EBA/GL/2017/05

11/09/2017

Κατευθυντήριες γραμμές

Κατευθυντήριες γραμμές σχετικά με την αξιολόγηση κινδύνων ΤΠΕ σύμφωνα με τη διαδικασία εποπτικού ελέγχου και αξιολόγησης (ΔΕΕΑ)

1. Συμμόρφωση και υποχρεώσεις υποβολής στοιχείων και αναφορών

Συμμόρφωση και υποχρεώσεις υποβολής στοιχείων και αναφορών

1. Το παρόν έγγραφο περιέχει κατευθυντήριες γραμμές 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 κατευθυντήριες γραμμές.

2. Οι κατευθυντήριες γραμμές 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 κατευθυντήριες γραμμές, 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 κατευθυντήριες γραμμές απευθύνονται κυρίως στα ιδρύματα.

Απαιτήσεις υποβολής στοιχείων και αναφορών

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 κατευθυντήριες γραμμές, ή άλλως να εκθέσουν τους λόγους μη συμμόρφωσης, έως τις 13.11.2017. Εάν η προθεσμία γνωστοποίησης παρέλθει άπρακτη, η ΕΑΤ θεωρεί 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/GL/2017/05». 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

5. Οι παρούσες κατευθυντήριες γραμμές, οι οποίες καταρτίστηκαν σύμφωνα με το άρθρο 107 παράγραφος 3 της οδηγίας 2013/36/ΕΕ[2], αποσκοπούν στο να διασφαλίσουν τη σύγκλιση των πρακτικών εποπτείας για την αξιολόγηση του κινδύνου τεχνολογιών πληροφορικής και επικοινωνιών (ΤΠΕ) στο πλαίσιο της διαδικασίας εποπτικού ελέγχου και αξιολόγησης (ΔΕΕΑ) που αναφέρεται στο άρθρο 97 της οδηγίας 2013/36/ΕΕ και προσδιορίζεται περαιτέρω στις κατευθυντήριες γραμμές σχετικά με κοινές διαδικασίες και μεθοδολογίες για τη διαδικασία εποπτικού ελέγχου και αξιολόγησης (ΔΕΕΑ) της ΕΑΤ[3]. Ειδικότερα, οι παρούσες κατευθυντήριες γραμμές προσδιορίζουν τα κριτήρια αξιολόγησης που θα πρέπει να εφαρμόζουν οι αρμόδιες αρχές για την εποπτική αξιολόγηση της διακυβέρνησης των ιδρυμάτων και της στρατηγικής τους σχετικά με τις ΤΠΕ καθώς και για την εποπτική αξιολόγηση της έκθεσης των ιδρυμάτων σε κινδύνους ΤΠΕ και των ελέγχων που αυτά εφαρμόζουν. Οι παρούσες κατευθυντήριες γραμμές αποτελούν αναπόσπαστο μέρος των κατευθυντήριων γραμμών ΔΕΕΑ της ΕΑΤ.

6. Οι αρμόδιες αρχές θα πρέπει να εφαρμόζουν τις παρούσες κατευθυντήριες γραμμές σύμφωνα με το επίπεδο εφαρμογής της ΔΕΕΑ που προσδιορίζεται στις κατευθυντήριες γραμμές ΔΕΕΑ της ΕΑΤ και σύμφωνα με το μοντέλο ελάχιστης συνεργασίας και τις απαιτήσεις αναλογικότητας που ορίζονται σε αυτές.

Αποδέκτες

7. Οι παρούσες κατευθυντήριες γραμμές απευθύνονται στις αρμόδιες αρχές που ορίζονται στο άρθρο 4 παράγραφος 2 σημείο i) του κανονισμού (ΕΕ) αριθ. 1093/2010.

Ορισμοί

8. Εκτός εάν προβλέπεται διαφορετικά, οι όροι που χρησιμοποιούνται και ορίζονται στην οδηγία 2013/36/ΕΕ, τον κανονισμό (ΕΕ) αριθ. 575/2013 και οι ορισμοί στις κατευθυντήριες γραμμές της ΕΑΤ για τη ΔΕΕΑ έχουν την ίδια έννοια και στις παρούσες κατευθυντήριες γραμμές. Επιπλέον, για τους σκοπούς του παρόντος εγγράφου ισχύουν οι ακόλουθοι ορισμοί:

[2] 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 (1) - ΕΕ L 176 της 27.6.2013.

[3] EBA/GL/2014/13

Συστήματα ΤΠΕ	Εγκατάσταση ΤΠΕ ως μέρος ενός μηχανισμού ή ενός δικτύου διασύνδεσης το οποίο υποστηρίζει τις λειτουργίες ενός ιδρύματος.
Υπηρεσίες ΤΠΕ	Υπηρεσίες παρεχόμενες από συστήματα ΤΠΕ σε έναν ή περισσότερους εσωτερικούς ή εξωτερικούς χρήστες. Περιλαμβάνονται, παραδείγματος χάριν, υπηρεσίες εισαγωγής δεδομένων, αποθήκευσης δεδομένων, επεξεργασίας δεδομένων και υποβολής αναφορών, αλλά και υπηρεσίες παρακολούθησης, υποστήριξης δραστηριοτήτων και υποστήριξης της λήψης αποφάσεων.
Κίνδυνος για τη διαθεσιμότητα και τη συνέχεια των ΤΠΕ	Ο κίνδυνος ύπαρξης δυσμενών επιπτώσεων στις επιδόσεις και τη διαθεσιμότητα συστημάτων και δεδομένων ΤΠΕ, συμπεριλαμβανομένης της αδυναμίας έγκαιρης ανάκτησης των υπηρεσιών του ιδρύματος, λόγω αστοχίας στοιχείων υλικού ή λογισμικού ΤΠΕ· αδυναμιών στη διαχείριση του συστήματος ΤΠΕ· ή οποιουδήποτε άλλου συμβάντος, όπως επεξηγείται περαιτέρω στο παράρτημα.
Κίνδυνος ασφάλειας των ΤΠΕ	Ο κίνδυνος μη εξουσιοδοτημένης πρόσβασης σε συστήματα και δεδομένα ΤΠΕ από σημείο εντός ή εκτός του ιδρύματος (π.χ. κυβερνοεπιθέσεις), όπως επεξηγείται περαιτέρω στο παράρτημα.
Κίνδυνος αλλαγών των ΤΠΕ	Ο κίνδυνος που ανακύπτει από την αδυναμία του ιδρύματος να διαχειριστεί αλλαγές σε συστήματα ΤΠΕ έγκαιρα και ελεγχόμενα, ιδίως στην περίπτωση προγραμμάτων μεγάλων και περίπλοκων αλλαγών, όπως επεξηγείται περαιτέρω στο παράρτημα.
Κίνδυνος ακεραιότητας δεδομένων ΤΠΕ	Ο κίνδυνος αποθήκευσης και επεξεργασίας από τα συστήματα ΤΠΕ ελλιπών, ανακριβών ή αντιφατικών δεδομένων των διαφόρων συστημάτων ΤΠΕ, για παράδειγμα λόγω ανεπαρκών ελέγχων ΤΠΕ ή λόγω απουσίας ελέγχων ΤΠΕ κατά τα διάφορα στάδια του κύκλου ζωής των δεδομένων ΤΠΕ (δηλαδή, σχεδιασμός της αρχιτεκτονικής δεδομένων, δημιουργία του μοντέλου δεδομένων και/ή λεξικών δεδομένων, επαλήθευση εισαγωγών δεδομένων, έλεγχος εξαγωγών δεδομένων, μεταφορές και επεξεργασία, συμπεριλαμβανομένων των αποτελεσμάτων παραγόμενων δεδομένων), γεγονός που πλήττει την ικανότητα ενός ιδρύματος να παρέχει υπηρεσίες και να παράγει πληροφορίες διαχείρισης (κινδύνου) και χρηματοοικονομικές πληροφορίες σωστά και έγκαιρα, όπως επεξηγείται περαιτέρω στο παράρτημα.

Κίνδυνος εξωτερικής ανάθεσης ΤΠΕ	Ο κίνδυνος πρόκλησης δυσμενών επιπτώσεων στις επιδόσεις και τη διαχείριση κινδύνων του ιδρύματος λόγω της πρόσληψης τρίτου μέρους ή άλλης οντότητας του ομίλου (ενδοομιλική ανάθεση σε τρίτους) για την παροχή συστημάτων ΤΠΕ ή σχετικών υπηρεσιών, όπως επεξηγείται περαιτέρω στο παράρτημα.

3. Εφαρμογή

Ημερομηνία εφαρμογής

9. Οι παρούσες κατευθυντήριες γραμμές εφαρμόζονται από την 1η Ιανουαρίου 2018.

4. Απαιτήσεις για την αξιολόγηση κινδύνου ΤΠΕ

Τίτλος 1 - Γενικές διατάξεις

10. Οι αρμόδιες αρχές θα πρέπει να διενεργήσουν την αξιολόγηση του κινδύνου ΤΠΕ, της ρύθμισης διακυβέρνησης και της στρατηγικής ΤΠΕ στο πλαίσιο της διαδικασίας εποπτικού ελέγχου και αξιολόγησης (ΔΕΕΑ) σύμφωνα με το μοντέλο ελάχιστης συνεργασίας και τα κριτήρια αναλογικότητας που προσδιορίζονται στον τίτλο 2 των κατευθυντήριων γραμμών ΔΕΕΑ της ΕΑΤ. Ειδικότερα, αυτό σημαίνει ότι:

    α. η συχνότητα της αξιολόγησης κινδύνου ΤΠΕ θα εξαρτάται από το μοντέλο ελάχιστης συνεργασίας βάσει της κατηγορίας ΔΕΕΑ στην οποία κατατάσσεται ένα ίδρυμα και του συγκεκριμένου προγράμματος εποπτικού ελέγχου που εφαρμόζει· και

    β. το βάθος, η λεπτομέρεια και η ένταση της αξιολόγησης των ΤΠΕ θα πρέπει να είναι ανάλογα του μεγέθους, της δομής και του επιχειρησιακού περιβάλλοντος του ιδρύματος, καθώς και της φύσης, της κλίμακας και της πολυπλοκότητας των δραστηριοτήτων του.

11. Η αρχή της αναλογικότητας εφαρμόζεται σε όλα τα σημεία των κατευθυντήριων γραμμών όσον αφορά το πεδίο εφαρμογής, τη συχνότητα και την ένταση της εποπτικής συνεργασίας και του διαλόγου με ένα ίδρυμα και τις εποπτικές προσδοκίες για τα πρότυπα που θα πρέπει να πληροί το ίδρυμα.

12. Οι αρμόδιες αρχές δύνανται να βασίζονται και να λαμβάνουν υπόψη το έργο που έχει επιτελέσει ήδη το ίδρυμα ή η αρμόδια αρχή στο πλαίσιο των αξιολογήσεων άλλων κινδύνων ή στοιχείων της ΔΕΕΑ για την επικαιροποίηση της αξιολόγησης. Πιο συγκεκριμένα, κατά τη διεξαγωγή των αξιολογήσεων που προσδιορίζονται στις παρούσες κατευθυντήριες γραμμές, οι αρμόδιες αρχές θα πρέπει να επιλέγουν την καταλληλότερη προσέγγιση και μεθοδολογία εποπτικής αξιολόγησης, η οποία ταιριάζει καλύτερα και είναι ανάλογη του ιδρύματος, και θα πρέπει να λαμβάνουν υπόψη τους στην αξιολόγηση που διενεργούν τα υπάρχοντα και διαθέσιμα έγγραφα τεκμηρίωσης [π.χ. σχετικές αναφορές και άλλα έγγραφα, συναντήσεις με στελέχη διαχείρισης (κινδύνου), διαπιστώσεις επιτόπιων ελέγχων] για την επικαιροποίηση της αξιολόγησης των αρμόδιων αρχών.

13. Οι αρμόδιες αρχές θα πρέπει να συνοψίζουν τις διαπιστώσεις των αξιολογήσεων που διενεργούν με βάση τα κριτήρια που προσδιορίζονται στις παρούσες κατευθυντήριες γραμμές και να τις χρησιμοποιούν για να αντλούν συμπεράσματα σχετικά με την αξιολόγηση των στοιχείων της ΔΕΕΑ που προσδιορίζονται στις κατευθυντήριες γραμμές ΔΕΕΑ της ΕΑΤ.

14. Ειδικότερα, η αξιολόγηση της διακυβέρνησης και της στρατηγικής ΤΠΕ που διεξάγεται σύμφωνα με τον τίτλο 2 των κατευθυντήριων γραμμών θα πρέπει να καταλήγει σε διαπιστώσεις οι οποίες λαμβάνονται

υπόψη στη σύνοψη διαπιστώσεων της αξιολόγησης του στοιχείου της ΔΕΕΑ που αφορά την εσωτερική διακυβέρνηση και τους ελέγχους σε επίπεδο ιδρύματος, όπως προσδιορίζεται στον τίτλο 5 των κατευθυντήριων γραμμών ΔΕΕΑ της ΕΑΤ. Επίσης η συγκεκριμένη αξιολόγηση πρέπει να αποτυπώνεται στην αντίστοιχη βαθμολόγηση του εν λόγω στοιχείου της ΔΕΕΑ. Επιπροσθέτως, οι αρμόδιες αρχές θα πρέπει να λαμβάνουν υπόψη ότι οποιαδήποτε σημαντική δυσμενής επίπτωση της αξιολόγησης της στρατηγικής ΤΠΕ στην επιχειρηματική στρατηγική του ιδρύματος ή οποιοσδήποτε προβληματισμός ότι το ίδρυμα μπορεί να μην διαθέτει επαρκείς πόρους ΤΠΕ και ικανότητες ΤΠΕ για την εκτέλεση και την υποστήριξη σημαντικών σχεδιαζόμενων στρατηγικών αλλαγών θα πρέπει να συμπεριλαμβάνεται στην ανάλυση επιχειρηματικού μοντέλου η οποία διενεργείται σύμφωνα με τον τίτλο 4 των κατευθυντήριων γραμμών ΔΕΕΑ της ΕΑΤ.

15. Το αποτέλεσμα της αξιολόγησης του κινδύνου ΤΠΕ, όπως προσδιορίζεται στον τίτλο 3 των κατευθυντήριων γραμμών, θα πρέπει να λαμβάνεται υπόψη στις διαπιστώσεις της αξιολόγησης επιχειρησιακού κινδύνου και να θεωρείται παράγοντας που επηρεάζει τη σχετική βαθμολογία που προσδιορίζεται στον τίτλο 6.4 των κατευθυντήριων γραμμών ΔΕΕΑ της ΕΑΤ.

16. Επισημαίνεται ότι, παρόλο που, γενικά, οι αρμόδιες αρχές θα πρέπει να αξιολογούν υποκατηγορίες κινδύνων στο πλαίσιο των γενικών κατηγοριών (δηλαδή, ο κίνδυνος ΤΠΕ θα αξιολογείται στο πλαίσιο του επιχειρησιακού κινδύνου), στην περίπτωση που οι αρμόδιες αρχές θεωρούν ορισμένες υποκατηγορίες ουσιώδεις, δύναται να αξιολογούν τις εν λόγω υποκατηγορίες μεμονωμένα. Για τον σκοπό αυτό, εάν η αρμόδια αρχή αποφασίσει ότι ο κίνδυνος ΤΠΕ είναι ουσιώδης, οι παρούσες κατευθυντήριες γραμμές παρέχουν επίσης έναν πίνακα βαθμολόγησης (πίνακας 1) ο οποίος θα πρέπει να χρησιμοποιείται για την απόδοση ανεξάρτητης βαθμολογίας υποκατηγορίας για τον κίνδυνο ΤΠΕ σύμφωνα με τη συνολική προσέγγιση για τη βαθμολόγηση των κινδύνων για το κεφάλαιο που ορίζεται στις κατευθυντήριες γραμμές ΔΕΕΑ της ΕΑΤ.

17. Για να καθοριστεί εάν ο κίνδυνος ΤΠΕ θα πρέπει να θεωρείται ουσιώδης και, επομένως, εάν ο κίνδυνος ΤΠΕ θα πρέπει να αξιολογηθεί και να βαθμολογηθεί ως επιμέρους υποκατηγορία επιχειρησιακού κινδύνου, οι αρμόδιες αρχές δύνανται να χρησιμοποιούν τα κριτήρια που προσδιορίζονται στο τμήμα 6.1 των κατευθυντήριων γραμμών ΔΕΕΑ της ΕΑΤ.

18. Κατά την εφαρμογή αυτών των κατευθυντήριων γραμμών, οι αρμόδιες αρχές θα πρέπει, εφόσον ενδείκνυται, να λαμβάνουν υπόψη τον μη εξαντλητικό κατάλογο υποκατηγοριών κινδύνου και σεναρίων κινδύνου ΤΠΕ που ορίζονται στο παράρτημα, επισημαίνοντας ότι το παράρτημα εστιάζεται σε κινδύνους ΤΠΕ που μπορεί να προκαλέσουν πολύ σοβαρές ζημίες. Οι αρμόδιες αρχές δύνανται να εξαιρέσουν ορισμένους από τους κινδύνους ΤΠΕ που περιλαμβάνονται στην ταξινόμηση, εάν δεν έχουν σημασία για την αξιολόγηση. Τα ιδρύματα αναμένεται να διατηρούν τις δικές τους ταξινομήσεις κινδύνων αντί να χρησιμοποιούν την ταξινόμηση κινδύνων ΤΠΕ που ορίζεται στο παράρτημα.

19. Όταν οι παρούσες κατευθυντήριες γραμμές εφαρμόζονται σε διασυνοριακούς τραπεζικούς ομίλους και τις οντότητές τους, και έχει συσταθεί σώμα εποπτών, οι εμπλεκόμενες αρμόδιες αρχές θα πρέπει, στο πλαίσιο της συνεργασίας τους για την αξιολόγηση ΔΕΕΑ σύμφωνα με την ενότητα 11.1 των κατευθυντήριων γραμμών ΔΕΕΑ της ΕΑΤ, να συντονίζουν στον μέγιστο δυνατό βαθμό το ακριβές και λεπτομερές πεδίο εφαρμογής κάθε πληροφορίας με συνέπεια για όλες τις οντότητες του ομίλου.

Τίτλος 2 - Αξιολόγηση της διακυβέρνησης και της στρατηγικής ΤΠΕ των ιδρυμάτων

2.1 Γενικές αρχές

20. Οι αρμόδιες αρχές θα πρέπει να αξιολογούν εάν το γενικό πλαίσιο διακυβέρνησης και εσωτερικού ελέγχου του ιδρύματος καλύπτει δεόντως τα συστήματα ΤΠΕ και τους σχετικούς κινδύνους και εάν το διοικητικό όργανο αντιμετωπίζει και διαχειρίζεται επαρκώς αυτά τα ζητήματα, καθώς οι ΤΠΕ είναι αναπόσπαστο μέρος της ορθής λειτουργίας ενός ιδρύματος.

21. Κατά τη διεξαγωγή αυτής της αξιολόγησης, οι αρμόδιες αρχές θα πρέπει να αναφέρονται στις απαιτήσεις και τα πρότυπα ορθής εσωτερικής διακυβέρνησης και στις ρυθμίσεις ελέγχου των κινδύνων που προσδιορίζονται στις κατευθυντήριες γραμμές της ΕΑΤ σχετικά με την εσωτερική διακυβέρνηση (GL 44)[4] και στα διεθνή έγγραφα καθοδήγησης στον συγκεκριμένο τομέα, στον βαθμό που οι εν λόγω πηγές αναφοράς ισχύουν για τα ιδιαίτερα αυτά συστήματα και κινδύνους ΤΠΕ.

22. Η αξιολόγηση με βάση τον παρόντα τίτλο δεν καλύπτει τα ειδικά στοιχεία της διακυβέρνησης, της διαχείρισης κινδύνων και των ελέγχων του συστήματος ΤΠΕ τα οποία εστιάζονται στη διαχείριση των ειδικών κινδύνων ΤΠΕ που αναφέρονται στον τίτλο 3 αυτών των κατευθυντήριων γραμμών, αλλά επικεντρώνεται στους παρακάτω τομείς:

    α. στρατηγική ΤΠΕ – εάν το ίδρυμα διαθέτει στρατηγική ΤΠΕ την οποία διαχειρίζεται κατάλληλα και η οποία είναι σύμφωνη με την επιχειρηματική στρατηγική του ιδρύματος·

    β. συνολική εσωτερική διακυβέρνηση – εάν οι ρυθμίσεις συνολικής εσωτερικής διακυβέρνησης του ιδρύματος είναι επαρκείς σε σχέση με τα συστήματα ΤΠΕ του ιδρύματος· και

    γ. κίνδυνος ΤΠΕ στο πλαίσιο διαχείρισης κινδύνων του ιδρύματος – εάν το πλαίσιο διαχείρισης κινδύνων και εσωτερικού ελέγχου του ιδρύματος διασφαλίζει επαρκώς τα συστήματα ΤΠΕ του ιδρύματος.

23. Παρόλο που το στοιχείο α) του σημείου 22 παρέχει πληροφορίες για στοιχεία της διακυβέρνησης του ιδρύματος, θα πρέπει να χρησιμοποιείται κυρίως για την αξιολόγηση του επιχειρηματικού μοντέλου που αναφέρεται στον τίτλο 4 των κατευθυντήριων γραμμών ΔΕΕΑ της ΕΑΤ. Τα στοιχεία β) και γ) συμπληρώνουν περαιτέρω αξιολογήσεις θεμάτων που καλύπτονται από τον τίτλο 5 των κατευθυντήριων γραμμών ΔΕΕΑ της ΕΑΤ και η αξιολόγηση που περιγράφεται στις παρούσες κατευθυντήριες γραμμές θα πρέπει να χρησιμοποιείται για την αντίστοιχη αξιολόγηση δυνάμει του τίτλου 5 των κατευθυντήριων γραμμών ΔΕΕΑ της ΕΑΤ.

[4] Κατευθυντήριες γραμμές της ΕΑΤ σχετικά με την εσωτερική διακυβέρνηση, GL 44, 27 Σεπτεμβρίου 2011.

24. Το αποτέλεσμα της εν λόγω αξιολόγησης θα πρέπει να λαμβάνεται υπόψη, εφόσον ενδείκνυται, στην αξιολόγηση της διαχείρισης κινδύνων και των ελέγχων που αναφέρεται στον τίτλο 3 των κατευθυντήριων γραμμών.

2.2 Στρατηγική ΤΠΕ

25. Σύμφωνα με το παρόν τμήμα, οι αρμόδιες αρχές θα πρέπει να αξιολογήσουν εάν το ίδρυμα εφαρμόζει στρατηγική ΤΠΕ η οποία υπόκειται σε κατάλληλη εποπτεία από το διοικητικό όργανο του ιδρύματος· η οποία συνάδει με την επιχειρηματική στρατηγική, ιδίως για τη συνεχή επικαιροποίηση των ΤΠΕ και για τον σχεδιασμό ή την υλοποίηση σημαντικών και περίπλοκων αλλαγών στις ΤΠΕ· και η οποία υποστηρίζει το επιχειρηματικό μοντέλο του ιδρύματος.

2.2.1 Ανάπτυξη και επάρκεια της στρατηγικής ΤΠΕ

26. Οι αρμόδιες αρχές θα πρέπει να αξιολογήσουν εάν το ίδρυμα διαθέτει πλαίσιο, ανάλογο της φύσης, της κλίμακας και της πολυπλοκότητας των δραστηριοτήτων ΤΠΕ που εκτελεί, για την προετοιμασία και την ανάπτυξη της στρατηγικής ΤΠΕ του ιδρύματος. Κατά τη διεξαγωγή αυτής της αξιολόγησης, οι αρμόδιες αρχές θα πρέπει να λαμβάνουν υπόψη εάν:

    α. τα ανώτατα διοικητικά στελέχη[5] του(των) επιχειρηματικού(-ών) τομέα(-ων) συμμετέχουν επαρκώς στον καθορισμό των στρατηγικών προτεραιοτήτων ΤΠΕ του ιδρύματος, εάν, αντιστρόφως, τα ανώτατα διοικητικά στελέχη του τμήματος ΤΠΕ έχουν λάβει γνώση της ανάπτυξης, του σχεδιασμού και της έναρξης σημαντικών επιχειρηματικών στρατηγικών και πρωτοβουλιών για τη διασφάλιση της συνεχούς ευθυγράμμισης μεταξύ των συστημάτων ΤΠΕ, των υπηρεσιών ΤΠΕ και του τμήματος ΤΠΕ (δηλαδή, όσων είναι υπεύθυνοι για τη διαχείριση και την ανάπτυξη αυτών των συστημάτων και υπηρεσιών) και της επιχειρηματικής στρατηγικής του ιδρύματος και εάν οι ΤΠΕ επικαιροποιούνται αποτελεσματικά·

    β. η στρατηγική ΤΠΕ είναι τεκμηριωμένη και υποστηρίζεται από συγκεκριμένα σχέδια εφαρμογής, ιδίως όσον αφορά τα σημαντικά ορόσημα και των σχεδιασμό των πόρων (συμπεριλαμβανομένων των χρηματοοικονομικών και ανθρώπινων πόρων), ώστε να εξασφαλίζεται ότι αυτά είναι ρεαλιστικά και επιτρέπουν την εφαρμογή της στρατηγικής ΤΠΕ·

    γ. το ίδρυμα επικαιροποιεί περιοδικά την στρατηγική ΤΠΕ που εφαρμόζει, ιδίως όταν αλλάζει την επιχειρηματική στρατηγική του, ώστε να εξασφαλίζεται η συνεχής ευθυγράμμιση μεταξύ των ΤΠΕ και των μεσομακροπρόθεσμων επιχειρηματικών στόχων, σχεδίων και δραστηριοτήτων· και

    δ. το διοικητικό όργανο του ιδρύματος εγκρίνει τη στρατηγική ΤΠΕ, τα σχέδια εφαρμογής της, και παρακολουθεί την εφαρμογή της.

[5] Ανώτατα διοικητικά στελέχη και διοικητικό όργανο, όπως ορίζονται στην οδηγία 2013/36/ΕΕ της 26ης Ιουνίου 2013 και ειδικότερα στο άρθρο 3 παράγραφος 7 (διοικητικό όργανο) και στο άρθρο 3 παράγραφος 9 (ανώτατα διοικητικά στελέχη).

2.2.2 Εφαρμογή της στρατηγικής ΤΠΕ

27. Εάν η στρατηγική ΤΠΕ του ιδρύματος απαιτεί την εφαρμογή σημαντικών και περίπλοκων αλλαγών στις ΤΠΕ ή αλλαγών οι οποίες έχουν ουσιώδεις επιπτώσεις στο επιχειρηματικό μοντέλο του ιδρύματος, οι αρμόδιες αρχές θα πρέπει να αξιολογήσουν εάν το ίδρυμα εφαρμόζει πλαίσιο ελέγχου, κατάλληλο του μεγέθους του, των δραστηριοτήτων ΤΠΕ που εκτελεί, καθώς και του επιπέδου των δραστηριοτήτων αλλαγής, για την υποστήριξη της αποτελεσματικής εφαρμογής της στρατηγικής ΤΠΕ του ιδρύματος. Κατά τη διεξαγωγή αυτής της αξιολόγησης, οι αρμόδιες αρχές θα πρέπει να λαμβάνουν υπόψη εάν το πλαίσιο ελέγχου:

    α. περιλαμβάνει διαδικασίες διακυβέρνησης (π.χ. παρακολούθηση προόδου και προϋπολογισμού και υποβολή αναφορών) και σχετικούς φορείς (π.χ. γραφείο διαχείρισης έργου, διευθύνουσα ομάδα ΤΠΕ ή ισοδύναμο φορέα) για την αποτελεσματική υποστήριξη της εφαρμογής των στρατηγικών προγραμμάτων ΤΠΕ·

    β. έχει ορίσει και κατανείμει ρόλους και αρμοδιότητες για την εφαρμογή στρατηγικών προγραμμάτων ΤΠΕ, δίδοντας ιδιαίτερη προσοχή στην εμπειρία των σημαντικότερων ενδιαφερόμενων φορέων στην οργάνωση, τη διεύθυνση και την παρακολούθηση σημαντικών και περίπλοκων αλλαγών σε ΤΠΕ και στη διαχείριση των ευρύτερων επιπτώσεων στην οργάνωση και το ανθρώπινο δυναμικό (π.χ. διαχείριση της αντίστασης στην αλλαγή, κατάρτιση, επικοινωνία)·

    γ. προβλέπει τη συμμετοχή των τμημάτων ανεξάρτητου ελέγχου και εσωτερικού ελέγχου ώστε να διασφαλιστεί ο εντοπισμός, η αξιολόγηση και ο αποτελεσματικός μετριασμός των κινδύνων που σχετίζονται με την εφαρμογή της στρατηγικής ΤΠΕ και η αποτελεσματικότητα του εφαρμοζόμενου πλαισίου διακυβέρνησης για την υλοποίηση της στρατηγικής ΤΠΕ· και

    δ. περιέχει διαδικασία σχεδιασμού και επανεξέτασης του σχεδιασμού η οποία παρέχει ευελιξία για την αντιμετώπιση σημαντικών ζητημάτων που εντοπίζονται (π.χ. προβλήματα ή καθυστερήσεις στην εφαρμογή) ή εξωτερικών εξελίξεων (π.χ. σημαντικές αλλαγές στο επιχειρηματικό περιβάλλον, τεχνολογικά ζητήματα ή καινοτομίες), ώστε να διασφαλίζεται η έγκαιρη προσαρμογή του στρατηγικού σχεδίου εφαρμογής.

2.3 Συνολική εσωτερική διακυβέρνηση

28. Σύμφωνα με τον τίτλο 5 των κατευθυντήριων γραμμών ΔΕΕΑ της ΕΑΤ, οι αρμόδιες αρχές θα πρέπει να αξιολογήσουν εάν το ίδρυμα διαθέτει κατάλληλη και διαφανή εταιρική δομή η οποία να εξυπηρετεί τον επιδιωκόμενο σκοπό και εάν έχει εφαρμόσει κατάλληλες ρυθμίσεις διακυβέρνησης. Όσον αφορά συγκεκριμένα τα συστήματα ΤΠΕ και σύμφωνα με τις κατευθυντήριες γραμμές της ΕΑΤ σχετικά με την εσωτερική διακυβέρνηση, αυτή η αξιολόγηση θα πρέπει να αξιολογεί, μεταξύ άλλων, εάν το ίδρυμα αποδεικνύει:

    α. αξιόπιστη και διαφανή οργανωτική δομή με σαφείς αρμοδιότητες για τις ΤΠΕ, συμπεριλαμβανομένου του διοικητικού οργάνου και των επιτροπών του, και ότι τα πρόσωπα που είναι κυρίως υπεύθυνα για τις ΤΠΕ (π.χ. υπεύθυνος πληροφορικής, γενικός διευθυντής ή ισοδύναμος ρόλος) έχουν επαρκή έμμεση ή άμεση πρόσβαση στο διοικητικό όργανο, ώστε να εξασφαλίζεται η επαρκής υποβολή αναφορών, συζήτηση και λήψη αποφάσεων σχετικά με

σημαντικές πληροφορίες ή ζητήματα που αφορούν τις ΤΠΕ σε επίπεδο διοικητικού οργάνου· και

β. ότι το διοικητικό όργανο γνωρίζει και αντιμετωπίζει τους κινδύνους που συνδέονται με τις ΤΠΕ.

29. Επιπλέον του τμήματος 5.2 των κατευθυντήριων γραμμών ΔΕΕΑ της ΕΑΤ, οι αρμόδιες αρχές θα πρέπει να αξιολογήσουν εάν η πολιτική και η στρατηγική εξωτερικής ανάθεσης ΤΠΕ του ιδρύματος λαμβάνουν υπόψη, όπου ενδείκνυται, τον αντίκτυπο της εξωτερικής ανάθεσης ΤΠΕ στις δραστηριότητες και το επιχειρηματικό μοντέλο του ιδρύματος.

2.4 Ο κίνδυνος ΤΠΕ στο πλαίσιο διαχείρισης κινδύνων του ιδρύματος

30. Κατά την αξιολόγηση της διαχείρισης κινδύνων και των εσωτερικών δικλείδων ασφάλειας του ιδρύματος σε επίπεδο ιδρύματος, όπως ορίζεται στον τίτλο 5 των κατευθυντήριων γραμμών ΔΕΕΑ της ΕΑΤ, οι αρμόδιες αρχές θα πρέπει να εξετάζουν εάν το πλαίσιο διαχείρισης κινδύνων και εσωτερικού ελέγχου του ιδρύματος διασφαλίζει επαρκώς τα συστήματα ΤΠΕ του ιδρύματος, κατά τρόπο ανάλογο του μεγέθους και των δραστηριοτήτων, καθώς και του προφίλ κινδύνων ΤΠΕ του ιδρύματος, όπως ορίζεται στον τίτλο 3. Ειδικότερα, οι αρμόδιες αρχές θα πρέπει να καθορίσουν εάν:

α. η διάθεση για ανάληψη κινδύνων και η εσωτερική διαδικασία αξιολόγησης της κεφαλαιακής επάρκειας (ICAAP) καλύπτουν τους κινδύνους ΤΠΕ, στο πλαίσιο της ευρύτερης κατηγορίας των επιχειρησιακών κινδύνων, για τον καθορισμό της συνολικής στρατηγικής κινδύνου και τον προσδιορισμό του εσωτερικού κεφαλαίου· και

β. οι κίνδυνοι ΤΠΕ εμπίπτουν στο πεδίο εφαρμογής των πλαισίων διαχείρισης κινδύνων και εσωτερικού ελέγχου σε επίπεδο ιδρύματος.

31. Οι αρμόδιες αρχές θα πρέπει να διενεργήσουν την αξιολόγηση που προβλέπεται στο στοιχείο α) ανωτέρω λαμβάνοντας υπόψη τόσο αναμενόμενα όσο και δυσμενή σενάρια, π.χ. σενάρια που περιλαμβάνονται στην προσομοίωση ακραίων καταστάσεων ειδικά για το ίδρυμα ή την εποπτική προσομοίωση ακραίων καταστάσεων.

32. Όσον αφορά ειδικότερα το στοιχείο β), οι αρμόδιες αρχές θα πρέπει να αξιολογήσουν εάν τα τμήματα ανεξάρτητου ελέγχου και εσωτερικού ελέγχου, όπως αναφέρεται λεπτομερώς στο σημείο 104 στοιχεία α) και δ) και το σημείο 105 στοιχεία α) και γ) των κατευθυντήριων γραμμών ΔΕΕΑ της ΕΑΤ, μπορούν να εξασφαλίσουν ένα επαρκές επίπεδο ανεξαρτησίας μεταξύ του ΤΠΕ και των τμημάτων ανεξάρτητου ελέγχου και εσωτερικού ελέγχου, δεδομένου του μεγέθους και του προφίλ κινδύνων ΤΠΕ του ιδρύματος.

2.5 Σύνοψη διαπιστώσεων

33. Τα αποτελέσματα αυτά θα πρέπει να αποτυπώνονται στην σύνοψη διαπιστώσεων σύμφωνα με τον τίτλο 5 των κατευθυντήριων γραμμών ΔΕΕΑ της ΕΑΤ και να αποτελούν μέρος της αντίστοιχης βαθμολογίας σύμφωνα με τα ζητήματα που τίθενται στον πίνακα 3 των κατευθυντήριων γραμμών ΔΕΕΑ της ΕΑΤ.

34. Για την αξιολόγηση της στρατηγικής ΤΠΕ, θα πρέπει να λαμβάνονται υπόψη τα ακόλουθα σημεία κατά την ολοκλήρωση της ανωτέρω αξιολόγησης:

    α. εάν οι αρμόδιες αρχές καταλήξουν στο συμπέρασμα ότι το πλαίσιο διακυβέρνησης του ιδρύματος είναι ανεπαρκές για την ανάπτυξη και την εφαρμογή της στρατηγικής ΤΠΕ του ιδρύματος σύμφωνα με το τμήμα 2.2, το συμπέρασμα αυτό θα πρέπει να λαμβάνεται υπόψη στην αξιολόγηση της εσωτερικής διακυβέρνησης του ιδρύματος που πραγματοποιείται βάσει του τίτλου 5 των κατευθυντήριων γραμμών ΔΕΕΑ της ΕΑΤ σύμφωνα με το σημείο 87 στοιχείο α)·

    β. εάν, βάσει των ανωτέρω αξιολογήσεων σύμφωνα με το τμήμα 2.2, οι αρμόδιες αρχές καταλήξουν στο συμπέρασμα ότι θα υπάρχει σημαντική απόκλιση μεταξύ της στρατηγικής ΤΠΕ και της επιχειρηματικής στρατηγικής η οποία μπορεί να έχει σημαντικές δυσμενείς επιπτώσεις στους μακροπρόθεσμους επιχειρηματικούς και/ή χρηματοοικονομικούς στόχους του ιδρύματος, στη βιωσιμότητα και/ή το επιχειρηματικό μοντέλο του ιδρύματος ή στους επιχειρηματικούς τομείς/κλάδους του ιδρύματος που έχουν προσδιοριστεί ως οι πλέον ουσιώδεις σύμφωνα με το σημείο 62 στοιχείο α) των κατευθυντήριων γραμμών ΔΕΕΑ της ΕΑΤ, το συμπέρασμα αυτό θα πρέπει να λαμβάνεται υπόψη στην αξιολόγηση του επιχειρηματικού μοντέλου βάσει του τίτλου 4 των κατευθυντήριων γραμμών ΔΕΕΑ σύμφωνα με το σημείο 70 στοιχεία β) και γ)· και

    γ. εάν, βάσει των ανωτέρω αξιολογήσεων σύμφωνα με το τμήμα 2.2, οι αρμόδιες αρχές καταλήξουν στο συμπέρασμα ότι το ίδρυμα μπορεί να μην διαθέτει επαρκείς πόρους ΤΠΕ και ικανότητες εφαρμογής ΤΠΕ για την πραγματοποίηση και την υποστήριξη σημαντικών σχεδιαζόμενων στρατηγικών αλλαγών, το συμπέρασμα αυτό θα πρέπει να λαμβάνεται υπόψη στην αξιολόγηση του επιχειρηματικού μοντέλου βάσει του τίτλου 4 των κατευθυντήριων γραμμών ΔΕΕΑ της ΕΑΤ σύμφωνα με το σημείο 70 στοιχείο β).

Τίτλος 3 - Αξιολόγηση της έκθεσης των ιδρυμάτων σε κινδύνους ΤΠΕ και των σχετικών ελέγχων

3.1 Γενικά ζητήματα

35. Οι αρμόδιες αρχές θα πρέπει να αξιολογήσουν εάν το ίδρυμα έχει εντοπίσει, αξιολογήσει και μετριάσει καταλλήλως τους κινδύνους ΤΠΕ που αντιμετωπίζει. Η διαδικασία αυτή θα πρέπει να αποτελεί μέρος του πλαισίου διαχείρισης επιχειρησιακών κινδύνων και να είναι σύμφωνη με την προσέγγιση που εφαρμόζεται για τον επιχειρησιακό κίνδυνο.

36. Οι αρμόδιες αρχές θα πρέπει να εντοπίσουν πρώτα τους ουσιώδεις εγγενείς κινδύνους ΤΠΕ στους οποίους εκτίθεται ή ενδέχεται να εκτεθεί το ίδρυμα και, κατόπιν, να αξιολογήσουν την αποτελεσματικότητα του πλαισίου διαχείρισης κινδύνων ΤΠΕ του ιδρύματος, καθώς και των διαδικασιών και των ελέγχων για τον μετριασμό αυτών των κινδύνων. Το αποτέλεσμα της αξιολόγησης θα πρέπει να αποτυπώνεται σε μια σύνοψη διαπιστώσεων η οποία χρησιμοποιείται για τη βαθμολόγηση του επιχειρησιακού κινδύνου που προβλέπεται στις κατευθυντήριες γραμμές ΔΕΕΑ. Στην περίπτωση που ο κίνδυνος ΤΠΕ θεωρείται ουσιώδης και οι αρμόδιες αρχές θέλουν να τον βαθμολογήσουν μεμονωμένα, θα πρέπει να χρησιμοποιούν τον πίνακα 1 για τη βαθμολόγησή του ως επιμέρους στοιχείο κινδύνου του επιχειρησιακού κινδύνου.

37. Κατά τη διεξαγωγή της αξιολόγησης σύμφωνα με τον παρόντα τίτλο, οι αρμόδιες αρχές θα πρέπει να χρησιμοποιούν όλες τις διαθέσιμες πηγές πληροφοριών που ορίζονται στην παράγραφο 127 του τίτλου 6 των κατευθυντήριων γραμμών ΔΕΕΑ της ΕΑΤ, π.χ. δραστηριότητες διαχείρισης κινδύνων του ιδρύματος, υποβολή αναφορών και αποτελέσματα, ως βάση για τον προσδιορισμό των προτεραιοτήτων που θέτουν για την εποπτική αξιολόγηση. Οι αρμόδιες αρχές θα πρέπει να χρησιμοποιούν επίσης άλλες πηγές πληροφοριών για τη διεξαγωγή αυτής της αξιολόγησης, συμπεριλαμβανομένων των ακόλουθων, εφόσον ενδείκνυται:

    α. αυτοαξιολογήσεων κινδύνων ΤΠΕ και ελέγχων [εάν παρέχονται στις πληροφορίες εσωτερικής διαδικασίας αξιολόγησης της κεφαλαιακής επάρκειας (ICAAP)]·
    β. πληροφοριών διαχείρισης σχετικά με τους κινδύνους ΤΠΕ οι οποίες έχουν υποβληθεί στο διοικητικό όργανο του ιδρύματος, π.χ. υποβολή περιοδικών αναφορών κινδύνων ΤΠΕ και αναφορών κινδύνων βάσει συγκεκριμένων συμβάντων (μεταξύ άλλων στην βάση δεδομένων επιχειρησιακών ζημιών), δεδομένα έκθεσης σε κινδύνους ΤΠΕ από το τμήμα διαχείρισης κινδύνων του ιδρύματος·
    γ. διαπιστώσεων εσωτερικών και εξωτερικών ελέγχων σχετικά με ΤΠΕ οι οποίες έχουν υποβληθεί στην ελεγκτική επιτροπή του ιδρύματος.

3.2 Προσδιορισμός ουσιωδών κινδύνων ΤΠΕ

38. Οι αρμόδιες αρχές θα πρέπει να εντοπίζουν τους ουσιώδεις κινδύνους ΤΠΕ στους οποίους εκτίθεται ή ενδέχεται να εκτίθεται το ίδρυμα ακολουθώντας τα παρακάτω βήματα.

3.2.1 Επανεξέταση του προφίλ κινδύνων ΤΠΕ του ιδρύματος

39. Κατά την επανεξέταση του προφίλ κινδύνων ΤΠΕ του ιδρύματος, οι αρμόδιες αρχές θα πρέπει να λαμβάνουν υπόψη όλες τις σχετικές πληροφορίες για την έκθεση του ιδρύματος σε κινδύνους ΤΠΕ, συμπεριλαμβανομένων των πληροφοριών της παραγράφου 37 και των ουσιωδών ανεπαρκειών ή αδυναμιών που έχουν εντοπιστεί στην οργάνωση ΤΠΕ και στους ελέγχους σε επίπεδο ιδρύματος, δυνάμει του τίτλου 2 των παρόντων κατευθυντήριων γραμμών και, εφόσον ενδείκνυται, να επανεξετάζουν τις πληροφορίες αυτές κατά αναλογικό τρόπο. Στο πλαίσιο αυτής της επανεξέτασης, οι αρμόδιες αρχές θα πρέπει να λαμβάνουν υπόψη:

α. τον ενδεχόμενο αντίκτυπο μιας σημαντικής διατάραξης των συστημάτων ΤΠΕ του ιδρύματος στο χρηματοπιστωτικό σύστημα είτε σε εγχώριο είτε σε διεθνές επίπεδο·

β. εάν το ίδρυμα ενδέχεται να υπόκειται σε κινδύνους που αφορούν την ασφάλεια των ΤΠΕ ή σε κινδύνους που αφορούν τη διαθεσιμότητα και τη συνέχεια των ΤΠΕ λόγω εξάρτησης από το διαδίκτυο, εφαρμογής καινοτόμων λύσεων ΤΠΕ σε μεγάλη έκταση ή άλλων επιχειρηματικών διαύλων διανομής που ενδέχεται να το καθιστούν πιθανότερο στόχο επιθέσεων από τον κυβερνοχώρο·

γ. εάν το ίδρυμα μπορεί να είναι περισσότερο εκτεθειμένο σε κινδύνους ασφάλειας ΤΠΕ, κινδύνους διαθεσιμότητας και συνέχειας των ΤΠΕ, κινδύνους ακεραιότητας δεδομένων ΤΠΕ ή κινδύνους αλλαγών των ΤΠΕ λόγω της πολυπλοκότητας (π.χ. ως αποτέλεσμα συγχωνεύσεων ή εξαγορών) ή του παρωχημένου χαρακτήρα των συστημάτων ΤΠΕ που διαθέτει·

δ. εάν το ίδρυμα πραγματοποιεί ουσιώδεις αλλαγές στα συστήματα ΤΠΕ που διαθέτει και/ή στο τμήμα ΤΠΕ (π.χ. ως αποτέλεσμα συγχωνεύσεων, εξαγορών, εκποιήσεων ή της αντικατάστασης των βασικών συστημάτων ΤΠΕ που διαθέτει), οι οποίες δύνανται να επηρεάσουν αρνητικά τη σταθερότητα ή την ορθή λειτουργία των συστημάτων ΤΠΕ και να προκαλέσουν ουσιώδεις κινδύνους διαθεσιμότητας και συνέχειας των ΤΠΕ, κινδύνους ασφάλειας των ΤΠΕ, κινδύνους αλλαγών των ΤΠΕ ή κινδύνους ακεραιότητας δεδομένων ΤΠΕ·

ε. εάν το ίδρυμα έχει αναθέσει εξωτερικά υπηρεσίες ΤΠΕ ή συστήματα ΤΠΕ εντός ή εκτός του ομίλου και, λόγω αυτής της ενέργειας, μπορεί να εκτίθεται σε ουσιώδεις κινδύνους εξωτερικής ανάθεσης ΤΠΕ·

στ. εάν το ίδρυμα εφαρμόζει επιθετικά μέτρα μείωσης του κόστους των ΤΠΕ τα οποία δύνανται να επιφέρουν μείωση των απαιτούμενων επενδύσεων σε ΤΠΕ, πόρων ΤΠΕ και τεχνογνωσίας στον τομέα της πληροφορικής και να αυξήσουν την έκθεση σε όλους τους τύπους κινδύνων ΤΠΕ στην ταξινόμηση·

ζ. εάν η τοποθεσία σημαντικών δραστηριοτήτων/ μηχανογραφικών κέντρων ΤΠΕ (π.χ. περιφέρειες, χώρες) δύναται να εκθέτει το ίδρυμα σε φυσικές καταστροφές (π.χ. πλημμύρες, σεισμούς), πολιτική αστάθεια ή εργασιακές διαμάχες και πολιτικές αναταραχές

οι οποίες μπορεί να επιφέρουν ουσιαστική αύξηση των κινδύνων διαθεσιμότητας και συνέχειας των ΤΠΕ και των κινδύνων ασφάλειας των ΤΠΕ.

3.2.2 Επανεξέταση των κρίσιμων συστημάτων και υπηρεσιών ΤΠΕ

40. Στο πλαίσιο της διαδικασίας εντοπισμού των κινδύνων ΤΠΕ, οι οποίοι ενδέχεται να έχουν ουσιώδη αρνητικό αντίκτυπο στο ίδρυμα από πλευράς προληπτικής εποπτείας, οι αρμόδιες αρχές θα πρέπει να εξετάζουν έγγραφα τεκμηρίωσης από το ίδρυμα και να διαμορφώνουν γνώμη σχετικά με τα συστήματα και τις υπηρεσίες ΤΠΕ που είναι κρίσιμες για την επαρκή λειτουργία, διαθεσιμότητα, συνέχεια και ασφάλεια των ουσιαστικών δραστηριοτήτων του ιδρύματος.

41. Για τον σκοπό αυτό, οι αρμόδιες αρχές θα πρέπει να επανεξετάζουν τη μεθοδολογία και τις διαδικασίες που εφαρμόζει το ίδρυμα για τον εντοπισμό των συστημάτων και των υπηρεσιών ΤΠΕ που είναι κρίσιμης σημασίας, λαμβάνοντας υπόψη ότι ορισμένα συστήματα και υπηρεσίες ΤΠΕ μπορεί να θεωρούνται κρίσιμα από το ίδρυμα από άποψη επιχειρηματικής συνέχειας και διαθεσιμότητας, ασφάλειας (π.χ. πρόληψη απάτης) και/ή εμπιστευτικότητας (εμπιστευτικά δεδομένα). Κατά τη διενέργεια της επανεξέτασης, οι αρμόδιες αρχές θα πρέπει να διενεργούν την επανεξέτασή τους λαμβάνοντας υπόψη ότι τα κρίσιμα συστήματα και οι κρίσιμες υπηρεσίες ΤΠΕ θα πρέπει να πληρούν τουλάχιστον μία από τις ακόλουθες προϋποθέσεις:

α. να υποστηρίζουν τις βασικές επιχειρηματικές λειτουργίες και διαύλους διανομής (π.χ. ΑΤΜ, δικτυοτραπεζική και τραπεζικές συναλλαγές μέσω κινητού τηλεφώνου) του ιδρύματος·

β. να υποστηρίζουν βασικές διαδικασίες διακυβέρνησης και εταιρικά τμήματα, συμπεριλαμβανομένης της διαχείρισης κινδύνων (π.χ. συστήματα διαχείρισης κινδύνων και ταμειακής διαχείρισης)·

γ. να πληρούν ειδικές νομικές και κανονιστικές απαιτήσεις (εάν υπάρχουν) οι οποίες επιβάλλουν αυστηρότερες απαιτήσεις διαθεσιμότητας, ανθεκτικότητας, εμπιστευτικότητας ή ασφάλειας (π.χ. νομοθεσία προστασίας δεδομένων ή πιθανοί «στόχοι χρόνου ανάκτησης» (RTO, ο μέγιστος χρόνος εντός του οποίου ένα σύστημα ή μια διαδικασία πρέπει να αποκατασταθεί κατόπιν ενός συμβάντος) και «στόχος σημείου ανάκτησης» (RPO, η μέγιστη χρονική περίοδος κατά τη διάρκεια της οποίας δύνανται να απολεσθούν δεδομένα στην περίπτωση ενός συμβάντος) για ορισμένες συστημικά σημαντικές υπηρεσίες (εάν και εφόσον προβλέπονται)·

δ. να επεξεργάζονται ή αποθηκεύουν εμπιστευτικά ή ευαίσθητα δεδομένα στα οποία τυχόν μη εξουσιοδοτημένη πρόσβαση θα μπορούσε να επηρεάσει σημαντικά τη φήμη, τα οικονομικά αποτελέσματα του ιδρύματος ή την ευρωστία και τη συνέχιση των δραστηριοτήτων του (π.χ. βάσεις δεδομένων με ευαίσθητα δεδομένα πελατών) και/ή

ε. να παρέχουν βασικές λειτουργίες οι οποίες είναι ζωτικής σημασίας για την επαρκή λειτουργία του ιδρύματος (π.χ. υπηρεσίες τηλεπικοινωνιών και συνδεσιμότητας, υπηρεσίες ΤΠΕ και ασφάλειας στον κυβερνοχώρο).

3.2.3 Προσδιορισμός ουσιωδών κινδύνων ΤΠΕ για κρίσιμα συστήματα και υπηρεσίες ΤΠΕ

42. Λαμβάνοντας υπόψη την εξέταση του προφίλ κινδύνων ΤΠΕ και των κρίσιμων συστημάτων και υπηρεσιών ΤΠΕ του ιδρύματος που αναφέρθηκε ανωτέρω, οι αρμόδιες αρχές θα πρέπει να

διαμορφώσουν άποψη σχετικά με τους ουσιώδεις κινδύνους ΤΠΕ που, κατά την εποπτική κρίση τους, μπορεί να έχουν σημαντικές επιπτώσεις από πλευράς προληπτικής εποπτείας στα κρίσιμα συστήματα και τις κρίσιμες υπηρεσίες ΤΠΕ του ιδρύματος.

43. Κατά την αξιολόγηση του δυνητικού αντίκτυπου των κινδύνων ΤΠΕ στα κρίσιμα συστήματα και τις κρίσιμες υπηρεσίες ΤΠΕ ενός ιδρύματος, οι αρμόδιες αρχές θα πρέπει να εξετάζουν:

   α. τον οικονομικό αντίκτυπο, συμπεριλαμβανομένης (ενδεικτικά) της απώλειας κεφαλαίων ή περιουσιακών στοιχείων, της ενδεχόμενης αποζημίωσης πελατών, των νομικών εξόδων και εξόδων αποκατάστασης, της συμβατικής αποζημίωσης, των απολεσθέντων εσόδων·

   β. το ενδεχόμενο διατάραξης της δραστηριότητας, λαμβάνοντας υπόψη (ενδεικτικά) την κρισιμότητα των χρηματοοικονομικών υπηρεσιών που επηρεάζονται· τον αριθμό των πελατών και/ή κλάδων και των εργαζομένων που ενδεχομένως επηρεάζονται·

   γ. τον δυνητικό αντίκτυπο στη φήμη του ιδρύματος βάσει της κρισιμότητας της τραπεζικής υπηρεσίας ή της επιχειρησιακής δραστηριότητας που επηρεάζεται (π.χ. κλοπή δεδομένων πελατών)· του εξωτερικού προφίλ/της προβολής των συστημάτων και των υπηρεσιών ΤΠΕ που επηρεάζονται (π.χ. συστήματα τραπεζικής μέσω κινητού τηλεφώνου ή ηλεκτρονικής τραπεζικής, σημείο πώλησης, ΑΤΜ ή συστήματα πληρωμών)·

   δ. τον κανονιστικό αντίκτυπο, συμπεριλαμβανομένου του ενδεχομένου δημόσιας επίπληξης από τη ρυθμιστική αρχή, επιβολής προστίμων ή ακόμα και μεταβολής των αδειών·

   ε. τον στρατηγικό αντίκτυπο στο ίδρυμα, για παράδειγμα εάν τίθενται σε κίνδυνο ή έχουν κλαπεί στρατηγικά σχέδια για προϊόντα ή επιχειρηματικά σχέδια.

44. Στη συνέχεια, οι αρμόδιες αρχές θα πρέπει να καταγράφουν τους κινδύνους ΤΠΕ που προσδιορίστηκαν και που θεωρούνται ουσιώδεις στις ακόλουθες κατηγορίες κινδύνων ΤΠΕ, για τις οποίες επιπρόσθετες περιγραφές και παραδείγματα κινδύνων παρέχονται στο παράρτημα. Οι αρμόδιες αρχές θα πρέπει να μελετούν τους κινδύνους ΤΠΕ που αναφέρονται στο παράρτημα στο πλαίσιο της αξιολόγησης δυνάμει του τίτλου 3:

   α. Κίνδυνος διαθεσιμότητας και συνέχειας των ΤΠΕ
   β. Κίνδυνος ασφάλειας των ΤΠΕ
   γ. Κίνδυνος αλλαγών των ΤΠΕ
   δ. Κίνδυνος ακεραιότητας δεδομένων ΤΠΕ
   ε. Κίνδυνος εξωτερικής ανάθεσης ΤΠΕ

   Η καταγραφή βοηθά τις αρμόδιες αρχές να προσδιορίζουν τους κινδύνους που είναι ουσιώδεις (εάν υπάρχουν) και, επομένως, που θα πρέπει να υποβληθούν σε στενότερη και βαθύτερη επανεξέταση κατά τα επόμενα στάδια της αξιολόγησης.

3.3 Αξιολόγηση των ελέγχων για τον μετριασμό ουσιωδών κινδύνων ΤΠΕ

45. Για την αξιολόγηση της εναπομένουσας έκθεσης του ιδρύματος σε κίνδυνο ΤΠΕ, οι αρμόδιες αρχές θα πρέπει να εξετάζουν πώς το ίδρυμα προσδιορίζει, παρακολουθεί, αξιολογεί και μετριάζει τους ουσιώδεις κινδύνους που έχουν προσδιοριστεί από τις αρμόδιες αρχές στην ανωτέρω αξιολόγηση.

46. Για τον σκοπό αυτό, οι αρμόδιες αρχές θα πρέπει να εξετάζουν, σε σχέση με τους ουσιώδεις κινδύνους ΤΠΕ που έχουν προσδιοριστεί:

    α. την εφαρμοζόμενη πολιτική διαχείρισης κινδύνων ΤΠΕ, τις σχετικές διαδικασίες και τα όρια ανοχής του κινδύνου·

    β. το εφαρμοζόμενο πλαίσιο οργανωτικής διαχείρισης και εποπτείας·

    γ. το εφαρμοζόμενο πεδίο κάλυψης εσωτερικού ελέγχου και τις σχετικές διαπιστώσεις· και

    δ. τους εφαρμοζόμενους ελέγχους κινδύνων ΤΠΕ που αφορούν συγκεκριμένα τον ουσιώδη κίνδυνο ΤΠΕ που προσδιορίστηκε.

47. Η αξιολόγηση θα πρέπει να λαμβάνει υπόψη το αποτέλεσμα της ανάλυσης του συνολικού πλαισίου διαχείρισης κινδύνων και εσωτερικού ελέγχου που αναφέρεται στον τίτλο 5 των κατευθυντήριων γραμμών ΔΕΕΑ της ΕΑΤ, καθώς και τη διακυβέρνηση και τη στρατηγική του ιδρύματος που αναφέρονται στον τίτλο 2 των κατευθυντήριων γραμμών, καθώς τυχόν σημαντικές ανεπάρκειες σε αυτούς τους τομείς δύνανται να επηρεάζουν σημαντικά την ικανότητα του ιδρύματος να διαχειρίζεται και να μετριάζει την έκθεσή του σε κίνδυνο ΤΠΕ. Εφόσον ενδείκνυται, οι αρμόδιες αρχές θα πρέπει να χρησιμοποιούν επίσης τις πηγές πληροφοριών που αναφέρονται στο σημείο 37 των κατευθυντήριων γραμμών.

48. Οι αρμόδιες αρχές θα πρέπει να πραγματοποιούν τα ακόλουθα βήματα αξιολόγησης κατά τρόπο ανάλογο προς τη φύση, την κλίμακα και την πολυπλοκότητα των δραστηριοτήτων του ιδρύματος και με την εφαρμογή κατάλληλου εποπτικού ελέγχου με βάση το προφίλ κινδύνων ΤΠΕ του ιδρύματος.

3.3.1 Πολιτική διαχείρισης κινδύνων ΤΠΕ, διαδικασίες και όρια ανοχής

49. Οι αρμόδιες αρχές θα πρέπει να εξετάζουν εάν το ίδρυμα διαθέτει κατάλληλες πολιτικές και διαδικασίες διαχείρισης κινδύνων, καθώς και σχετικά όρια ανοχής, για τους ουσιώδεις κινδύνους ΤΠΕ που έχουν προσδιοριστεί. Τα στοιχεία αυτά μπορεί να αποτελούν μέρος του πλαισίου διαχείρισης επιχειρησιακών κινδύνων ή χωριστό έγγραφο. Για την αξιολόγηση αυτή, οι αρμόδιες αρχές θα πρέπει να λαμβάνουν υπόψη εάν:

    α. η πολιτική διαχείρισης κινδύνων είναι επισημοποιημένη και εγκεκριμένη από το διοικητικό όργανο και περιέχει επαρκή καθοδήγηση σχετικά με τη διάθεση του ιδρύματος να αναλαμβάνει κινδύνους ΤΠΕ και σχετικά με τους κύριους επιδιωκόμενους στόχους διαχείρισης κινδύνων ΤΠΕ και/ή τα εφαρμοζόμενα όρια ανοχής των κινδύνων ΤΠΕ. Η σχετική πολιτική διαχείρισης κινδύνων ΤΠΕ θα πρέπει επίσης να έχει κοινοποιηθεί σε όλα τα σχετικά ενδιαφερόμενα μέρη·

β. η εφαρμοστέα πολιτική καλύπτει όλα τα σημαντικά στοιχεία διαχείρισης κινδύνου για τους ουσιώδεις κινδύνους ΤΠΕ που έχουν προσδιοριστεί·

γ. το ίδρυμα εφαρμόζει μια διεργασία και βασικές διαδικασίες για τον προσδιορισμό [π.χ. αυτοαξιολογήσεις ελέγχου κινδύνων (RSCA), ανάλυση σεναρίων κινδύνου) και την παρακολούθηση των σχετικών ουσιωδών κινδύνων ΤΠΕ· και

δ. το ίδρυμα εφαρμόζει διαδικασία υποβολής αναφορών διαχείρισης κινδύνων ΤΠΕ η οποία παρέχει εγκαίρως πληροφορίες στα ανώτατα διοικητικά στελέχη και το διοικητικό όργανο και η οποία επιτρέπει στα ανώτατα διοικητικά στελέχη και/ή το διοικητικό όργανο να αξιολογούν και να παρακολουθούν εάν τα σχέδια και τα μέτρα μετριασμού των κινδύνων ΤΠΕ συνάδουν με την εγκεκριμένη διάθεση για ανάληψη κινδύνων και/ή τα εγκεκριμένα όρια ανοχής (κατά περίπτωση), καθώς και να παρακολουθούν τυχόν αλλαγές στους ουσιώδεις κινδύνους ΤΠΕ.

3.3.2 Πλαίσιο οργανωτικής διαχείρισης και εποπτείας

50. Οι αρμόδιες αρχές θα πρέπει να αξιολογούν πώς ενσωματώνονται στην εσωτερική οργάνωση οι εφαρμοζόμενοι ρόλοι και αρμοδιότητες διαχείρισης κινδύνου για τη διαχείριση και την εποπτεία των ουσιωδών κινδύνων ΤΠΕ που έχουν προσδιοριστεί. Από την άποψη αυτή, οι αρμόδιες αρχές θα πρέπει να αξιολογούν εάν το ίδρυμα αποδεικνύει:

α. σαφείς ρόλους και αρμοδιότητες για τον προσδιορισμό, την αξιολόγηση, την παρακολούθηση, τον μετριασμό, την υποβολή αναφορών και την εποπτεία των σχετικών ουσιωδών κινδύνων ΤΠΕ·

β. ότι οι αρμοδιότητες και οι ρόλοι που αφορούν τους κινδύνους έχουν κοινοποιηθεί, κατανεμηθεί και ενσωματωθεί σαφώς σε όλα τα σχετικά μέρη (π.χ. τομείς επιχειρηματικής δραστηριότητας, τμήμα πληροφορικής) και τις διαδικασίες του οργανισμού, συμπεριλαμβανομένων των ρόλων και των αρμοδιοτήτων για τη συλλογή και τον συνυπολογισμό των πληροφοριών κινδύνου και την υποβολή σχετικών αναφορών στα ανώτατα διοικητικά στελέχη και/ή το διοικητικό όργανο·

γ. ότι οι δραστηριότητες διαχείρισης κινδύνων ΤΠΕ εκτελούνται με επαρκείς και ποιοτικά κατάλληλους ανθρώπινους και τεχνικούς πόρους. Για να αξιολογηθεί η αξιοπιστία των εφαρμοστέων σχεδίων μετριασμού του κινδύνου, οι αρμόδιες αρχές θα πρέπει να αξιολογούν επίσης εάν το ίδρυμα έχει κατανείμει επαρκείς οικονομικούς προϋπολογισμούς και/ή άλλους απαιτούμενους πόρους για την εφαρμογή τους·

δ. κατάλληλη παρακολούθηση και αντίδραση του διοικητικού οργάνου όσον αφορά σημαντικές διαπιστώσεις των τμημάτων ανεξάρτητου ελέγχου σχετικά με τον κίνδυνο (τους κινδύνους) ΤΠΕ, λαμβάνοντας υπόψη την πιθανή ανάθεση ορισμένων ζητημάτων σε επιτροπή, εφόσον υφίσταται· και

ε. ότι οι εξαιρέσεις από τους ισχύοντες κανονισμούς και τις ισχύουσες πολιτικές ΤΠΕ καταγράφονται και υπόκεινται σε τεκμηριωμένο έλεγχο και υποβολή αναφορών από το τμήμα ανεξάρτητου ελέγχου, με ιδιαίτερη έμφαση στους σχετικούς κινδύνους.

3.3.3 Καλυπτόμενο πεδίο και διαπιστώσεις εσωτερικού ελέγχου

51. Οι αρμόδιες αρχές θα πρέπει να εξετάζουν εάν το τμήμα εσωτερικού ελέγχου είναι αποτελεσματικό όσον αφορά τον έλεγχο του εφαρμοζόμενου πλαισίου ελέγχου κινδύνων ΤΠΕ, ελέγχοντας εάν:

    α. ο έλεγχος του πλαισίου ελέγχου κινδύνων ΤΠΕ διενεργείται με την απαιτούμενη ποιότητα, συχνότητα και βάθος και είναι ανάλογος του μεγέθους, των δραστηριοτήτων και του προφίλ κινδύνου ΤΠΕ του ιδρύματος·

    β. το πλάνο ελέγχων περιλαμβάνει ελέγχους των κρίσιμων κινδύνων ΤΠΕ που έχουν προσδιοριστεί από το ίδρυμα·

    γ. οι σημαντικές διαπιστώσεις του ελέγχου ΤΠΕ, συμπεριλαμβανομένων των δράσεων που έχουν συμφωνηθεί, αναφέρονται στο διοικητικό όργανο· και

    δ. οι διαπιστώσεις του ελέγχου ΤΠΕ, συμπεριλαμβανομένων των δράσεων που έχουν συμφωνηθεί, παρακολουθούνται και οι εκθέσεις προόδου επανεξετάζονται περιοδικά από τα ανώτατα διοικητικά στελέχη και/ή την ελεγκτική επιτροπή.

3.3.4 Έλεγχοι κινδύνων ΤΠΕ που αφορούν συγκεκριμένα τους προσδιορισμένους ουσιώδεις κινδύνους ΤΠΕ

52. Για τους προσδιορισμένους ουσιώδεις κινδύνους ΤΠΕ, οι αρμόδιες αρχές θα πρέπει να αξιολογούν εάν το ίδρυμα εφαρμόζει ειδικούς ελέγχους για την αντιμετώπιση αυτών των κινδύνων. Στα ακόλουθα τμήματα παρατίθεται μη εξαντλητικός κατάλογος των ειδικών ελέγχων που πρέπει να λαμβάνονται υπόψη κατά την αξιολόγηση των ουσιωδών κινδύνων που έχουν προσδιοριστεί σύμφωνα με το σημείο 3.2.3 και που καταγράφηκαν στις ακόλουθες κατηγορίες κινδύνων ΤΠΕ:

    α. κίνδυνοι διαθεσιμότητας και συνέχειας των ΤΠΕ·
    β. κίνδυνοι ασφάλειας των ΤΠΕ·
    γ. κίνδυνοι αλλαγών των ΤΠΕ·
    δ. κίνδυνοι ακεραιότητας δεδομένων ΤΠΕ·
    ε. κίνδυνοι εξωτερικής ανάθεσης ΤΠΕ.

(α) Έλεγχοι για τη διαχείριση ουσιωδών κινδύνων διαθεσιμότητας και συνέχειας των ΤΠΕ

53. Εκτός των απαιτήσεων που ορίζονται στις κατευθυντήριες γραμμές ΔΕΕΑ της ΕΑΤ (σημεία 279-281), οι αρμόδιες αρχές θα πρέπει να αξιολογούν εάν το ίδρυμα εφαρμόζει κατάλληλο πλαίσιο για τον προσδιορισμό, την κατανόηση, τη μέτρηση και τον μετριασμό των κινδύνων διαθεσιμότητας και συνέχειας των ΤΠΕ.

54. Για την εν λόγω αξιολόγηση, οι αρμόδιες αρχές θα πρέπει να λαμβάνουν υπόψη ιδιαιτέρως εάν το πλαίσιο:

    α. προσδιορίζει τις κρίσιμες διαδικασίες ΤΠΕ και τα σχετικά υποστηρικτικά συστήματα ΤΠΕ που θα πρέπει να αποτελούν μέρος των σχεδίων ανθεκτικότητας και συνέχειας των δραστηριοτήτων με:

        i. ολοκληρωμένη ανάλυση των αλληλεξαρτήσεων μεταξύ των κρίσιμων επιχειρηματικών διαδικασιών και των υποστηρικτικών προγραμμάτων·

ii. προσδιορισμό των στόχων ανάκτησης για τα υποστηρικτικά συστήματα ΤΠΕ (π.χ. που καθορίζονται συνήθως από την επιχείρηση και/ή τους κανονισμούς από πλευράς στόχων χρόνου ανάκτησης (RTO) και στόχων σημείου ανάκτησης (RPO)·

iii. κατάλληλο σχεδιασμό έκτακτης ανάγκης ώστε να εξασφαλίζεται η διαθεσιμότητα, η συνέχεια και η ανάκτηση κρίσιμων συστημάτων και υπηρεσιών ΤΠΕ για την ελαχιστοποίηση της διατάραξης των δραστηριοτήτων ενός ιδρύματος εντός αποδεκτών ορίων.

β. διαθέτει πολιτικές και πρότυπα περιβάλλοντος ελέγχου της ανθεκτικότητας και της συνέχειας των δραστηριοτήτων, καθώς και επιχειρησιακούς ελέγχους οι οποίοι περιλαμβάνουν:

i. μέτρα ώστε να αποφεύγεται η πιθανότητα ένα μεμονωμένο σενάριο, συμβάν ή μια μεμονωμένη καταστροφή να έχει επιπτώσεις στα συστήματα παραγωγής και ανάκτησης ΤΠΕ·

ii. διαδικασίες δημιουργίας αντιγράφων ασφαλείας και ανάκτησης συστήματος ΤΠΕ για κρίσιμο λογισμικό και κρίσιμα δεδομένα, οι οποίες εξασφαλίζουν ότι αυτά τα αντίγραφα ασφαλείας αποθηκεύονται σε μια ασφαλή και επαρκώς απομακρυσμένη τοποθεσία, ώστε ένα συμβάν ή μια καταστροφή να μην μπορεί να καταστρέψει ή να αλλοιώσει αυτά τα κρίσιμα δεδομένα·

iii. λύσεις παρακολούθησης για τον έγκαιρο εντοπισμό συμβάντων που αφορούν τη διαθεσιμότητα ή τη συνέχεια των ΤΠΕ·

iv. τεκμηριωμένη διαδικασία διαχείρισης και κλιμάκωσης συμβάντων, η οποία παρέχει επίσης καθοδήγηση σχετικά με τους διάφορους ρόλους και τις διάφορες αρμοδιότητες διαχείρισης και κλιμάκωσης συμβάντων, τα μέλη της επιτροπής (των επιτροπών) διαχείρισης κρίσεων και την ιεραρχική δομή στην περίπτωση έκτακτης ανάγκης·

v. φυσικά μέτρα για την προστασία της κρίσιμης υποδομής ΤΠΕ του ιδρύματος (π.χ. μηχανογραφικά κέντρα) από περιβαλλοντικούς κινδύνους (π.χ. πλημμύρες και άλλες φυσικές καταστροφές) και την εξασφάλιση κατάλληλου περιβάλλοντος λειτουργίας για τα συστήματα ΤΠΕ (π.χ. κλιματισμός)·

vi. διαδικασίες, ρόλους και αρμοδιότητες για να εξασφαλίζεται επίσης ότι τα συστήματα και οι υπηρεσίες ΤΠΕ που ανατίθενται σε τρίτους καλύπτονται από επαρκείς λύσεις και επαρκή σχέδια ανθεκτικότητας και συνέχειας των δραστηριοτήτων·

vii. σχεδιασμό επιδόσεων και ικανοτήτων ΤΠΕ και λύσεις παρακολούθησης για κρίσιμα συστήματα και υπηρεσίες ΤΠΕ με καθορισμένες απαιτήσεις διαθεσιμότητας για τον έγκαιρο εντοπισμό σημαντικών περιορισμών στις επιδόσεις και τις ικανότητες·

viii. λύσεις για την προστασία κρίσιμων δραστηριοτήτων ή υπηρεσιών στο διαδίκτυο (π.χ. υπηρεσιών ηλεκτρονικής τραπεζικής), όπου είναι απαραίτητο και ενδείκνυται, έναντι επιθέσεων «άρνησης υπηρεσίας» και άλλων επιθέσεων στον κυβερνοχώρο οι οποίες έχουν στόχο την παρεμπόδιση ή τη διατάραξη της πρόσβασης στις εν λόγω δραστηριότητες και υπηρεσίες.

γ. υποβάλλει σε δοκιμές τις λύσεις διαθεσιμότητας και συνέχειας ΤΠΕ με βάση μια σειρά ρεαλιστικών σεναρίων, συμπεριλαμβανομένων επιθέσεων στον κυβερνοχώρο, δοκιμών

αυτόματης μεταγωγής σε εφεδρεία και δοκιμών δημιουργίας αντιγράφων ασφαλείας για κρίσιμο λογισμικό και δεδομένα, οι οποίες:

i. είναι σχεδιασμένες, επισημοποιημένες και τεκμηριωμένες και τα αποτελέσματα των δοκιμών χρησιμοποιούνται για την ενίσχυση της αποτελεσματικότητας των λύσεων διαθεσιμότητας και συνέχειας των ΤΠΕ·

ii. περιλαμβάνουν ενδιαφερόμενα μέρη και λειτουργίες εντός του οργανισμού, όπως διαχείριση των τομέων επιχειρηματικής δραστηριότητας, συμπεριλαμβανομένων των ομάδων συνέχειας των δραστηριοτήτων, αντιμετώπισης συμβάντων και κρίσεων, καθώς και σχετικά εξωτερικά ενδιαφερόμενα μέρη του οικοσυστήματος·

iii. το διοικητικό όργανο και τα ανώτατα διοικητικά στελέχη συμμετέχουν κατάλληλα (π.χ. στο πλαίσιο ομάδων διαχείρισης κρίσεων) και ενημερώνονται σχετικά με τα αποτελέσματα των δοκιμών.

(β) Έλεγχοι για τη διαχείριση ουσιωδών κινδύνων ασφάλειας των ΤΠΕ

55. Οι αρμόδιες αρχές θα πρέπει να αξιολογούν εάν το ίδρυμα διαθέτει αποτελεσματικό πλαίσιο για τον προσδιορισμό, την κατανόηση, τη μέτρηση και τον μετριασμό του κινδύνου ασφάλειας των ΤΠΕ. Για την εν λόγω αξιολόγηση, οι αρμόδιες αρχές θα πρέπει να λαμβάνουν υπόψη ιδιαιτέρως εάν το πλαίσιο λαμβάνει υπόψη:

α. σαφώς καθορισμένους ρόλους και αρμοδιότητες σχετικά με:

i. το πρόσωπο (τα πρόσωπα) και/ή τις επιτροπές που είναι υπεύθυνες και/ή υπόλογες για την καθημερινή διαχείριση της ασφάλειας των ΤΠΕ και την εκπόνηση των πρωταρχικών πολιτικών ασφάλειας των ΤΠΕ, με ιδιαίτερη προσοχή στην απαιτούμενη ανεξαρτησία τους·

ii. τον σχεδιασμό, την εφαρμογή, τη διαχείριση και την παρακολούθηση των ελέγχων ασφάλειας ΤΠΕ·

iii. την προστασία κρίσιμων συστημάτων και υπηρεσιών ΤΠΕ μέσω της υιοθέτησης, για παράδειγμα, μιας διαδικασίας αξιολόγησης της τρωτότητας, διαχείρισης πρόχειρων διορθώσεων (patch) λογισμικού, προστασίας τελικού σημείου (π.χ. από ιούς κακόβουλου λογισμικού), εργαλείων εντοπισμού και πρόληψης εισβολών·

iv. την παρακολούθηση, την ταξινόμηση και τον χειρισμό εξωτερικών ή εσωτερικών συμβάσεων ασφάλειας ΤΠΕ· συμπεριλαμβανομένης της αντιμετώπισης συμβάντων και της συνέχισης και ανάκτησης συστημάτων και υπηρεσιών ΤΠΕ·

v. τακτικές και προληπτικές αξιολογήσεις απειλών για τη διατήρηση κατάλληλων ελέγχων ασφάλειας.

β. μια πολιτική για την ασφάλεια των ΤΠΕ η οποία λαμβάνει υπόψη και, κατά περίπτωση, συμμορφώνεται με διεθνώς αναγνωρισμένα πρότυπα ασφάλειας και αρχές ασφάλειας ΤΠΕ (π.χ. την «αρχή του ελάχιστου προνομίου», δηλαδή τον περιορισμό της πρόσβασης σε ένα ελάχιστο επίπεδο το οποίο επιτρέπει την κανονική λειτουργία για διαχείριση δικαιωμάτων πρόσβασης, και την αρχή της «άμυνας σε βάθος», δηλαδή πολυεπίπεδους μηχανισμούς ασφάλειας οι οποίοι

αυξάνουν την ασφάλεια του συστήματος συνολικά για τον σχεδιασμό μιας αρχιτεκτονικής ασφάλειας)·

γ. διαδικασία για τον εντοπισμό συστημάτων, υπηρεσιών ΤΠΕ και ανάλογων απαιτήσεων ασφάλειας που αποτυπώνουν ενδεχόμενο κίνδυνο απάτης και/ή πιθανές εσφαλμένες χρήσεις και/ή καταχρήσεις εμπιστευτικών δεδομένων, καθώς και τεκμηριωμένες προσδοκίες ασφάλειας που πρέπει να τηρούνται για τα εν λόγω εντοπισμένα συστήματα, υπηρεσίες και δεδομένα ΤΠΕ, οι οποίες είναι σύμφωνες με την ανοχή κινδύνου του ιδρύματος και η ορθή εφαρμογή των οποίων παρακολουθείται·

δ. τεκμηριωμένη διαδικασία διαχείρισης και κλιμάκωσης συμβάντων ασφάλειας η οποία παρέχει καθοδήγηση σχετικά με τους διάφορους ρόλους και τις διάφορες αρμοδιότητες διαχείρισης και κλιμάκωσης συμβάντων, τα μέλη της επιτροπής (των επιτροπών) διαχείρισης κρίσεων και την ιεραρχική δομή στην περίπτωση περιστατικών έκτακτης ανάγκης ασφάλειας·

ε. τήρηση αρχείων ημερολογίου των δραστηριοτήτων χρηστών και διαχειριστών, ώστε να εξασφαλίζεται η αποτελεσματική παρακολούθηση, ο έγκαιρος εντοπισμός και η αντιμετώπιση μη εξουσιοδοτημένων δραστηριοτήτων και για να υποστηρίζονται ή να διενεργούνται εγκληματολογικές έρευνες για συμβάντα ασφάλειας. Το ίδρυμα θα πρέπει να εφαρμόζει πολιτικές τήρησης αρχείων ημερολογίου οι οποίες καθορίζουν κατάλληλους τύπους αρχείων ημερολογίου που πρέπει να τηρούνται και την περίοδο διατήρησής τους·

στ. εκστρατείες ευαισθητοποίησης και ενημέρωσης ή πρωτοβουλίες για την ενημέρωση όλων των επιπέδων του ιδρύματος σχετικά με την ασφαλή χρήση και την προστασία των συστημάτων ΤΠΕ του ιδρύματος και τους κύριους κινδύνους ασφάλειας ΤΠΕ (ή άλλους κινδύνους) που θα πρέπει να γνωρίζουν, ιδίως όσον αφορά τις υπάρχουσες και εξελισσόμενες απειλές στον κυβερνοχώρο (π.χ. ιούς υπολογιστών, πιθανές εσωτερικές ή εξωτερικές καταχρήσεις ή επιθέσεις, κυβερνοεπιθέσεις) και τον ρόλο τους στον μετριασμό των παραβιάσεων της ασφάλειας·

ζ. κατάλληλα μέτρα φυσικής ασφάλειας (π.χ. κλειστό κύκλωμα τηλεόρασης, αντικλεπτικός συναγερμός, πόρτες ασφαλείας) για την πρόληψη της μη εξουσιοδοτημένης φυσικής πρόσβασης σε κρίσιμα και ευαίσθητα συστήματα ΤΠΕ (π.χ. μηχανογραφικά κέντρα)·

η. μέτρα για την προστασία των συστημάτων ΤΠΕ από επιθέσεις από το διαδίκτυο (π.χ. κυβερνοεπιθέσεις) ή άλλα εξωτερικά δίκτυα (π.χ. παραδοσιακές συνδέσεις τηλεπικοινωνιών ή συνδέσεις με έμπιστους συνεργάτες). Οι αρμόδιες αρχές θα πρέπει να εξετάζουν εάν το πλαίσιο του ιδρύματος λαμβάνει υπόψη:

   i. διαδικασία και λύσεις για τη διατήρηση ενός ολοκληρωμένου και επίκαιρου καταλόγου και μιας επισκόπησης όλων των εξωτερικών σημείων σύνδεσης δικτύου (π.χ. δικτυακών τόπων, εφαρμογών διαδικτύου, ασύρματων δικτύων, πρόσβασης εξ αποστάσεως) μέσω των οποίων τρίτοι θα μπορούσαν να διεισδύσουν στα εσωτερικά συστήματα ΤΠΕ·

   ii. μέτρα ασφάλειας τα οποία τελούν υπό στενή διαχείριση και παρακολούθηση (π.χ. τείχη προστασίας, διακομιστές μεσολάβησης, αναμεταδότες ηλεκτρονικού ταχυδρομείου, προγράμματα σάρωσης για τον εντοπισμό ιών και περιεχομένου) για τη διασφάλιση της εισερχόμενης και εξερχόμενης κυκλοφορίας δικτύου (π.χ. μηνύματα ηλεκτρονικού ταχυδρομείου) και των εξωτερικών συνδέσεων δικτύου μέσω των οποίων τρίτοι θα μπορούσαν να διεισδύσουν στα εσωτερικά συστήματα ΤΠΕ·

iii. διαδικασίες και λύσεις για τη διασφάλιση δικτυακών τόπων και εφαρμογών που μπορούν να υποστούν άμεσα επιθέσεις από το διαδίκτυο και/ή εξωτερικά σημεία και που μπορούν να λειτουργήσουν ως σημείο εισόδου στα εσωτερικά συστήματα ΤΠΕ. Γενικά, πρόκειται για έναν συνδυασμό αναγνωρισμένων πρακτικών ασφαλούς ανάπτυξης, πρακτικών ενίσχυσης και σάρωσης τρωτών σημείων του συστήματος ΤΠΕ και/ή την εφαρμογή πρόσθετων λύσεων ασφάλειας, όπως, για παράδειγμα, τειχών προστασίας εφαρμογών και/ή συστημάτων ανίχνευσης εισβολής (IDS) και/ή πρόληψης εισβολής (IPS)·

iv. περιοδικές δοκιμές διείσδυσης ασφάλειας για την αξιολόγηση της αποτελεσματικότητας των εφαρμοζόμενων μέτρων και διαδικασιών ασφάλειας των ΤΠΕ στον κυβερνοχώρο και εσωτερικής ασφάλειας. Οι δοκιμές αυτές θα πρέπει να διενεργούνται από προσωπικό και/ή εξωτερικούς εμπειρογνώμονες που διαθέτουν την απαραίτητη τεχνογνωσία και τα τεκμηριωμένα αποτελέσματα και συμπεράσματα των δοκιμών θα πρέπει να υποβάλλονται στα ανώτατα διοικητικά στελέχη και/ή το διοικητικό όργανο. Εφόσον είναι αναγκαίο και ενδείκνυται, το ίδρυμα θα πρέπει να μαθαίνει από τις εν λόγω δοκιμές ποιες περαιτέρω βελτιώσεις θα πρέπει να πραγματοποιήσει στους ελέγχους και τις διαδικασίες ασφάλειας και/ή ποιων σημείων την αποτελεσματικότητα θα πρέπει να επιβεβαιώσει καλύτερα.

(γ) Έλεγχοι για τη διαχείριση ουσιωδών κινδύνων αλλαγών των ΤΠΕ

56. Οι αρμόδιες αρχές θα πρέπει να αξιολογούν εάν το ίδρυμα εφαρμόζει αποτελεσματικό πλαίσιο για τον προσδιορισμό, την κατανόηση, τη μέτρηση και τον μετριασμό του κινδύνου αλλαγών των ΤΠΕ, ανάλογο της φύσης, της κλίμακας και της πολυπλοκότητας των δραστηριοτήτων του ιδρύματος και του προφίλ κινδύνου ΤΠΕ του ιδρύματος. Το πλαίσιο του ιδρύματος θα πρέπει να καλύπτει τους κινδύνους που σχετίζονται με την ανάπτυξη, τη δοκιμή και την έγκριση αλλαγών στα συστήματα ΤΠΕ, συμπεριλαμβανομένης της ανάπτυξης ή της αλλαγής λογισμικού, πριν από τη μεταφορά τους σε περιβάλλον παραγωγής, και να εξασφαλίζει κατάλληλη διαχείριση των κύκλου ζωής των ΤΠΕ. Για την εν λόγω αξιολόγηση, οι αρμόδιες αρχές θα πρέπει να λαμβάνουν υπόψη ιδιαιτέρως εάν το πλαίσιο λαμβάνει υπόψη:

α. τεκμηριωμένες διαδικασίες για τη διαχείριση και τον έλεγχο αλλαγών σε συστήματα ΤΠΕ (π.χ. διαμόρφωση και διαχείριση πρόχειρων διορθώσεων) και δεδομένα ΤΠΕ (π.χ. διόρθωση σφαλμάτων προγραμματισμού ή διορθώσεις δεδομένων), οι οποίες εξασφαλίζουν την επαρκή διαχείριση των κινδύνων ΤΠΕ σε περίπτωση σημαντικών αλλαγών ΤΠΕ που μπορεί να επηρεάσουν σημαντικά το προφίλ κινδύνου του ιδρύματος ή την έκθεσή του στον κίνδυνο·

β. προδιαγραφές σχετικά με τον απαιτούμενο διαχωρισμό καθηκόντων κατά τα διάφορα στάδια των εφαρμοζόμενων διαδικασιών αλλαγής των ΤΠΕ (π.χ. σχεδιασμός και ανάπτυξη λύσεων, δοκιμή και έγκριση νέου λογισμικού και/ή αλλαγών, μεταφορά και εφαρμογή στο περιβάλλον παραγωγής και διόρθωση σφαλμάτων προγραμματισμού), με έμφαση στις εφαρμοζόμενες λύσεις και τον διαχωρισμό καθηκόντων για τη διαχείριση και τον έλεγχο αλλαγών στα συστήματα και τα δεδομένα ΤΠΕ παραγωγής από το προσωπικό ΤΠΕ (π.χ. σχεδιαστές, διαχειριστές συστημάτων ΤΠΕ, διαχειριστές βάσεων δεδομένων) ή οποιοδήποτε άλλο μέρος (π.χ. επαγγελματικούς χρήστες, παρόχους υπηρεσιών)·

γ. περιβάλλοντα δοκιμής που αποτυπώνουν επαρκώς τα περιβάλλοντα παραγωγής·

δ. κατάλογο των υφιστάμενων εφαρμογών και συστημάτων ΤΠΕ στο περιβάλλον παραγωγής, καθώς και το περιβάλλον δοκιμής και ανάπτυξης, ώστε να είναι δυνατή η κατάλληλη διαχείριση, εφαρμογή και παρακολούθηση των απαιτούμενων αλλαγών (π.χ. ενημερώσεων εκδόσεων ή αναβαθμίσεων, πρόχειρων διορθώσεων συστημάτων, αλλαγών διαμόρφωσης) για τα εμπλεκόμενα συστήματα ΤΠΕ·

ε. διαδικασία παρακολούθησης και διαχείρισης του κύκλου ζωής των χρησιμοποιούμενων συστημάτων ΤΠΕ, ώστε να εξασφαλίζεται ότι εξακολουθούν να πληρούν και να υποστηρίζουν τις πραγματικές απαιτήσεις διαχείρισης δραστηριοτήτων και κινδύνων. Επίσης πρέπει να διασφαλίζεται ότι οι λύσεις και τα συστήματα ΤΠΕ που χρησιμοποιούνται εξακολουθούν να υποστηρίζονται από τους προμηθευτές τους και ότι η εν λόγω υποστήριξη συνοδεύεται από κατάλληλες διαδικασίες κύκλου ζωής ανάπτυξης λογισμικού (SDLC)·

στ. σύστημα ελέγχου του πηγαίου κώδικα λογισμικού και κατάλληλες διαδικασίες για την πρόληψη μη εξουσιοδοτημένων αλλαγών στον πηγαίο κώδικα λογισμικού που αναπτύσσεται εσωτερικά·

ζ. διαδικασία διεξαγωγής ελέγχου ασφάλειας και τρωτότητας νέων ή σημαντικά τροποποιημένων συστημάτων ΤΠΕ και λογισμικού, πριν την έγκρισή τους για παραγωγή και την έκθεσή τους σε πιθανές κυβερνοεπιθέσεις·

η. διαδικασία και λύσεις για την πρόληψη της μη εξουσιοδοτημένης ή ακούσιας κοινολόγησης εμπιστευτικών δεδομένων, κατά την αντικατάσταση, αρχειοθέτηση, απόρριψη ή καταστροφή συστημάτων ΤΠΕ·

θ. ανεξάρτητο έλεγχο και διαδικασίες επικύρωσης για τη μείωση των κινδύνων πρόκλησης ανθρώπινων σφαλμάτων κατά την πραγματοποίηση αλλαγών στα συστήματα ΤΠΕ που μπορεί να έχουν σοβαρές δυσμενείς επιπτώσεις στη διαθεσιμότητα, τη συνέχεια ή την ασφάλεια του ιδρύματος (π.χ. σημαντικές αλλαγές στη διαμόρφωση του τείχους προστασίας) ή στην ασφάλεια του ιδρύματος (π.χ. αλλαγές στα τείχη προστασίας).

(δ) Έλεγχοι για τη διαχείριση ουσιωδών κινδύνων ακεραιότητας δεδομένων ΤΠΕ

57. Οι αρμόδιες αρχές θα πρέπει να αξιολογούν εάν το ίδρυμα εφαρμόζει αποτελεσματικό πλαίσιο για τον προσδιορισμό, την κατανόηση, τη μέτρηση και τον μετριασμό του κινδύνου ακεραιότητας δεδομένων ΤΠΕ, ανάλογο της φύσης, της κλίμακας και της πολυπλοκότητας των δραστηριοτήτων του ιδρύματος και του προφίλ κινδύνου ΤΠΕ του ιδρύματος. Το πλαίσιο του ιδρύματος θα πρέπει να λαμβάνει υπόψη τους κινδύνους που σχετίζονται με τη διατήρηση της ακεραιότητας των δεδομένων που αποθηκεύονται και υφίστανται επεξεργασία από τα συστήματα ΤΠΕ. Για την εν λόγω αξιολόγηση, οι αρμόδιες αρχές θα πρέπει να λαμβάνουν υπόψη ιδιαιτέρως εάν το πλαίσιο λαμβάνει υπόψη:

α. πολιτική που ορίζει τους ρόλους και τις αρμοδιότητες για τη διαχείριση της ακεραιότητας των δεδομένων στα συστήματα ΤΠΕ (π.χ. αρχιτέκτονας δεδομένων, υπεύθυνοι δεδομένων [6], θεματοφύλακες δεδομένων[7], ιδιοκτήτες/επόπτες δεδομένων[8]). Παρέχεται καθοδήγηση σχετικά με

[6] Ο υπεύθυνος δεδομένων (data officer) είναι υπεύθυνος για την επεξεργασία και τη χρήση των δεδομένων.

[7] Ο θεματοφύλακας δεδομένων (data custodian) είναι υπεύθυνος για την ασφαλή φύλαξη, μεταφορά και αποθήκευση των δεδομένων.

τα δεδομένα που είναι κρίσιμης σημασίας από άποψη ακεραιότητας των δεδομένων και θα πρέπει να υπόκεινται σε ειδικούς ελέγχους ΤΠΕ (π.χ. αυτόματους ελέγχους επικύρωσης εισόδου, ελέγχους μεταφοράς δεδομένων, συμφωνίες στοιχείων κ.λπ.) ή επανεξετάσεις (π.χ. έλεγχο συμβατότητας με την αρχιτεκτονική δεδομένων) στα διάφορα στάδια του κύκλου ζωής των δεδομένων ΤΠΕ·

β. τεκμηριωμένη αρχιτεκτονική δεδομένων, μοντέλο δεδομένων και/ή λεξικό δεδομένων, το οποίο επικυρώνεται από τα σχετικά ενδιαφερόμενα μέρη της επιχείρησης και του τμήματος πληροφορικής για την υποστήριξη της απαιτούμενης συνοχής των δεδομένων σε όλα τα συστήματα ΤΠΕ και για τη διασφάλιση της συνεχούς ευθυγράμμισης της αρχιτεκτονικής, του μοντέλου και/ή του λεξικού δεδομένων με τις ανάγκες διαχείρισης των δραστηριοτήτων και των κινδύνων·

γ. πολιτική σχετικά με την επιτρεπόμενη χρήση των συστημάτων τελικού χρήστη (end user computing) και την εξάρτηση από τέτοια συστήματα, ιδίως όσον αφορά τον προσδιορισμό, την καταχώριση και την τεκμηρίωση σημαντικών λύσεων συστημάτων τελικού χρήστη (π.χ. κατά την επεξεργασία σημαντικών δεδομένων) και τα αναμενόμενα επίπεδα ασφάλειας για την πρόληψη μη εξουσιοδοτημένων τροποποιήσεων, τόσο στο ίδιο το εργαλείο όσο και στα δεδομένα που αποθηκεύονται σε αυτό·

δ. τεκμηριωμένες διαδικασίες χειρισμού εξαιρέσεων για την επίλυση των ζητημάτων ακεραιότητας δεδομένων ΤΠΕ που έχουν εντοπισθεί, σύμφωνα με την κρισιμότητα και την ευαισθησία τους.

58. Στην περίπτωση εποπτευόμενων ιδρυμάτων που εμπίπτουν στο πεδίο εφαρμογής των αρχών του προτύπου BCBS 239 για την αποτελεσματική συγκέντρωση δεδομένων κινδύνου και αναφορά κινδύνων[9], οι αρμόδιες αρχές θα πρέπει να εξετάζουν την ανάλυση κινδύνων που διενεργούν τα ιδρύματα σχετικά με τις ικανότητές τους αναφοράς κινδύνων και συγκέντρωσης δεδομένων σε σύγκριση με τις αρχές και τα σχετικά έγγραφα τεκμηρίωσης, λαμβάνοντας υπόψη το χρονοδιάγραμμα εφαρμογής και τις μεταβατικές ρυθμίσεις που προβλέπονται σε αυτές τις αρχές.

(ε) Έλεγχοι για τη διαχείριση ουσιωδών κινδύνων εξωτερικής ανάθεσης ΤΠΕ

59. Οι αρμόδιες αρχές θα πρέπει να αξιολογούν εάν η στρατηγική εξωτερικής ανάθεσης του ιδρύματος, σύμφωνα με τις απαιτήσεις των κατευθυντήριων γραμμών της Επιτροπής Ευρωπαϊκών Αρχών Τραπεζικής Εποπτείας σχετικά με την εξωτερική ανάθεση (2006) και επιπλέον της απαίτησης του σημείου 85 στοιχείο δ) των κατευθυντήριων γραμμών ΔΕΕΑ της ΕΑΤ, εφαρμόζεται καταλλήλως για την εξωτερική ανάθεση ΤΠΕ, συμπεριλαμβανομένης της ανάθεσης σε άλλες οντότητες εντός του ομίλου για την παροχή υπηρεσιών ΤΠΕ εντός του ομίλου. Κατά την αξιολόγηση των κινδύνων εξωτερικής ανάθεσης ΤΠΕ, οι αρμόδιες αρχές θα πρέπει να λαμβάνουν υπόψη ότι οι κίνδυνοι εξωτερικής ανάθεσης ΤΠΕ μπορούν να καλύπτονται επίσης στο πλαίσιο της αξιολόγησης των εγγενών

[8] Ο επόπτης δεδομένων (data steward) είναι υπεύθυνος για τη διαχείριση και την καταλληλότητα των στοιχείων των δεδομένων – τόσο του περιεχομένου όσο και των μεταδεδομένων.

[9] Επιτροπή της Βασιλείας για την τραπεζική εποπτεία, Principles for effective risk data aggregation and risk reporting (Αρχές αποτελεσματικής συγκέντρωσης δεδομένων κινδύνου και υποβολής στοιχείων κινδύνου), Ιανουάριος 2013, διαθέσιμο στο διαδίκτυο στη διεύθυνση: http://www.bis.org/publ/bcbs239.pdf.

επιχειρησιακών κινδύνων δυνάμει του σημείου 240 στοιχείο ι) των κατευθυντήριων γραμμών ΔΕΕΑ της ΕΑΤ, ώστε να αποφεύγεται η επικάλυψη ενεργειών ή η διπλή προσμέτρηση.

60. Οι αρμόδιες αρχές θα πρέπει να αξιολογούν ιδίως εάν το ίδρυμα εφαρμόζει αποτελεσματικό πλαίσιο για τον προσδιορισμό, την κατανόηση και τη μέτρηση του κινδύνου εξωτερικής ανάθεσης ΤΠΕ και, ιδίως, ελέγχους και ένα περιβάλλον ελέγχου για τον μετριασμό των κινδύνων που αφορούν σημαντικές υπηρεσίες ΤΠΕ που ανατίθενται εξωτερικά, το οποίο να είναι ανάλογο του μεγέθους, των δραστηριοτήτων και του προφίλ κινδύνου ΤΠΕ του ιδρύματος και να περιλαμβάνει:

α. αξιολόγηση του αντίκτυπου της εξωτερικής ανάθεσης ΤΠΕ στη διαχείριση κινδύνων του ιδρύματος όσον αφορά τη χρήση παρόχων υπηρεσιών (π.χ. παρόχων υπηρεσιών υπολογιστικού νέφους) και τις υπηρεσίες τους κατά τη διαδικασία προμήθειας, η οποία είναι τεκμηριωμένη και λαμβάνεται υπόψη από τα ανώτατα διοικητικά στελέχη ή το διοικητικό όργανο για τη λήψη ή όχι της απόφασης εξωτερικής ανάθεσης των υπηρεσιών. Το ίδρυμα θα πρέπει να εξετάζει τις πολιτικές διαχείρισης κινδύνων ΤΠΕ, τους ελέγχους ΤΠΕ και το περιβάλλον ελέγχου του παρόχου υπηρεσιών ώστε να εξασφαλίζει ότι επιτυγχάνουν τους στόχους εσωτερικής διαχείρισης κινδύνων του ιδρύματος και τη διάθεσή του για ανάληψη κινδύνων. Η εν λόγω εξέταση θα πρέπει να επικαιροποιείται περιοδικά κατά τη διάρκεια της συμβατικής περιόδου εξωτερικής ανάθεσης, λαμβάνοντας υπόψη τα χαρακτηριστικά των υπηρεσιών που έχουν ανατεθεί εξωτερικά·

β. παρακολούθηση των κινδύνων ΤΠΕ των υπηρεσιών που έχουν ανατεθεί εξωτερικά κατά τη διάρκεια της συμβατικής περιόδου εξωτερικής ανάθεσης στο πλαίσιο της διαχείρισης κινδύνων του ιδρύματος, η οποία χρησιμοποιείται στην υποβολή στοιχείων για τη διαχείριση κινδύνων ΤΠΕ του ιδρύματος (π.χ. υποβολή στοιχείων συνέχειας των δραστηριοτήτων, υποβολή στοιχείων ασφάλειας)·

γ. παρακολούθηση και σύγκριση των επιπέδων των υπηρεσιών που παρασχέθηκαν με τα επίπεδα των υπηρεσιών που είχαν συμφωνηθεί συμβατικά, στο πλαίσιο της σύμβασης εξωτερικής ανάθεσης ή της συμφωνίας επιπέδου εξυπηρέτησης (SLA)· και

δ. επαρκές προσωπικό, επαρκείς πόροι και αρμοδιότητες για την παρακολούθηση και τη διαχείριση των κινδύνων ΤΠΕ από τις υπηρεσίες που έχουν ανατεθεί εξωτερικά.

3.4 Σύνοψη διαπιστώσεων και βαθμολόγηση

61. Κατόπιν της ανωτέρω αξιολόγησης, οι αρμόδιες αρχές θα πρέπει να διαμορφώσουν γνώμη σχετικά με τον κίνδυνο ΤΠΕ του ιδρύματος. Η γνώμη αυτή θα πρέπει να αποτυπώνεται σε μια σύνοψη διαπιστώσεων την οποία θα πρέπει να λαμβάνουν υπόψη οι αρμόδιες αρχές κατά τη βαθμολόγηση του επιχειρησιακού κινδύνου σύμφωνα με τον πίνακα 6 των κατευθυντήριων γραμμών ΔΕΕΑ της ΕΑΤ. Οι αρμόδιες αρχές θα πρέπει να βασίζουν την άποψή τους στους ουσιώδεις κινδύνους ΤΠΕ λαμβάνοντας υπόψη τα ακόλουθα ζητήματα που θα χρησιμοποιούνται στην αξιολόγηση επιχειρησιακών κινδύνων:

α. Ζητήματα κινδύνου

i. Το προφίλ κινδύνου ΤΠΕ και η έκθεση σε κίνδυνο ΤΠΕ του ιδρύματος·
ii. Τα κρίσιμα συστήματα και οι κρίσιμες υπηρεσίες ΤΠΕ που έχουν εντοπιστεί·
iii. Η σημαντικότητα του κινδύνου ΤΠΕ όσον αφορά τα κρίσιμα συστήματα ΤΠΕ.

β. Ζητήματα διαχείρισης και ελέγχων

i. Εάν υπάρχει συνέπεια μεταξύ της πολιτικής και στρατηγικής διαχείρισης κινδύνων ΤΠΕ του ιδρύματος και της συνολικής στρατηγικής του, καθώς και της διάθεσής του για ανάληψη κινδύνων·
ii. εάν το οργανωτικό πλαίσιο διαχείρισης κινδύνων ΤΠΕ είναι ισχυρό και προβλέπει σαφείς αρμοδιότητες και σαφή διαχωρισμό καθηκόντων μεταξύ των υπευθύνων ανάληψης κινδύνων και των τμημάτων διαχείρισης και ελέγχου·
iii. εάν τα συστήματα μέτρησης, παρακολούθησης και υποβολής στοιχείων κινδύνων ΤΠΕ είναι κατάλληλα· και
iv. εάν τα πλαίσια ελέγχου των ουσιωδών κινδύνων ΤΠΕ είναι ορθά.

62. Εάν οι αρμόδιες αρχές θεωρούν ότι ο κίνδυνος ΤΠΕ είναι ουσιώδης και η αρμόδια αρχή αποφασίσει να αξιολογήσει και να βαθμολογήσει τον εν λόγω κίνδυνο ως υποκατηγορία του επιχειρησιακού κινδύνου, σχετικά ζητήματα βαθμολόγησης του κινδύνου ΤΠΕ αναφέρονται στον παρακάτω πίνακα (πίνακας 1).

Πίνακας 1: Εποπτικά ζητήματα για τη βαθμολόγηση κινδύνων ΤΠΕ

Βαθμολογία κινδύνου	**Εποπτική γνώμη**	**Ζητήματα σχετικά με τον εγγενή κίνδυνο**	**Ζητήματα σχετικά με την επαρκή διαχείριση και τους ελέγχους**
1	Δεν υπάρχει ευδιάκριτος κίνδυνος σημαντικών επιπτώσεων προληπτικής εποπτείας στο ίδρυμα λαμβάνοντας υπόψη το επίπεδο εγγενούς κινδύνου, τη διαχείριση και τους ελέγχους.	• Οι πηγές πληροφοριών που πρέπει να εξετάζονται σύμφωνα με την παράγραφο 37 δεν αποκάλυψαν σημαντική έκθεση σε κίνδυνο ΤΠΕ. • Ο χαρακτήρας του προφίλ κινδύνου ΤΠΕ του ιδρύματος, σε συνάρτηση με τον έλεγχο των κρίσιμων συστημάτων ΤΠΕ και των ουσιωδών κινδύνων ΤΠΕ για τα συστήματα και τις υπηρεσίες ΤΠΕ, δεν αποκάλυψαν ουσιώδεις κινδύνους ΤΠΕ.	• Η πολιτική και η στρατηγική κινδύνου ΤΠΕ του ιδρύματος είναι ανάλογες της συνολικής στρατηγικής του και της διάθεσής του για ανάληψη κινδύνων. • Το οργανωτικό πλαίσιο που αφορά τον κίνδυνο ΤΠΕ είναι ισχυρό και
2	Υπάρχει χαμηλός κίνδυνος σημαντικών επιπτώσεων προληπτικής εποπτείας στο ίδρυμα λαμβάνοντας υπόψη το επίπεδο εγγενούς κινδύνου,	• Οι πηγές πληροφοριών που πρέπει να εξετάζονται σύμφωνα με την παράγραφο 37 δεν αποκάλυψαν σημαντική έκθεση σε κίνδυνο ΤΠΕ. • Ο χαρακτήρας του προφίλ κινδύνου ΤΠΕ του ιδρύματος, σε συνάρτηση με τον έλεγχο των κρίσιμων συστημάτων ΤΠΕ και των ουσιωδών κινδύνων ΤΠΕ για	

	τη διαχείριση και τους ελέγχους.	τα συστήματα και τις υπηρεσίες ΤΠΕ αποκάλυψαν περιορισμένη έκθεση σε κίνδυνο ΤΠΕ (π.χ. όχι έως 2 από τις 5 προκαθορισμένες κατηγορίες κινδύνου ΤΠΕ).	προβλέπει σαφείς αρμοδιότητες και σαφή διαχωρισμό καθηκόντων μεταξύ των υπευθύνων ανάληψης κινδύνου και των τμημάτων διαχείρισης και ελέγχου. • Τα συστήματα μέτρησης, παρακολούθησης και υποβολής στοιχείων κινδύνου ΤΠΕ είναι κατάλληλα. • Το πλαίσιο ελέγχου του κινδύνου ΤΠΕ είναι ισχυρό.
3	Υπάρχει μέτριος κίνδυνος σημαντικών επιπτώσεων προληπτικής εποπτείας στο ίδρυμα λαμβάνοντας υπόψη το επίπεδο εγγενούς κινδύνου, τη διαχείριση και τους ελέγχους.	• Οι πηγές πληροφοριών που πρέπει να εξετάζονται σύμφωνα με την παράγραφο 37 αποκάλυψαν ενδείξεις πιθανής σημαντικής έκθεσης σε κίνδυνο ΤΠΕ. • Ο χαρακτήρας του προφίλ κινδύνου ΤΠΕ του ιδρύματος, σε συνάρτηση με τον έλεγχο των κρίσιμων συστημάτων ΤΠΕ και των ουσιωδών κινδύνων ΤΠΕ για τα συστήματα και τις υπηρεσίες ΤΠΕ, αποκάλυψαν οξυμένη έκθεση σε κίνδυνο ΤΠΕ (π.χ. τουλάχιστον 3 από τις 5 προκαθορισμένες κατηγορίες κινδύνου ΤΠΕ).	
4	Υπάρχει υψηλός κίνδυνος σημαντικών επιπτώσεων προληπτικής εποπτείας στο ίδρυμα λαμβάνοντας υπόψη το επίπεδο εγγενούς κινδύνου, τη διαχείριση και τους ελέγχους.	• Οι πηγές πληροφοριών που πρέπει να εξετάζονται σύμφωνα με την παράγραφο 37 παρείχαν πολλαπλές ενδείξεις σημαντικής έκθεσης σε κίνδυνο ΤΠΕ. • Ο χαρακτήρας του προφίλ κινδύνου ΤΠΕ του ιδρύματος, σε συνάρτηση με τον έλεγχο των κρίσιμων συστημάτων ΤΠΕ και των ουσιωδών κινδύνων ΤΠΕ για τα συστήματα και τις υπηρεσίες ΤΠΕ, αποκάλυψαν υψηλή έκθεση σε κίνδυνο ΤΠΕ (π.χ. 4 ή 5 από τις 5 προκαθορισμένες κατηγορίες κινδύνου ΤΠΕ).	

Παράρτημα – Ταξινόμηση κινδύνων ΤΠΕ

5 κατηγορίες κινδύνων ΤΠΕ με μη εξαντλητικό κατάλογο των κινδύνων ΤΠΕ με δυνητικές επιπτώσεις υψηλής σοβαρότητας και/ή επιχειρησιακές επιπτώσεις, επιπτώσεις στη φήμη ή οικονομικές επιπτώσεις

Κατηγορίες κινδύνων ΤΠΕ	Κίνδυνοι ΤΠΕ (μη εξαντλητική αναφορά[10])	Περιγραφή κινδύνων	Παραδείγματα
Κίνδυνοι διαθεσιμότητας και συνέχειας των ΤΠΕ	Ανεπαρκής διαχείριση ικανοτήτων	Η έλλειψη πόρων (π.χ. υλικού, λογισμικού, προσωπικού, παρόχων υπηρεσιών) μπορεί να προκαλέσει αδυναμία κλιμάκωσης της υπηρεσίας για την κάλυψη των επιχειρηματικών αναγκών, διακοπή του συστήματος, υποβάθμιση υπηρεσίας και/ή επιχειρησιακά σφάλματα.	• Η ανεπάρκεια ικανοτήτων μπορεί να επηρεάσει τους ρυθμούς μετάδοσης και τη διαθεσιμότητα του δικτύου (διαδικτύου) για υπηρεσίες όπως η δικτυοτραπεζική. • Η έλλειψη προσωπικού (εσωτερικού ή παρεχόμενου από τρίτους) μπορεί να προκαλέσει διακοπές στο σύστημα και/ή επιχειρησιακά σφάλματα.
	Αστοχίες συστήματος ΤΠΕ	Απώλεια διαθεσιμότητας λόγω αστοχιών υλικού.	• Αστοχία/δυσλειτουργία εξοπλισμού αποθήκευσης (σκληρών δίσκων), διακομιστή ή άλλου εξοπλισμού ΤΠΕ που προκαλείται π.χ. από έλλειψη συντήρησης.
		Απώλεια διαθεσιμότητας λόγω βλάβης λογισμικού και σφαλμάτων προγραμματισμού (bugs).	• Ατέρμων βρόχος σε λογισμικό εφαρμογών εμποδίζει την εκτέλεση συναλλαγών. • Διακοπές λόγω συνεχιζόμενης χρήσης παρωχημένων συστημάτων και λύσεων ΤΠΕ που δεν πληρούν πλέον τις παρούσες απαιτήσεις διαθεσιμότητας και ανθεκτικότητας και/ή δεν υποστηρίζονται πλέον από τους προμηθευτές τους.
	Ανεπαρκής σχεδιασμός συνέχειας ΤΠΕ	Αστοχία λύσεων σχεδιαζόμενης διαθεσιμότητας και/συνέχειας ΤΠΕ και/ή αποκατάστασης σε περίπτωση καταστροφής (π.χ. εφεδρικού κέντρου	• Διαφορές διαμόρφωσης μεταξύ του πρωτογενούς και του δευτερογενούς κέντρου δεδομένων δύναται να προκαλέσουν αδυναμία του εφεδρικού

[10] Οι κίνδυνοι ΤΠΕ αναφέρονται στην κατηγορία κινδύνων την οποία επηρεάζουν περισσότερο αλλά μπορεί να έχουν επιπτώσεις και σε άλλες κατηγορίες κινδύνων

Κατηγορίες κινδύνων ΤΠΕ	Κίνδυνοι ΤΠΕ (μη εξαντλητική αναφορά[10])	Περιγραφή κινδύνων	Παραδείγματα
	και αποκατάστασης σε περίπτωση καταστροφής	δεδομένων αποκατάστασης) όταν ενεργοποιούνται για την αντιμετώπιση ενός συμβάντος.	κέντρου δεδομένων να παρέχει τη σχεδιαζόμενη συνέχεια υπηρεσίας.
	Κυβερνοεπιθέσεις που προκαλούν διακοπές και καταστροφές	Επιθέσεις για διάφορους σκοπούς (π.χ. ακτιβισμό, εκβιασμό) οι οποίες προκαλούν υπερφόρτωση των συστημάτων και του δικτύου και εμποδίζουν την πρόσβαση σε υπηρεσίες υπολογιστών στο διαδίκτυο από τους νόμιμους χρήστες τους.	• Κατανεμημένες επιθέσεις άρνησης εξυπηρέτησης (DDoS attacks) πραγματοποιούνται μέσω πολλαπλών συστημάτων πληροφορικής στο διαδίκτυο τα οποία ελέγχονται από πληροφορικό πειρατή (hacker) ο οποίος αποστέλλει μεγάλες ποσότητες φαινομενικά νόμιμων αιτημάτων εξυπηρέτησης σε υπηρεσίες στο διαδίκτυο (π.χ. δικτυοτραπεζική).
Κίνδυνοι ασφάλειας των ΤΠΕ	Κυβερνοεπιθέσεις και άλλες εξωτερικές επιθέσεις που βασίζονται σε ΤΠΕ	Επιθέσεις που πραγματοποιούνται από το διαδίκτυο ή εξωτερικά δίκτυα για διάφορους σκοπούς (π.χ. απάτη, κατασκοπία, ακτιβισμό/δολιοφθορά, κυβερνοτρομοκρατία) με τη χρήση διάφορων τεχνικών (π.χ. χειραγώγησης, απόπειρας εισβολής μέσω της εκμετάλλευσης τρωτών σημείων, εγκατάστασης κακόβουλου λογισμικού) που έχουν αποτέλεσμα τη ανάληψη του ελέγχου εσωτερικών συστημάτων ΤΠΕ.	Διάφοροι τύποι επιθέσεων: • Μόνιμη προηγμένη απειλή (APT) για την ανάληψη του ελέγχου εσωτερικών συστημάτων ή την κλοπή πληροφοριών (π.χ. πληροφοριών σχετικών με την κλοπή ταυτότητας, στοιχείων πιστωτικής κάρτας). • Κακόβουλο λογισμικό (π.χ. ransomware) που κρυπτογραφεί δεδομένα με σκοπό τον εκβιασμό. • Μόλυνση εσωτερικών συστημάτων ΤΠΕ από προγράμματα «δούρειους ίππους» για την εκτέλεση ενεργειών κακόβουλων συστημάτων με συγκαλυμμένο τρόπο. • Εκμετάλλευση των τρωτών σημείων των συστημάτων ΤΠΕ και/ή των εφαρμογών (web) [π.χ. επίθεση τύπου SQL injection (έγχυση SQL)] για την απόκτηση πρόσβασης στο εσωτερικό σύστημα ΤΠΕ.
		Εκτέλεση δόλιων συναλλαγών πληρωμών από πληροφορικούς πειρατές μέσω της παραβίασης ή της παράκαμψης της ασφάλειας υπηρεσιών ηλεκτρονικής τραπεζικής και πληρωμών και/ή μέσω της επίθεσης και	• Επιθέσεις κατά υπηρεσιών ηλεκτρονικής τραπεζικής ή πληρωμών με στόχο τη διάπραξη μη εγκεκριμένων συναλλαγών. • Δημιουργία και αποστολή δόλιων συναλλαγών

Κατηγορίες κινδύνων ΤΠΕ	Κίνδυνοι ΤΠΕ (μη εξαντλητική αναφορά[10])	Περιγραφή κινδύνων	Παραδείγματα
		της εκμετάλλευσης τρωτών όσον αφορά την ασφάλεια σημείων στα εσωτερικά συστήματα πληρωμών του ιδρύματος.	πληρωμών από σημεία εντός των εσωτερικών συστημάτων πληρωμών του ιδρύματος (π.χ. δόλια μηνύματα κωδικού SWIFT).
		Εκτέλεση δόλιων συναλλαγών χρεογράφων από πληροφορικούς πειρατές μέσω της παραβίασης ή της παράκαμψης της ασφάλειας των υπηρεσιών ηλεκτρονικής τραπεζικής που παρέχουν επίσης πρόσβαση στους λογαριασμούς χρεογράφων του πελάτη.	• Επιθέσεις διόγκωσης και πώλησης (pump and dump) κατά τις οποίες οι επιτιθέμενοι αποκτούν πρόσβαση σε λογαριασμούς χρεογράφων ηλεκτρονικής τραπεζικής των πελατών και δίνουν δόλιες εντολές αγοράς ή πώλησης για να επηρεάσουν την αγοραία τιμή και/ή να αποκομίσουν κέρδη με βάση θέσεις χρεογράφων που έχουν προηγουμένως δημιουργήσει.
		Επιθέσεις σε συνδέσεις επικοινωνιών και συζητήσεις κάθε είδους ή σε συστήματα ΤΠΕ με στόχο τη συλλογή πληροφοριών και/ή τη διάπραξη απάτης.	• Λαθρακρόαση/υποκλοπή μη προστατευμένης διαβίβασης δεδομένων επαλήθευσης σε αποκρυπτογράφητο κείμενο.
	Ανεπαρκής εσωτερική ασφάλεια ΤΠΕ	Απόκτηση μη εξουσιοδοτημένης πρόσβασης σε κρίσιμα συστήματα ΤΠΕ από σημεία εντός του ιδρύματος για διάφορους σκοπούς (π.χ. απάτη, εκτέλεση και απόκρυψη δραστηριοτήτων δόλιων συναλλαγών, κλοπή δεδομένων, ακτιβισμό/δολιοφθορά) με διάφορες τεχνικές (π.χ. κατάχρηση και/ή κλιμάκωση προνομίων, κλοπή ταυτότητας, κοινωνική μηχανική, εκμετάλλευση τρωτών σημείων σε συστήματα ΤΠΕ, εγκατάσταση κακόβουλου λογισμικού).	• Εγκατάσταση λογισμικού καταγραφής πληκτρολογήσεων (key logger) για την κλοπή αναγνωριστικών και κωδικών πρόσβασης των χρηστών για την απόκτηση μη εξουσιοδοτημένης πρόσβασης σε εμπιστευτικά δεδομένα και/ή τη διάπραξη απάτης. • Παραβίαση/τυχαία εύρεση κωδικών πρόσβασης χαμηλής ασφάλειας για την απόκτηση παράνομων ή αυξημένων δικαιωμάτων πρόσβασης. • Ο διαχειριστής του συστήματος χρησιμοποιεί τα λειτουργικά συστήματα ή τα προγράμματα γενικής χρήσης βάσεων δεδομένων (για απευθείας τροποποιήσεις βάσεων δεδομένων) για τη διάπραξη απάτης.
		Μη εξουσιοδοτημένοι χειρισμοί των ΤΠΕ λόγω ανεπαρκών διαδικασιών και πρακτικών διαχείρισης της πρόσβασης σε ΤΠΕ.	• Μη απενεργοποίηση ή διαγραφή περιττών λογαριασμών, όπως λογαριασμών προσωπικού που άλλαξε τμήμα και/ή αποχώρησε από το

Κατηγορίες κινδύνων ΤΠΕ	Κίνδυνοι ΤΠΕ (μη εξαντλητική αναφορά[10])	Περιγραφή κινδύνων	Παραδείγματα
			ίδρυμα, συμπεριλαμβανομένων φιλοξενούμενων ή προμηθευτών που δεν χρειάζονται πλέον πρόσβαση, μέσω των οποίων παρέχεται μη εξουσιοδοτημένη πρόσβαση σε συστήματα ΤΠΕ. • Χορήγηση υπερβολικών δικαιωμάτων και προνομίων πρόσβασης, η οποία επιτρέπει τη μη εξουσιοδοτημένη πρόσβαση και/ή καθιστά δυνατή την απόκρυψη δόλιων δραστηριοτήτων.
		Απειλές κατά της ασφάλειας λόγω έλλειψης ευαισθητοποίησης για την ασφάλεια, καθώς οι εργαζόμενοι δεν κατανοούν, παραμελούν ή δεν συμμορφώνονται με πολιτικές και διαδικασίες ασφάλειας ΤΠΕ.	• Εργαζόμενοι οι οποίοι εξαπατώνται ώστε να παράσχουν συνδρομή για μια επίθεση (π.χ. κοινωνική μηχανική). • Εσφαλμένες πρακτικές σχετικά με τα διαπιστευτήρια: κοινή χρήση κωδικών πρόσβασης, χρήση κωδικών πρόσβασης που είναι εύκολο να μαντέψει κανείς, χρήση του ίδιου κωδικού πρόσβασης για πολλούς διαφορετικούς σκοπούς, κ.λπ. • Αποθήκευση μη κρυπτογραφημένων εμπιστευτικών δεδομένων σε φορητούς υπολογιστές και σε φορητές λύσεις αποθήκευσης δεδομένων (π.χ. κλειδιά USB) που μπορούν να χαθούν ή να κλαπούν.
		Μη εξουσιοδοτημένη αποθήκευση ή μεταφορά εμπιστευτικών πληροφοριών εκτός του ιδρύματος.	• Κλοπή ή σκόπιμη διαρροή ή λαθραία διακίνηση εμπιστευτικών πληροφοριών σε μη εξουσιοδοτημένα πρόσωπα ή στο κοινό.
	Ανεπαρκής φυσική ασφάλεια ΤΠΕ	Παράνομη χρήση ή κλοπή περιουσιακών στοιχείων ΤΠΕ μέσω φυσικής πρόσβασης η οποία προκαλεί ζημία, απώλεια περιουσιακών στοιχείων ή δεδομένων ή καθιστά δυνατή την υλοποίηση άλλων απειλών.	• Πραγματική διάρρηξη σε κτίρια γραφείων και/ή μηχανογραφικά κέντρα για την κλοπή εξοπλισμού ΤΠΕ (π.χ. επιτραπέζιων υπολογιστών, φορητών υπολογιστών, λύσεων αποθήκευσης) και/ή την αντιγραφή δεδομένων μέσω φυσικής πρόσβασης σε συστήματα ΤΠΕ.

Κατηγορίες κινδύνων ΤΠΕ	Κίνδυνοι ΤΠΕ (μη εξαντλητική αναφορά[10])	Περιγραφή κινδύνων	Παραδείγματα
		Εκούσια ή ακούσια ζημία σε φυσικά περιουσιακά στοιχεία ΤΠΕ λόγω τρομοκρατίας, ατυχημάτων ή ατυχών/εσφαλμένων χειρισμών από το προσωπικό του ιδρύματος και/ή τρίτα μέρη (προμηθευτές, τεχνικούς).	• Φυσική τρομοκρατία (π.χ. τρομοκρατικές βόμβες) ή δολιοφθορά περιουσιακών στοιχείων ΤΠΕ. • Καταστροφή μηχανογραφικού κέντρου από πυρκαγιά, διαρροή νερού ή άλλους παράγοντες.
		Ανεπαρκής φυσική προστασία έναντι φυσικών καταστροφών η οποία προκαλεί μερική ή πλήρη καταστροφή συστημάτων ΤΠΕ/κέντρων δεδομένων από φυσικές καταστροφές.	• Σεισμοί, ακραία υψηλές θερμοκρασίες, ανεμοθύελλες, χιονοθύελλες, πλημμύρες, πυρκαγιές, κεραυνοί.
Κίνδυνοι αλλαγών ΤΠΕ	Ανεπαρκείς έλεγχοι των αλλαγών συστημάτων ΤΠΕ και της ανάπτυξης ΤΠΕ	Συμβάντα προκαλούμενα από σφάλματα ή τρωτά σημεία που δεν έχουν εντοπιστεί ως αποτέλεσμα αλλαγής (π.χ. απρόβλεπτες επιπτώσεις μιας αλλαγής ή μη κατάλληλη διαχείριση μιας αλλαγής λόγω έλλειψης δοκιμών ή ακατάλληλων πρακτικών διαχείρισης των αλλαγών) π.χ. σε λογισμικό, συστήματα ΤΠΕ και δεδομένα ΤΠΕ.	• Έγκριση για σκοπούς παραγωγής λογισμικού που δεν έχει υποβληθεί σε επαρκείς δοκιμές ή αλλαγές διαμόρφωσης με απρόσμενες δυσμενείς επιπτώσεις σε δεδομένα (π.χ. αλλοίωση, διαγραφή) και/ή στις επιδόσεις του συστήματος ΤΠΕ (π.χ. τεχνική βλάβη, υποβάθμιση επιδόσεων). • Ανεξέλεγκτες αλλαγές σε συστήματα ή δεδομένα ΤΠΕ στο περιβάλλον παραγωγής. • Έγκριση για σκοπούς παραγωγής συστημάτων ΤΠΕ και εφαρμογών διαδικτύου ανεπαρκούς ασφάλειας, η οποία παρέχει σε πληροφορικούς πειρατές ευκαιρίες να επιτεθούν στις παρεχόμενες υπηρεσίες διαδικτύου και/ή να παραβιάσουν τα εσωτερικά συστήματα ΤΠΕ. • Ανεξέλεγκτες αλλαγές στον πηγαίο κώδικα εσωτερικά αναπτυγμένου λογισμικού. • Ανεπαρκείς δοκιμές λόγω απουσίας κατάλληλου περιβάλλοντος δοκιμής.
	Ακατάλληλη αρχιτεκτονική ΤΠΕ	Μη ικανοποιητική διαχείριση αρχιτεκτονικής ΤΠΕ κατά τον σχεδιασμό, τη δημιουργία και τη συντήρηση συστημάτων ΤΠΕ (π.χ. λογισμικού, υλικού, δεδομένων) που μπορεί να οδηγήσει, με την πάροδο του χρόνου, σε περίπλοκα, δύσκολα, δύσκαμπτα και δαπανηρά	• Ανεπαρκής διαχείριση αλλαγών σε συστήματα ΤΠΕ, λογισμικό και/ή δεδομένα κατά τη διάρκεια παρατεταμένης χρονικής περιόδου, οι οποίες οδηγούν σε πολύπλοκα, ετερογενή και δύσκολα όσον αφορά τη διαχείρισή τους συστήματα και

Κατηγορίες κινδύνων ΤΠΕ	Κίνδυνοι ΤΠΕ (μη εξαντλητική αναφορά[10])	Περιγραφή κινδύνων	Παραδείγματα
		όσον αφορά τη διαχείρισή τους συστήματα ΤΠΕ, τα οποία δεν είναι πλέον επαρκώς ευθυγραμμισμένα με τις ανάγκες της επιχείρησης και υπολείπονται των πραγματικών απαιτήσεων διαχείρισης κινδύνου.	αρχιτεκτονικές ΤΠΕ, γεγονός που προκαλεί πολλές δυσμενείς επιπτώσεις όσον αφορά τη διαχείριση των δραστηριοτήτων και των κινδύνων (π.χ. έλλειψη ευελιξίας, συμβάντα και αστοχίες ΤΠΕ, υψηλό λειτουργικό κόστος, αποδυναμωμένη ασφάλεια και ανθεκτικότητα ΤΠΕ, μειωμένη ποιότητα δεδομένων και μειωμένες ικανότητες υποβολής αναφορών). • Υπερβολική προσαρμογή στις ανάγκες του χρήση και επέκταση πακέτων εμπορικού λογισμικού με εσωτερικά αναπτυγμένο λογισμικό, οι οποίες δεν επιτρέπουν την εφαρμογή μελλοντικών εκδόσεων και αναβαθμίσεων του εμπορικού λογισμικού και επιφέρει τον κίνδυνο μη υποστήριξης στο μέλλον από τον προμηθευτή.
	Ανεπαρκής διαχείριση κύκλου ζωής και πρόχειρων διορθώσεων	Μη διατήρηση επαρκούς καταλόγου όλων των περιουσιακών στοιχείων ΤΠΕ για την υποστήριξη ορθών πρακτικών διαχείρισης κύκλου ζωής και πρόχειρων διορθώσεων και σε συνδυασμό με αυτές. Αυτό οδηγεί σε συστήματα ΤΠΕ στα οποία δεν έχουν γίνει οι απαραίτητες διορθώσεις (και είναι, επομένως, περισσότερο ευάλωτα) και τα οποία είναι παρωχημένα και, συνεπώς, ενδέχεται να μην υποστηρίζουν τις ανάγκες διαχείρισης δραστηριοτήτων και κινδύνων.	• Μη διορθωμένα και παρωχημένα συστήματα ΤΠΕ που μπορεί να προκαλέσουν δυσμενείς επιπτώσεις όσον αφορά τη διαχείριση δραστηριοτήτων και κινδύνων (π.χ. έλλειψη ευελιξίας, διακοπές λειτουργίας ΤΠΕ, αποδυναμωμένη ασφάλεια και ανθεκτικότητα ΤΠΕ).
Κίνδυνοι ακεραιότητας δεδομένων ΤΠΕ	Δυσλειτουργική επεξεργασία ή δυσλειτουργικός χειρισμός δεδομένων ΤΠΕ	Σφάλματα ή αστοχίες συστημάτων, επικοινωνίας και/ή εφαρμογών ή μια εσφαλμένα εκτελεσμένη διαδικασία εξαγωγής, μεταφοράς και φόρτωση (ETL) δεδομένων είναι πιθανό να προκαλέσει αλλοίωση ή απώλεια δεδομένων.	• Σφάλμα συστήματος πληροφορικής κατά τη μαζική επεξεργασία στοιχείων (batch processing) το οποίο προκαλεί εσφαλμένα υπόλοιπα σε τραπεζικούς λογαριασμούς του πελάτη. • Ερωτήματα που δεν εκτελούνται σωστά. • Απώλεια δεδομένων λόγω σφάλματος κατά την αντιγραφή δεδομένων (δημιουργία αντιγράφων

Κατηγορίες κινδύνων ΤΠΕ	Κίνδυνοι ΤΠΕ (μη εξαντλητική αναφορά[10])	Περιγραφή κινδύνων	Παραδείγματα
			ασφάλειας).
	Μη ικανοποιητικά σχεδιασμένοι έλεγχοι επικύρωσης δεδομένων σε συστήματα ΤΠΕ	Σφάλματα που αφορούν έλλειψη ελέγχων ή μη αποτελεσματικούς αυτοματοποιημένους ελέγχους εισαγωγής και αποδοχής δεδομένων (π.χ. για χρησιμοποιημένα δεδομένα τρίτων), ελέγχους μεταφοράς, επεξεργασίας και εξαγωγής δεδομένων στα συστήματα ΤΠΕ (π.χ. ελέγχους επικύρωσης εισαγωγής, συμφωνία στοιχείων).	• Ανεπαρκής ή μη έγκυρη μορφοποίηση/επικύρωση εισαγωγών δεδομένων σε εφαρμογές και/ή διασυνδέσεις χρήστη. • Απουσία ελέγχων συμφωνίας δεδομένων σε σχέση με τα παραγόμενα αποτελέσματα. • Απουσία ελέγχων στις διαδικασίες εξαγωγής δεδομένων που εκτελούνται (π.χ. ερωτήματα βάσης δεδομένων) που οδηγούν σε εσφαλμένα δεδομένα. • Χρήση εσφαλμένων εξωτερικών δεδομένων.
	Μη ικανοποιητικά ελεγχόμενες αλλαγές δεδομένων σε συστήματα ΤΠΕ παραγωγής.	Σφάλματα δεδομένων που προκαλούνται λόγω έλλειψης ελέγχων της ορθότητας και του δικαιολογημένου χαρακτήρα των χειρισμών δεδομένων που πραγματοποιούνται στην παραγωγή συστημάτων ΤΠΕ.	• Απευθείας πρόσβαση και αλλαγή των δεδομένων στα συστήματα ΤΠΕ παραγωγής από αναλυτές λογισμικού και διαχειριστές βάσεων δεδομένων κατά μη ελεγχόμενο τρόπο, π.χ. στην περίπτωση ενός συμβάντος ΤΠΕ.
	Αρχιτεκτονική δεδομένων, ροές δεδομένων, μοντέλα δεδομένων ή λεξικά δεδομένα που δεν έχουν σχεδιαστεί ικανοποιητικά και/ή δεν υφίστανται ικανοποιητική διαχείριση.	Αρχιτεκτονικές δεδομένων, μοντέλα δεδομένων, ροές δεδομένων ή λεξικά δεδομένων τα οποία δεν υφίστανται ικανοποιητική διαχείριση μπορούν να οδηγήσουν σε πολλαπλές εκδόσεις των ίδιων δεδομένων στα διάφορα συστήματα ΤΠΕ, οι οποίες δεν συμφωνούν πλέον λόγω των διαφορετικών μοντέλων δεδομένων ή ορισμών δεδομένων που έχουν χρησιμοποιηθεί και/ή διαφορών στην υποκείμενη διαδικασία παραγωγής και αλλαγής δεδομένων.	• Η ύπαρξη διαφορετικών βάσεων δεδομένων πελατών ανά προϊόν ή επιχειρηματική μονάδα με διαφορετικούς ορισμούς και πεδία δεδομένων, η οποία έχει ως αποτέλεσμα δεδομένα πελατών σε επίπεδο χρηματοπιστωτικού συστήματος ή ομίλου τα οποία δεν έχουν υποβληθεί σε συμφωνία και τα οποία είναι δύσκολο να συγκριθούν και να ενοποιηθούν.

Κατηγορίες κινδύνων ΤΠΕ	Κίνδυνοι ΤΠΕ (μη εξαντλητική αναφορά[10])	Περιγραφή κινδύνων	Παραδείγματα
Κίνδυνοι εξωτερικής ανάθεσης ΤΠΕ	Ανεπαρκής ανθεκτικότητα υπηρεσιών τρίτων ή άλλης οντότητας του ομίλου	Μη διαθεσιμότητα κρίσιμων υπηρεσιών ΤΠΕ, υπηρεσιών τηλεπικοινωνιών και βοηθητικών παροχών που έχουν ανατεθεί σε τρίτους. Απώλεια ή αλλοίωση κρίσιμων/ευαίσθητων δεδομένων που έχουν ανατεθεί στον πάροχο υπηρεσίας.	• Μη διαθεσιμότητα βασικών υπηρεσιών λόγω αστοχιών σε συστήματα ή εφαρμογές ΤΠΕ των προμηθευτών (εξωτερικά ανατεθειμένα συστήματα ή εφαρμογές). • Διακοπή τηλεπικοινωνιακών συνδέσεων. • Μη επαρκής παροχή ηλεκτρισμού.
	Ανεπαρκής διαχείριση της εξωτερικής ανάθεσης.	Σοβαρή υποβάθμιση ή αστοχίες υπηρεσίας λόγω ανεπαρκούς ετοιμότητας ή διαδικασιών ελέγχου του παρόχου υπηρεσιών στον οποίο έχει γίνει η εξωτερική ανάθεση. Η μη αποτελεσματική διαχείριση της εξωτερικής ανάθεσης μπορεί να έχει ως αποτέλεσμα την έλλειψη κατάλληλων δεξιοτήτων και ικανοτήτων για τον προσδιορισμό, την αξιολόγηση, τον μετριασμό και την παρακολούθηση σε πλήρες επίπεδο των κινδύνων ΤΠΕ και μπορεί να περιορίσει τις επιχειρησιακές ικανότητες των ιδρυμάτων.	• Μη ικανοποιητικές διαδικασίες χειρισμού συμβάντων, μη ικανοποιητικοί μηχανισμοί συμβατικού ελέγχου και μη ικανοποιητικές εγγυήσεις στο πλαίσιο της σύμβασης με τον πάροχο της υπηρεσίας που αυξάνουν την εξάρτηση από τρίτους και προμηθευτές όσον αφορά βασικά στελέχη τους. • Ακατάλληλοι έλεγχοι διαχείρισης αλλαγών σχετικά με το περιβάλλον ΤΠΕ του παρόχου υπηρεσίας μπορούν να προκαλέσουν σοβαρή υποβάθμιση ή αστοχία της υπηρεσίας.
	Ανεπαρκής ασφάλεια τρίτων ή άλλης οντότητας του ομίλου	Πειρατεία στα συστήματα ΤΠΕ ανεξάρτητων παρόχων υπηρεσιών με άμεσες επιπτώσεις στις υπηρεσίες που έχουν ανατεθεί εξωτερικά ή σε κρίσιμα/εμπιστευτικά δεδομένα που είναι αποθηκευμένα στον πάροχο υπηρεσιών. Απόκτηση από το προσωπικό του παρόχου υπηρεσιών μη εξουσιοδοτημένης πρόσβασης σε κρίσιμα/ευαίσθητα δεδομένα τα οποία είναι αποθηκευμένα στον πάροχο υπηρεσιών.	• Πειρατεία σε παρόχους υπηρεσιών από εγκληματίες ή τρομοκράτες, ως σημείο εισόδου στα συστήματα ΤΠΕ των ιδρυμάτων ή για την πρόσβαση/καταστροφή κρίσιμων ή ευαίσθητων δεδομένων αποθηκευμένων στον πάροχο υπηρεσιών. • Απόπειρα κλοπής και πώλησης ευαίσθητων δεδομένων από κακόβουλα πρόσωπα εντός του παρόχου υπηρεσιών.