EBA/REC/2017/03

28/03/2018

Συστάσεις

σχετικά με την εξωτερική ανάθεση δραστηριοτήτων σε παρόχους υπηρεσιών υπολογιστικού νέφους

1. Συμμόρφωση και υποχρεώσεις υποβολής στοιχείων και αναφορών

Καθεστώς των συστάσεων

1. Το παρόν έγγραφο περιέχει συστάσεις οι οποίες εκδίδονται βάσει του άρθρου 16 του κανονισμού (ΕΕ) αριθ. 1093/2010[1]. Σύμφωνα με το άρθρο 16 παράγραφος 3 του κανονισμού (ΕΕ) αριθ. 1093/2010, οι αρμόδιες αρχές και τα χρηματοοικονομικά ιδρύματα καταβάλλουν κάθε δυνατή προσπάθεια για να συμμορφωθούν με τις συστάσεις.

2. Οι συστάσεις παρουσιάζουν την άποψη της ΕΑΤ σχετικά με τις ενδεδειγμένες εποπτικές πρακτικές στο πλαίσιο του Ευρωπαϊκού Συστήματος Χρηματοοικονομικής Εποπτείας ή σχετικά με τον τρόπο ορθής εφαρμογής της ενωσιακής νομοθεσίας στον συγκεκριμένο τομέα. Οι αρμόδιες αρχές, όπως ορίζονται στο άρθρο 4 παράγραφος 2 του κανονισμού (ΕΕ) αριθ. 1093/2010, προς τις οποίες απευθύνονται οι συστάσεις , πρέπει να συμμορφωθούν ενσωματώνοντάς τες δεόντως στις πρακτικές τους (π.χ. τροποποιώντας το νομικό τους πλαίσιο ή τις εποπτικές διαδικασίες τους), συμπεριλαμβανομένων των σημείων στα οποία οι συστάσεις απευθύνονται κυρίως στα ιδρύματα.

Απαιτήσεις υποβολής στοιχείων

3. Σύμφωνα με το άρθρο 16 παράγραφος 3 του κανονισμού (ΕΕ) αριθ. 1093/2010, οι αρμόδιες αρχές πρέπει να γνωστοποιήσουν στην ΕΑΤ εάν συμμορφώνονται ή προτίθενται να συμμορφωθούν προς τις παρούσες συστάσεις, ή άλλως να εκθέσουν τους λόγους μη συμμόρφωσης, έως τις 28.05.2018. Εάν η προθεσμία γνωστοποίησης παρέλθει άπρακτη, η ΕΑΤ θα θεωρήσει ότι οι αρμόδιες αρχές δεν συμμορφώνονται. Οι γνωστοποιήσεις πρέπει να αποστέλλονται, με την υποβολή του εντύπου που παρέχεται στον δικτυακό τόπο της ΕΑΤ, στην ηλεκτρονική διεύθυνση compliance@eba.europa.eu με την επισήμανση «EBA/REC/2017/03». Οι γνωστοποιήσεις πρέπει να υποβάλλονται από πρόσωπα δεόντως εξουσιοδοτημένα να γνωστοποιούν τη συμμόρφωση εκ μέρους των αρμόδιων αρχών τους. Οποιαδήποτε μεταβολή στην κατάσταση συμμόρφωσης πρέπει επίσης να αναφέρεται στην ΕΑΤ.

4. Οι γνωστοποιήσεις δημοσιεύονται στον δικτυακό τόπο της ΕΑΤ, σύμφωνα με το άρθρο 16 παράγραφος 3.

[1] Κανονισμός (ΕΕ) αριθ. 1093/2010 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Νοεμβρίου 2010, σχετικά με τη σύσταση Ευρωπαϊκής Εποπτικής Αρχής (Ευρωπαϊκή Αρχή Τραπεζών), την τροποποίηση της απόφασης αριθ. 716/2009/ΕΚ και την κατάργηση της απόφασης 2009/78/ΕΚ της Επιτροπής (ΕΕ L 331 της 15.12.2010, σ.12).

2. Αντικείμενο, πεδίο εφαρμογής και ορισμοί

Αντικείμενο και πεδίο εφαρμογής

1. Οι παρούσες συστάσεις προσδιορίζουν περαιτέρω τις προϋποθέσεις για την εξωτερική ανάθεση δραστηριοτήτων, όπως αναφέρεται στις κατευθυντήριες γραμμές της Επιτροπής Ευρωπαϊκών Αρχών Τραπεζικής Εποπτείας (ΕΕΑΤΕ), της 14ης Δεκεμβρίου 2006, σχετικά με την εξωτερική ανάθεση δραστηριοτήτων, και εφαρμόζονται για την εξωτερική ανάθεση δραστηριοτήτων από ιδρύματα, όπως ορίζονται στο άρθρο 4 παράγραφος 1 σημείο 3) του κανονισμού (ΕΕ) αριθ. 575/2013, σε παρόχους υπηρεσιών υπολογιστικού νέφους.

Αποδέκτες

2. Οι παρούσες συστάσεις απευθύνονται στις αρμόδιες αρχές, όπως ορίζονται στο άρθρο 4 παράγραφος 2 στοιχείο i) του κανονισμού (ΕΕ) αριθ. 1093/2010, και στα ιδρύματα, όπως ορίζονται στο άρθρο 4 παράγραφος 1 σημείο 3) του κανονισμού (ΕΕ) αριθ. 575/2013[2].

Ορισμοί

3. Εκτός εάν προβλέπεται διαφορετικά, οι όροι που χρησιμοποιούνται και ορίζονται στην οδηγία 2013/36/ΕΕ[3] για τις κεφαλαιακές απαιτήσεις και στις κατευθυντήριες γραμμές της ΕΕΑΤΕ έχουν την ίδια έννοια και στις παρούσες συστάσεις. Επιπλέον, για τους σκοπούς του παρόντος εγγράφου ισχύουν οι ακόλουθοι ορισμοί:

Υπηρεσίες υπολογιστικού νέφους	Υπηρεσίες που παρέχονται με τη χρήση υπολογιστικού νέφους, δηλαδή ενός μοντέλου για τη διευκόλυνση της από οπουδήποτε, εύκολης, κατ' αίτηση δικτυακής πρόσβασης σε κοινή ομάδα διαμορφώσιμων υπολογιστικών πόρων (π.χ. δικτύων, διακομιστών, αποθηκευτικών χώρων, εφαρμογών και υπηρεσιών) που μπορούν να παρασχεθούν και να διατεθούν ταχέως, με ελάχιστη διαχειριστική προσπάθεια ή αλληλεπίδραση με τον πάροχο υπηρεσίας.
Δημόσιο υπολογιστικό νέφος	Υποδομή υπολογιστικού νέφους η οποία είναι διαθέσιμη για ανοικτή χρήση από το ευρύ κοινό.

[2] Κανονισμός (ΕΕ) αριθ. 575/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 26ης Ιουνίου 2013, σχετικά με τις απαιτήσεις προληπτικής εποπτείας για πιστωτικά ιδρύματα και επιχειρήσεις επενδύσεων και την τροποποίηση του κανονισμού (ΕΕ) αριθ. 648/2012.

[3] Οδηγία 2013/36/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 26ης Ιουνίου 2013, σχετικά με την πρόσβαση στη δραστηριότητα πιστωτικών ιδρυμάτων και την προληπτική εποπτεία πιστωτικών ιδρυμάτων και επιχειρήσεων επενδύσεων, για την τροποποίηση της οδηγίας 2002/87/ΕΚ και για την κατάργηση των οδηγιών 2006/48/ΕΚ και 2006/49/ΕΚ.

Ιδιωτικό υπολογιστικό νέφος	Υποδομή υπολογιστικού νέφους η οποία είναι διαθέσιμη για αποκλειστική χρήση από ένα και μόνο ίδρυμα.
Κοινοτικό υπολογιστικό νέφος	Υποδομή υπολογιστικού νέφους η οποία είναι διαθέσιμη για αποκλειστική χρήση από συγκεκριμένη κοινότητα ιδρυμάτων, συμπεριλαμβανομένης της περίπτωσης διαφόρων ιδρυμάτων ενός και μόνο ομίλου.
Υβριδικό υπολογιστικό νέφος	Υποδομή υπολογιστικού νέφους η οποία περιλαμβάνει δύο ή περισσότερες διακριτές υποδομές υπολογιστικού νέφους.

3. Εφαρμογή

Ημερομηνία εφαρμογής

5. Οι παρούσες συστάσεις εφαρμόζονται από την 1η Ιουλίου 2018.

4. Συστάσεις σχετικά με την εξωτερική ανάθεση δραστηριοτήτων σε παρόχους υπηρεσιών υπολογιστικού νέφους

4.1 Αξιολόγηση σημαντικότητας

1. Τα ιδρύματα που προβαίνουν σε εξωτερική ανάθεση δραστηριοτήτων οφείλουν, πριν από οποιαδήποτε εξωτερική ανάθεση δραστηριοτήτων τους, να αξιολογούν ποιες δραστηριότητες πρέπει να θεωρούνται σημαντικές. Τα ιδρύματα θα πρέπει να διενεργούν την εν λόγω αξιολόγηση της σημαντικότητας των δραστηριοτήτων βάσει της κατευθυντήριας γραμμής 1 στοιχείο στ) των κατευθυντήριων γραμμών της ΕΕΑΤΕ και ειδικότερα σε σχέση με την εξωτερική ανάθεση δραστηριοτήτων σε παρόχους υπηρεσιών υπολογιστικού νέφους να λαμβάνουν υπόψη όλα τα ακόλουθα στοιχεία:

   (α) την κρισιμότητα και το προφίλ εγγενούς κινδύνου των δραστηριοτήτων που πρόκειται να αποτελέσουν αντικείμενο εξωτερικής ανάθεσης, δηλαδή αν πρόκειται για δραστηριότητες οι οποίες είναι κρίσιμης σημασίας για την επιχειρησιακή συνέχεια/βιωσιμότητα του ιδρύματος και τις υποχρεώσεις του έναντι των πελατών·

   (β) τις άμεσες λειτουργικές επιπτώσεις των διακοπών λειτουργίας, καθώς και τους σχετικούς νομικούς κινδύνους και κινδύνους φήμης·

   (γ) τις επιπτώσεις που ενδέχεται να έχει οποιαδήποτε διαταραχή της δραστηριότητας στις προοπτικές εσόδων του ιδρύματος·

   (δ) τις δυνητικές επιπτώσεις που θα μπορούσε να έχει η παραβίαση της εμπιστευτικότητας ή η αδυναμία διασφάλισης της ακεραιότητας των δεδομένων στο ίδρυμα και στους πελάτες του.

4.2 Καθήκον επαρκούς ενημέρωσης των εποπτικών αρχών

2. Τα ιδρύματα που προβαίνουν σε εξωτερική ανάθεση δραστηριοτήτων οφείλουν να ενημερώνουν επαρκώς τις αρμόδιες αρχές για τις σημαντικές δραστηριότητες που πρόκειται να αποτελέσουν αντικείμενο εξωτερικής ανάθεσης σε παρόχους υπηρεσιών υπολογιστικού νέφους. Τα ιδρύματα θα πρέπει να προβαίνουν στην εν λόγω ενημέρωση βάσει της παραγράφου 4.3 των κατευθυντήριων γραμμών της ΕΕΑΤΕ και, σε κάθε περίπτωση, να θέτουν στη διάθεση των αρμόδιων αρχών τις ακόλουθες πληροφορίες:

   (α) την επωνυμία του παρόχου υπηρεσιών υπολογιστικού νέφους και την επωνυμία της μητρικής εταιρείας του (εάν υπάρχει)·
   (β) περιγραφή των δραστηριοτήτων και των δεδομένων που πρόκειται να αποτελέσουν αντικείμενο εξωτερικής ανάθεσης·

(γ) τη χώρα ή τις χώρες στις οποίες πρόκειται να παρέχεται η υπηρεσία (συμπεριλαμβανομένης της τοποθεσίας που βρίσκονται τα δεδομένα)·
(δ) την ημερομηνία έναρξης παροχής της υπηρεσίας·
(ε) την τελευταία ημερομηνία ανανέωσης της σύμβασης (κατά περίπτωση)·
(στ) το εφαρμοστέο δίκαιο που διέπει τη σύμβαση·
(ζ) την ημερομηνία λήξης της παροχής της υπηρεσίας ή την επόμενη ημερομηνία ανανέωσης της σύμβασης (κατά περίπτωση).

3. Επιπλέον των πληροφοριών που παρέχονται σύμφωνα με το προηγούμενο σημείο, η αρμόδια αρχή μπορεί να ζητήσει από το ίδρυμα που προβαίνει σε εξωτερική ανάθεση δραστηριοτήτων συμπληρωματικές πληροφορίες σχετικά με την ανάλυση κινδύνου που έχει διενεργήσει για τις σημαντικές δραστηριότητες που πρόκειται να αποτελέσουν αντικείμενο εξωτερικής ανάθεσης, όπως οι ακόλουθες:

(α) κατά πόσον ο πάροχος υπηρεσιών υπολογιστικού νέφους διαθέτει σχέδιο επιχειρησιακής συνέχειας, το οποίο είναι κατάλληλο για τις υπηρεσίες που παρέχονται στο ίδρυμα που προβαίνει σε εξωτερική ανάθεση δραστηριοτήτων·
(β) κατά πόσον το ίδρυμα που προβαίνει σε εξωτερική ανάθεση δραστηριοτήτων διαθέτει στρατηγική εξόδου σε περίπτωση μονομερούς καταγγελίας της σύμβασης ή διακοπής της παροχής των υπηρεσιών από τον πάροχο υπηρεσιών υπολογιστικού νέφους·
(γ) κατά πόσον το ίδρυμα που προβαίνει σε εξωτερική ανάθεση δραστηριοτήτων διατηρεί τις δεξιότητες και τους πόρους που απαιτούνται για την επαρκή παρακολούθηση των δραστηριοτήτων που αποτελούν αντικείμενο εξωτερικής ανάθεσης.

4. Το ίδρυμα που προβαίνει σε εξωτερική ανάθεση δραστηριοτήτων οφείλει να τηρεί επικαιροποιημένο μητρώο πληροφοριών σχετικά με το σύνολο των σημαντικών και μη σημαντικών δραστηριοτήτων του που αποτελούν αντικείμενο εξωτερικής ανάθεσης σε παρόχους υπηρεσιών υπολογιστικού νέφους, τόσο σε επίπεδο ιδρύματος όσο και σε επίπεδο ομίλου. Το ίδρυμα που προβαίνει σε εξωτερική ανάθεση δραστηριοτήτων θα πρέπει να θέτει στη διάθεση της αρμόδιας αρχής, κατόπιν αιτήματός της, αντίγραφο της συμφωνίας εξωτερικής ανάθεσης, καθώς και τις συναφείς πληροφορίες που έχουν καταχωριστεί στο εν λόγω μητρώο, ανεξάρτητα από το αν η δραστηριότητα που αποτελεί αντικείμενο εξωτερικής ανάθεσης σε πάροχο υπηρεσιών υπολογιστικού νέφους έχει αξιολογηθεί από το ίδρυμα ως σημαντική.

5. Στο μητρώο που αναφέρεται στο προηγούμενο σημείο θα πρέπει να περιλαμβάνονται, τουλάχιστον, οι ακόλουθες πληροφορίες:

(α) οι πληροφορίες που αναφέρονται στο σημείο 2 στοιχεία α) έως ζ), εάν δεν έχουν ακόμη παρασχεθεί·
(β) το είδος εξωτερικής ανάθεσης δραστηριοτήτων (το μοντέλο υπηρεσιών υπολογιστικού νέφους και το μοντέλο ανάπτυξης υπολογιστικού νέφους, δηλαδή δημόσιο/ιδιωτικό/υβριδικό/κοινοτικό υπολογιστικό νέφος)·
(γ) τα μέρη που λαμβάνουν υπηρεσίες υπολογιστικού νέφους στο πλαίσιο της συμφωνίας εξωτερικής ανάθεσης·

(δ) αποδεικτικά στοιχεία της έγκρισης της εξωτερικής ανάθεσης δραστηριοτήτων από το διοικητικό όργανο ή από τις εξουσιοδοτημένες επιτροπές του, εάν υπάρχουν·
(ε) τα ονόματα των υπεργολάβων, εάν υπάρχουν·
(στ) η χώρα στην οποία είναι εγγεγραμμένος ο πάροχος υπηρεσιών υπολογιστικού νέφους / ο κύριος υπεργολάβος·
(ζ) αν η εξωτερική ανάθεση δραστηριοτήτων έχει χαρακτηριστεί ως σημαντική (ναι/όχι)·
(η) η ημερομηνία της τελευταίας αξιολόγησης που διενήργησε το ίδρυμα όσον αφορά τη σημαντικότητα των δραστηριοτήτων που αποτελούν αντικείμενο εξωτερικής ανάθεσης·
(θ) κατά πόσον ο πάροχος υπηρεσιών υπολογιστικού νέφους / ο υπεργολάβος ή οι υπεργολάβοι υποστηρίζουν επιχειρηματικές δραστηριότητες που είναι χρονικά κρίσιμης σημασίας (ναι/όχι)·
(ι) αξιολόγηση της δυνατότητας υποκατάστασης του παρόχου υπηρεσιών υπολογιστικού νέφους (ως εύκολης, δύσκολης ή αδύνατης)·
(ια) προσδιορισμός εναλλακτικού παρόχου υπηρεσιών, όπου αυτό είναι εφικτό·
(ιβ) η ημερομηνία της τελευταίας αξιολόγησης κινδύνων της ρύθμισης εξωτερικής ανάθεσης ή υπεργολαβίας.

4.3 Δικαιώματα πρόσβασης και ελέγχου

Για τα ιδρύματα

6. Βάσει της κατευθυντήριας γραμμής 8 σημείο 2 στοιχείο ζ) των κατευθυντήριων γραμμών της ΕΕΑΤΕ και για τους σκοπούς της εξωτερικής ανάθεσης δραστηριοτήτων υπολογιστικού νέφους, τα ιδρύματα που προβαίνουν σε εξωτερική ανάθεση δραστηριοτήτων θα πρέπει ακόμη να διασφαλίζουν τη σύναψη γραπτής συμφωνίας με τον πάροχο υπηρεσιών υπολογιστικού νέφους, σύμφωνα με την οποία ο εν λόγω πάροχος αναλαμβάνει την υποχρέωση:

   (α) να παρέχει στο ίδρυμα, σε οποιονδήποτε τρίτο τον οποίο ορίζει το ίδρυμα για τον σκοπό αυτόν, καθώς και στον ελεγκτή του τακτικού ελέγχου οικονομικών καταστάσεων του ιδρύματος, πλήρη πρόσβαση στις επιχειρησιακές εγκαταστάσεις του (έδρα και κέντρα επιχειρήσεων), συμπεριλαμβανομένων όλων των συσκευών, συστημάτων, δικτύων και δεδομένων που χρησιμοποιούνται για την παροχή των υπηρεσιών που αποτελούν αντικείμενο εξωτερικής ανάθεσης (δικαίωμα πρόσβασης)·

   (β) να εκχωρεί στο ίδρυμα, σε οποιονδήποτε τρίτο τον οποίο ορίζει το ίδρυμα για τον σκοπό αυτόν, καθώς και στον ελεγκτή που υπογράφει οικονομικές καταστάσεις του ιδρύματος, χωρίς περιορισμούς δικαιώματα επιθεώρησης και ελέγχου σε σχέση με τις υπηρεσίες που αποτελούν αντικείμενο εξωτερικής ανάθεσης (δικαίωμα ελέγχου).

7. Η αποτελεσματική άσκηση των δικαιωμάτων πρόσβασης και ελέγχου δεν θα πρέπει να παρεμποδίζεται ούτε να περιορίζεται από συμβατικές ρυθμίσεις. Εάν η διεξαγωγή ελέγχων ή η χρήση ορισμένων τεχνικών ελέγχου ενδέχεται να δημιουργεί κίνδυνο για το περιβάλλον άλλου

πελάτη, θα πρέπει να συμφωνούνται εναλλακτικοί τρόποι για την παροχή παρόμοιου επιπέδου διασφάλισης με αυτό που απαιτείται από το ίδρυμα.

8. Το ίδρυμα που προβαίνει σε εξωτερική ανάθεση δραστηριοτήτων θα πρέπει να ασκεί τα δικαιώματά πρόσβασης και ελέγχου με γνώμονα τον κίνδυνο. Σε περίπτωση που το ίδρυμα που προβαίνει σε εξωτερική ανάθεση δραστηριοτήτων δεν χρησιμοποιεί τους δικούς του ελεγκτικούς πόρους, θα πρέπει να εξετάζει το ενδεχόμενο χρήσης τουλάχιστον ενός από τα ακόλουθα μέσα:

   (α) Ομαδοποιημένοι έλεγχοι οι οποίοι διοργανώνονται από κοινού με άλλους πελάτες του ίδιου παρόχου υπηρεσιών υπολογιστικού νέφους, και διενεργούνται από τους εν λόγω πελάτες ή από τρίτο τον οποίο ορίζουν οι ίδιοι, με σκοπό την αποδοτικότερη χρήση των ελεγκτικών πόρων και τη μείωση του οργανωτικού φόρτου, τόσο για τους πελάτες όσο και για τον πάροχο υπηρεσιών υπολογιστικού νέφους.

   (β) Πιστοποιήσεις τρίτων και εκθέσεις ελέγχου τρίτων ή εσωτερικές εκθέσεις ελέγχου που καθίστανται διαθέσιμες από τον πάροχο υπηρεσιών υπολογιστικού νέφους, υπό τις ακόλουθες προϋποθέσεις:

      i. Το ίδρυμα που προβαίνει σε εξωτερική ανάθεση δραστηριοτήτων διασφαλίζει ότι το πεδίο εφαρμογής της πιστοποίησης ή της έκθεσης ελέγχου καλύπτει τα συστήματα (δηλαδή τις διαδικασίες, τις εφαρμογές, την υποδομή, τα μηχανογραφικά κέντρα κ.λπ.) και τους μηχανισμούς που χαρακτηρίζονται ως σημαντικοί από το ίδρυμα που προβαίνει σε εξωτερική ανάθεση δραστηριοτήτων.
      ii. Το ίδρυμα που προβαίνει σε εξωτερική ανάθεση δραστηριοτήτων διενεργεί εμπεριστατωμένη αξιολόγηση του περιεχομένου των πιστοποιήσεων ή των εκθέσεων ελέγχου σε συνεχή βάση και συγκεκριμένα διασφαλίζει ότι οι σημαντικοί μηχανισμοί ελέγχου εξακολουθούν να καλύπτονται στις μελλοντικές εκδόσεις μιας έκθεσης ελέγχου και επαληθεύει ότι η πιστοποίηση ή η έκθεση ελέγχου δεν είναι παρωχημένη.
      iii. Το ίδρυμα που προβαίνει σε εξωτερική ανάθεση δραστηριοτήτων είναι πεπεισμένο για τις ικανότητες του μέρους που πραγματοποιεί την πιστοποίηση ή τον έλεγχο (π.χ. όσον αφορά την εναλλαγή των εταιρειών πιστοποίησης ή ελέγχου, τα προσόντα, την εμπειρογνωσία, την επανεκτέλεση/επαλήθευση των αποδεικτικών στοιχείων στον υποκείμενο φάκελο ελέγχου).
      iv. Οι πιστοποιήσεις εκδίδονται και οι έλεγχοι εκτελούνται βάσει ευρέως αναγνωρισμένων προτύπων και περιλαμβάνουν δοκιμαστικό έλεγχο της επιχειρησιακής αποτελεσματικότητας των σημαντικών μηχανισμών ελέγχου που εφαρμόζονται.
      v. Το ίδρυμα που προβαίνει σε εξωτερική ανάθεση δραστηριοτήτων έχει το συμβατικό δικαίωμα να ζητεί την επέκταση του πεδίου εφαρμογής των πιστοποιήσεων ή των εκθέσεων ελέγχου σε μερικά συστήματα ή μηχανισμούς ελέγχου που σχετίζονται με την εν λόγω ανάθεση. Τα αιτήματα για την τροποποίηση του πεδίου εφαρμογής θα πρέπει να είναι εύλογα ως προς τον

αριθμό και τη συχνότητα υποβολής τους, αλλά και θεμιτά από πλευράς διαχείρισης κινδύνου.

9. Λαμβανομένου υπόψη ότι οι λύσεις υπολογιστικού νέφους χαρακτηρίζονται από υψηλό επίπεδο τεχνικής πολυπλοκότητας, το ίδρυμα που προβαίνει σε εξωτερική ανάθεση δραστηριοτήτων θα πρέπει να επαληθεύει ότι το προσωπικό που διενεργεί τον έλεγχο –είτε πρόκειται για τους εσωτερικούς ελεγκτές του είτε για την ομάδα ελεγκτών που ενεργούν εξ ονόματός του είτε για τους διορισμένους ελεγκτές του παρόχου υπηρεσιών υπολογιστικού νέφους– ή, κατά περίπτωση, το προσωπικό που επανεξετάζει την πιστοποίηση τρίτου ή τις εκθέσεις ελέγχου του παρόχου υπηρεσιών έχει αποκτήσει τις κατάλληλες δεξιότητες και γνώσεις για την εκτέλεση αποτελεσματικών και κατάλληλων ελέγχων και/ή αξιολογήσεων των λύσεων υπολογιστικού νέφους.

Για τις αρμόδιες αρχές

10. Βάσει της κατευθυντήριας γραμμής 8 σημείο 2 στοιχείο η) των κατευθυντήριων γραμμών της ΕΕΑΤΕ και για τους σκοπούς της εξωτερικής ανάθεσης δραστηριοτήτων υπολογιστικού νέφους, τα ιδρύματα που προβαίνουν σε εξωτερική ανάθεση δραστηριοτήτων θα πρέπει να διασφαλίζουν τη σύναψη γραπτής συμφωνίας με τον πάροχο υπηρεσιών υπολογιστικού νέφους, σύμφωνα με την οποία ο εν λόγω πάροχος αναλαμβάνει την υποχρέωση:

    (α) να παρέχει στην αρμόδια αρχή εποπτείας του ιδρύματος που προβαίνει σε εξωτερική ανάθεση δραστηριοτήτων (ή σε τυχόν τρίτο τον οποίο ορίζει η εν λόγω αρχή για τον σκοπό αυτόν) πλήρη πρόσβαση στις επιχειρησιακές εγκαταστάσεις του παρόχου υπηρεσιών υπολογιστικού νέφους (έδρα και κέντρα επιχειρήσεων), συμπεριλαμβανομένων όλων των συσκευών, συστημάτων, δικτύων και δεδομένων που χρησιμοποιούνται για την παροχή των υπηρεσιών στο ίδρυμα που προβαίνει σε εξωτερική ανάθεση δραστηριοτήτων (δικαίωμα πρόσβασης)·

    (β) να εκχωρεί στην αρμόδια αρχή εποπτείας του ιδρύματος που προβαίνει σε εξωτερική ανάθεση δραστηριοτήτων (ή σε οποιονδήποτε τρίτο τον οποίο ορίζει η εν λόγω αρχή για τον σκοπό αυτόν) χωρίς περιορισμούς δικαιώματα επιθεώρησης και ελέγχου σε σχέση με τις υπηρεσίες που αποτελούν αντικείμενο εξωτερικής ανάθεσης (δικαίωμα ελέγχου).

11. Το ίδρυμα που προβαίνει σε εξωτερική ανάθεση δραστηριοτήτων θα πρέπει να διασφαλίζει ότι οι συμβατικές ρυθμίσεις δεν παρεμποδίζουν την άσκηση των εποπτικών καθηκόντων ή την επίτευξη των στόχων της οικείας αρμόδιας αρχής.

12. Οι πληροφορίες που συγκεντρώνουν οι αρμόδιες αρχές από την άσκηση των δικαιωμάτων πρόσβασης και ελέγχου θα πρέπει να υπόκεινται στις απαιτήσεις τήρησης του επαγγελματικού απορρήτου και εμπιστευτικότητας που αναφέρονται στο άρθρο 53 και επόμενα της οδηγίας 2013/36/ΕΕ (τέταρτη οδηγία για τις κεφαλαιακές απαιτήσεις, ΟΚΑ IV). Οι αρμόδιες αρχές θα πρέπει να αποφεύγουν να υπογράφουν κάθε είδους συμβατική συμφωνία ή δήλωση που θα παρεμπόδιζε τη συμμόρφωσή τους προς τις διατάξεις του ενωσιακού δικαίου σχετικά

με την εμπιστευτικότητα, την τήρηση του επαγγελματικού απορρήτου και την ανταλλαγή πληροφοριών.

13. Βάσει των διαπιστώσεων του ελέγχου που διενεργεί, η αρμόδια αρχή θα πρέπει να αντιμετωπίζει τυχόν ελλείψεις που εντοπίζονται, εφόσον κρίνεται αναγκαίο, επιβάλλοντας μέτρα απευθείας στο ίδρυμα που προβαίνει σε εξωτερική ανάθεση δραστηριοτήτων.

4.4 Ειδικότερα όσον αφορά το δικαίωμα πρόσβασης

14. Η συμφωνία που αναφέρεται στα σημεία 6 και 10 θα πρέπει να περιλαμβάνει τις ακόλουθες διατάξεις:

(α) Πριν από την πραγματοποίηση προγραμματιζόμενης επιτόπιας επίσκεψης, το μέρος που προτίθεται να ασκήσει το δικαίωμα πρόσβασής του (ίδρυμα, αρμόδια αρχή, ελεγκτής ή τρίτος που ενεργεί για λογαριασμό του ιδρύματος ή της αρμόδιας αρχής) θα πρέπει να παρέχει ειδοποίηση για την επιτόπια επίσκεψη στις σχετικές επιχειρησιακές εγκαταστάσεις εντός εύλογου χρονικού διαστήματος, εκτός εάν δεν είναι εφικτή η έγκαιρη πρότερη κοινοποίηση λόγω κατάστασης έκτακτης ανάγκης ή κρίσης.

(β) Στο πλαίσιο της επιτόπιας επίσκεψης, ο πάροχος υπηρεσιών υπολογιστικού νέφους υποχρεούται να συνεργάζεται πλήρως με τις ενδεδειγμένες αρμόδιες αρχές, καθώς και με το ίδρυμα και τον ελεγκτή του.

4.5 Ασφάλεια των δεδομένων και των συστημάτων

15. Όπως ορίζεται στην κατευθυντήρια γραμμή 8 σημείο 2 στοιχείο ε) των κατευθυντήριων γραμμών της ΕΕΑΤΕ, η σύμβαση εξωτερικής ανάθεσης θα πρέπει να υποχρεώνει τον πάροχο υπηρεσιών εξωτερικής ανάθεσης να προστατεύει την εμπιστευτικότητα των πληροφορικών που διαβιβάζονται από το χρηματοπιστωτικό ίδρυμα. Σύμφωνα με την κατευθυντήρια γραμμή 6 σημείο 6 στοιχείο ε) των κατευθυντήριων γραμμών της ΕΕΑΤΕ, τα ιδρύματα θα πρέπει να εφαρμόζουν ρυθμίσεις για τη διασφάλιση της συνέχειας των υπηρεσιών που παρέχονται από παρόχους υπηρεσιών εξωτερικής ανάθεσης. Βάσει της κατευθυντήριας γραμμής 8 σημείο 2 στοιχείο β) και της κατευθυντήριας γραμμής 9 των κατευθυντήριων γραμμών της ΕΕΑΤΕ, οι αντίστοιχες ανάγκες των ιδρυμάτων που προβαίνουν σε εξωτερική ανάθεση δραστηριοτήτων όσον αφορά την ποιότητα και τις επιδόσεις θα πρέπει να ενσωματώνονται σε γραπτές συμβάσεις εξωτερικής ανάθεσης και συμφωνίες επιπέδου υπηρεσιών. Οι εν λόγω πτυχές ασφάλειας θα πρέπει επίσης να αποτελούν αντικείμενο παρακολούθησης σε διαρκή βάση (κατευθυντήρια γραμμή 7).

16. Για τους σκοπούς του προηγούμενου σημείου, το ίδρυμα θα πρέπει να προβαίνει, πριν από την εξωτερική ανάθεση δραστηριοτήτων και για τους σκοπούς της τεκμηρίωσης της σχετικής απόφασης, τουλάχιστον στις ακόλουθες ενέργειες:

(α) να προσδιορίζει και να ταξινομεί τις δραστηριότητές του, τις διαδικασίες και τα σχετικά δεδομένα και συστήματα ως προς τον βαθμό ευαισθησίας τους και τις απαιτούμενες διασφαλίσεις·

(β) να πραγματοποιεί ενδελεχή, βασιζόμενη στον κίνδυνο, επιλογή των δραστηριοτήτων, των διαδικασιών και των σχετικών δεδομένων και συστημάτων που εξετάζονται με σκοπό την εξωτερική τους ανάθεση σε φορέα παροχής λύσεων υπολογιστικού νέφους·

(γ) να καθορίζει και να αποφασίζει κατάλληλο επίπεδο προστασίας της εμπιστευτικότητας των δεδομένων, της συνέχειας των δραστηριοτήτων που αποτελούν αντικείμενο εξωτερικής ανάθεσης, καθώς και της ακεραιότητας και της ιχνηλασιμότητας των δεδομένων και των συστημάτων στο πλαίσιο της προτιθέμενης εξωτερικής ανάθεσης δραστηριοτήτων υπολογιστικού νέφους. Τα ιδρύματα θα πρέπει επίσης να εξετάζουν το ενδεχόμενο λήψης ειδικών μέτρων, όπου αυτό κρίνεται αναγκαίο, για τα δεδομένα σε μεταφορά, τα δεδομένα σε μνήμη και τα δεδομένα σε αδράνεια, όπως η χρήση τεχνολογιών κρυπτογράφησης, σε συνδυασμό με κατάλληλη αρχιτεκτονική διαχείρισης κλειδιών.

17. Κατά συνέπεια, τα ιδρύματα θα πρέπει να διασφαλίζουν τη σύναψη γραπτής συμφωνίας με τον πάροχο υπηρεσιών υπολογιστικού νέφους, στο πλαίσιο της οποίας καθορίζονται, μεταξύ άλλων, οι υποχρεώσεις του παρόχου βάσει του σημείου 16 στοιχείο γ).

18. Τα ιδρύματα θα πρέπει να παρακολουθούν σε διαρκή βάση τις επιδόσεις των δραστηριοτήτων και των μέτρων ασφάλειας σύμφωνα με την κατευθυντήρια γραμμή 7 των κατευθυντήριων γραμμών της ΕΕΑΤΕ, συμπεριλαμβανομένων τυχόν συμβάντων, και να ελέγχουν, κατά περίπτωση, κατά πόσον η εξωτερική ανάθεση των δραστηριοτήτων τους συνάδει με τα οριζόμενα στα προηγούμενα σημεία·θα πρέπει επίσης να λαμβάνουν αμέσως τυχόν απαιτούμενα διορθωτικά μέτρα.

4.6 Τοποθεσία που βρίσκονται τα δεδομένα και επεξεργασία των δεδομένων

19. Όπως ορίζεται στην κατευθυντήρια γραμμή 4 σημείο 4 των κατευθυντήριων γραμμών της ΕΕΑΤΕ, εφιστάται ιδιαιτέρως η προσοχή των ιδρυμάτων κατά τη σύναψη και τη διαχείριση συμφωνιών εξωτερικής ανάθεσης εκτός του ΕΟΧ λόγω των πιθανών κινδύνων αφενός ως προς την προστασία των δεδομένων και αφετέρου ως προς την άσκηση αποτελεσματικής εποπτείας από την εποπτική αρχή.

20. Το ίδρυμα που προβαίνει σε εξωτερική ανάθεση δραστηριοτήτων θα πρέπει να υιοθετεί μια προσέγγιση βάσει κινδύνου όσον αφορά τις παραμέτρους σχετικά με την τοποθεσία τόσο των δεδομένων όσο και της επεξεργασίας των δεδομένων κατά την εξωτερική ανάθεση δραστηριοτήτων σε περιβάλλον υπολογιστικού νέφους. Στο πλαίσιο της αξιολόγησης θα πρέπει να εξετάζονται οι δυνητικές επιπτώσεις κινδύνου, συμπεριλαμβανομένων των νομικών κινδύνων και των ζητημάτων συμμόρφωσης, καθώς και οι εποπτικοί περιορισμοί που συνδέονται με τις χώρες στις οποίες παρέχονται ή αναμένεται να παρέχονται οι υπηρεσίες που αποτελούν αντικείμενο εξωτερικής ανάθεσης και στις οποίες αποθηκεύονται ή αναμένεται να αποθηκεύονται τα δεδομένα. Η αξιολόγηση θα πρέπει να περιλαμβάνει παραμέτρους σχετικά με την ευρύτερη πολιτική σταθερότητα και σταθερότητα σε επίπεδο ασφάλειας των υπό εξέταση δικαιοδοσιών· τους ισχύοντες νόμους στις εν λόγω δικαιοδοσίες (συμπεριλαμβανομένων των νόμων περί προστασίας των δεδομένων)·και τις διατάξεις σχετικά με την επιβολή του νόμου που εφαρμόζονται στις εν λόγω δικαιοδοσίες, συμπεριλαμβανομένων των νομοθετικών διατάξεων περί αφερεγγυότητας που θα εφαρμόζονταν σε περίπτωση πτώχευσης του παρόχου υπηρεσιών υπολογιστικού νέφους. Το ίδρυμα που προβαίνει σε εξωτερική ανάθεση δραστηριοτήτων θα πρέπει να διασφαλίζει ότι οι εν λόγω κίνδυνοι διατηρούνται εντός αποδεκτών ορίων, τα οποία είναι ανάλογα της σημαντικότητας της δραστηριότητας που αποτελεί αντικείμενο εξωτερικής ανάθεσης.

4.7 Διαδοχικές εξωτερικές αναθέσεις δραστηριοτήτων

21. Όπως ορίζεται στην κατευθυντήρια γραμμή 10 των κατευθυντήριων γραμμών της ΕΕΑΤΕ, τα ιδρύματα θα πρέπει να λαμβάνουν υπόψη τους κινδύνους που συνδέονται με τις «διαδοχικές» εξωτερικές αναθέσεις δραστηριοτήτων, σε περίπτωση που ο πάροχος υπηρεσιών εξωτερικής ανάθεσης αναθέτει, βάσει υπεργολαβίας, στοιχεία της αντίστοιχης υπηρεσίας σε άλλους παρόχους. Το ίδρυμα που προβαίνει σε εξωτερική ανάθεση δραστηριοτήτων θα πρέπει να συναινεί για τις διαδοχικές εξωτερικές αναθέσεις δραστηριοτήτων μόνον εάν ο υπεργολάβος συμμορφώνεται επίσης πλήρως με τις υποχρεώσεις που προβλέπονται μεταξύ του ιδρύματος που προβαίνει σε εξωτερική ανάθεση δραστηριοτήτων και του παρόχου υπηρεσιών εξωτερικής ανάθεσης. Επιπλέον, το ίδρυμα που προβαίνει σε εξωτερική ανάθεση δραστηριοτήτων θα πρέπει να λαμβάνει κατάλληλα μέτρα για την αντιμετώπιση του κινδύνου τυχόν αδυναμίας ή αποτυχίας παροχής των υπεργολαβικών δραστηριοτήτων που έχει σημαντική επίδραση στις ικανότητες του παρόχου υπηρεσιών εξωτερικής ανάθεσης όσον αφορά την τήρηση των υποχρεώσεών του στο πλαίσιο της συμφωνίας εξωτερικής ανάθεσης.

22. Στη συμφωνία εξωτερικής ανάθεσης μεταξύ του ιδρύματος που προβαίνει σε εξωτερική ανάθεση δραστηριοτήτων και του παρόχου υπηρεσιών υπολογιστικού νέφους θα πρέπει να προσδιορίζονται όλοι οι τύποι δραστηριοτήτων που εξαιρούνται από τη δυνητική ανάθεση υπεργολαβίας και να επισημαίνεται ότι ο πάροχος υπηρεσιών υπολογιστικού νέφους διατηρεί την πλήρη ευθύνη καθώς και την εποπτεία των εν λόγω υπηρεσιών τις οποίες αναθέτει στο πλαίσιο υπεργολαβίας.

23. Η συμφωνία εξωτερικής ανάθεσης θα πρέπει επίσης να περιλαμβάνει για τον πάροχο υπηρεσιών υπολογιστικού νέφους την υποχρέωση ενημέρωσης του ιδρύματος που προβαίνει σε εξωτερική ανάθεση δραστηριοτήτων σχετικά με κάθε προγραμματιζόμενη σημαντική αλλαγή, όσον αφορά τους υπεργολάβους ή τις υπεργολαβικές υπηρεσίες που κατονομάζονται στην αρχική συμφωνία, η οποία ενδέχεται να επηρεάσει την ικανότητα του παρόχου υπηρεσιών να τηρήσει τις υποχρεώσεις του δυνάμει της συμφωνίας εξωτερικής ανάθεσης. Η προθεσμία κοινοποίησης για τις εν λόγω αλλαγές θα πρέπει να συμφωνείται εκ των προτέρων βάσει σύμβασης, ώστε να παρέχεται η δυνατότητα στο ίδρυμα που προβαίνει σε εξωτερική ανάθεση δραστηριοτήτων να διενεργεί αξιολόγηση των κινδύνων όσον αφορά τις επιπτώσεις των προτεινόμενων αλλαγών πριν τεθεί πράγματι σε ισχύ η αλλαγή όσον αφορά τους υπεργολάβους ή τις υπεργολαβικές υπηρεσίες.

24. Σε περίπτωση που ο πάροχος υπηρεσιών υπολογιστικού νέφους προγραμματίζει αλλαγές σε σχέση με υπεργολάβο ή υπεργολαβικές υπηρεσίες, οι οποίες αλλαγές θα μπορούσαν να έχουν δυσμενή επίδραση στην αξιολόγηση κινδύνων των συμφωνηθεισών υπηρεσιών, το ίδρυμα που προβαίνει σε εξωτερική ανάθεση δραστηριοτήτων θα πρέπει να έχει το δικαίωμα να καταγγείλει τη σύμβαση.

25. Το ίδρυμα που προβαίνει σε εξωτερική ανάθεση δραστηριοτήτων θα πρέπει να εξετάζει ι και να παρακολουθεί τις επιδόσεις της συνολικής υπηρεσίας σε διαρκή βάση, ανεξάρτητα από το αν αυτή παρέχεται από τον πάροχο υπηρεσιών υπολογιστικού νέφους ή από υπεργολάβους του.

4.8 Σχέδια έκτακτης ανάγκης και στρατηγικές εξόδου

26. Όπως ορίζεται στην κατευθυντήρια γραμμή 6 παράγραφος 6.1, στην κατευθυντήρια γραμμή 6 σημείο 6 στοιχείο ε) και στην κατευθυντήρια γραμμή 8 σημείο 2 στοιχείο δ) των κατευθυντήριων γραμμών της ΕΕΑΤΕ, το ίδρυμα που προβαίνει σε εξωτερική ανάθεση δραστηριοτήτων θα πρέπει να σχεδιάζει και να εφαρμόζει κατάλληλα μέτρα για τη διατήρηση της επιχειρησιακής του συνέχειας σε περίπτωση αδυναμίας ή επιδείνωσης σε μη αποδεκτό βαθμό της παροχής υπηρεσιών από πάροχο υπηρεσιών εξωτερικής ανάθεσης. Τα εν λόγω μέτρα θα πρέπει να περιλαμβάνουν σχεδιασμό έκτακτης ανάγκης και σαφώς καθορισμένη στρατηγική εξόδου. Επιπλέον, η σύμβαση εξωτερικής ανάθεσης θα πρέπει να περιέχει ρήτρα καταγγελίας και διαχείρισης εξόδου, ώστε να παρέχεται η δυνατότητα μεταφοράς των δραστηριοτήτων που παρέχονται από τον πάροχο υπηρεσιών εξωτερικής ανάθεσης σε άλλον πάροχο υπηρεσιών εξωτερικής ανάθεσης ή η δυνατότητα εκ νέου ενσωμάτωσής τους στο ίδρυμα που προβαίνει σε εξωτερική ανάθεση δραστηριοτήτων.

27. Το ίδρυμα που προβαίνει σε εξωτερική ανάθεση δραστηριοτήτων θα πρέπει επίσης να διασφαλίζει τη δυνατότητα εξόδου του από λύσεις εξωτερικής ανάθεσης δραστηριοτήτων υπολογιστικού νέφους, εάν αυτό κριθεί αναγκαίο, χωρίς αδικαιολόγητη διαταραχή της παροχής υπηρεσιών εκ μέρους του ή δυσμενείς επιπτώσεις στη συμμόρφωσή του προς το κανονιστικό καθεστώς, και χωρίς αυτό να αποβαίνει σε βάρος της συνέχειας και της ποιότητας της παροχής υπηρεσιών εκ μέρους του προς τους πελάτες. Για την επίτευξη του σκοπού αυτού, το ίδρυμα που προβαίνει σε εξωτερική ανάθεση δραστηριοτήτων θα πρέπει:

(α) να καταρτίζει και να εφαρμόζει σχέδια εξόδου τα οποία είναι ολοκληρωμένα, τεκμηριωμένα και έχουν υποβληθεί σε επαρκή δοκιμαστικό έλεγχο, όπου αυτό κρίνεται σκόπιμο·

(β) να προσδιορίζει εναλλακτικές λύσεις και να καταρτίζει σχέδια μετάβασης, ώστε να είναι σε θέση να προβαίνει σε άρση και μεταφορά υφιστάμενων δραστηριοτήτων και δεδομένων από τον πάροχο υπηρεσιών υπολογιστικού νέφους στις εν λόγω λύσεις κατά τρόπο ελεγχόμενο και επαρκώς δοκιμασμένο, λαμβάνοντας υπόψη τα ζητήματα θέσης των δεδομένων και διατήρησης της επιχειρησιακής συνέχειας κατά το στάδιο της μετάβασης·

(γ) να διασφαλίζει ότι η συμφωνία εξωτερικής ανάθεσης περιλαμβάνει για τον πάροχο υπηρεσιών υπολογιστικού νέφους την υποχρέωση να παρέχει επαρκή στήριξη στο ίδρυμα που προβαίνει σε εξωτερική ανάθεση δραστηριοτήτων για την ομαλή μεταφορά της δραστηριότητας σε άλλον πάροχο υπηρεσιών ή στην άμεση διαχείριση του ιδρύματος που προβαίνει σε εξωτερική ανάθεση δραστηριοτήτων σε περίπτωση καταγγελίας της συμφωνίας εξωτερικής ανάθεσης.

28. Κατά την ανάπτυξη στρατηγικών εξόδου, το ίδρυμα που προβαίνει σε εξωτερική ανάθεση δραστηριοτήτων θα πρέπει να λαμβάνει υπόψη τα εξής:

(α) την ανάπτυξη βασικών δεικτών κινδύνου για τον προσδιορισμό του μη αποδεκτού επιπέδου υπηρεσίας·

(β) τη διενέργεια ανάλυσης επιχειρηματικών επιπτώσεων κατ' αναλογία ως προς τις δραστηριότητες που αποτελούν αντικείμενο εξωτερικής ανάθεσης για τον προσδιορισμό των ανθρώπινων και υλικών πόρων που θα απαιτούνταν για την εφαρμογή του σχεδίου εξόδου, καθώς και του εκτιμώμενου χρόνου εφαρμογής του·

(γ) την ανάθεση ρόλων και αρμοδιοτήτων στο πλαίσιο της διαχείρισης των σχεδίων εξόδου και των δραστηριοτήτων μετάβασης·

(δ) τον καθορισμό κριτηρίων επιτυχούς μετάβασης.

29. Το ίδρυμα που προβαίνει σε εξωτερική ανάθεση δραστηριοτήτων θα πρέπει να προβλέπει τη χρήση δεικτών οι οποίοι μπορούν να ενεργοποιήσουν το σχέδιο εξόδου στο πλαίσιο της

διαρκούς παρακολούθησης και εποπτείας που ασκεί επί των υπηρεσιών που παρέχονται από τον πάροχο υπηρεσιών υπολογιστικού νέφους.