διαδικασία λήψης αποφάσεων αναφορικά με τη διοίκησή της, και περιλαμβάνουν πρόσωπα που διευθύνουν πραγματικά τις δραστηριότητες της οντότητας.</p> <p>Πρόκειται για τα διοικητικά όργανα στο ανώτερο επίπεδο διοίκησης ενός οργανισμού.</p> <p>Ο όρος ορίζεται στο άρθρο 3 παράγραφος 1 σημείο 20 του κανονισμού για τους δείκτες αναφοράς και στο άρθρο 2 παράγραφος 1 σημείο 22 του κανονισμού MIFIR.</p> <p>Καλύπτει τις εξής έννοιες:</p> <ul style="list-style-type: none"> ▪ το «διοικητικό ή εποπτικό όργανο» ενός ΟΑΠΙ, το οποίο ανήκει στην «ανώτερη διοίκηση», όπως ορίζεται στον κανονισμό ΟΑΠΙ, άρθρο 3 παράγραφος 1 στοιχείο ιδ) ▪ «το διοικητικό ή το εποπτικό συμβούλιο, ή και τα δύο, σύμφωνα με το εθνικό δίκαιο των εταιρειών», όπως ορίζεται στον κανονισμό EMIR, άρθρο 2 σημείο 27
<p>Εκτελεστική ανώτερη διοίκηση</p>	<p>Τα ανώτερα στελέχη που διευθύνουν την εποπτευόμενη οντότητα σε καθημερινή βάση. Είναι συνήθως ο διευθύνων σύμβουλος (CEO) ή ισοδύναμο στέλεχος και οι άμεσα υφιστάμενοί του.</p>
<p>Εποπτευόμενες οντότητες</p>	<p>Για τους σκοπούς των παρουσών κατευθυντήριων γραμμών, πρόκειται για τις οντότητες που εμπίπτουν στην εποπτική αρμοδιότητα της ESMA, συγκεκριμένα:</p> <ul style="list-style-type: none"> ▪ BMA ▪ ΟΑΠΙ ▪ ΠΥΑΔ (εξαιρουμένων των παρόχων ενοποιημένου δελτίου συναλλαγών) ▪ SR ▪ ΑΚΣ
<p>Συναφείς κανονισμοί</p>	<p>Για τους σκοπούς των παρουσών κατευθυντήριων γραμμών, οι συναφείς κανονισμοί είναι οι εξής:</p> <ul style="list-style-type: none"> ▪ Κανονισμός για τους δείκτες αναφοράς ▪ Κανονισμός ΟΑΠΙ

- Κανονισμός EMIR
- Κανονισμός για τις αγορές χρηματοπιστωτικών μέσων (MiFIR)
- Κανονισμός για την τιτλοποίηση (SecR)
- Κανονισμός για τις συναλλαγές χρηματοδότησης τίτλων (SFTR)

Υποδομές διαφάνειας της αγοράς

Για τους σκοπούς των παρουσών κατευθυντήριων γραμμών, ο όρος αναφέρεται σε:

- παρόχους υπηρεσιών αναφοράς δεδομένων
- αρχεία καταγραφής τιτλοποιήσεων και
- αρχεία καταγραφής συναλλαγών

3 Σκοπός

5. Οι παρούσες κατευθυντήριες γραμμές καθορίζουν τις προσδοκίες της ESMA όσον αφορά τις συνιστώσες και τα χαρακτηριστικά ενός αποτελεσματικού πλαισίου εσωτερικού ελέγχου και τις λειτουργίες των διαφόρων εσωτερικών ελέγχων εντός μιας εποπτευόμενης οντότητας.

4 Υποχρεώσεις συμμόρφωσης και υποβολής στοιχείων και αναφορών

4.1 Καθεστώς των κατευθυντήριων γραμμών

6. Το παρόν έγγραφο περιέχει κατευθυντήριες γραμμές, οι οποίες εκδίδονται βάσει του άρθρου 16 του κανονισμού ESMA. Σύμφωνα με το άρθρο 16 παράγραφος 3 του κανονισμού ESMA, οι εποπτευόμενες οντότητες καταβάλλουν κάθε δυνατή προσπάθεια για να συμμορφωθούν με τις κατευθυντήριες γραμμές.

4.2 Απαιτήσεις υποβολής στοιχείων και αναφορών

7. Οι συμμετέχοντες στις χρηματοοικονομικές αγορές στους οποίους εφαρμόζονται οι παρούσες κατευθυντήριες γραμμές δεν υποχρεούνται να γνωστοποιούν κατά πόσον συμμορφώνονται με τις παρούσες κατευθυντήριες γραμμές. Η ESMA θα αξιολογεί την εφαρμογή των παρουσών κατευθυντήριων γραμμών από τις εποπτευόμενες οντότητες μέσω της συνεχούς εποπτείας και παρακολούθησης των δραστηριοτήτων τους.

8. Η ESMA θα τηρεί την αρχή της αναλογικότητας κατά την εφαρμογή των παρουσών κατευθυντήριων γραμμών. Ενώ όλες οι εποπτευόμενες οντότητες οφείλουν να αποδεικνύουν ότι διαθέτουν τις συνιστώσες και τα χαρακτηριστικά αποτελεσματικού συστήματος εσωτερικού ελέγχου που περιγράφονται στις παρούσες κατευθυντήριες γραμμές, η ESMA θα διαβαθμίσει τις προσδοκίες της σύμφωνα με την ενότητα 4.2 ανάλογα με τη φύση, την κλίμακα, την πολυπλοκότητα και το συνολικό προφίλ κινδύνου της εποπτευόμενης οντότητας και με βάση τον τρόπο με τον οποίο αυτά τα χαρακτηριστικά μπορεί να επηρεάσουν την προστασία των επενδυτών, την εύρυθμη λειτουργία της αγοράς και τη χρηματοπιστωτική σταθερότητα.
9. Κατά την αξιολόγηση της φύσης της εποπτευόμενης οντότητας, η ESMA λαμβάνει υπόψη την επιχειρηματική δραστηριότητα και το είδος των δραστηριοτήτων της εποπτευόμενης οντότητας, συμπεριλαμβανομένου του ρόλου/της αποστολής της στην αγορά, το είδος, την ποικιλομορφία και την κρισιμότητα των προϊόντων και των υπηρεσιών που προσφέρει.
10. Κατά την αξιολόγηση της κλίμακας των δραστηριοτήτων της εποπτευόμενης οντότητας, η ESMA θα λαμβάνει υπόψη σχετικούς παράγοντες, όπως το προσωπικό, τα έσοδα, τον αριθμό των πελατών και των προϊόντων, το μερίδιο αγοράς, τις διασυνδέσεις με άλλους κλάδους/υποδομές, τις βοηθητικές υπηρεσίες και τη σχέση τους με τις βασικές υπηρεσίες, καθώς και άλλους παράγοντες που αφορούν ειδικά το μέγεθος και τον αντίκτυπο στην αγορά της εποπτευόμενης οντότητας.
11. Κατά την αξιολόγηση της πολυπλοκότητας της εποπτευόμενης οντότητας, η ESMA λαμβάνει υπόψη, μεταξύ άλλων παραγόντων, την οργανωτική της δομή και τις ρυθμίσεις (δομή/σχέσεις ομίλου, κοινές υπηρεσίες, εξωτερική ανάθεση δραστηριοτήτων κ.λπ.), καθώς και τα λειτουργικά της χαρακτηριστικά σε σχέση με τα πρόσωπα, τις διαδικασίες, την τεχνολογία, τις προσφορές προϊόντων και τις διασυνδέσεις.
12. Η ESMA, κατά τη διαβάθμιση των προσδοκιών της, λαμβάνει υπόψη τις προϋποθέσεις καταχώρισης ή αναγνώρισης της εποπτευόμενης οντότητας. Η φύση, η κλίμακα και η πολυπλοκότητα μιας εποπτευόμενης οντότητας μπορεί να αλλάξουν μετά την εγγραφή της ή την αναγνώρισή της, και είναι ευθύνη της εποπτευόμενης οντότητας να διασφαλίσει ότι οι εσωτερικοί έλεγχοί της παραμένουν ανάλογοι με τη φύση, την κλίμακα και την πολυπλοκότητά της. Η ESMA θα γνωστοποιεί μέσω της εποπτείας της εάν έχει υψηλότερο επίπεδο προσδοκιών, βάσει των τμημάτων 5.1 και 5.2, από εκείνα που καθορίζονται κατά την καταχώριση ή την αναγνώριση.

5 Κατευθυντήριες γραμμές σχετικά με τους εσωτερικούς ελέγχους

13. Προκειμένου να αποδείξουν ότι συμμορφώνονται με την παράγραφο 2 των παρουσών κατευθυντήριων γραμμών, οι εποπτευόμενες οντότητες θα πρέπει να αποδείξουν ότι οι πολιτικές, οι διαδικασίες και οι πρακτικές εργασίας τους επιτυγχάνουν τους στόχους που ορίζονται στο τμήμα **5.1** (Πλαίσιο εσωτερικού ελέγχου) και στο τμήμα **5.2** (Λειτουργίες εσωτερικού ελέγχου) των παρουσών κατευθυντήριων γραμμών.

5.1 Πλαίσιο εσωτερικού ελέγχου

14. Προκειμένου να διασφαλιστεί ένα αποτελεσματικό πλαίσιο εσωτερικού ελέγχου, οι εποπτευόμενες οντότητες θα πρέπει να έχουν τις ακόλουθες συνιστώσες και χαρακτηριστικά στις πολιτικές, τις διαδικασίες και τις εργασιακές πρακτικές τους.

Γενικές αρχές

15. Το διοικητικό όργανο της εποπτευόμενης οντότητας θα πρέπει να είναι υπόλογο για την εποπτεία και την έγκριση όλων των συνιστωσών του πλαισίου εσωτερικού ελέγχου, καθώς και για τη μέριμνα ότι οι εν λόγω συνιστώσες υπόκεινται σε παρακολούθηση και επικαιροποιούνται τακτικά από την εκτελεστική ανώτερη διοίκηση. Η εκτελεστική ανώτερη διοίκηση θα πρέπει να είναι επιφορτισμένη με τη θέσπιση, υλοποίηση και επικαιροποίηση των γραπτώς τεκμηριωμένων πολιτικών, διαδικασιών και πρακτικών εσωτερικού ελέγχου που υποστηρίζουν τις συνιστώσες του πλαισίου εσωτερικού ελέγχου.
16. Στο πλαίσιο της υλοποίησης των εν λόγω πολιτικών και διαδικασιών, μια εποπτευόμενη οντότητα θα πρέπει να διαθέτει σαφείς, διαφανείς και τεκμηριωμένες διαδικασίες λήψης αποφάσεων, καθώς και σαφή κατανομή ρόλων και αρμοδιοτήτων στο πλαίσιο εσωτερικού ελέγχου της, συμπεριλαμβανομένων των επιχειρηματικών τομέων και των λειτουργιών εσωτερικού ελέγχου της.

Συνιστώσα 1.1 Περιβάλλον ελέγχου

17. Το διοικητικό όργανο και η εκτελεστική ανώτερη διοίκηση της εποπτευόμενης οντότητας δίνουν από κοινού το παράδειγμα για τη σημασία του εσωτερικού ελέγχου. Η εκτελεστική ανώτερη διοίκηση είναι υπεύθυνη για την ανάπτυξη και τη διενέργεια του εσωτερικού ελέγχου, καθώς και για την αξιολόγηση της επάρκειας και της αποτελεσματικότητας του περιβάλλοντος ελέγχου. Το διοικητικό όργανο θα πρέπει να ασκεί την εποπτεία της εκτελεστικής ανώτερης διοίκησης στους τομείς αυτούς.

Χαρακτηριστικά

- 1.1.1** Η εκτελεστική ανώτερη διοίκηση θα πρέπει να είναι υπεύθυνη για τη διασφάλιση ενός ισχυρού πνεύματος δεοντολογίας και συμμόρφωσης εντός της εποπτευόμενης οντότητας μέσω της εφαρμογής πολιτικών και διαδικασιών που διέπουν τη συμπεριφορά του προσωπικού της εποπτευόμενης οντότητας.
- 1.1.2** Η εκτελεστική ανώτερη διοίκηση της εποπτευόμενης οντότητας θα πρέπει να έχει την ευθύνη να διασφαλίζει ότι οι πολιτικές και οι διαδικασίες της εποπτευόμενης οντότητας:
- i. προσδιορίζουν ότι η επιχειρηματική δραστηριότητα της εποπτευόμενης οντότητας θα πρέπει να διεξάγεται σύμφωνα με τους σχετικούς κανονισμούς και τις εταιρικές αξίες της εποπτευόμενης οντότητας·
 - ii. αποσαφηνίζουν ότι, επιπλέον, της συμμόρφωσης προς τις νομοθετικές και κανονιστικές απαιτήσεις και τις εσωτερικές πολιτικές, αναμένεται από το προσωπικό να συμπεριφέρεται με ειλικρίνεια και ακεραιότητα και να εκτελεί τα καθήκοντά του με τη δέουσα δεξιότητα, φροντίδα και επιμέλεια· και
 - iii. διασφαλίζουν ότι το προσωπικό είναι ενήμερο για τα εσωτερικά και εξωτερικά πειθαρχικά μέτρα, καθώς και για τις νομικές ενέργειες και κυρώσεις που ενδέχεται να συνεπάγεται η διάπραξη παραπτώματων.
- 1.1.3** Η εκτελεστική ανώτερη διοίκηση της εποπτευόμενης οντότητας θα πρέπει να θεσπίζει, να διατηρεί και να επικαιροποιεί ανά τακτά χρονικά διαστήματα κατάλληλες και γραπτώς τεκμηριωμένες πολιτικές, μηχανισμούς και διαδικασίες εσωτερικού ελέγχου.
- 1.1.4** Η εκτελεστική ανώτερη διοίκηση της εποπτευόμενης οντότητας θα πρέπει να διατηρεί την ευθύνη για τις δραστηριότητες που ανατίθενται σε εξωτερικούς παρόχους υπηρεσιών ή σε επιχειρηματικούς εταίρους.

Συνιστώσα 1.2 Διαχείριση κινδύνων

18. Για τους σκοπούς της αποτελεσματικής διαχείρισης κινδύνων, οι εποπτευόμενες οντότητες θα πρέπει να διασφαλίζουν ότι διαθέτουν μια δυναμική και συνεχώς εξελισσόμενη διαδικασία για τον εντοπισμό, την αξιολόγηση και τη μέτρηση όλων των κινδύνων που θα μπορούσαν να επηρεάσουν την ικανότητα της εποπτευόμενης οντότητας να εκπληρώνει τις υποχρεώσεις της βάσει των σχετικών κανονισμών ή τη συνέχιση της λειτουργίας της. Για παράδειγμα, περιλαμβάνονται κίνδυνοι που προκύπτουν από τη χρήση νέων τεχνολογιών από την εποπτευόμενη οντότητα και από αλλαγές στο εξωτερικό της τοπίο κινδύνων. Η διαδικασία θα πρέπει να παρέχει στην

εποπτευόμενη οντότητα τη δυνατότητα να παρακολουθεί, να διαχειρίζεται, να μετράζει και να αναφέρει δεόντως τους σημαντικούς κινδύνους για την επίτευξη των εν λόγω στόχων.

Χαρακτηριστικά

- 1.2.1** Η εποπτευόμενη οντότητα θα πρέπει να διεξάγει τις εσωτερικές της αξιολογήσεις κινδύνων σύμφωνα με μια καθορισμένη και ολοκληρωμένη μεθοδολογία εκτίμησης κινδύνων.
- 1.2.2** Η εποπτευόμενη οντότητα θα πρέπει να καθορίζει τη διάθεση ανάληψης κινδύνου και να προσδιορίζει τα επίπεδα ανοχής κινδύνου.
- 1.2.3** Η μεθοδολογία εκτίμησης κινδύνου της εποπτευόμενης οντότητας θα πρέπει να περιλαμβάνει όλους τους επιχειρηματικούς τομείς και τις λειτουργίες εσωτερικού ελέγχου της εποπτευόμενης οντότητας.
- 1.2.4** Η διαδικασία εκτίμησης κινδύνων της εποπτευόμενης οντότητας θα πρέπει να εντοπίζει και να αξιολογεί τις αλλαγές που θα μπορούσαν να επηρεάσουν σημαντικά το σύστημα εσωτερικού ελέγχου. Στις αλλαγές αυτές περιλαμβάνονται οι αλλαγές στο περιβάλλον, την οργάνωση, τις δραστηριότητες και τις λειτουργίες της εποπτευόμενης οντότητας.
- 1.2.5** Η μεθοδολογία αξιολόγησης κινδύνων της εποπτευόμενης οντότητας θα πρέπει να υπόκειται σε συνεχή εξέλιξη και βελτίωση.

Συνιστώσα 1.3 Δραστηριότητες δικλίδων ελέγχου

- 19. Οι δραστηριότητες δικλίδων ελέγχου θα πρέπει να έχουν από τη φύση τους προληπτική, ανιχνευτική, διορθωτική ή αποτρεπτική δράση.

Χαρακτηριστικά

- 1.3.1** *Διαχωρισμός καθηκόντων* – Η εποπτευόμενη οντότητα θα πρέπει να διασφαλίζει τον κατάλληλο διαχωρισμό καθηκόντων για τη διαχείριση των κινδύνων σύγκρουσης συμφερόντων, απάτης και ανθρώπινου σφάλματος. Ο διαχωρισμός των καθηκόντων θα πρέπει να διασφαλίζει ότι τα μέλη του προσωπικού που είναι υπεύθυνα για την εκτέλεση ενός καθήκοντος δεν είναι τα μόνα υπεύθυνα για την έγκριση του αποτελέσματος της άσκησης του καθήκοντος αυτού. Ειδικότερα, τα μέλη του προσωπικού που είναι υπεύθυνα για την ανάπτυξη, την υλοποίηση ή την έγκριση μιας εργασίας/ενέργειας δεν είναι τα μόνα υπεύθυνα για την επικύρωση, την αξιολόγηση και την

αναθεώρησή της.⁸ Όταν το πρόβλημα αυτό δεν μπορεί να αποφευχθεί, θα πρέπει να μετριάσει με το να μην είναι τα μέλη του προσωπικού αποκλειστικά υπεύθυνα για τη δραστηριότητα.⁹

- 1.3.2** *Τεκμηρίωση* – Η εποπτευόμενη οντότητα θα πρέπει να τεκμηριώνει τις πολιτικές και διαδικασίες που καλύπτουν όλους τους τομείς των επιχειρηματικών δραστηριοτήτων της, σύμφωνα με τις διατάξεις των συναφών κανονισμών.
- 1.3.3** *Τεκμηριωμένοι έλεγχοι και δοκιμές ελέγχου* – Η εποπτευόμενη οντότητα θα πρέπει να τεκμηριώνει τους βασικούς ελέγχους που εφαρμόζει για να διασφαλίζει την τήρηση των πολιτικών και διαδικασιών που έχουν θεσπιστεί σύμφωνα με τους συναφείς κανονισμούς.
- 1.3.4** *Ανάθεση ευθυνών* – Η εποπτευόμενη οντότητα θα πρέπει να αναθέτει με σαφή και καθορισμένο τρόπο τους ρόλους ή τις λειτουργίες που θα είναι αρμόδιες για τη διενέργεια ελέγχων σχετικά με τις υποχρεώσεις που απορρέουν από τους συναφείς κανονισμούς και να προσδιορίζει τους αντίστοιχους ρόλους και αρμοδιότητες. Κατά την ανάθεση των εν λόγω ρόλων, η εποπτευόμενη οντότητα θα πρέπει να διακρίνει τους καθημερινούς ελέγχους σε επιχειρηματικό επίπεδο από όσους διενεργούνται από ειδικές λειτουργίες ελέγχου.
- 1.3.5** *Εξουσιοδοτήσεις και εγκρίσεις* – Η εποπτευόμενη οντότητα θα πρέπει να διαθέτει διαδικασίες ή μηχανισμούς εξουσιοδότησης που να διασφαλίζουν ότι μόνο εξουσιοδοτημένα άτομα έχουν πρόσβαση σε πληροφορίες και εργαλεία, βάσει της αρχής της ανάγκης γνώσης και της ελάχιστης προνομιακής πρόσβασης. Η εποπτευόμενη οντότητα θα πρέπει επίσης να διαθέτει διαδικασίες ή μηχανισμούς σε όλες τις επιχειρηματικές δραστηριότητες προκειμένου να διασφαλίζεται ότι οι δραστηριότητες εγκρίνονται και εκτελούνται μόνο από μέλη του προσωπικού που ενεργούν εντός του πεδίου της αρμοδιότητάς τους.¹⁰

⁸ Για παράδειγμα, τα μέλη του προσωπικού που είναι αρμόδια για τις δραστηριότητες ανάπτυξης συστημάτων δεν θα πρέπει να συμμετέχουν στη διαχείριση βάσεων δεδομένων, σε λειτουργίες ΤΠ, καθώς και στη διαχείριση και συντήρηση συστημάτων και δικτύων ΤΠ. Για τους ΟΑΠΙ, i) τα πρόσωπα που διεξάγουν την ανάλυση μιας αξιολόγησης πιστοληπτικής ικανότητας δεν θα πρέπει να είναι αποκλειστικά υπεύθυνα για την έγκριση της αξιολόγησης πιστοληπτικής ικανότητας, ii) τα πρόσωπα που είναι υπεύθυνα για την ανάπτυξη των μεθοδολογιών αξιολόγησης πιστοληπτικής ικανότητας δεν θα πρέπει να είναι αποκλειστικά υπεύθυνα για την έγκρισή τους, iii) τα πρόσωπα που είναι υπεύθυνα για την επικύρωση, την αξιολόγηση ή την επανεξέταση μιας μεθοδολογίας αξιολόγησης πιστοληπτικής ικανότητας δεν θα πρέπει να είναι αποκλειστικά υπεύθυνα για την έγκριση της επικύρωσης, της αξιολόγησης ή της επανεξέτασης.

⁹ Για παράδειγμα, μέσω ελέγχου από δύο άτομα.

¹⁰ Για παράδειγμα, για τους ΟΑΠΙ, μόνο τα πρόσωπα που έχουν οριστεί ως υπεύθυνα για τα αντίστοιχα καθήκοντα θα πρέπει να διενεργούν τη διαδικασία αξιολόγησης πιστοληπτικής ικανότητας, την επικύρωση των μεθοδολογιών και την επανεξέταση των αποτελεσμάτων της επικύρωσης.

1.3.6 *Επαληθεύσεις, επικυρώσεις, συμφωνίες και επανεξετάσεις* — Η εποπτευόμενη οντότητα θα πρέπει να λαμβάνει μέτρα για τον εντοπισμό ακατάλληλων, μη εγκεκριμένων, εσφαλμένων ή δόλιων δραστηριοτήτων και την έγκαιρη ανάληψη δράσης σε περίπτωση τέτοιων δραστηριοτήτων.¹¹

1.3.7 *Τεχνολογία πληροφοριών και επικοινωνιών (ΤΠΕ) Γενικοί έλεγχοι* (μόνο για εποπτευόμενες οντότητες που δεν υπόκεινται στον κανονισμό DORA) – Η εποπτευόμενη οντότητα πρέπει να εφαρμόζει στρατηγικές, πολιτικές και διαδικασίες που διασφαλίζουν την ψηφιακή επιχειρησιακή ανθεκτικότητα των συστημάτων ΤΠΕ της εποπτευόμενης οντότητας στην υποστήριξη των επιχειρηματικών διαδικασιών της.

Η εποπτευόμενη οντότητα θα πρέπει να σχεδιάζει αναλογικά τους ελέγχους και τις λύσεις ΤΠΕ που εφαρμόζει. Ως εκ τούτου, οι έλεγχοι ΤΠΕ θα διαφέρουν μεταξύ των οργανισμών ανάλογα με τη φύση, την κλίμακα και την πολυπλοκότητα των υποκείμενων επιχειρηματικών διαδικασιών και των σχετικών λειτουργιών που υποστηρίζονται από τα εν λόγω συστήματα.

Οι εποπτευόμενες οντότητες θα πρέπει να διασφαλίζουν ότι διαθέτουν επαρκείς ελέγχους για τη διασφάλιση της ποιότητας των δεδομένων, όσον αφορά τη διαθεσιμότητα, την εμπιστευτικότητα και την ακεραιότητα των δεδομένων, συμπεριλαμβανομένης της επικύρωσης των δεδομένων, των ελέγχων επεξεργασίας και των διαδικασιών ελέγχου των αρχείων δεδομένων.

Η εποπτευόμενη οντότητα θα πρέπει να θεσπίσει σχετικό σύστημα διαχείρισης της ασφάλειας των πληροφοριών και σχετικές δραστηριότητες ελέγχου. Στο πλαίσιο αυτό, η εποπτευόμενη οντότητα θα πρέπει να προσδιορίζει τους αναγκαίους ελέγχους προκειμένου να διασφαλίζει τη γνησιότητα, την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των πληροφοριών, καθώς αυτές υποβάλλονται σε επεξεργασία από την πηγή έως τον τελικό χρήστη.

Η εποπτευόμενη οντότητα θα πρέπει να καθορίζει και να τεκμηριώνει όλες τις σχετικές δραστηριότητες ελέγχου των διαδικασιών αγοράς, ανάπτυξης και συντήρησης ΤΠΕ.

¹¹ Αυτό περιλαμβάνει την επικύρωση δεδομένων και τους ελέγχους καταχωρίσεων, καθώς και την αναθεώρηση των καταλόγων για την εξουσιοδοτημένη πρόσβαση σε εμπιστευτικές πληροφορίες. Για τους ΟΑΠΙ, οι εν λόγω έλεγχοι ισχύουν για τις δραστηριότητες αξιολόγησης πιστοληπτικής ικανότητας και για τις διαδικασίες στις οποίες βασίζονται οι εν λόγω δραστηριότητες, όπως η επικύρωση της μεθοδολογίας/του υποδείγματος αξιολόγησης πιστοληπτικής ικανότητας.

Συνιστώσα 1.4 Ενημέρωση και επικοινωνία

20. Οι εποπτευόμενες οντότητες θα πρέπει να θεσπίσουν διαδικασίες για την καθοδική («προς τα κάτω») κοινοποίηση ακριβών, ολοκληρωμένων και ποιοτικών πληροφοριών στο προσωπικό και τα εξωτερικά ενδιαφερόμενα μέρη. Οι εποπτευόμενες οντότητες θα πρέπει επίσης να θεσπίζουν διαδικασίες για την τακτική υποβολή πληροφοριών σχετικά με το σύστημα εσωτερικού ελέγχου και τις δραστηριότητες στο διοικητικό όργανο και την εκτελεστική ανώτερη διοίκηση, μεταξύ άλλων πληροφορίες σχετικά με τη συμπεριφορά και τη συμμόρφωση με τους εσωτερικούς ελέγχους.

Χαρακτηριστικά

- 1.4.1** Η εποπτευόμενη οντότητα θα πρέπει να διασφαλίζει την κατάλληλη εσωτερική και εξωτερική επικοινωνία, ανταλλάσσοντας εγκαίρως ακριβείς, πλήρεις και καλής ποιότητας πληροφορίες με τις αγορές, τους πελάτες, τους χρήστες των προϊόντων και των υπηρεσιών της, καθώς και τις ρυθμιστικές αρχές.
- 1.4.2** Η εποπτευόμενη οντότητα θα πρέπει να δημιουργήσει διαύλους ανοδικής επικοινωνίας, συμπεριλαμβανομένης μιας διαδικασίας καταγγελίας δυσλειτουργιών, για να είναι δυνατή η αναφορά σημαντικών ζητημάτων εσωτερικού ελέγχου στο διοικητικό όργανο και την εκτελεστική ανώτερη διοίκηση. Το διοικητικό όργανο και η εκτελεστική ανώτερη διοίκηση θα πρέπει επίσης να λαμβάνουν τακτικές ενημερώσεις σχετικά με το σύστημα και τις δραστηριότητες εσωτερικού ελέγχου, μεταξύ άλλων και σχετικά με την ασφάλεια των πληροφοριών. Η εποπτευόμενη οντότητα θα πρέπει να διαθέτει διαδικασίες παραπομπής συμβάντων στο κατάλληλο επίπεδο σε περίπτωση ουσιώδους διαφωνίας μεταξύ των λειτουργιών εσωτερικού ελέγχου και των επιχειρησιακών μονάδων.
- 1.4.3** Η εποπτευόμενη οντότητα θα πρέπει να καθιερώσει διαύλους καθοδικής επικοινωνίας μεταξύ του διοικητικού οργάνου, της εκτελεστικής ανώτερης διοίκησης, των λειτουργιών ελέγχου και του προσωπικού. Στους εν λόγω διαύλους θα πρέπει να περιλαμβάνονται τακτικές επικαιροποιήσεις των στόχων και των αρμοδιοτήτων για τον εσωτερικό έλεγχο, η κοινοποίηση καθορισμένων ζητημάτων συμμόρφωσης ή ασφάλειας πληροφοριών καθώς και οι παρουσιάσεις και η επιμόρφωση σχετικά με πολιτικές και διαδικασίες.

Συνιστώσα 1.5 Δραστηριότητες παρακολούθησης

21. Οι εποπτευόμενες οντότητες θα πρέπει να διασφαλίζουν ότι αναλαμβάνουν δραστηριότητες παρακολούθησης που θα συμβάλουν στην εξακρίβωση της ύπαρξης και της αποτελεσματικής λειτουργίας των συνιστωσών του συστήματος εσωτερικού ελέγχου της εποπτευόμενης οντότητας.

Χαρακτηριστικά

- 1.5.1** Η εποπτευόμενη οντότητα θα πρέπει να διασφαλίζει ότι οι αξιολογήσεις του συστήματος εσωτερικού ελέγχου πραγματοποιούνται στα διαφορετικά επίπεδα της εποπτευόμενης οντότητας, όπως στα επιχειρηματικά καθήκοντα, τις λειτουργίες ελέγχου και τις λειτουργίες εσωτερικής επιθεώρησης ή ανεξάρτητης αξιολόγησης.
- 1.5.2** Οι δραστηριότητες παρακολούθησης θα πρέπει να σχεδιάζονται και να διεξάγονται κατά τρόπο που να επιτρέπει στην εποπτευόμενη οντότητα να ελέγχει κατά πόσον πληροί τις νομικές και κανονιστικές απαιτήσεις της, συμπεριλαμβανομένης της τήρησης των εσωτερικών κωδίκων δεοντολογίας, πολιτικών και διαδικασιών της. Συμπεριλαμβάνονται οι πολιτικές και διαδικασίες ασφάλειας πληροφοριών της εποπτευόμενης οντότητας.
- 1.5.3** Οι αξιολογήσεις των συστημάτων εσωτερικού ελέγχου θα πρέπει να διεξάγονται σε τακτική ή θεματική βάση, ή με συνδυασμό των δύο μεθόδων.
- 1.5.4** Οι εποπτευόμενες οντότητες θα πρέπει να ενσωματώνουν τις εν εξελίξει αξιολογήσεις στις επιχειρηματικές διαδικασίες και να τις προσαρμόζουν στις μεταβαλλόμενες συνθήκες.
- 1.5.5** Οι εποπτευόμενες οντότητες θα πρέπει να διασφαλίζουν ότι οι ελλείψεις που προσδιορίζονται από τις αξιολογήσεις παρακολούθησης και οι απαραίτητες διορθωτικές ενέργειες αναφέρονται στο διοικητικό όργανο και την εκτελεστική ανώτερη διοίκηση που θα πρέπει στη συνέχεια να παρακολουθούν την έγκαιρη υλοποίηση της/των διορθωτικής(-ών) ενέργειας (-ών).
- 1.5.6** Σε περίπτωση εξωτερικής ανάθεσης, η εποπτευόμενη οντότητα θα πρέπει να αναθέσει σε μέλος του προσωπικού τα καθήκοντα παρακολούθησης των επιχειρηματικών διαδικασιών που αποτελούν αντικείμενο εξωτερικής ανάθεσης. Οι εποπτευόμενες οντότητες θα πρέπει να διασφαλίζουν ότι παρέχονται στον πάροχο υπηρεσιών επαρκείς πληροφορίες σχετικά με τους στόχους και τις προσδοκίες παράδοσης, καθώς και ότι ο έλεγχος δέουσας επιμέλειας διενεργείται πριν από τον διορισμό του παρόχου.

5.2 Λειτουργίες εσωτερικού ελέγχου

22. Προκειμένου να διασφαλίζεται η αποτελεσματικότητα των λειτουργιών εσωτερικού ελέγχου (ΕΕ), οι εποπτευόμενες οντότητες θα πρέπει να περιλαμβάνουν τις ακόλουθες συνιστώσες και χαρακτηριστικά στις πολιτικές, τις διαδικασίες και τις εργασιακές πρακτικές τους.

Γενικές αρχές

23. Η ESMA θεωρεί ότι οι λειτουργίες ΕΕ των εποπτευόμενων οντοτήτων θα πρέπει να διαθέτουν επαρκείς πόρους και να είναι στελεχωμένες με άτομα που είναι αρκούντως εξειδικευμένα να εκτελέσουν τα καθήκοντά τους. Τα μέλη του προσωπικού που εργάζονται στις λειτουργίες ΕΕ θα πρέπει να διαθέτουν επαρκείς τεχνικές γνώσεις σχετικά με τις δραστηριότητες της εποπτευόμενης οντότητας και τους συναφείς κινδύνους. Σε περιπτώσεις όπου η εποπτευόμενη οντότητα έχει αναθέσει τα επιχειρησιακά καθήκοντα μιας λειτουργίας ΕΕ σε τρίτο σε επίπεδο ομίλου ή σε εξωτερικό φορέα, η ESMA θεωρεί ότι η εποπτευόμενη οντότητα παραμένει πλήρως υπεύθυνη για τις δραστηριότητες της λειτουργίας ΕΕ την οποία έχει αναθέσει. Οι εποπτευόμενες οντότητες θα πρέπει να διασφαλίζουν ότι το προσωπικό που είναι αρμόδιο για τις λειτουργίες ΕΕ θα πρέπει να διαθέτει την κατάλληλη αρχαιότητα ώστε να έχει την απαραίτητη εξουσία να εκπληρώσει τις αρμοδιότητές του. Για παράδειγμα, τα μέλη του προσωπικού που είναι υπεύθυνα για τις λειτουργίες συμμόρφωσης, διαχείρισης κινδύνων, εσωτερικής επιθεώρησης, διαχείρισης ασφάλειας πληροφοριών, επανεξέτασης (για ΟΑΠΙ) και εποπτείας (για ΒΜΑ) θα πρέπει να έχουν απεριόριστη πρόσβαση και να υποβάλλουν τακτικά εκθέσεις στο διοικητικό όργανο.
24. Οι δραστηριότητες μπορούν να διεξάγονται σε επίπεδο ομίλου ή από άλλες νομικές οντότητες με εταιρική δομή υπό την προϋπόθεση ότι η δομή του ομίλου δεν δυσχεραίνει την ικανότητα του διοικητικού οργάνου της εποπτευόμενης οντότητας να ασκεί εποπτεία, ούτε την ικανότητα της εκτελεστικής ανώτερης διοίκησης να διαχειρίζεται αποτελεσματικά τους κινδύνους, ή της ESMA να εποπτεύει αποτελεσματικά την οντότητα. Σε όλες τις περιπτώσεις εφαρμόζεται η κατευθυντήρια γραμμή 1.1.4.
25. Για να διασφαλιστεί η ανεξαρτησία των λειτουργιών ΕΕ της εποπτευόμενης οντότητας, η ESMA αναμένει από τις εποπτευόμενες οντότητες να λάβουν υπόψη τους τις ακόλουθες αρχές κατά τον προσδιορισμό των αρμοδιοτήτων και των ευθυνών των οικείων λειτουργιών εσωτερικού ελέγχου:
- i. οι λειτουργίες ΕΕ θα πρέπει να είναι από οργανωτικής πλευράς ανεξάρτητες από τα καθήκοντα/δραστηριότητες για τις οποίες τους έχει ανατεθεί η ευθύνη παρακολούθησης, επιθεώρησης και ελέγχου
 - ii. οι λειτουργίες ΕΕ δεν θα πρέπει να εκτελούν επιχειρησιακά καθήκοντα που εμπíπτουν στο εύρος των επιχειρηματικών δραστηριοτήτων για τις οποίες τους έχει ανατεθεί η ευθύνη παρακολούθησης, επιθεώρησης και ελέγχου
 - iii. Το μέλος του προσωπικού που είναι υπεύθυνο για τη λειτουργία ΕΕ δεν θα πρέπει να λογοδοτεί σε άτομο που έχει ευθύνη για τη διαχείριση των δραστηριοτήτων τις οποίες παρακολουθεί, επιθεωρεί ή ελέγχει η εν λόγω λειτουργία ΕΕ.

26. Το προσωπικό που έχει αρμοδιότητες σχετικές με τις λειτουργίες εσωτερικού ελέγχου θα πρέπει να έχει πρόσβαση σε σχετική εσωτερική ή εξωτερική επαγγελματική κατάρτιση ούτως ώστε να διασφαλίζεται ότι διαθέτει επαρκείς δεξιότητες για να εκτελέσει τα καθήκοντά του.

Αναλογικότητα – Λειτουργίες εσωτερικού ελέγχου

27. Ενώ όλες οι εποπτευόμενες οντότητες αναμένεται να διαθέτουν τα χαρακτηριστικά αποτελεσματικών λειτουργιών εσωτερικού ελέγχου που περιγράφονται στις παρούσες κατευθυντήριες γραμμές, η ESMA προσαρμόζει τις προσδοκίες της ανάλογα με τη φύση, την κλίμακα και την πολυπλοκότητα της εποπτευόμενης οντότητας, όπως περιγράφεται στην ενότητα 3.4 των παρουσών κατευθυντήριων γραμμών.
28. Στην παρούσα ενότητα παρουσιάζεται λεπτομερέστερα ο τρόπος με τον οποίο η ESMA λαμβάνει υπόψη την αναλογικότητα κατά την εποπτεία των λειτουργιών ΕΕ.

Διαχωρισμός των καθηκόντων

29. Ο διαχωρισμός των καθηκόντων θα πρέπει να λαμβάνεται υπόψη κατά την ανάπτυξη των δραστηριοτήτων ελέγχου. Ενδέχεται, ωστόσο, να υπάρχουν ορισμένες περιπτώσεις στις οποίες το δίκαιο της Ένωσης δεν απαιτεί διαχωρισμό των καθηκόντων και ο εν λόγω διαχωρισμός δεν είναι πρακτικός, λαμβάνοντας υπόψη τη φύση, την κλίμακα και την πολυπλοκότητα της εποπτευόμενης οντότητας. Σε αυτήν την περίπτωση, εναλλακτικοί έλεγχοι μπορεί να είναι καταλληλότεροι. Σε περίπτωση που χρησιμοποιούνται άλλοι έλεγχοι, οι εποπτευόμενες οντότητες θα πρέπει να τεκμηριώνουν το σκεπτικό της ρύθμισης, να προσδιορίζουν τους πιθανούς κινδύνους, να εφαρμόζουν αντισταθμιστικούς ελέγχους για την αντιμετώπισή τους και να αποδεικνύουν ότι η ρύθμιση δεν βλάπτει το περιβάλλον ελέγχου.

Πόροι

30. Για ορισμένες εποπτευόμενες οντότητες ενδέχεται να μην είναι αναλογικό να διαθέτουν προσωπικό πλήρους απασχόλησης σε όλες τις λειτουργίες, δεδομένης της φύσης, της κλίμακας και της πολυπλοκότητάς τους. Σε αυτές τις περιπτώσεις, μια εποπτευόμενη οντότητα μπορεί να επιλέξει να προσαρμόσει τις ώρες των πόρων ώστε να ταιριάζουν με τις δραστηριότητες ελέγχου ή να αναθέσει τη δραστηριότητα σε τρίτο.

Εξειδίκευση στο πλαίσιο των Λειτουργιών

31. Καθώς μια εποπτευόμενη οντότητα αναπτύσσεται και το περιβάλλον ελέγχου της ωριμάζει, θα πρέπει να αξιοποιεί την εξειδίκευση του προσωπικού της, ώστε να επωφελείται από την εμπειρογνωμοσύνη του σε βασικές διαδικασίες ή τομείς κινδύνου. Εποπτευόμενες οντότητες ορισμένης φύσης, κλίμακας και πολυπλοκότητας θα πρέπει να

διαθέτουν ειδικές ομάδες παρακολούθησης ή έρευνας στο πλαίσιο της λειτουργίας τους συμμόρφωσης.

Ωριμότητα των δραστηριοτήτων ελέγχου

32. Η ωριμότητα των δραστηριοτήτων ελέγχου (δηλαδή χειρωνακτικές, υβριδικές, αυτοματοποιημένες δραστηριότητες και, σε ορισμένες περιπτώσεις, δραστηριότητες που ενσωματώνουν εργαλεία τεχνητής νοημοσύνης) θα πρέπει να αντικατοπτρίζει τη φύση, την κλίμακα, την πολυπλοκότητα και το συνολικό προφίλ κινδύνου της εποπτευόμενης οντότητας. Για τις εποπτευόμενες οντότητες συγκεκριμένης φύσης, κλίμακας και πολυπλοκότητας, θα πρέπει να υπάρχει υψηλότερος βαθμός αυτοματοποιημένων ελέγχων, καθώς και μεγαλύτερη ενοποίηση μεταξύ των συστημάτων των ελεγκτικών λειτουργιών, προκειμένου να βελτιστοποιηθούν οι δραστηριότητες παρακολούθησης και η διαδικασία υποβολής αναφορών της εποπτευόμενης οντότητας προς την εκτελεστική ανώτερη διοίκηση και το διοικητικό όργανο σχετικά με τις πληροφορίες διαχείρισης.

Συνιστώσα 2.1 Λειτουργία συμμόρφωσης

33. Η λειτουργία συμμόρφωσης μιας εποπτευόμενης οντότητας είναι υπεύθυνη για την παρακολούθηση και την υποβολή αναφορών σχετικά με τη συμμόρφωση της εποπτευόμενης οντότητας και των υπαλλήλων της με τις υποχρεώσεις της δυνάμει του σχετικού κανονισμού. Η λειτουργία συμμόρφωσης είναι αρμόδια για μεταγενέστερες τροποποιήσεις στη νομοθεσία και τον κανονισμό που διέπουν τις δραστηριότητές της εποπτευόμενης οντότητας. Η λειτουργία συμμόρφωσης είναι, επίσης, αρμόδια για την παροχή συμβουλών στο διοικητικό όργανο σχετικά με τη νομοθεσία, τους κανόνες, τους κανονισμούς και τα πρότυπα με τα οποία πρέπει να συμμορφώνεται η εποπτευόμενη οντότητα, και για την αξιολόγηση, σε συνεργασία με άλλες συναφείς λειτουργίες, του πιθανού αντικτύπου τυχόν τροποποιήσεων του νομικού ή κανονιστικού περιβάλλοντος στις δραστηριότητες της εποπτευόμενης οντότητας.

Χαρακτηριστικά

- 2.1.1** Η λειτουργία συμμόρφωσης πρέπει να ασκεί τα καθήκοντά της ανεξάρτητα από τους επιχειρηματικούς τομείς και να υποβάλλει τακτικές εκθέσεις στο διοικητικό όργανο της εποπτευόμενης οντότητας και, κατά περίπτωση, απευθείας στα ανεξάρτητα μη εκτελεστικά στελέχη.
- 2.1.2** Η λειτουργία κανονιστικής συμμόρφωσης θα πρέπει να παρέχει συμβουλές και να βοηθά τα μέλη του προσωπικού να συμμορφώνονται με τις υποχρεώσεις με βάση τον συναφή κανονισμό. Η λειτουργία συμμόρφωσης θα πρέπει να ενεργεί με προληπτικό τρόπο κατά τον προσδιορισμό των κινδύνων και της ενδεχόμενης μη συμμόρφωσης μέσω της έγκαιρης παρακολούθησης και αξιολόγησης των δραστηριοτήτων, καθώς και της παρακολούθησης τυχόν διορθωτικών μέτρων.

- 2.1.3** Η λειτουργία συμμόρφωσης θα πρέπει να διασφαλίζει ότι η παρακολούθηση της συμμόρφωσης πραγματοποιείται βάσει ενός δομημένου και ορθά καθορισμένου προγράμματος παρακολούθησης της συμμόρφωσης. Το πεδίο εφαρμογής των δραστηριοτήτων συμμόρφωσης θα πρέπει να καλύπτει όλες τις επιχειρηματικές διαδικασίες και τα συστήματα ΤΠ που θα μπορούσαν να επηρεάσουν τη συμμόρφωση της εποπτευόμενης οντότητας με τον συναφή κανονισμό.
- 2.1.4** Η λειτουργία συμμόρφωσης, όπου κρίνεται σκόπιμο σε συνεργασία με άλλες αρμόδιες λειτουργίες, θα πρέπει να αξιολογεί τον αντίκτυπο που ενδέχεται να έχουν τυχόν τροποποιήσεις του νομοθετικού ή κανονιστικού περιβάλλοντος στις δραστηριότητες του οργανισμού, και να επικοινωνεί, κατά περίπτωση, με τη λειτουργία διαχείρισης κινδύνου σχετικά με τον κίνδυνο συμμόρφωσης της εποπτευόμενης οντότητας.
- 2.1.5** Η λειτουργία συμμόρφωσης θα πρέπει να διασφαλίζει την τήρηση των πολιτικών συμμόρφωσης και να υποβάλλει εκθέσεις στο διοικητικό όργανο και την εκτελεστική ανώτερη διοίκηση σχετικά με τον κίνδυνο συμμόρφωσης της εποπτευόμενης οντότητας.
- 2.1.6** Η λειτουργία συμμόρφωσης θα πρέπει να συνεργάζεται με τη λειτουργία διαχείρισης κινδύνου για την ανταλλαγή πληροφοριών που είναι απαραίτητες για τα αντίστοιχα καθήκοντά τους.
- 2.1.7** Τα ευρήματα της λειτουργίας συμμόρφωσης θα πρέπει να λαμβάνονται υπόψη από το διοικητικό όργανο και την εκτελεστική ανώτερη διοίκηση, καθώς και από τη λειτουργία διαχείρισης κινδύνων στο πλαίσιο των διαδικασιών αξιολόγησης κινδύνων.

Συνιστώσα 2.2 Λειτουργία διαχείρισης κινδύνων

34. Η λειτουργία διαχείρισης κινδύνου της εποπτευόμενης οντότητας είναι αρμόδια για την ανάπτυξη και υλοποίηση του πλαισίου διαχείρισης κινδύνου.

Χαρακτηριστικά

- 2.2.1** Η λειτουργία διαχείρισης κινδύνων πρέπει να εκτελεί τα καθήκοντά της ανεξάρτητα από τους επιχειρηματικούς τομείς και τις μονάδες των οποίων τους κινδύνους εποπτεύει, αλλά δεν πρέπει να κωλύεται να αλληλεπιδρά μαζί τους.
- 2.2.2** Η λειτουργία διαχείρισης κινδύνων θα πρέπει να διασφαλίζει τον εντοπισμό, την αξιολόγηση και τη μέτρηση όλων των κινδύνων που θα μπορούσαν να επηρεάσουν την ικανότητα της εποπτευόμενης οντότητας να εκπληρώσει τις υποχρεώσεις της σύμφωνα με τους συναφείς κανονισμούς ή τη συνέχιση της λειτουργίας της. Στη συνέχεια, οι σημαντικοί κίνδυνοι για τους εν λόγω στόχους

θα πρέπει να παρακολουθούνται, να τυγχάνουν διαχείρισης, να μετριάζονται και να αναφέρονται δεόντως και εγκαίρως από και προς τις οικείες μονάδες της εποπτευόμενης οντότητας.

2.2.3 Η λειτουργία διαχείρισης κινδύνων θα πρέπει να παρακολουθεί το προφίλ κινδύνου της εποπτευόμενης οντότητας σε σχέση με τη διάθεση ανάληψης κινδύνων της εποπτευόμενης οντότητας, προκειμένου να διευκολύνει τη λήψη αποφάσεων.

2.2.4 Η λειτουργία διαχείρισης κινδύνου θα πρέπει να παρέχει συμβουλές σχετικά με προτάσεις και αποφάσεις κινδύνου που λαμβάνονται από τους επιχειρηματικούς τομείς, και να ενημερώνει το διοικητικό όργανο σχετικά με το κατά πόσον οι εν λόγω αποφάσεις συνάδουν με τη διάθεση για ανάληψη κινδύνων και τους στόχους της εποπτευόμενης οντότητας.

2.2.5 Η λειτουργία διαχείρισης κινδύνων θα πρέπει να προτείνει βελτιώσεις στο πλαίσιο της διαχείρισης κινδύνων καθώς και τροποποιήσεις των πολιτικών και των διαδικασιών διαχείρισης κινδύνων, όπου κρίνεται απαραίτητο. Η λειτουργία διαχείρισης κινδύνων θα πρέπει να επανεξετάζει τα όρια κινδύνου σύμφωνα με τυχόν αλλαγές στη διάθεση ανάληψης κινδύνων του οργανισμού.

Συνιστώσα 2.3 Λειτουργία διαχείρισης της ασφάλειας των πληροφοριών (μόνο για εποπτευόμενες οντότητες που δεν υπόκεινται στον κανονισμό DORA)

35. Η λειτουργία διαχείρισης της ασφάλειας των πληροφοριών μιας εποπτευόμενης οντότητας είναι υπεύθυνη για την ανάπτυξη και την εφαρμογή της ασφάλειας των πληροφοριών εντός της εποπτευόμενης οντότητας. Η εποπτευόμενη οντότητα θα πρέπει να συγκροτήσει μια λειτουργία που προάγει μια νοοτροπία ασφάλειας των πληροφοριών εντός της εποπτευόμενης οντότητας.

Χαρακτηριστικά

2.3.1 Η λειτουργία διαχείρισης της ασφάλειας των πληροφοριών θα πρέπει να είναι υπεύθυνη για την επανεξέταση και την παρακολούθηση της συμμόρφωσης της εποπτευόμενης οντότητας με τις πολιτικές και τις διαδικασίες ασφάλειας πληροφοριών της εποπτευόμενης οντότητας.

2.3.2 Η λειτουργία διαχείρισης της ασφάλειας των πληροφοριών θα πρέπει να διαχειρίζεται τις δραστηριότητες ασφάλειας των πληροφοριών της εποπτευόμενης οντότητας.

- 2.3.3** Η υπηρεσία διαχείρισης της ασφάλειας των πληροφοριών θα πρέπει να αναπτύσσει και να εφαρμόζει πρόγραμμα ευαισθητοποίησης του προσωπικού σε θέματα ασφάλειας πληροφοριών με σκοπό την ενίσχυση της νοοτροπίας ασφάλειας των πληροφοριών και την ανάπτυξη ευρείας κατανόησης του πλαισίου ασφάλειας πληροφοριών της εποπτευόμενης οντότητας.
- 2.3.4** Η λειτουργία διαχείρισης της ασφάλειας των πληροφοριών θα πρέπει να υποβάλλει εκθέσεις και να συμβουλεύει το διοικητικό όργανο και την εκτελεστική ανώτερη διοίκηση σχετικά με την κατάσταση του συστήματος διαχείρισης της ασφάλειας των πληροφοριών και τους κινδύνους (π.χ. πληροφορίες σχετικά με έργα ασφάλειας πληροφοριών, συμβάντα ασφάλειας πληροφοριών και τα αποτελέσματα των αξιολογήσεων της ασφάλειας των πληροφοριών).

Συνιστώσα 2.4 Λειτουργία εσωτερικής επιθεώρησης

36. Η λειτουργία εσωτερικής επιθεώρησης μιας εποπτευόμενης οντότητας είναι υπεύθυνη να παρέχει ανεξάρτητες, αντικειμενικές διασφαλίσεις και συμβουλές για τη βελτίωση των δραστηριοτήτων του οργανισμού. Βοηθά τον οργανισμό να επιτύχει τους στόχους του, ορίζοντας μια συστηματική και πειθαρχημένη προσέγγιση για την αξιολόγηση και τη βελτίωση της αποτελεσματικότητας του συστήματος εσωτερικού ελέγχου.

Χαρακτηριστικά

- 2.4.1** Η λειτουργία εσωτερικής επιθεώρησης θα πρέπει να εκτελεί τα καθήκοντά της ανεξάρτητα από τους επιχειρηματικούς τομείς και άλλες λειτουργίες εσωτερικού ελέγχου. Θα πρέπει να διέπεται από χάρτη εσωτερικής επιθεώρησης που ορίζει τον ρόλο και τις αρμοδιότητές της και υπόκειται στην εποπτεία του διοικητικού οργάνου.
- 2.4.2** Η λειτουργία εσωτερικού ελέγχου θα πρέπει να ακολουθεί μια προσέγγιση βασισμένη στον κίνδυνο και να συμμορφώνεται με τα διεθνή πρότυπα εσωτερικής επιθεώρησης.
- 2.4.3** Η λειτουργία εσωτερικής επιθεώρησης θα πρέπει να προβαίνει σε ανεξάρτητη αξιολόγηση και να παρέχει αντικειμενικές διαβεβαιώσεις ότι οι δραστηριότητες της εποπτευόμενης οντότητας, συμπεριλαμβανομένων των δραστηριοτήτων που έχουν ανατεθεί σε τρίτο, συμμορφώνονται με τις πολιτικές και διαδικασίες της εποπτευόμενης οντότητας, καθώς και με τις ισχύουσες νομικές και κανονιστικές απαιτήσεις.
- 2.4.4** Η λειτουργία εσωτερικής επιθεώρησης θα πρέπει να καταρτίζει τουλάχιστον μία φορά το χρόνο, με βάση τους ετήσιους στόχους εσωτερικής επιθεώρησης, ένα σχέδιο επιθεώρησης το οποίο υπόκειται στην εποπτεία του διοικητικού οργάνου.

- 2.4.5** Η λειτουργία εσωτερικής επιθεώρησης θα πρέπει να υποβάλλει τακτικές εκθέσεις στα ανεξάρτητα μέλη του διοικητικού οργάνου ή στην ελεγκτική επιτροπή, εάν υφίσταται.
- 2.4.6** Η λειτουργία εσωτερικής επιθεώρησης θα πρέπει να κοινοποιεί τις συστάσεις της σχετικά με την εσωτερική επιθεώρηση με σαφή και συνεπή τρόπο που να επιτρέπει στο διοικητικό όργανο και την εκτελεστική ανώτερη διοίκηση να κατανοήσουν την ουσία των συστάσεων και να θέσουν με ανάλογο τρόπο τις προτεραιότητές τους.
- 2.4.7** Οι συστάσεις στο πλαίσιο της εσωτερικής επιθεώρησης θα πρέπει να υπόκεινται σε επίσημη διαδικασία παρακολούθησης από τα κατάλληλα επίπεδα της διοίκησης προκειμένου να υποβάλλονται σχετικές αναφορές και να διασφαλίζεται η αποτελεσματική και έγκαιρη υλοποίησή τους.

Συνιστώσα 2.5 Λειτουργία επανεξέτασης (μόνο για τους ΟΑΠΙ)

37. Η λειτουργία επανεξέτασης ενός ΟΑΠΙ είναι υπεύθυνη να επανεξετάζει τις μεθοδολογίες αξιολόγησης της πιστοληπτικής ικανότητας τουλάχιστον μία φορά το χρόνο. Η λειτουργία επανεξέτασης ενός ΟΑΠΙ είναι επίσης υπεύθυνη για την επικύρωση και την επανεξέταση νέων μεθοδολογιών, καθώς και οποιωνδήποτε αλλαγών στις υφιστάμενες μεθοδολογίες.

Χαρακτηριστικά

- 2.5.1** Η λειτουργία επανεξέτασης θα πρέπει να εκτελεί τα καθήκοντά της ανεξάρτητα από τους επιχειρηματικούς τομείς που είναι υπεύθυνοι για τις δραστηριότητες αξιολόγησης πιστοληπτικής ικανότητας, και θα πρέπει να υποβάλλει τακτικές εκθέσεις στα ανεξάρτητα μη εκτελεστικά στελέχη (INED) του ΟΑΠΙ.
- 2.5.2** Οι μέτοχοι ή το προσωπικό του ΟΑΠΙ που συμμετέχουν στην ανάπτυξη των επιχειρηματικών δραστηριοτήτων δεν θα πρέπει να εκτελούν καθήκοντα της λειτουργίας επανεξέτασης.
- 2.5.3** Οι αναλυτές δεν θα πρέπει να συμμετέχουν στην έγκριση νέων ή την επαλήθευση και επανεξέταση των υφιστάμενων μεθοδολογιών, προτύπων ή βασικών παραδοχών αξιολόγησης πιστοληπτικής ικανότητας που έχουν εκπονήσει.
- 2.5.4** Το προσωπικό της λειτουργίας επανεξέτασης θα πρέπει είτε να είναι αποκλειστικά υπεύθυνο είτε να διαθέτει την πλειονότητα των δικαιωμάτων ψήφου στις επιτροπές που είναι αρμόδιες για την έγκριση μεθοδολογιών, προτύπων ή βασικών παραδοχών αξιολόγησης πιστοληπτικής ικανότητας.

- 2.5.5** Το προσωπικό της λειτουργίας επανεξέτασης που είναι υπεύθυνο για την επικύρωση ή/και την επανεξέταση μιας μεθοδολογίας, και το οποίο συμμετέχει επίσης στη φάση ανάπτυξής της, δεν θα πρέπει να είναι αποκλειστικά υπεύθυνο ή να έχει την πλειονότητα των δικαιωμάτων ψήφου στις επιτροπές έγκρισης μεθοδολογίας.
- 2.5.6** Σε περίπτωση εξωτερικής ανάθεσης της λειτουργίας επανεξέτασης, ο ΟΑΠΙ θα πρέπει να λαμβάνει υπόψη την κατευθυντήρια γραμμή 1.5.6. Επιπλέον, ο ΟΑΠΙ θα πρέπει να διαθέτει κατάλληλους μηχανισμούς εσωτερικού ελέγχου που θα διασφαλίζουν ότι συμμορφώνεται με τις κανονιστικές απαιτήσεις και τηρεί κατάλληλα αναλυτικά πρότυπα ποιότητας.

Συνοίστωση 2.6 Λειτουργία εποπτείας (μόνο για τους BMA)¹²

38. Η λειτουργία εποπτείας εποπτεύει τις κύριες πτυχές της παροχής δεικτών αναφοράς. Αυτό περιλαμβάνει, μεταξύ άλλων, την επανεξέταση του ορισμού και της μεθοδολογίας του δείκτη αναφοράς, τη διαχείριση τρίτων μερών που συμμετέχουν στην παροχή του δείκτη αναφοράς, την αξιολόγηση εσωτερικών και εξωτερικών ελέγχων ή επανεξετάσεων του πλαισίου ελέγχου του διαχειριστή και την αναφορά τυχόν σχετικών παραπτώματων στις σχετικές αρμόδιες αρχές.

Χαρακτηριστικά

- 2.6.1** Η λειτουργία εποπτείας ενός BMA διατηρεί την ανεξαρτησία της από κάθε διοικητικό όργανο ή λειτουργία του BMA και οποιοδήποτε εξωτερικό μέρος. Η ανεξαρτησία προϋποθέτει ότι τα μέλη της λειτουργίας εποπτείας δεν υπόκεινται σε συγκρούσεις συμφερόντων μεταξύ των δραστηριοτήτων που ασκούν ως μέλη της λειτουργίας εποπτείας και των άλλων δραστηριοτήτων τους. Ο BMA θα πρέπει να εφαρμόσει ένα λειτουργικό πλαίσιο εσωτερικού ελέγχου για την πρόληψη και τον μετριασμό τυχόν συγκρούσεων συμφερόντων.
- 2.6.2** Ο BMA θα πρέπει να διαθέτει σαφείς πολιτικές και διαδικασίες σχετικά με τη σύσταση και τις αρμοδιότητες της λειτουργίας εποπτείας και των μελών της, συμπεριλαμβανομένων πολιτικών και διαδικασιών για την επικαιροποίηση της μεθοδολογίας των δεικτών αναφοράς και την επανεξέταση της ακεραιότητας των δεδομένων.

¹² Οι μη σημαντικοί BMA που εφαρμόζουν το άρθρο 26 του κανονισμού BMR αναμένεται να εφαρμόζουν τις παρούσες κατευθυντήριες γραμμές κατ' αναλογία προς τις απαιτήσεις του άρθρου 26.

- 2.6.3** Η λειτουργία εποπτείας ενός BMA θα πρέπει να διενεργεί τακτικά αυτοαξιολόγηση προκειμένου να αξιολογεί την αποτελεσματικότητά της και την καταλληλότητα των μελών της για τον σκοπό της λειτουργίας, να εντοπίζει πιθανές συγκρούσεις συμφερόντων και να προτείνει τομείς βελτίωσης, εφόσον κρίνεται απαραίτητο.
- 2.6.4** Η λειτουργία εποπτείας ενός BMA θα πρέπει να διατηρεί έναν καθορισμένο και τακτικό διάλογο επικοινωνίας με το διοικητικό όργανο, την εκτελεστική ανώτερη διοίκηση και άλλες βασικές λειτουργίες. Η λειτουργία εποπτείας ενός BMA θα πρέπει επίσης να είναι σε θέση να έχει πρόσβαση και να θέτει υπό αμφισβήτηση τις πληροφορίες της διοίκησης, καθώς και να λαμβάνει ενημερώσεις σχετικά με την κατάσταση των διορθωτικών μέτρων κατόπιν εσωτερικών και εξωτερικών ελέγχων, εκθέσεων κινδύνου και εκθέσεων συμμόρφωσης.
- 2.6.5** Η λειτουργία εποπτείας ενός BMA πρέπει να διατηρεί έναν καθορισμένο διάλογο επικοινωνίας με τις αρμόδιες αρχές, συμπεριλαμβανομένης της αναφοράς τυχόν παραβάσεων ή παρανομιών εκ μέρους διαχειριστών ή συνεισφερόντων.