Κατευθυντήριες γραμμές

EBA/GL/2019/04

28 Νοεμβρίου 2019

Κατευθυντήριες γραμμές της ΕΑΤ σχετικά με τη διαχείριση κινδύνων ΤΠΕ και ασφάλειας

Υποχρεώσεις συμμόρφωσης και υποβολής στοιχείων και αναφορών

Καθεστώς των κατευθυντήριων γραμμών

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 νομοθεσίας της Ευρωπαϊκής Ένωσης 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 ([DD.MM.YYYY]). 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/2019/04». 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).

Αντικείμενο, πεδίο εφαρμογής και ορισμοί

Αντικείμενο

5. Οι παρούσες κατευθυντήριες γραμμές βασίζονται στις διατάξεις του άρθρου 74 της οδηγίας 2013/36/ΕΕ (CRD) σχετικά με την εσωτερική διακυβέρνηση και απορρέουν από την εντολή έκδοσης κατευθυντήριων γραμμών βάσει του άρθρου 95 παράγραφος 3 της οδηγίας (ΕΕ) 2015/2366 (PSD2).

6. Οι παρούσες κατευθυντήριες γραμμές προσδιορίζουν τα μέτρα διαχείρισης κινδύνου που πρέπει να λαμβάνονται αφενός από τα χρηματοοικονομικά ιδρύματα (όπως ορίζονται στην παράγραφο 9 κατωτέρω) σύμφωνα με το άρθρο 74 της οδηγίας CRD με σκοπό τη διαχείριση των κινδύνων ΤΠΕ και ασφάλειας για όλες τις δραστηριότητες, και αφετέρου από τους παρόχους υπηρεσιών πληρωμών (ΠΥΠ, όπως ορίζονται στην παράγραφο 9 κατωτέρω), σύμφωνα με το άρθρο 95 παράγραφος 1 της PSD2, με σκοπό τη διαχείριση των λειτουργικών κινδύνων και των κινδύνων ασφάλειας (που αντιστοιχούν στους «κινδύνους ΤΠΕ και ασφάλειας») σε σχέση με τις υπηρεσίες πληρωμών που παρέχουν. Οι παρούσες κατευθυντήριες γραμμές περιλαμβάνουν απαιτήσεις ασφάλειας πληροφοριών, συμπεριλαμβανομένης της ασφάλειας στον κυβερνοχώρο, στον βαθμό που οι πληροφορίες φυλάσσονται σε συστήματα ΤΠΕ.

Πεδίο εφαρμογής

7. Οι παρούσες κατευθυντήριες γραμμές εφαρμόζονται σε σχέση με τη διαχείριση των κινδύνων ΤΠΕ και ασφάλειας στα χρηματοοικονομικά ιδρύματα (όπως ορίζονται στην παράγραφο 9). Για τους σκοπούς των παρουσών κατευθυντήριων γραμμών, ο όρος «κίνδυνοι ΤΠΕ και ασφάλειας» καλύπτει τους «λειτουργικούς κινδύνους και κινδύνους ασφάλειας» ή «κινδύνους λειτουργίας και ασφάλειας» που αναφέρονται στο άρθρο 95 της PSD2 για την παροχή υπηρεσιών πληρωμών.

8. Όσον αφορά τους ΠΥΠ (όπως ορίζονται στην παράγραφο 9), οι παρούσες κατευθυντήριες γραμμές εφαρμόζονται στην παροχή εκ μέρους τους υπηρεσιών πληρωμών, σύμφωνα με το πεδίο εφαρμογής και την εντολή του άρθρου 95 της PSD2. Όσον αφορά τα ιδρύματα (όπως ορίζονται στην παράγραφο 9), οι παρούσες κατευθυντήριες γραμμές εφαρμόζονται στο σύνολο των δραστηριοτήτων που ασκούν.

Αποδέκτες

9. Οι παρούσες κατευθυντήριες γραμμές απευθύνονται στα χρηματοοικονομικά ιδρύματα, τα οποία για τους σκοπούς των παρουσών κατευθυντήριων γραμμών αναφέρονται (1) στους ΠΥΠ όπως ορίζονται στο άρθρο 4 παράγραφος 11 της PSD2 και (2) στα ιδρύματα, με την έννοια των πιστωτικών ιδρυμάτων και των επιχειρήσεων επενδύσεων όπως ορίζονται στο άρθρο 4

παράγραφος 1 σημείο 3 του κανονισμού (ΕΕ) αριθ. 575/2013. Οι κατευθυντήριες γραμμές ισχύουν επίσης για τις αρμόδιες αρχές όπως ορίζονται στο άρθρο 4 παράγραφος 1 σημείο 40 του κανονισμού (ΕΕ) αριθ. 575/2013, συμπεριλαμβανομένης της Ευρωπαϊκής Κεντρικής Τράπεζας σε ό,τι αφορά ζητήματα που σχετίζονται με τα καθήκοντα που της ανατίθενται βάσει του κανονισμού (ΕΕ) αριθ. 1024/2013, καθώς και για τις αρμόδιες αρχές βάσει της PSD2, όπως ορίζονται στο άρθρο 4 παράγραφος 2 σημείο i) του κανονισμού (ΕΕ) αριθ. 1093/2010.

Ορισμοί

10. Εκτός εάν προβλέπεται διαφορετικά, οι όροι που χρησιμοποιούνται και ορίζονται στην οδηγία 2013/36/ΕΕ (CRD), στον κανονισμό (ΕΕ) αριθ. 575/2013 (CRR) και στην οδηγία (ΕΕ) 2015/2366 (PSD2) έχουν την ίδια έννοια και στις κατευθυντήριες γραμμές. Επιπλέον, για τους σκοπούς των παρουσών κατευθυντήριων γραμμών ισχύουν οι ακόλουθοι ορισμοί:

Κίνδυνος ΤΠΕ και ασφάλειας	Κίνδυνος ζημίας λόγω παραβίασης της εμπιστευτικότητας, αστοχίας της ακεραιότητας συστημάτων και δεδομένων, ακαταλληλότητας ή μη διαθεσιμότητας συστημάτων και δεδομένων, ή αδυναμίας αλλαγής τεχνολογίας πληροφοριών (ΤΠ) εντός εύλογου χρονικού διαστήματος και με εύλογο κόστος όταν οι απαιτήσεις του περιβάλλοντος ή των επιχειρηματικών δραστηριοτήτων μεταβάλλονται (δηλ. ευελιξία)[2]. Στο πλαίσιο αυτό περιλαμβάνονται κίνδυνοι ασφάλειας που προκύπτουν λόγω ανεπάρκειας ή αστοχίας εσωτερικών διεργασιών ή εξωτερικών συμβάντων, μεταξύ των οποίων περιλαμβάνονται και οι επιθέσεις στον κυβερνοχώρο ή η ανεπαρκής υλική ασφάλεια.
Διοικητικό όργανο	α) Για τα πιστωτικά ιδρύματα και τις επιχειρήσεις επενδύσεων, ο όρος αυτός έχει την ίδια έννοια με τον ορισμό που παρατίθεται στο άρθρο 3 παράγραφος 1 σημείο 7 της οδηγίας 2013/36/ΕΕ. β) Για τα ιδρύματα πληρωμών ή ιδρύματα ηλεκτρονικού χρήματος, με τον όρο αυτόν νοούνται τα διευθυντικά στελέχη ή οι υπεύθυνοι για τη διαχείριση των ιδρυμάτων πληρωμών και των ιδρυμάτων ηλεκτρονικού χρήματος και, κατά περίπτωση, οι υπεύθυνοι για τη διαχείριση των δραστηριοτήτων υπηρεσιών πληρωμών των ιδρυμάτων πληρωμών και των ιδρυμάτων ηλεκτρονικού χρήματος. γ) Για τους ΠΥΠ που αναφέρονται στο άρθρο 1 παράγραφος 1 στοιχεία γ), ε) και στ) της οδηγίας (ΕΕ) 2015/2366, ο όρος αυτός έχει την έννοια που του αποδίδεται από την ισχύουσα ενωσιακή ή εθνική νομοθεσία.

[2] Ορισμός από τις κατευθυντήριες γραμμές της ΕΑΤ σχετικά με τις κοινές διαδικασίες και μεθόδους για τη διαδικασία εποπτικού ελέγχου και αξιολόγησης, της 19ης Δεκεμβρίου 2014 (EBA/GL/2014/13), όπως τροποποιήθηκαν με το έγγραφο EBA/GL/2018/03.

Περιστατικό λειτουργικού κινδύνου ή περιστατικό ασφάλειας	Μεμονωμένο συμβάν ή σειρά συνδεόμενων συμβάντων μη προγραμματισμένων από το χρηματοοικονομικό ίδρυμα, τα οποία έχουν ή ενδέχεται να έχουν δυσμενείς επιπτώσεις στην ακεραιότητα, τη διαθεσιμότητα, την εμπιστευτικότητα και/ή την αυθεντικότητα των υπηρεσιών.
Ανώτερα διοικητικά στελέχη	α) Για τα πιστωτικά ιδρύματα και τις επιχειρήσεις επενδύσεων, ο όρος αυτός έχει την ίδια έννοια με τον ορισμό που παρατίθεται στο άρθρο 3 παράγραφος 1 σημείο 9 της οδηγίας 2013/36/ΕΕ. β) Για τα ιδρύματα πληρωμών και τα ιδρύματα ηλεκτρονικού χρήματος, με τον όρο αυτόν νοούνται τα φυσικά πρόσωπα που ασκούν εκτελεστικά καθήκοντα σε ίδρυμα και τα οποία είναι υπεύθυνα και λογοδοτούν στο διοικητικό όργανο για την καθημερινή διοίκηση του ιδρύματος. γ) Για τους ΠΥΠ που αναφέρονται στο άρθρο 1 παράγραφος 1 στοιχεία γ), ε) και στ) της οδηγίας (ΕΕ) 2015/2366, ο όρος αυτός έχει την έννοια που του αποδίδεται από την ισχύουσα ενωσιακή ή εθνική νομοθεσία.
Διάθεση ανάληψης κινδύνου	Το συγκεντρωτικό επίπεδο και τα είδη των κινδύνων που είναι πρόθυμοι να αναλάβουν οι ΠΥΠ και τα ιδρύματα στο πλαίσιο της ικανότητάς τους για ανάληψη κινδύνων, και σύμφωνα με το επιχειρηματικό τους μοντέλο, προκειμένου να επιτύχουν τους στρατηγικούς στόχους τους.
Λειτουργία εσωτερικού ελέγχου	α) Για τα πιστωτικά ιδρύματα και τις επιχειρήσεις επενδύσεων, η λειτουργία εσωτερικού ελέγχου ορίζεται όπως αναφέρεται στην ενότητα 22 των κατευθυντήριων γραμμών της ΕΑΤ σχετικά με την εσωτερική διακυβέρνηση (EBA/GL/2017/11). β) Για τους ΠΥΠ που δεν είναι πιστωτικά ιδρύματα, η λειτουργία εσωτερικού ελέγχου πρέπει να είναι λειτουργικά ανεξάρτητη από τον ΠΥΠ ή εντός αυτού, και μπορεί να αποτελεί λειτουργία εσωτερικών και/ή εξωτερικών ελεγκτών.
Έργα ΤΠΕ	Κάθε έργο, ή μέρος έργου, στο πλαίσιο του οποίου αλλάζουν, αντικαθίστανται, καταργούνται ή εφαρμόζονται συστήματα ΤΠΕ. Τα έργα ΤΠΕ μπορούν να αποτελούν μέρος ευρύτερων προγραμμάτων ΤΠΕ ή μετασχηματισμού επιχειρήσεων.
Τρίτος	Οργανισμός ο οποίος έχει συνάψει επιχειρηματικές σχέσεις ή συμβάσεις με οντότητα για την παροχή προϊόντος ή υπηρεσίας[3].
Πληροφοριακός πόρος	Συλλογή πληροφοριών, είτε υλικών είτε άυλων, που αξίζει να προστατεύονται.
Πόρος ΤΠΕ	Πόρος είτε λογισμικού είτε υλισμικού που απαντά στο επιχειρηματικό περιβάλλον.

[3] Ορισμός από τα θεμελιώδη στοιχεία της G7 για τη διαχείριση των κινδύνων του κυβερνοχώρου έναντι τρίτων στον χρηματοπιστωτικό τομέα.

Συστήματα ΤΠΕ[4]	Εγκατάσταση ΤΠΕ ως μέρος ενός μηχανισμού ή ενός δικτύου διασύνδεσης το οποίο υποστηρίζει τις λειτουργίες ενός χρηματοοικονομικού ιδρύματος.
Υπηρεσίες ΤΠΕ[5]	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.

Εφαρμογή

Ημερομηνία εφαρμογής

11. Οι παρούσες κατευθυντήριες γραμμές εφαρμόζονται από την 30ή Ιουνίου 2020.

Κατάργηση

12. Οι κατευθυντήριες γραμμές σχετικά με τα μέτρα ασφάλειας για τους λειτουργικούς κινδύνους και τους κινδύνους ασφάλειας (EBA/GL/2017/17) που εκδόθηκαν το 2017 θα καταργηθούν από τις παρούσες κατευθυντήριες γραμμές κατά την ημερομηνία έναρξης εφαρμογής των παρουσών κατευθυντήριων γραμμών.

Κατευθυντήριες γραμμές σχετικά με τη διαχείριση κινδύνων ΤΠΕ και ασφάλειας

1.1. Αναλογικότητα

1. Όλα τα χρηματοοικονομικά ιδρύματα θα πρέπει να συμμορφώνονται με τις διατάξεις που προβλέπονται στις παρούσες κατευθυντήριες γραμμές με τρόπο αναλογικό και λαμβάνοντας υπόψη το μέγεθος των χρηματοοικονομικών ιδρυμάτων, την εσωτερική τους οργάνωση, καθώς και τη φύση, την κλίμακα, την πολυπλοκότητα και τον βαθμό επικινδυνότητας των υπηρεσιών και των προϊόντων που παρέχουν ή προτίθενται να παρέχουν τα χρηματοοικονομικά ιδρύματα.

[4] Ορισμός από τις κατευθυντήριες γραμμές σχετικά με την αξιολόγηση κινδύνων ΤΠΕ σύμφωνα με τη διαδικασία εποπτικού ελέγχου και αξιολόγησης (ΔΕΕΑ) (EBA/GL/ 2017/05).
[5] Στο ίδιο.

1.2. Διακυβέρνηση και στρατηγική

1.2.1. Διακυβέρνηση

2. Το διοικητικό όργανο θα πρέπει να διασφαλίζει ότι τα χρηματοοικονομικά ιδρύματα διαθέτουν επαρκές πλαίσιο εσωτερικής διακυβέρνησης και εσωτερικού ελέγχου για τους οικείους κινδύνους ΤΠΕ και ασφάλειας. Το διοικητικό όργανο θα πρέπει να καθορίζει σαφείς ρόλους και αρμοδιότητες για τα τμήματα ΤΠΕ, τη διαχείριση κινδύνων ασφάλειας πληροφοριών, καθώς και για την επιχειρησιακή συνέχεια, συμπεριλαμβανομένων και αυτών που αφορούν το ίδιο το διοικητικό όργανο και τις επιτροπές του.

3. Το διοικητικό όργανο θα πρέπει να μεριμνά ώστε ο αριθμός και οι δεξιότητες των μελών του προσωπικού των χρηματοοικονομικών ιδρυμάτων να επαρκούν για την υποστήριξη σε διαρκή βάση των λειτουργικών τους αναγκών στον τομέα των ΤΠΕ και των διεργασιών τους όσον αφορά τη διαχείριση των κινδύνων ΤΠΕ και ασφάλειας, καθώς και για τη διασφάλιση της εφαρμογής της οικείας στρατηγικής ΤΠΕ. Το διοικητικό όργανο θα πρέπει να διασφαλίζει ότι ο διαθέσιμος προϋπολογισμός είναι κατάλληλος για την εκπλήρωση των προαναφερόμενων υποχρεώσεων. Επιπλέον, τα χρηματοοικονομικά ιδρύματα θα πρέπει να μεριμνούν ώστε όλα τα μέλη του προσωπικού, συμπεριλαμβανομένων των προσώπων που κατέχουν καίριες θέσεις, να λαμβάνουν κατάλληλη κατάρτιση σχετικά με τους κινδύνους ΤΠΕ και ασφάλειας, μεταξύ άλλων και όσον αφορά την ασφάλεια πληροφοριών, σε ετήσια βάση ή συχνότερα, εάν απαιτείται (βλ. επίσης ενότητα 1.4.7).

4. Το διοικητικό όργανο υπέχει συνολική υποχρέωση λογοδοσίας για τον καθορισμό, την έγκριση και την επίβλεψη της εφαρμογής της στρατηγικής ΤΠΕ των χρηματοοικονομικών ιδρυμάτων στο πλαίσιο της συνολικής τους επιχειρηματικής στρατηγικής, καθώς και για τη δημιουργία αποτελεσματικού πλαισίου διαχείρισης κινδύνων για τους κινδύνους ΤΠΕ και ασφάλειας.

1.2.2. Στρατηγική

5. Η στρατηγική ΤΠΕ θα πρέπει να εναρμονίζεται με τη συνολική επιχειρηματική στρατηγική των χρηματοοικονομικών ιδρυμάτων και θα πρέπει να ορίζει τα εξής:

    α) τον τρόπο με τον οποίο θα πρέπει να εξελίσσεται η ΤΠΕ των χρηματοοικονομικών ιδρυμάτων ώστε να υποστηρίζει αποτελεσματικά την επιχειρηματική τους στρατηγική και να συμμετέχει σε αυτή, συμπεριλαμβανομένης της εξέλιξης της οργανωτικής δομής, των αλλαγών των συστημάτων ΤΠΕ και των κύριων αλληλεξαρτήσεων με τρίτους·

    β) την προγραμματισμένη στρατηγική και εξέλιξη της αρχιτεκτονικής της ΤΠΕ, συμπεριλαμβανομένων των αλληλεξαρτήσεων με τρίτους·

    γ) σαφείς στόχους ασφάλειας πληροφοριών, με ιδιαίτερη έμφαση στα συστήματα ΤΠΕ και στις υπηρεσίες, στο προσωπικό και στις διεργασίες ΤΠΕ.

6. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να καταρτίζουν σύνολα σχεδίων δράσης τα οποία περιέχουν τα μέτρα που πρέπει να λαμβάνονται για την επίτευξη του στόχου της στρατηγικής ΤΠΕ. Θα πρέπει να διαβιβάζονται σε όλα τα μέλη του αρμόδιου προσωπικού

(συμπεριλαμβανομένων των αναδόχων και των τρίτων παρόχων, κατά περίπτωση και όπου κρίνεται σκόπιμο). Τα σχέδια δράσης θα πρέπει να επανεξετάζονται σε περιοδική βάση ώστε να διασφαλίζεται η συνάφεια και η καταλληλότητά τους. Τα χρηματοοικονομικά ιδρύματα θα πρέπει επίσης να δημιουργούν διεργασίες για την παρακολούθηση και τη μέτρηση της αποτελεσματικότητας της εφαρμογής της οικείας στρατηγικής ΤΠΕ.

1.2.3. Χρήση τρίτων παρόχων

7. Με την επιφύλαξη των κατευθυντήριων γραμμών της ΕΑΤ σχετικά με την εξωτερική ανάθεση δραστηριοτήτων (EBA/GL/2019/02) και του άρθρου 19 της PSD2, τα χρηματοοικονομικά ιδρύματα θα πρέπει να διασφαλίζουν την αποτελεσματικότητα των μέτρων μείωσης των κινδύνων όπως ορίζονται από το οικείο πλαίσιο διαχείρισης κινδύνων, συμπεριλαμβανομένων των μέτρων που προβλέπονται στις παρούσες κατευθυντήριες γραμμές, σε περιπτώσεις εξωτερικής ανάθεσης λειτουργικών δραστηριοτήτων των υπηρεσιών πληρωμών και/ή των υπηρεσιών ΤΠΕ και των συστημάτων ΤΠΕ οποιασδήποτε δραστηριότητας, μεταξύ άλλων και σε οντότητες του ομίλου, ή σε περιπτώσεις χρήσης τρίτων.

8. Προκειμένου να διασφαλίζεται η συνέχεια των υπηρεσιών ΤΠΕ και των συστημάτων ΤΠΕ, τα χρηματοοικονομικά ιδρύματα θα πρέπει να μεριμνούν ώστε οι συμβάσεις και τα Συμβόλαια Διασφάλισης Επιπέδου Ποιότητας (τόσο υπό κανονικές συνθήκες όσο και σε περίπτωση διαταραχής των υπηρεσιών — βλ. επίσης ενότητα 1.7.2) που συνάπτονται με παρόχους (εξωτερικούς παρόχους, οντότητες ομίλου ή τρίτους παρόχους) να περιλαμβάνουν τα εξής:

   α) κατάλληλους και αναλογικούς στόχους και μέτρα που αφορούν την ασφάλεια πληροφοριών και περιλαμβάνουν απαιτήσεις όπως ελάχιστες απαιτήσεις ασφάλειας στον κυβερνοχώρο, προδιαγραφές του κύκλου ζωής των δεδομένων του χρηματοοικονομικού ιδρύματος, τυχόν απαιτήσεις σχετικά με την κρυπτογράφηση δεδομένων, διεργασίες ασφάλειας δικτύου και παρακολούθησης της ασφάλειας, καθώς και την τοποθεσία των μηχανογραφικών κέντρων ·

   β) διαδικασίες χειρισμού περιστατικών λειτουργικού κινδύνου και περιστατικών ασφάλειας, συμπεριλαμβανομένης της υποβολής εκθέσεων και της παραπομπής σε ανώτερη βαθμίδα της ιεραρχικής κλίμακας.

9. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να παρακολουθούν και να ζητούν διαβεβαίωση σχετικά με το επίπεδο συμμόρφωσης των εν λόγω προμηθευτών με τους αντικειμενικούς σκοπούς, τα μέτρα και τους στόχους επιδόσεων του χρηματοοικονομικού ιδρύματος όσον αφορά την ασφάλεια.

1.3. Πλαίσιο διαχείρισης κινδύνων ΤΠΕ και ασφάλειας

1.3.1. Οργάνωση και στόχοι

10. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να προσδιορίζουν και να διαχειρίζονται τους οικείους κινδύνους ΤΠΕ και ασφάλειας. Το τμήμα ή τα τμήματα ΤΠΕ που είναι αρμόδια για τα συστήματα ΤΠΕ, τις διεργασίες και τις λειτουργίες ασφάλειας θα πρέπει να διαθέτουν κατάλληλες διαδικασίες και ελέγχους, ώστε να διασφαλίζεται τόσο ο προσδιορισμός, η

ανάλυση, η μέτρηση, η παρακολούθηση, η διαχείριση, η αναφορά και η διατήρηση όλων των κινδύνων εντός των ορίων της διάθεσης ανάληψης κινδύνου του χρηματοοικονομικού ιδρύματος όσο και η συμμόρφωση των έργων και των συστημάτων που παραδίδουν, καθώς και των δραστηριοτήτων που ασκούν, με τις εξωτερικές και εσωτερικές απαιτήσεις.

11. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να αναθέτουν την ευθύνη για τη διαχείριση και την επίβλεψη των κινδύνων ΤΠΕ και ασφάλειας σε μία λειτουργία ελέγχου, τηρώντας τις απαιτήσεις της ενότητας 19 των κατευθυντήριων γραμμών της ΕΑΤ σχετικά με την εσωτερική διακυβέρνηση (EBA/GL/2017/11). Τα χρηματοοικονομικά ιδρύματα θα πρέπει να διασφαλίζουν την ανεξαρτησία και την αντικειμενικότητα της εν λόγω λειτουργίας ελέγχου, διαχωρίζοντάς την δεόντως από τις διεργασίες των λειτουργιών ΤΠΕ. Αυτή η λειτουργία ελέγχου θα πρέπει να λογοδοτεί απευθείας στο διοικητικό όργανο και να είναι υπεύθυνη για την παρακολούθηση και τον έλεγχο της τήρησης του πλαισίου διαχείρισης κινδύνων ΤΠΕ και ασφάλειας. Θα πρέπει να διασφαλίζει τον προσδιορισμό, τη μέτρηση, την αξιολόγηση, τη διαχείριση, την παρακολούθηση και την αναφορά των κινδύνων ΤΠΕ και ασφάλειας. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να μεριμνούν ώστε η συγκεκριμένη λειτουργία ελέγχου να μην είναι υπεύθυνη για τη διενέργεια οποιουδήποτε εσωτερικού ελέγχου.

    Η λειτουργία εσωτερικού ελέγχου θα πρέπει, εφαρμόζοντας μια προσέγγιση βάσει κινδύνου, να έχει την ικανότητα να προβαίνει σε ανεξάρτητη αξιολόγηση και να παρέχει αντικειμενική διαβεβαίωση όσον αφορά τη συμμόρφωση όλων των δραστηριοτήτων και των μονάδων του χρηματοοικονομικού ιδρύματος που αφορούν την ΤΠΕ και την ασφάλεια με τις πολιτικές και τις διαδικασίες του χρηματοοικονομικού ιδρύματος, καθώς και με τις εξωτερικές απαιτήσεις, τηρώντας τις απαιτήσεις της ενότητας 22 των κατευθυντήριων γραμμών της ΕΑΤ σχετικά με την εσωτερική διακυβέρνηση (EBA/GL/2017/11).

12. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να ορίζουν και να αναθέτουν τους κύριους ρόλους και αρμοδιότητες, καθώς και τις σχετικές γραμμές αναφοράς που απαιτούνται για να είναι αποτελεσματικό το πλαίσιο διαχείρισης κινδύνων ΤΠΕ και ασφάλειας. Το πλαίσιο αυτό θα πρέπει να εντάσσεται πλήρως στις συνολικές διεργασίες διαχείρισης κινδύνων των χρηματοοικονομικών ιδρυμάτων, καθώς και να εναρμονίζεται απόλυτα με αυτές.

13. Το πλαίσιο διαχείρισης κινδύνων ΤΠΕ και ασφάλειας θα πρέπει να περιλαμβάνει την εφαρμογή διεργασιών με στόχο:

    α) τον καθορισμό της διάθεσης ανάληψης κινδύνου όσον αφορά τους κινδύνους ΤΠΕ και ασφάλειας, σύμφωνα με τη διάθεση ανάληψης κινδύνου του χρηματοοικονομικού ιδρύματος·
    β) τον προσδιορισμό και την αξιολόγηση των κινδύνων ΤΠΕ και ασφάλειας στους οποίους εκτίθεται ένα χρηματοοικονομικό ίδρυμα·
    γ) τον καθορισμό μέτρων μείωσης των κινδύνων, συμπεριλαμβανομένης της εφαρμογής δικλείδων ασφαλείας, για τη μείωση των κινδύνων ΤΠΕ και ασφάλειας·
    δ) την παρακολούθηση της αποτελεσματικότητας των εν λόγω μέτρων, καθώς και του αριθμού των αναφερόμενων περιστατικών, συμπεριλαμβανομένων —όσον αφορά τους ΠΥΠ— των περιστατικών που αναφέρονται σύμφωνα με το άρθρο 96 της PSD2 και

επηρεάζουν τις σχετικές με την ΤΠΕ δραστηριότητες, και την ανάληψη δράσης για τη διόρθωση των μέτρων όπου κρίνεται αναγκαίο·

ε) την υποβολή αναφορών στο διοικητικό όργανο όσον αφορά τους κινδύνους ΤΠΕ και ασφάλειας και τις αντίστοιχες δικλείδες ασφαλείας·

στ) τον προσδιορισμό και τη διερεύνηση της παρουσίας τυχόν κινδύνων ΤΠΕ και ασφάλειας που προκύπτουν από οποιαδήποτε μείζονα αλλαγή στο σύστημα ΤΠΕ ή στις υπηρεσίες, τις διεργασίες ή τις διαδικασίες ΤΠΕ και/ή έπειτα από κάθε σημαντικό περιστατικό λειτουργικού κινδύνου ή περιστατικό ασφάλειας.

14. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να μεριμνούν ώστε το πλαίσιο διαχείρισης κινδύνων ΤΠΕ και ασφάλειας να τεκμηριώνεται, καθώς και να βελτιώνεται διαρκώς, με βάση τα «διδάγματα που αντλούνται» κατά την εφαρμογή και την παρακολούθησή του. Το πλαίσιο διαχείρισης κινδύνων ΤΠΕ και ασφάλειας θα πρέπει να εγκρίνεται και να επανεξετάζεται, τουλάχιστον μία φορά ετησίως, από το διοικητικό όργανο.

1.3.2. Προσδιορισμός λειτουργιών, διεργασιών και πόρων

15. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να προσδιορίζουν, να καταρτίζουν και να επικαιροποιούν τη χαρτογράφηση των επιχειρηματικών τους λειτουργιών, ρόλων και υποστηρικτικών διεργασιών ώστε να προσδιορίζεται η σημασία κάθε επιμέρους λειτουργίας, ρόλου και υποστηρικτικής διεργασίας, καθώς και των αλληλεξαρτήσεών τους, σε σχέση με τους κινδύνους ΤΠΕ και ασφάλειας.

16. Επιπλέον, τα χρηματοοικονομικά ιδρύματα θα πρέπει να προσδιορίζουν, να καταρτίζουν και να επικαιροποιούν τη χαρτογράφηση των πληροφοριακών πόρων που υποστηρίζουν τις επιχειρηματικές τους λειτουργίες και υποστηρικτικές διεργασίες, για παράδειγμα των συστημάτων ΤΠΕ, του προσωπικού, των αναδόχων, τρίτων μερών καθώς και των διασυνδέσεων με άλλα εσωτερικά και εξωτερικά συστήματα και διεργασίες προκειμένου να είναι σε θέση, τουλάχιστον, να διαχειρίζονται τους πληροφοριακούς πόρους που υποστηρίζουν τις κρίσιμες επιχειρηματικές λειτουργίες και διεργασίες τους.

1.3.3. Κατηγοριοποίηση και αξιολόγηση κινδύνων

17. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να κατηγοριοποιούν τις επιχειρηματικές λειτουργίες, τις υποστηρικτικές διεργασίες και τους πληροφοριακούς πόρους που αναφέρονται στις παραγράφους 15 και 16 βάσει της κρισιμότητάς τους.

18. Για τον καθορισμό της κρισιμότητας των εν λόγω προσδιοριζόμενων επιχειρηματικών λειτουργιών, υποστηρικτικών διεργασιών και πληροφοριακών πόρων, τα χρηματοοικονομικά ιδρύματα θα πρέπει, κατ’ ελάχιστον, να λαμβάνουν υπόψη τις απαιτήσεις εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας. Θα πρέπει να ανατίθενται σαφώς καθήκοντα λογοδοσίας και ευθύνης για τους πληροφοριακούς πόρους.

19. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να επανεξετάζουν την επάρκεια της κατηγοριοποίησης των πληροφοριακών πόρων και της σχετικής τεκμηρίωσης κατά τη διενέργεια της αξιολόγησης κινδύνων.

20. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να προσδιορίζουν τους κινδύνους ΤΠΕ και ασφάλειας που έχουν αντίκτυπο στις επιχειρηματικές λειτουργίες, στις υποστηρικτικές διεργασίες και στους πληροφοριακούς πόρους που προσδιορίζονται και κατηγοριοποιούνται βάσει της κρισιμότητάς τους. Η αξιολόγηση κινδύνων θα πρέπει να διενεργείται και να τεκμηριώνεται σε ετήσια βάση ή σε βραχύτερα διαστήματα εάν απαιτείται. Οι εν λόγω αξιολογήσεις κινδύνων θα πρέπει επίσης να διενεργούνται σε περίπτωση τυχόν μείζονος αλλαγής στην υποδομή, τις διεργασίες ή τις διαδικασίες που επηρεάζουν τις επιχειρηματικές λειτουργίες, τις υποστηρικτικές διεργασίες ή τους πληροφοριακούς πόρους και, ως εκ τούτου, η τρέχουσα αξιολόγηση κινδύνων των χρηματοοικονομικών ιδρυμάτων θα πρέπει να επικαιροποιείται.

21. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να διασφαλίζουν τη συνεχή παρακολούθηση των απειλών και ευπαθειών που αφορούν τις επιχειρηματικές λειτουργίες, τις υποστηρικτικές διεργασίες και τους πληροφοριακούς πόρους τους, ενώ επίσης θα πρέπει να επανεξετάζουν τακτικά τα σενάρια κινδύνων που τα επηρεάζουν.

1.3.4. Μείωση των κινδύνων

22. Βάσει των αξιολογήσεων κινδύνων, τα χρηματοοικονομικά ιδρύματα θα πρέπει να καθορίζουν τα μέτρα που απαιτούνται για τη μείωση των προσδιοριζόμενων κινδύνων ΤΠΕ και ασφάλειας σε αποδεκτά επίπεδα, καθώς και να προσδιορίζουν κατά πόσον απαιτούνται αλλαγές στις υφιστάμενες επιχειρηματικές διεργασίες, στα μέτρα ελέγχου, στα συστήματα ΤΠΕ και στις υπηρεσίες ΤΠΕ. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να λαμβάνουν υπόψη τον χρόνο που απαιτείται για την εφαρμογή των εν λόγω αλλαγών και τον χρόνο λήψης κατάλληλων προσωρινών μέτρων μείωσης των κινδύνων για να ελαχιστοποιήσουν τους κινδύνους ΤΠΕ και ασφάλειας, ώστε να παραμείνουν εντός των ορίων της διάθεσης ανάληψης κινδύνων ΤΠΕ και ασφάλειας του εκάστοτε χρηματοοικονομικού ιδρύματος.

23. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να καθορίζουν και να εφαρμόζουν μέτρα για τη μείωση των προσδιοριζόμενων κινδύνων ΤΠΕ και ασφάλειας και για την προστασία των πληροφοριακών πόρων βάσει της κατηγοριοποίησής τους.

1.3.5. Υποβολή εκθέσεων

24. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να υποβάλλουν σαφώς και εγκαίρως στο διοικητικό όργανο εκθέσεις σχετικά με τα αποτελέσματα της αξιολόγησης κινδύνων. Οι εν λόγω εκθέσεις υποβάλλονται με την επιφύλαξη της υποχρέωσης των ΠΥΠ να παρέχουν στις αρμόδιες αρχές επικαιροποιημένη και ολοκληρωμένη αξιολόγηση κινδύνων, όπως προβλέπεται στο άρθρο 95 παράγραφος 2 της οδηγίας (ΕΕ) 2015/2366.

1.3.6. Εσωτερικός έλεγχος

25. Η διακυβέρνηση, τα συστήματα και οι διεργασίες ενός χρηματοοικονομικού ιδρύματος ως προς τους οικείους κινδύνους ΤΠΕ και ασφάλειας θα πρέπει να υποβάλλονται σε διαδικασία εσωτερικού ελέγχου σε περιοδική βάση, που διενεργείται από ελεγκτές οι οποίοι διαθέτουν επαρκείς γνώσεις, δεξιότητες και εξειδίκευση σε θέματα κινδύνων ΤΠΕ και ασφάλειας καθώς

και σε θέματα πληρωμών (για τους ΠΥΠ), ώστε να παρέχεται στο διοικητικό όργανο ανεξάρτητη διαβεβαίωση όσον αφορά την αποτελεσματικότητά τους. Οι ελεγκτές θα πρέπει να είναι ανεξάρτητοι εσωτερικοί ή εξωτερικοί ελεγκτές του χρηματοοικονομικού ιδρύματος. Για τον προσδιορισμό της συχνότητας και του σημείου εστίασης των εν λόγω ελέγχων θα πρέπει να συνεκτιμώνται οι αντίστοιχοι κίνδυνοι ΤΠΕ και ασφάλειας.

26. Το διοικητικό όργανο του χρηματοοικονομικού ιδρύματος θα πρέπει να εγκρίνει το σχέδιο ελέγχου, συμπεριλαμβανομένων τυχόν ελέγχων ΤΠΕ και κάθε πιθανής σημαντικής τροποποίησής του. Το σχέδιο ελέγχου και η εκτέλεσή του, συμπεριλαμβανομένης της συχνότητας των ελέγχων, θα πρέπει να αντικατοπτρίζει και να είναι ανάλογο προς τους εγγενείς κινδύνους ΤΠΕ και ασφάλειας του χρηματοοικονομικού ιδρύματος και θα πρέπει να επικαιροποιείται ανά τακτά χρονικά διαστήματα.

27. Θα πρέπει να δημιουργηθεί επίσημη διαδικασία παρακολούθησης η οποία θα περιλαμβάνει διατάξεις για την έγκαιρη επαλήθευση και αποκατάσταση κρίσιμων ευρημάτων ελέγχου ΤΠΕ.

1.4. Ασφάλεια πληροφοριών

1.4.1. Πολιτική ασφάλειας πληροφοριών

28. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να αναπτύσσουν και να τεκμηριώνουν πολιτική ασφάλειας πληροφοριών στην οποία θα πρέπει να καθορίζονται οι αρχές και οι κανόνες υψηλού επιπέδου για την προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων και των πληροφοριών των χρηματοοικονομικών ιδρυμάτων και των πελατών τους. Όσον αφορά τους ΠΥΠ, η πολιτική αυτή προσδιορίζεται στο έγγραφο που περιγράφει την πολιτική ασφάλειας, το οποίο πρέπει να εγκρίνεται σύμφωνα με το άρθρο 5 παράγραφος 1 στοιχείο ι) της οδηγίας (ΕΕ) 2015/2366. Η πολιτική ασφάλειας πληροφοριών θα πρέπει να συνάδει με τους στόχους της ασφάλειας πληροφοριών του χρηματοοικονομικού ιδρύματος και να βασίζεται στα σχετικά αποτελέσματα της διαδικασίας αξιολόγησης κινδύνων. Η πολιτική θα πρέπει να εγκρίνεται από το διοικητικό όργανο.

29. Η πολιτική θα πρέπει να περιλαμβάνει περιγραφή των κύριων ρόλων και αρμοδιοτήτων της διαχείρισης ασφάλειας πληροφοριών και θα πρέπει να καθορίζει τις απαιτήσεις για το προσωπικό και τους αναδόχους, τις διεργασίες και την τεχνολογία σε σχέση με την ασφάλεια πληροφοριών, αναγνωρίζοντας ότι το προσωπικό και οι ανάδοχοι σε όλα τα επίπεδα έχουν ευθύνες όσον αφορά τη διασφάλιση της ασφάλειας πληροφοριών των χρηματοοικονομικών ιδρυμάτων. Η πολιτική θα πρέπει να διασφαλίζει την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των κρίσιμων λογικών και υλικών περιουσιακών στοιχείων, των πόρων, καθώς και των ευαίσθητων δεδομένων των χρηματοοικονομικών ιδρυμάτων τόσο όταν τα στοιχεία αυτά τελούν σε κατάσταση αποθήκευσης, όσο και όταν βρίσκονται σε κατάσταση διαβίβασης ή χρήσης. Η πολιτική ασφάλειας πληροφοριών θα πρέπει να κοινοποιείται στο σύνολο των μελών του προσωπικού και των αναδόχων του χρηματοοικονομικού ιδρύματος.

30. Βάσει της πολιτικής ασφάλειας πληροφοριών, τα χρηματοοικονομικά ιδρύματα θα πρέπει να θεσπίζουν και να εφαρμόζουν μέτρα ασφάλειας για τη μείωση των κινδύνων ΤΠΕ και ασφάλειας στους οποίους εκτίθενται. Τα μέτρα αυτά θα πρέπει να περιλαμβάνουν:

α) την οργάνωση και τη διακυβέρνηση σύμφωνα με τις παραγράφους 10 και 11·
β) τη λογική ασφάλεια (ενότητα 1.4.2)·
γ) τη φυσική ασφάλεια (ενότητα 1.4.3)·
δ) την ασφάλεια των λειτουργιών ΤΠΕ (ενότητα 1.4.4)·
ε) την παρακολούθηση της ασφάλειας (ενότητα 1.4.5)·
στ) επανεξετάσεις, αξιολογήσεις και δοκιμές της ασφάλειας πληροφοριών (ενότητα 1.4.6)·
ζ) κατάρτιση και ευαισθητοποίηση σε θέματα ασφάλειας πληροφοριών (ενότητα 1.4.7).

1.4.2. Λογική ασφάλεια

31. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να καθορίζουν, να τεκμηριώνουν και να εφαρμόζουν διαδικασίες για τον έλεγχο της λογικής πρόσβασης (διαχείριση ταυτότητας και πρόσβασης). Οι διαδικασίες αυτές θα πρέπει να εφαρμόζονται, να επιβάλλονται, να παρακολουθούνται και να επανεξετάζονται σε περιοδική βάση. Οι διαδικασίες θα πρέπει επίσης να περιλαμβάνουν ελέγχους για την παρακολούθηση ασυνήθιστων ενεργειών. Σε περίπτωση που ο όρος «χρήστης» περιλαμβάνει επίσης τεχνικούς χρήστες, στο πλαίσιο των εν λόγω διαδικασιών θα πρέπει να εφαρμόζονται, κατ' ελάχιστον, τα ακόλουθα στοιχεία:

α) **Ελάχιστη απαιτούμενη πληροφόρηση, ελάχιστα προνόμια και διαχωρισμός καθηκόντων:** τα χρηματοοικονομικά ιδρύματα θα πρέπει να διαχειρίζονται τα δικαιώματα πρόσβασης σε πληροφοριακούς πόρους και τα υποστηρικτικά συστήματά τους βάσει της αρχής της «ελάχιστης απαιτούμενης πληροφόρησης», συμπεριλαμβανομένης της απομακρυσμένης πρόσβασης. Στους χρήστες θα πρέπει να χορηγούνται ελάχιστα δικαιώματα πρόσβασης τα οποία είναι απολύτως απαραίτητα για την εκτέλεση των καθηκόντων τους (αρχή των «ελάχιστων προνομίων»), δηλαδή θα πρέπει να αποτρέπεται η αδικαιολόγητη πρόσβαση σε μεγάλο σύνολο δεδομένων ή να αποτρέπεται η χορήγηση συνδυασμένων δικαιωμάτων πρόσβασης που θα μπορούσαν να χρησιμοποιηθούν για την παράκαμψη ελέγχων (αρχή του «διαχωρισμού των καθηκόντων»).
β) **Λογοδοσία χρήστη:** τα χρηματοοικονομικά ιδρύματα θα πρέπει να περιορίζουν, στο μέτρο του δυνατού, τη χρήση γενικών και κοινών λογαριασμών χρηστών και να διασφαλίζουν τη δυνατότητα ταυτοποίησης των χρηστών για τις ενέργειες που πραγματοποιούνται στα συστήματα ΤΠΕ.
γ) **Δικαιώματα διαβαθμισμένης πρόσβασης:** τα χρηματοοικονομικά ιδρύματα θα πρέπει να εφαρμόζουν ισχυρούς μηχανισμούς ελέγχου για τη διαβαθμισμένη πρόσβαση στα συστήματά τους, περιορίζοντας αυστηρά την πρόσβαση και παρακολουθώντας επισταμένως τους λογαριασμούς με αυξημένα δικαιώματα πρόσβασης στα συστήματα (π.χ. λογαριασμούς διαχειριστών). Για την εξασφάλιση ασφαλούς επικοινωνίας και τη μείωση του κινδύνου, η απομακρυσμένη διοικητική πρόσβαση σε κρίσιμα συστήματα ΤΠΕ θα πρέπει να επιτρέπεται μόνο με βάση την αρχή της ελάχιστης απαιτούμενης πληροφόρησης και εφόσον χρησιμοποιούνται διαδικασίες αυστηρής αυθεντικοποίησης.

δ) **Καταγραφή της δραστηριότητας των χρηστών:** κατ' ελάχιστον, θα πρέπει να καταγράφονται και να παρακολουθούνται όλες οι δραστηριότητες των προνομιούχων χρηστών. Τα αρχεία καταγραφής πρόσβασης θα πρέπει να προστατεύονται από μη εξουσιοδοτημένη τροποποίηση ή διαγραφή και να διατηρούνται για χρονικό διάστημα ανάλογο της κρισιμότητας των επιχειρηματικών λειτουργιών, των υποστηρικτικών διεργασιών και των πληροφοριακών πόρων που έχουν προσδιοριστεί, σύμφωνα με την ενότητα 1.3.3, με την επιφύλαξη των απαιτήσεων διατήρησης που προβλέπονται στο ενωσιακό και στο εθνικό δίκαιο. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να χρησιμοποιούν τις εν λόγω πληροφορίες για να διευκολύνουν την αναγνώριση και τη διερεύνηση ασυνήθιστων δραστηριοτήτων που έχουν εντοπιστεί κατά την παροχή υπηρεσιών.

ε) **Διαχείριση πρόσβασης:** τα δικαιώματα πρόσβασης θα πρέπει να χορηγούνται, να ανακαλούνται ή να τροποποιούνται εγκαίρως, σύμφωνα με ροές εργασίας έγκρισης που έχουν προκαθοριστεί και στις οποίες συμμετέχει ο επιχειρηματικός ιδιοκτήτης των πληροφοριών που αποτελούν αντικείμενο πρόσβασης (ιδιοκτήτης πληροφοριακών πόρων). Σε περίπτωση λύσης της υπαλληλικής σχέσης, τα δικαιώματα πρόσβασης θα πρέπει να ανακαλούνται αμέσως.

στ) **Επανεξέταση πρόσβασης:** τα δικαιώματα πρόσβασης θα πρέπει να επανεξετάζονται σε περιοδική βάση ώστε να διασφαλίζεται ότι οι χρήστες δεν διαθέτουν υπερβολικά προνόμια και ότι τα δικαιώματα πρόσβασης ανακαλούνται όταν δεν είναι πλέον απαραίτητα.

ζ) **Μέθοδοι αυθεντικοποίησης:** τα χρηματοοικονομικά ιδρύματα θα πρέπει να επιβάλλουν μεθόδους αυθεντικοποίησης οι οποίες χαρακτηρίζονται από επαρκές επίπεδο αξιοπιστίας ώστε να διασφαλίζεται με κατάλληλο και αποτελεσματικό τρόπο η συμμόρφωση προς τις πολιτικές και τις διαδικασίες ελέγχου της πρόσβασης. Οι μέθοδοι αυθεντικοποίησης θα πρέπει να είναι ανάλογες προς τον βαθμό κρισιμότητας των συστημάτων ΤΠΕ, των πληροφοριών ή των διεργασιών που αποτελούν αντικείμενο πρόσβασης. Στο πλαίσιο αυτό θα πρέπει να περιλαμβάνονται, κατ' ελάχιστον, σύνθετοι κωδικοί πρόσβασης ή ισχυρότερες μέθοδοι αυθεντικοποίησης (όπως η αυθεντικοποίηση δύο παραγόντων), βάσει του αντίστοιχου κινδύνου.

32. Η ηλεκτρονική πρόσβαση από εφαρμογές σε δεδομένα και συστήματα ΤΠΕ θα πρέπει να περιορίζεται στο ελάχιστο επίπεδο που απαιτείται για την παροχή της αντίστοιχης υπηρεσίας.

1.4.3. Φυσική ασφάλεια

33. Τα μέτρα φυσικής ασφάλειας των χρηματοοικονομικών ιδρυμάτων θα πρέπει να καθορίζονται, να τεκμηριώνονται και να εφαρμόζονται για την προστασία των εγκαταστάσεων, των μηχανογραφικών κέντρων και των ευαίσθητων χώρων τους από μη εξουσιοδοτημένη πρόσβαση και από περιβαλλοντικούς κινδύνους.

34. Η φυσική πρόσβαση σε συστήματα ΤΠΕ θα πρέπει να επιτρέπεται μόνο σε εξουσιοδοτημένα άτομα. Η εξουσιοδότηση θα πρέπει να παρέχεται ανάλογα με τα καθήκοντα και τις αρμοδιότητες του ατόμου, και να περιορίζεται σε άτομα που υποβάλλονται σε κατάλληλη κατάρτιση και παρακολούθηση. Η φυσική πρόσβαση θα πρέπει να επανεξετάζεται σε

περιοδική βάση ώστε να διασφαλίζεται η άμεση ανάκληση μη αναγκαίων δικαιωμάτων πρόσβασης όταν αυτά δεν είναι απαραίτητα.

35. Τα ενδεδειγμένα μέτρα για την προστασία από περιβαλλοντικούς κινδύνους θα πρέπει να είναι ανάλογα προς τη σημασία των κτιρίων και την κρισιμότητα των λειτουργιών ή των συστημάτων ΤΠΕ που βρίσκονται στα εν λόγω κτίρια.

1.4.4. Ασφάλεια λειτουργιών ΤΠΕ

36. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να εφαρμόζουν διαδικασίες για την πρόληψη της εμφάνισης ζητημάτων ασφάλειας στα συστήματα ΤΠΕ και στις υπηρεσίες ΤΠΕ, ενώ θα πρέπει επίσης να ελαχιστοποιούν τις επιπτώσεις τους στην παροχή υπηρεσιών ΤΠΕ. Στις διαδικασίες αυτές θα πρέπει να περιλαμβάνονται τα ακόλουθα μέτρα:

    α) εντοπισμός πιθανών ευπαθειών, οι οποίες θα πρέπει να αξιολογούνται και να αποκαθίστανται διασφαλίζοντας ότι το λογισμικό και το υλικολογισμικό είναι ενημερωμένα, συμπεριλαμβανομένου του λογισμικού που παρέχουν τα χρηματοοικονομικά ιδρύματα στους εσωτερικούς και τους εξωτερικούς χρήστες τους, εγκαθιστώντας κρίσιμες ενημερώσεις ασφάλειας ή εφαρμόζοντας αντισταθμιστικούς ελέγχους·
    β) εφαρμογή βασικών γραμμών ασφαλούς παραμετροποίησης δικτυακών στοιχείων·
    γ) υλοποίηση κατάτμησης δικτύου (network segmentation), συστημάτων πρόληψης απώλειας δεδομένων και κρυπτογράφηση της κίνησης του δικτύου (σύμφωνα με την κατηγοριοποίηση των δεδομένων)·
    δ) εφαρμογή της προστασίας των ακραίων σημείων, συμπεριλαμβανομένων διακομιστών, σταθμών εργασίας και φορητών συσκευών· τα χρηματοοικονομικά ιδρύματα θα πρέπει να αξιολογούν αν τα τελικά σημεία πληρούν τα πρότυπα ασφάλειας τα οποία ορίζουν τα ίδια τα ιδρύματα πριν χορηγήσουν σε αυτά πρόσβαση στο εταιρικό δίκτυο·
    ε) εξασφάλιση της εφαρμογής μηχανισμών για την επαλήθευση της ακεραιότητας του λογισμικού, του υλικολογισμικού και των δεδομένων·
    στ) κρυπτογράφηση των δεδομένων όταν τελούν σε κατάσταση αποθήκευσης και διαβίβασης (σύμφωνα με την κατηγοριοποίηση των δεδομένων).

37. Επιπλέον, τα χρηματοοικονομικά ιδρύματα θα πρέπει, σε συνεχή βάση, να προσδιορίζουν αν οι αλλαγές στο υφιστάμενο λειτουργικό περιβάλλον επηρεάζουν τα ισχύοντα μέτρα ασφάλειας ή απαιτούν τη θέσπιση πρόσθετων μέτρων για τη δέουσα μείωση των σχετικών κινδύνων. Οι αλλαγές αυτές θα πρέπει να αποτελούν μέρος της επίσημης διαδικασίας διαχείρισης αλλαγών που εφαρμόζεται από τα χρηματοοικονομικά ιδρύματα και η οποία θα πρέπει να διασφαλίζει ότι οι αλλαγές προγραμματίζονται, υποβάλλονται σε δοκιμές, τεκμηριώνονται, εγκρίνονται και υλοποιούνται δεόντως.

1.4.5. Παρακολούθηση της ασφάλειας

38. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να αναπτύσσουν και να εφαρμόζουν πολιτικές και διαδικασίες για τον εντοπισμό ασυνήθιστων δραστηριοτήτων με ενδεχόμενο αντίκτυπο στην

ασφάλεια των πληροφοριών των χρηματοοικονομικών ιδρυμάτων και να αντιμετωπίζουν αυτά τα συμβάντα δεόντως. Στο πλαίσιο αυτής της συνεχούς παρακολούθησης, τα χρηματοοικονομικά ιδρύματα θα πρέπει να διαθέτουν κατάλληλες και αποτελεσματικές δυνατότητες για τον εντοπισμό και την αναφορά φυσικής ή λογικής παρείσφρησης καθώς και παραβιάσεων της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριακών πόρων. Οι διεργασίες συνεχούς παρακολούθησης και εντοπισμού θα πρέπει να καλύπτουν:

α) συναφείς εσωτερικούς και εξωτερικούς παράγοντες, συμπεριλαμβανομένων διαχειριστικών λειτουργιών που καλύπτουν τόσο επιχειρηματικές ανάγκες όσο και ΤΠΕ·
β) συναλλαγές, για τον εντοπισμό κατάχρησης πρόσβασης τόσο από τρίτους ή άλλες οντότητες όσο και εσωτερικής κατάχρησης πρόσβασης·
γ) πιθανές εσωτερικές και εξωτερικές απειλές.

39. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να δημιουργούν και να εφαρμόζουν διεργασίες και οργανωτικές δομές για τον προσδιορισμό και τη συνεχή παρακολούθηση απειλών για την ασφάλεια που θα μπορούσαν να επηρεάσουν σημαντικά την ικανότητά τους να παρέχουν υπηρεσίες. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να παρακολουθούν ενεργά τις τεχνολογικές εξελίξεις προκειμένου να διασφαλίζουν ότι έχουν επίγνωση των κινδύνων ασφάλειας. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να εφαρμόζουν μέτρα ανίχνευσης, για παράδειγμα για τον εντοπισμό πιθανών διαρροών πληροφοριών, κακόβουλου κώδικα, λοιπών απειλών για την ασφάλεια και ευρέως γνωστών ευπαθειών λογισμικού και υλικού, και θα πρέπει να ελέγχουν αν υπάρχουν αντίστοιχες ενημερώσεις ασφάλειας.

40. Η διεργασία παρακολούθησης της ασφάλειας θα πρέπει επίσης να βοηθά τα χρηματοοικονομικά ιδρύματα να κατανοούν τη φύση των περιστατικών λειτουργικού κινδύνου ή των περιστατικών ασφάλειας, να προσδιορίζουν τάσεις και να στηρίζουν τις έρευνες του οργανισμού.

1.4.6. Επανεξετάσεις, αξιολογήσεις και δοκιμές της ασφάλειας πληροφοριών

41. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να διενεργούν διάφορες επανεξετάσεις, αξιολογήσεις και δοκιμές της ασφάλειας πληροφοριών, ώστε να διασφαλίζεται ο αποτελεσματικός εντοπισμός ευπαθειών στα συστήματα ΤΠΕ και στις υπηρεσίες ΤΠΕ των χρηματοοικονομικών ιδρυμάτων. Για παράδειγμα, τα χρηματοοικονομικά ιδρύματα μπορούν να προβαίνουν σε ανάλυση ελλείψεων με βάση τα πρότυπα ασφάλειας πληροφοριών, τους ελέγχους συμμόρφωσης, τους εσωτερικούς και εξωτερικούς ελέγχους των συστημάτων πληροφοριών ή τους ελέγχους φυσικής ασφάλειας. Επιπλέον, τα ιδρύματα θα πρέπει να λαμβάνουν υπόψη ορθές πρακτικές, όπως επισκόπηση πηγαίου κώδικα, αξιολογήσεις ευπαθειών, δοκιμές παρείσδυσης και ασκήσεις «κόκκινης ομάδας».

42. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να θεσπίζουν και να εφαρμόζουν πλαίσιο δοκιμών ασφάλειας πληροφοριών το οποίο επικυρώνει την αξιοπιστία και την αποτελεσματικότητα των οικείων μέτρων ασφάλειας πληροφοριών, καθώς και να διασφαλίζουν ότι στο εν λόγω πλαίσιο λαμβάνονται υπόψη απειλές και ευπάθειες, οι οποίες προσδιορίζονται μέσω της παρακολούθησης απειλών και της διαδικασίας αξιολόγησης κινδύνων ΤΠΕ και ασφάλειας.

43. Το πλαίσιο δοκιμών ασφάλειας πληροφοριών θα πρέπει να διασφαλίζει ότι οι δοκιμές:

    α) εκτελούνται από ανεξάρτητους φορείς διεξαγωγής δοκιμών που διαθέτουν επαρκείς γνώσεις, δεξιότητες και εξειδίκευση στη διενέργεια δοκιμών όσον αφορά μέτρα ασφάλειας πληροφοριών και δεν εμπλέκονται στην ανάπτυξη των μέτρων ασφάλειας πληροφοριών·

    β) περιλαμβάνουν επαρκείς ελέγχους ευπαθειών και δοκιμές παρείσδυσης (μεταξύ των οποίων και δοκιμές παρείσδυσης βάσει απειλών όπου κρίνεται αναγκαίο και σκόπιμο) ανάλογα με το επίπεδο κινδύνου που προσδιορίζεται σε σχέση με τις επιχειρηματικές διεργασίες και τα συστήματα.

44. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να διενεργούν συνεχείς και επαναλαμβανόμενες δοκιμές των μέτρων ασφάλειας. Οι εν λόγω δοκιμές θα πρέπει να διενεργούνται τουλάχιστον σε ετήσια βάση για το σύνολο των κρίσιμων συστημάτων ΤΠΕ (παράγραφος 17), ενώ για τους ΠΥΠ θα εντάσσονται στο πλαίσιο της ολοκληρωμένης αξιολόγησης των κινδύνων ασφάλειας που συνδέονται με τις υπηρεσίες πληρωμών τις οποίες παρέχουν, σύμφωνα με το άρθρο 95 παράγραφος 2 της PSD2. Τα συστήματα μη κρίσιμης σημασίας θα πρέπει να υποβάλλονται τακτικά σε δοκιμή σύμφωνα με μια προσέγγιση που βασίζεται στον κίνδυνο, αλλά τουλάχιστον ανά 3 έτη.

45. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να διασφαλίζουν ότι οι δοκιμές των μέτρων ασφάλειας διενεργούνται σε περίπτωση αλλαγών στην υποδομή, στις διεργασίες ή στις διαδικασίες, καθώς και σε περίπτωση αλλαγών λόγω μειζόνων περιστατικών λειτουργικού κινδύνου ή μειζόνων περιστατικών ασφάλειας ή λόγω της έκδοσης νέων ή σημαντικά τροποποιημένων κρίσιμων εφαρμογών διαδικτύου.

46. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να παρακολουθούν και να αξιολογούν τα αποτελέσματα των δοκιμών ασφάλειας και να επικαιροποιούν αναλόγως και χωρίς αδικαιολόγητες καθυστερήσεις τα μέτρα ασφάλειάς τους στην περίπτωση των κρίσιμων συστημάτων ΤΠΕ.

47. Για τους ΠΥΠ, το πλαίσιο δοκιμών θα πρέπει επίσης να περιλαμβάνει τα μέτρα ασφάλειας που αφορούν 1) τα τερματικά πληρωμών και τις συσκευές που χρησιμοποιούνται για την παροχή υπηρεσιών πληρωμών, 2) τα τερματικά πληρωμών και τις συσκευές που χρησιμοποιούνται για την αυθεντικοποίηση των χρηστών υπηρεσιών πληρωμών και 3) τις συσκευές και το λογισμικό που παρέχει ο ΠΥΠ στους χρήστες υπηρεσιών πληρωμών για την παραγωγή/λήψη κωδικού αυθεντικοποίησης (κλειδάριθμων).

48. Βάσει των απειλών για την ασφάλεια που παρατηρούνται και των αλλαγών που επέρχονται, θα πρέπει να διενεργούνται δοκιμές σύμφωνα με σενάρια συναφών και γνωστών δυνητικών επιθέσεων.

1.4.7. Κατάρτιση και ευαισθητοποίηση σε θέματα ασφάλειας πληροφοριών

49. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να εφαρμόζουν εκπαιδευτικό πρόγραμμα, συμπεριλαμβανομένων περιοδικών προγραμμάτων ευαισθητοποίησης σε θέματα ασφάλειας, για όλο το προσωπικό και τους αναδόχους, προκειμένου να διασφαλίζεται η επαρκής κατάρτισή τους για την άσκηση των καθηκόντων και των αρμοδιοτήτων τους σύμφωνα με τις σχετικές πολιτικές και διαδικασίες ασφάλειας για τη μείωση των φαινομένων ανθρώπινου σφάλματος, κλοπής, απάτης, κατάχρησης ή απώλειας και να γνωρίζουν πώς πρέπει να αντιμετωπίζουν τους κινδύνους που συνδέονται με την ασφάλεια των πληροφοριών. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να διασφαλίζουν ότι το εκπαιδευτικό πρόγραμμα παρέχει κατάρτιση για το σύνολο των μελών του προσωπικού και των αναδόχων τουλάχιστον σε ετήσια βάση.

1.5. Διαχείριση λειτουργιών ΤΠΕ

50. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να διαχειρίζονται τις οικείες λειτουργίες ΤΠΕ βάσει τεκμηριωμένων και εφαρμοζόμενων διεργασιών και διαδικασιών [οι οποίες περιλαμβάνουν, όσον αφορά τους ΠΥΠ, το έγγραφο που περιγράφει την πολιτική ασφάλειας σύμφωνα με το άρθρο 5 παράγραφος 1 στοιχείο ι) της PSD2] που εγκρίνονται από το διοικητικό όργανο. Το εν λόγω σύνολο εγγράφων θα πρέπει να καθορίζει τον τρόπο με τον οποίο τα χρηματοοικονομικά ιδρύματα διασφαλίζουν τη λειτουργία, την παρακολούθηση και τον έλεγχο των συστημάτων ΤΠΕ και των υπηρεσιών ΤΠΕ τους, συμπεριλαμβανομένης της τεκμηρίωσης των κρίσιμων λειτουργιών ΤΠΕ, ενώ επίσης θα πρέπει να παρέχει στα χρηματοοικονομικά ιδρύματα τη δυνατότητα τήρησης επικαιροποιημένου καταλόγου πόρων ΤΠΕ.

51. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να μεριμνούν ώστε οι επιδόσεις των οικείων λειτουργιών ΤΠΕ να συνάδουν με τις απαιτήσεις των επιχειρηματικών δραστηριοτήτων τους. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να διατηρούν και να βελτιώνουν, όπου είναι εφικτό, την αποτελεσματικότητα των οικείων λειτουργιών ΤΠΕ, συμπεριλαμβανομένης, ενδεικτικά, της ανάγκης εξέτασης του τρόπου με τον οποίο μπορούν να ελαχιστοποιηθούν πιθανά σφάλματα που προκύπτουν από την εκτέλεση χειροκίνητων εργασιών.

52. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να εφαρμόζουν διαδικασίες καταγραφής και παρακολούθησης για τις κρίσιμες λειτουργίες ΤΠΕ, ώστε να είναι εφικτή η ανίχνευση, η ανάλυση και η διόρθωση σφαλμάτων.

53. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να τηρούν επικαιροποιημένο κατάλογο των πόρων τους ΤΠΕ (συμπεριλαμβανομένων των συστημάτων ΤΠΕ, των συσκευών δικτύου, των βάσεων δεδομένων κ.λπ.). Στον κατάλογο πόρων ΤΠΕ θα πρέπει να αποθηκεύονται οι παράμετροι των πόρων ΤΠΕ, καθώς και οι σύνδεσμοι και οι αλληλεξαρτήσεις μεταξύ των διαφόρων πόρων ΤΠΕ, ώστε να είναι εφικτή η εφαρμογή ορθής διεργασίας παραμετροποίησης και διαχείρισης αλλαγών.

54. Ο κατάλογος πόρων ΤΠΕ θα πρέπει να χαρακτηρίζεται από επαρκή βαθμό λεπτομέρειας ώστε να παρέχεται η δυνατότητα άμεσου προσδιορισμού του πόρου ΤΠΕ, της θέσης του, της κατηγοριοποίησης ασφάλειας και του καθεστώτος ιδιοκτησίας του. Θα πρέπει να τεκμηριώνονται οι αλληλεξαρτήσεις μεταξύ των πόρων ώστε να διευκολύνεται η αντιμετώπιση περιστατικών ασφάλειας και περιστατικών λειτουργικού κινδύνου, συμπεριλαμβανομένων των επιθέσεων στον κυβερνοχώρο.

55. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να παρακολουθούν και να διαχειρίζονται τους κύκλους ζωής των πόρων ΤΠΕ ώστε να διασφαλίζεται ότι εξακολουθούν να πληρούν και να υποστηρίζουν τις απαιτήσεις διαχείρισης των επιχειρηματικών δραστηριοτήτων και των κινδύνων. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να παρακολουθούν αν οι πόροι ΤΠΕ τους υποστηρίζονται από τους εξωτερικούς ή εσωτερικούς τους προμηθευτές και σχεδιαστές εφαρμογών, καθώς και αν όλες οι σχετικές ενημερώσεις και αναβαθμίσεις εφαρμόζονται βάσει τεκμηριωμένων διεργασιών. Οι κίνδυνοι που απορρέουν από παρωχημένους ή μη υποστηριζόμενους πόρους ΤΠΕ θα πρέπει να αξιολογούνται και να περιορίζονται.

56. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να εφαρμόζουν διεργασίες σχεδιασμού και παρακολούθησης των επιδόσεων και των ικανοτήτων με σκοπό την έγκαιρη πρόληψη, ανίχνευση και αντιμετώπιση σημαντικών ζητημάτων όσον αφορά τις επιδόσεις των συστημάτων και τις ελλείψεις ικανοτήτων ΤΠΕ.

57. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να καθορίζουν και να εφαρμόζουν διαδικασίες δημιουργίας εφεδρικών αντιγράφων και αποκατάστασης δεδομένων και συστημάτων ΤΠΕ, ώστε να διασφαλίζεται η δυνατότητα ανάκτησής τους όπως απαιτείται. Το πεδίο εφαρμογής και η συχνότητα της δημιουργίας εφεδρικών αντιγράφων θα πρέπει να καθορίζονται σύμφωνα με τις απαιτήσεις επιχειρησιακής ανάκτησης και την κρισιμότητα των δεδομένων και των συστημάτων ΤΠΕ και να αξιολογούνται με βάση τη διενεργηθείσα αξιολόγηση κινδύνων. Οι δοκιμές των διαδικασιών δημιουργίας εφεδρικών αντιγράφων και αποκατάστασης θα πρέπει να διενεργούνται σε περιοδική βάση.

58. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να διασφαλίζουν ότι τα εφεδρικά αντίγραφα δεδομένων και συστημάτων ΤΠΕ αποθηκεύονται με ασφάλεια και σε αρκετά απομακρυσμένη τοποθεσία από τον κύριο χώρο, ώστε να μην εκτίθενται στους ίδιους κινδύνους.

1.5.1 Διαχείριση περιστατικών και προβλημάτων ΤΠΕ

59. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να δημιουργούν και να εφαρμόζουν διεργασία διαχείρισης περιστατικών και προβλημάτων για την παρακολούθηση και την καταγραφή περιστατικών λειτουργικού κινδύνου και περιστατικών ασφάλειας ΤΠΕ, καθώς και για να εξασφαλίζεται η δυνατότητα των χρηματοοικονομικών ιδρυμάτων να συνεχίζουν ή να επανεκκινούν, εγκαίρως, τις κρίσιμες επιχειρηματικές λειτουργίες και διεργασίες σε περίπτωση εμφάνισης διαταραχών. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να καθορίζουν κατάλληλα κριτήρια και κατώτατα όρια για την κατηγοριοποίηση συμβάντων ως περιστατικών λειτουργικού κινδύνου ή περιστατικών ασφάλειας, όπως προβλέπεται στην ενότητα «Ορισμοί» του παρόντος εγγράφου, καθώς και δείκτες έγκαιρης προειδοποίησης που θα πρέπει να χρησιμεύουν ως συναγερμοί ώστε να καθίσταται δυνατός ο έγκαιρος εντοπισμός

των εν λόγω περιστατικών. Όσον αφορά τους ΠΥΠ, τα εν λόγω κριτήρια και κατώτατα όρια εφαρμόζονται με την επιφύλαξη της ταξινόμησης μειζόνων συμβάντων σύμφωνα με το άρθρο 96 της PSD2 και τις κατευθυντήριες γραμμές για την αναφορά μειζόνων συμβάντων δυνάμει της PSD2 (EBA/GL/2017/10).

60. Για την ελαχιστοποίηση των επιπτώσεων δυσμενών συμβάντων και την εξασφάλιση της δυνατότητας έγκαιρης ανάκτησης, τα χρηματοοικονομικά ιδρύματα θα πρέπει να δημιουργούν κατάλληλες διεργασίες και οργανωτικές δομές για τη διασφάλιση συνεκτικής και ολοκληρωμένης παρακολούθησης, χειρισμού και μεταγενέστερης παρακολούθησης των περιστατικών λειτουργικού κινδύνου και των περιστατικών ασφάλειας, καθώς και για τη διασφάλιση του προσδιορισμού και της εξάλειψης των βασικών αιτιών με σκοπό την πρόληψη της εμφάνισης επαναλαμβανόμενων περιστατικών. Στη διεργασία διαχείρισης περιστατικών και προβλημάτων θα πρέπει να καθορίζονται:

α) οι διαδικασίες για τον προσδιορισμό, την ανίχνευση, την καταγραφή, την κατηγοριοποίηση και την ταξινόμηση των περιστατικών βάσει προτεραιοποίησης ανάλογα με την κρισιμότητα των επιχειρησιακών λειτουργιών·

β) οι ρόλοι και οι αρμοδιότητες για διαφορετικά σενάρια περιστατικών (π.χ. σφάλματα, δυσλειτουργίες, επιθέσεις στον κυβερνοχώρο)·

γ) διαδικασίες διαχείρισης προβλημάτων για τον προσδιορισμό, την ανάλυση και την επίλυση των βασικών αιτιών ενός ή περισσότερων περιστατικών: τα χρηματοοικονομικά ιδρύματα θα πρέπει να αναλύουν τα περιστατικά λειτουργικού κινδύνου ή τα περιστατικά ασφάλειας που είναι πιθανό να επηρεάζουν το χρηματοοικονομικό ίδρυμα και έχουν προσδιοριστεί ή έχουν εμφανιστεί εντός και/ή εκτός του οργανισμού, ενώ επίσης θα πρέπει να λαμβάνουν υπόψη τα κύρια διδάγματα που αντλούνται από τις εν λόγω αναλύσεις και να επικαιροποιούν αναλόγως τα μέτρα ασφάλειας·

δ) αποτελεσματικά σχέδια εσωτερικής επικοινωνίας, συμπεριλαμβανομένων διαδικασιών γνωστοποίησης περιστατικών και παραπομπής σε ανώτερη βαθμίδα της ιεραρχικής κλίμακας —οι οποίες καλύπτουν επίσης καταγγελίες πελατών σχετικά με θέματα ασφάλειας— ώστε να διασφαλίζεται ότι:

i) τα περιστατικά με δυνητικά σοβαρές δυσμενείς επιπτώσεις σε συστήματα και υπηρεσίες ΤΠΕ κρίσιμης σημασίας αναφέρονται στα αρμόδια ανώτερα διοικητικά στελέχη και στα ανώτερα διοικητικά στελέχη ΤΠΕ,

ii) το διοικητικό όργανο ενημερώνεται σε ad hoc βάση σε περίπτωση σημαντικών περιστατικών και ενημερώνεται επιπροσθέτως, τουλάχιστον, για τις επιπτώσεις, την αντιμετώπιση και τους πρόσθετους ελέγχους που πρέπει να καθοριστούν συνεπεία των περιστατικών·

ε) διαδικασίες αντιμετώπισης περιστατικών για τη μείωση των επιπτώσεων που συνδέονται με τα περιστατικά και για την εξασφάλιση της δυνατότητας έγκαιρης και ασφαλούς επιχειρησιακής λειτουργίας της υπηρεσίας·

στ) ειδικά σχέδια εξωτερικής επικοινωνίας για τις κρίσιμες επιχειρηματικές λειτουργίες και διεργασίες, με στόχο:

i) τη συνεργασία με τους σχετικούς ενδιαφερομένους για την αποτελεσματική αντιμετώπιση και ανάκτηση μετά το περιστατικό,
ii) την έγκαιρη παροχή πληροφοριών σε εξωτερικά μέρη (π.χ. πελάτες, άλλους συμμετέχοντες στην αγορά, εποπτική αρχή) κατά περίπτωση και σύμφωνα με τις ισχύουσες κανονιστικές διατάξεις.

1.6. Διαχείριση έργων και αλλαγών ΤΠΕ

1.6.1. Διαχείριση έργων ΤΠΕ

61. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να εφαρμόζουν πρόγραμμα και/ή διαδικασία διακυβέρνησης έργων για τον καθορισμό των ρόλων, των αρμοδιοτήτων και των υποχρεώσεων λογοδοσίας με σκοπό την αποτελεσματική υποστήριξη της υλοποίησης της στρατηγικής ΤΠΕ.

62. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να μεριμνούν δεόντως για την παρακολούθηση και τη μείωση των κινδύνων που απορρέουν από το οικείο χαρτοφυλάκιο έργων ΤΠΕ (διαχείριση προγράμματος), λαμβάνοντας επίσης υπόψη τους κινδύνους που ενδέχεται να προκύπτουν από αλληλεξαρτήσεις μεταξύ διαφόρων έργων και από την εξάρτηση πολλαπλών έργων από τους ίδιους πόρους και/ή την ίδια εξειδίκευση.

63. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να καταρτίζουν και να εφαρμόζουν πολιτική διαχείρισης έργων ΤΠΕ η οποία περιλαμβάνει τουλάχιστον:

α) στόχους έργου·
β) ρόλους και αρμοδιότητες·
γ) αξιολόγηση κινδύνων έργου·
δ) σχέδιο, χρονοδιάγραμμα και στάδια έργου·
ε) βασικά ορόσημα·
στ) απαιτήσεις διαχείρισης αλλαγών.

64. Η πολιτική διαχείρισης έργων ΤΠΕ θα πρέπει να διασφαλίζει ότι οι απαιτήσεις ασφάλειας πληροφοριών αναλύονται και εγκρίνονται από λειτουργία η οποία είναι ανεξάρτητη από τη λειτουργία ανάπτυξης.

65. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να διασφαλίζουν ότι στην ομάδα έργου να εκπροσωπούνται όλοι οι τομείς που επηρεάζονται από το έργο ΤΠΕ και ότι η ομάδα έργου διαθέτει τις γνώσεις που απαιτούνται για την εξασφάλιση της ασφαλούς και επιτυχούς υλοποίησης του έργου.

66. Η κατάρτιση και η πρόοδος των έργων ΤΠΕ, καθώς και οι σχετικοί κίνδυνοί τους, θα πρέπει να αποτελούν αντικείμενο εκθέσεων που υποβάλλονται στο διοικητικό όργανο, είτε μεμονωμένα είτε συγκεντρωτικά, ανάλογα με τη σημασία και το μέγεθος των έργων ΤΠΕ, σε τακτική και ad hoc βάση, κατά περίπτωση. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να συμπεριλαμβάνουν τον κίνδυνο έργου στο πλαίσιο της διαχείρισης κινδύνων τους.

1.6.2. Απόκτηση και ανάπτυξη συστημάτων ΤΠΕ

67. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να αναπτύσσουν και να εφαρμόζουν διαδικασία η οποία διέπει την απόκτηση, την ανάπτυξη και τη συντήρηση συστημάτων ΤΠΕ. Η διαδικασία αυτή θα πρέπει να σχεδιάζεται με τη χρήση προσέγγισης βάσει κινδύνου.

68. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να μεριμνούν ώστε, πριν από οποιαδήποτε απόκτηση ή ανάπτυξη συστημάτων ΤΠΕ, να ορίζονται με σαφήνεια και να εγκρίνονται από την αρμόδια δομή διαχείρισης επιχειρηματικών δραστηριοτήτων οι λειτουργικές και μη λειτουργικές απαιτήσεις (συμπεριλαμβανομένων των απαιτήσεων ασφάλειας πληροφοριών).

69. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να διασφαλίζουν ότι εφαρμόζονται μέτρα για τη μείωση του κινδύνου ακούσιας τροποποίησης ή εσκεμμένης παραποίησης των συστημάτων ΤΠΕ κατά τη διάρκεια της ανάπτυξης και υλοποίησης του περιβάλλοντος παραγωγής.

70. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να διαθέτουν μεθοδολογία για τις δοκιμές και την έγκριση των συστημάτων ΤΠΕ πριν από την πρώτη χρήση τους. Στην μεθοδολογία αυτή θα πρέπει να λαμβάνεται υπόψη η κρισιμότητα των επιχειρησιακών διεργασιών και πόρων. Οι δοκιμές θα πρέπει να εξασφαλίζουν ότι τα νέα συστήματα ΤΠΕ λειτουργούν σύμφωνα με τα προβλεπόμενα. Θα πρέπει επίσης να χρησιμοποιούν περιβάλλοντα δοκιμών τα οποία αντικατοπτρίζουν επαρκώς το περιβάλλον παραγωγής.

71. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να υποβάλλουν σε δοκιμές τα συστήματα ΤΠΕ, τις υπηρεσίες ΤΠΕ και τα μέτρα ασφάλειας πληροφοριών για τον προσδιορισμό πιθανών αδυναμιών, παραβιάσεων και περιστατικών ασφάλειας.

72. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να υλοποιούν χωριστά περιβάλλοντα ΤΠΕ για τη διασφάλιση του κατάλληλου διαχωρισμού καθηκόντων και για τη μείωση των επιπτώσεων των μη επαληθευμένων αλλαγών στα συστήματα παραγωγής. Ειδικότερα, τα χρηματοοικονομικά ιδρύματα θα πρέπει να μεριμνούν για τον διαχωρισμό των περιβαλλόντων παραγωγής από τα περιβάλλοντα ανάπτυξης, δοκιμών και από άλλα μη παραγωγικά περιβάλλοντα. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να διασφαλίζουν την ακεραιότητα και την εμπιστευτικότητα των δεδομένων παραγωγής σε μη παραγωγικά περιβάλλοντα. Η πρόσβαση στα δεδομένα παραγωγής περιορίζεται σε εξουσιοδοτημένους χρήστες.

73. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να εφαρμόζουν μέτρα για την προστασία της ακεραιότητας του πηγαίου κώδικα των συστημάτων ΤΠΕ που αναπτύσσονται εσωτερικά. Θα πρέπει επίσης να τεκμηριώνουν την ανάπτυξη, την εφαρμογή, τη λειτουργία και/ή την παραμετροποίηση των συστημάτων ΤΠΕ κατά τρόπο ολοκληρωμένο, ώστε να περιορίζεται τυχόν αδικαιολόγητη εξάρτηση από ειδικούς επί του αντικειμένου αυτού. Η τεκμηρίωση του συστήματος ΤΠΕ θα πρέπει να περιλαμβάνει, κατά περίπτωση, τουλάχιστον την τεκμηρίωση για τον χρήστη, την τεχνική τεκμηρίωση του συστήματος και τις διαδικασίες λειτουργίας.

74. Οι διεργασίες των χρηματοοικονομικών ιδρυμάτων για την απόκτηση και την ανάπτυξη συστημάτων ΤΠΕ θα πρέπει να εφαρμόζονται επίσης σε συστήματα ΤΠΕ των οποίων η ανάπτυξη ή η διαχείριση πραγματοποιείται από τους τελικούς χρήστες της επιχειρηματικής λειτουργίας εκτός του οργανισμού ΤΠΕ (π.χ. υπολογιστικές εφαρμογές τελικού χρήστη) με

προσέγγιση βάσει κινδύνου. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να τηρούν μητρώο των εν λόγω εφαρμογών για την υποστήριξη των κρίσιμων επιχειρηματικών λειτουργιών ή διεργασιών.

1.6.3. Διαχείριση αλλαγών ΤΠΕ

75. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να δημιουργούν και να εφαρμόζουν διεργασία διαχείρισης αλλαγών ΤΠΕ ώστε να διασφαλίζεται ότι όλες οι αλλαγές στα συστήματα ΤΠΕ καταγράφονται, υποβάλλονται σε δοκιμές, αξιολογούνται, εγκρίνονται, υλοποιούνται και επαληθεύονται με ελεγχόμενο τρόπο. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να χειρίζονται τις αλλαγές κατά τη διάρκεια περιπτώσεων έκτακτης ανάγκης (δηλαδή αλλαγές που πρέπει να επέλθουν το συντομότερο δυνατόν) σύμφωνα με διαδικασίες που παρέχουν επαρκείς διασφαλίσεις.

76. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να προσδιορίζουν αν οι αλλαγές στο υφιστάμενο λειτουργικό περιβάλλον επηρεάζουν τα ισχύοντα μέτρα ασφάλειας ή απαιτούν τη θέσπιση πρόσθετων μέτρων για τη μείωση των αντίστοιχων κινδύνων. Οι αλλαγές αυτές θα πρέπει να πραγματοποιούνται σύμφωνα με την επίσημη διαδικασία διαχείρισης αλλαγών που εφαρμόζουν τα χρηματοοικονομικά ιδρύματα.

1.7. Διαχείριση της επιχειρησιακής συνέχειας

77. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να καθιερώσουν διαδικασία διαχείρισης της επιχειρησιακής συνέχειας με στόχο τη μεγιστοποίηση της ικανότητάς τους να παρέχουν υπηρεσίες σε συνεχή βάση και τον περιορισμό των ζημιών σε περίπτωση σοβαρής διαταραχής της δραστηριότητάς τους, σύμφωνα με το άρθρο 85 παράγραφος 2 της οδηγίας 2013/36/ΕΕ και τον τίτλο VI των κατευθυντήριων γραμμών της ΕΑΤ σχετικά με την εσωτερική διακυβέρνηση (EBA/GL/2017/11).

1.7.1. Ανάλυση των επιχειρηματικών επιπτώσεων

78. Στο πλαίσιο της χρηστής διαχείρισης της επιχειρησιακής συνέχειας, τα χρηματοοικονομικά ιδρύματα θα πρέπει να διενεργούν ανάλυση των επιχειρηματικών επιπτώσεων, αναλύοντας την έκθεσή τους σε σοβαρές διαταραχές της δραστηριότητάς τους και αξιολογώντας τις πιθανές επιπτώσεις τους (μεταξύ άλλων όσον αφορά την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα), βάσει ποσοτικού και ποιοτικού προσδιορισμού, χρησιμοποιώντας εσωτερικά και/ή εξωτερικά δεδομένα (π.χ. δεδομένα τρίτου παρόχου που αφορούν επιχειρηματική διεργασία ή δημόσια διαθέσιμα δεδομένα που ενδέχεται να αφορούν την ανάλυση των επιχειρηματικών επιπτώσεων) και ανάλυση σεναρίων. Στην ανάλυση των επιχειρηματικών επιπτώσεων θα πρέπει να λαμβάνεται επίσης υπόψη η κρισιμότητα των επιχειρηματικών λειτουργιών, των υποστηρικτικών διεργασιών, των τρίτων και των πληροφοριακών πόρων που προσδιορίζονται και κατηγοριοποιούνται, καθώς και των αλληλεξαρτήσεών τους, σύμφωνα με την ενότητα 1.3.3.

79. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να διασφαλίζουν ότι τα συστήματα ΤΠΕ και οι υπηρεσίες ΤΠΕ τους σχεδιάζονται και συνάδουν με την ανάλυση των επιχειρηματικών

επιπτώσεων που διενεργούν, για παράδειγμα εξασφαλίζοντας την εφεδρεία ορισμένων κρίσιμων στοιχείων για την πρόληψη διαταραχών λόγω συμβάντων που μπορεί να προκαλέσουν επιπτώσεις στα εν λόγω στοιχεία.

1.7.2. Σχεδιασμός επιχειρησιακής συνέχειας

80. Βάσει των οικείων αναλύσεων των επιχειρηματικών επιπτώσεων, τα χρηματοοικονομικά ιδρύματα θα πρέπει να καταρτίζουν σχέδια για τη διασφάλιση της επιχειρησιακής συνέχειας (σχέδια επιχειρησιακής συνέχειας, ΣΕΣ), τα οποία θα πρέπει να τεκμηριώνονται και να εγκρίνονται από τα διοικητικά τους όργανα. Στα σχέδια θα πρέπει να εξετάζονται ειδικά οι κίνδυνοι οι οποίοι θα μπορούσαν να έχουν δυσμενείς επιπτώσεις στα συστήματα ΤΠΕ και στις υπηρεσίες ΤΠΕ. Τα σχέδια θα πρέπει να υποστηρίζουν τους στόχους για την προστασία και, εφόσον απαιτείται, την αποκατάσταση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των επιχειρηματικών λειτουργιών, των υποστηρικτικών διεργασιών και των πληροφοριακών πόρων τους. Κατά την κατάρτιση των εν λόγω σχεδίων, τα χρηματοοικονομικά ιδρύματα θα πρέπει να συντονίζονται με τους σχετικούς εσωτερικούς και εξωτερικούς ενδιαφερομένους, κατά περίπτωση.

81. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να θέτουν σε εφαρμογή σχέδια επιχειρησιακής συνέχειας ώστε να διασφαλίζεται ότι μπορούν να αντιδράσουν κατάλληλα σε πιθανά σενάρια αστοχίας και ότι είναι σε θέση να ανακτήσουν τις λειτουργίες των κρίσιμων επιχειρηματικών δραστηριοτήτων τους έπειτα από διαταραχές στο πλαίσιο ενός στόχου χρόνου ανάκτησης (ΣΧΑ, στόχος χρόνου ανάκτησης: ο μέγιστος χρόνος εντός του οποίου ένα σύστημα ή μία διεργασία πρέπει να αποκατασταθεί έπειτα από κάποιο περιστατικό) και ενός στόχου σημείου ανάκτησης (ΣΣΑ, στόχος σημείου ανάκτησης: η μέγιστη χρονική περίοδος κατά τη διάρκεια της οποίας είναι αποδεκτή η απώλεια δεδομένων σε περίπτωση συμβάντος ή περιστατικού). Σε περιπτώσεις σοβαρής διαταραχής της δραστηριότητας που ενεργοποιεί συγκεκριμένα σχέδια επιχειρησιακής συνέχειας, τα χρηματοοικονομικά ιδρύματα θα πρέπει να ιεραρχούν κατά σειρά προτεραιότητας τις ενέργειες επιχειρησιακής συνέχειας χρησιμοποιώντας μια προσέγγιση βάσει κινδύνου η οποία μπορεί να στηρίζεται στις αξιολογήσεις κινδύνων που διενεργούνται σύμφωνα με την ενότητα 1.3.3. Στην περίπτωση των ΠΥΠ, η διαδικασία αυτή, μεταξύ άλλων, μπορεί, για παράδειγμα, να διευκολύνει την περαιτέρω επεξεργασία κρίσιμων συναλλαγών ενόσω συνεχίζονται οι προσπάθειες αποκατάστασης.

82. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να εξετάζουν στα σχέδια επιχειρησιακής συνέχειας πληθώρα διαφορετικών σεναρίων, συμπεριλαμβανομένων ακραίων αλλά πιθανών σεναρίων στα οποία ενδέχεται να εκτεθούν, συμπεριλαμβανομένων και σεναρίων επιθέσεων στον κυβερνοχώρο, και θα πρέπει να αξιολογούν τις δυνητικές επιπτώσεις των εν λόγω σεναρίων. Με βάση τα σενάρια αυτά, τα χρηματοοικονομικά ιδρύματα θα πρέπει να περιγράφουν τον τρόπο διασφάλισης της συνέχειας των συστημάτων και των υπηρεσιών ΤΠΕ, καθώς και της ασφάλειας πληροφοριών του χρηματοοικονομικού ιδρύματος.

1.7.3. Σχέδια αντιμετώπισης και ανάκτησης

83. Βάσει των αναλύσεων των επιχειρηματικών επιπτώσεων (παράγραφος 78) και των εύλογων σεναρίων (παράγραφος 82), τα χρηματοοικονομικά ιδρύματα θα πρέπει να καταρτίζουν σχέδια αντιμετώπισης και ανάκτησης. Στα σχέδια αυτά θα πρέπει να προσδιορίζονται οι συνθήκες οι οποίες ενδέχεται να προκαλέσουν την άμεση ενεργοποίηση των σχεδίων, καθώς και τα μέτρα που θα πρέπει να λαμβάνονται για τη διασφάλιση της διαθεσιμότητας, της συνέχειας και της ανάκτησης, τουλάχιστον, των κρίσιμων συστημάτων ΤΠΕ και υπηρεσιών ΤΠΕ των χρηματοοικονομικών ιδρυμάτων. Τα σχέδια αντιμετώπισης και ανάκτησης θα πρέπει να αποσκοπούν στην επίτευξη των στόχων ανάκτησης των λειτουργιών των χρηματοοικονομικών ιδρυμάτων.

84. Στα σχέδια αντιμετώπισης και ανάκτησης θα πρέπει να λαμβάνονται υπόψη τόσο βραχυπρόθεσμες όσο και μακροπρόθεσμες επιλογές ανάκτησης. Τα σχέδια θα πρέπει:

    α) να εστιάζουν στην ανάκτηση της λειτουργίας των κρίσιμων επιχειρηματικών λειτουργιών, των υποστηρικτικών διεργασιών, των πληροφοριακών πόρων, καθώς και των αλληλεξαρτήσεών τους, ώστε να αποφεύγονται δυσμενείς επιπτώσεις στη λειτουργία των χρηματοοικονομικών ιδρυμάτων και στο χρηματοπιστωτικό σύστημα, καθώς επίσης και στα συστήματα πληρωμών και τους χρήστες υπηρεσιών πληρωμών, και να διασφαλίζεται η εκτέλεση εκκρεμών συναλλαγών πληρωμών·

    β) να είναι τεκμηριωμένα και να τίθενται στη διάθεση των επιχειρηματικών και υποστηρικτικών μονάδων, και να είναι εύκολα προσβάσιμα σε περίπτωση έκτακτης ανάγκης·

    γ) να επικαιροποιούνται με βάση τα διδάγματα που αντλούνται από τα περιστατικά, τις δοκιμές, τους νέους κινδύνους που προσδιορίζονται και τις απειλές, καθώς και τους μεταβαλλόμενους στόχους και τις προτεραιότητες ανάκτησης.

85. Στα σχέδια θα πρέπει να λαμβάνονται επίσης υπόψη εναλλακτικές επιλογές σε περίπτωση που η ανάκτηση μπορεί να μην είναι εφικτή σε βραχυπρόθεσμο ορίζοντα λόγω κόστους, κινδύνων, υλικοτεχνικής υποστήριξης ή απρόβλεπτων περιστάσεων.

86. Επιπλέον, στο πλαίσιο των σχεδίων αντιμετώπισης και ανάκτησης, τα χρηματοοικονομικά ιδρύματα θα πρέπει να εξετάζουν και να εφαρμόζουν μέτρα συνέχειας για τη μείωση αστοχιών τρίτων παρόχων, που είναι καίριας σημασίας για τη συνέχεια των υπηρεσιών ΤΠΕ ενός χρηματοοικονομικού ιδρύματος [σύμφωνα με τις διατάξεις των κατευθυντήριων γραμμών της ΕΑΤ σχετικά με την εξωτερική ανάθεση δραστηριοτήτων (EBA/GL/2019/02) όσον αφορά τα σχέδια επιχειρησιακής συνέχειας].

1.7.4. Δοκιμή των σχεδίων

87. Τα χρηματοοικονομικά ιδρύματα θα πρέπει να υποβάλλουν σε δοκιμή τα σχέδια επιχειρησιακής συνέχειάς τους σε περιοδική βάση. Ειδικότερα, θα πρέπει να διασφαλίζουν ότι διενεργείται δοκιμή των κρίσιμων επιχειρηματικών λειτουργιών, των υποστηρικτικών διεργασιών και των πληροφοριακών πόρων τους, καθώς και των αλληλεξαρτήσεών τους

(συμπεριλαμβανομένων των αλληλεξαρτήσεων με τρίτους, κατά περίπτωση) τουλάχιστον σε ετήσια βάση, σύμφωνα με την παράγραφο 89.

88. Τα σχέδια επιχειρησιακής συνέχειας θα πρέπει να επικαιροποιούνται τουλάχιστον ετησίως με βάση τα αποτελέσματα των δοκιμών, τις τρέχουσες πληροφορίες σχετικά με απειλές και τα διδάγματα που αντλούνται από προηγούμενα συμβάντα. Κάθε αλλαγή στους στόχους ανάκτησης (συμπεριλαμβανομένων των στόχων χρόνου ανάκτησης και των στόχων σημείου ανάκτησης) και/ή αλλαγή στις επιχειρηματικές λειτουργίες, στις υποστηρικτικές διεργασίες και στους πληροφοριακούς πόρους θα πρέπει επίσης να λαμβάνεται υπόψη, κατά περίπτωση, ως βάση για την επικαιροποίηση των σχεδίων επιχειρησιακής συνέχειας.

89. Στο πλαίσιο της δοκιμής των σχεδίων επιχειρησιακής συνέχειάς τους, τα χρηματοοικονομικά ιδρύματα θα πρέπει να καταδεικνύουν ότι είναι σε θέση να διατηρήσουν τη βιωσιμότητα της δραστηριότητάς τους έως ότου αποκατασταθούν οι κρίσιμες λειτουργίες. Ειδικότερα, η δοκιμή θα πρέπει:

    α) να περιλαμβάνει δοκιμή επαρκούς συνόλου σοβαρών αλλά εύλογων σεναρίων, μεταξύ των οποίων συγκαταλέγονται τα σενάρια που εξετάζονται για την κατάρτιση των σχεδίων επιχειρησιακής συνέχειας (καθώς και δοκιμή των υπηρεσιών που παρέχονται από τρίτους, κατά περίπτωση)· στο πλαίσιο αυτό θα πρέπει να περιλαμβάνεται η μετάβαση των κρίσιμων επιχειρηματικών λειτουργιών, υποστηρικτικών διεργασιών και πληροφοριακών πόρων στο περιβάλλον ανάκαμψης από καταστροφή και η απόδειξη της δυνατότητας λειτουργίας τους με τον συγκεκριμένο τρόπο για επαρκώς αντιπροσωπευτικό χρονικό διάστημα, καθώς και της δυνατότητας μετέπειτα αποκατάστασης της κανονικής λειτουργίας·

    β) να είναι σχεδιασμένη κατά τρόπον ώστε να θέτει υπό αμφισβήτηση τις υποθέσεις στις οποίες στηρίζονται τα σχέδια επιχειρησιακής συνέχειας, συμπεριλαμβανομένων των ρυθμίσεων διακυβέρνησης και των σχεδίων επικοινωνίας σε καταστάσεις κρίσεων· και

    γ) να περιλαμβάνει διαδικασίες για την επαλήθευση της ικανότητας του προσωπικού και των αναδόχων τους, των συστημάτων ΤΠΕ και των υπηρεσιών ΤΠΕ να αντεπεξέρχονται επαρκώς στα σενάρια που ορίζονται στην παράγραφο 89 στοιχείο α).

90. Τα αποτελέσματα της δοκιμής θα πρέπει να τεκμηριώνονται, ενώ επίσης τυχόν διαπιστωθείσες ελλείψεις που προκύπτουν από τις δοκιμές θα πρέπει να αναλύονται, να αντιμετωπίζονται και να αναφέρονται στο διοικητικό όργανο.

1.7.5. Επικοινωνία σε καταστάσεις κρίσεων

91. Σε περίπτωση διακοπής λειτουργίας ή έκτακτης ανάγκης, και κατά τη διάρκεια της εφαρμογής των σχεδίων επιχειρησιακής συνέχειας, τα χρηματοοικονομικά ιδρύματα θα πρέπει να διασφαλίζουν την εφαρμογή αποτελεσματικών μέτρων επικοινωνίας σε καταστάσεις κρίσεων, ούτως ώστε όλοι οι σχετικοί εσωτερικοί και εξωτερικοί ενδιαφερόμενοι, συμπεριλαμβανομένων των αρμόδιων αρχών εφόσον απαιτείται βάσει εθνικών κανονιστικών ρυθμίσεων, και επίσης οι σχετικοί πάροχοι υπηρεσιών (εξωτερικοί πάροχοι, οντότητες ομίλου ή τρίτοι πάροχοι) να ενημερώνονται με έγκαιρο και κατάλληλο τρόπο.

1.8. Διαχείριση σχέσεων με χρήστες υπηρεσιών πληρωμών

92. Οι ΠΥΠ θα πρέπει να δημιουργούν και να εφαρμόζουν διεργασίες υποστήριξης και καθοδήγησης προς τους χρήστες υπηρεσιών πληρωμών με σκοπό την ενίσχυση της ευαισθητοποίησής τους σχετικά με τους κινδύνους ασφάλειας που συνδέονται με τις υπηρεσίες πληρωμών.

93. Η υποστήριξη και η καθοδήγηση που παρέχεται στους χρήστες υπηρεσιών πληρωμών θα πρέπει να επικαιροποιείται ανάλογα με όποιες νέες απειλές και ευπάθειες προκύπτουν, ενώ επίσης οι αλλαγές θα πρέπει να ανακοινώνονται στους χρήστες υπηρεσιών πληρωμών.

94. Όπου είναι δυνατό βάσει των λειτουργικών δυνατοτήτων των προϊόντων, οι ΠΥΠ θα πρέπει να επιτρέπουν στους χρήστες υπηρεσιών πληρωμών να απενεργοποιούν συγκεκριμένες από τις παρεχόμενες λειτουργίες πληρωμών.

95. Εάν, σύμφωνα με το άρθρο 68 παράγραφος 1 της οδηγίας (ΕΕ) 2015/2366, ένας ΠΥΠ έχει συμφωνήσει με τον πληρωτή την ύπαρξη ορίων δαπάνης όσον αφορά τις πράξεις πληρωμής που εκτελούνται μέσω συγκεκριμένων μέσων πληρωμών, ο ΠΥΠ θα πρέπει να παρέχει στον πληρωτή τη δυνατότητα να προσαρμόζει τα εν λόγω όρια μέχρι το ανώτατο συμφωνηθέν όριο.

96. Οι ΠΥΠ θα πρέπει να παρέχουν στους χρήστες υπηρεσιών πληρωμών τη δυνατότητα να λαμβάνουν ειδοποιήσεις σχετικά με κινηθείσες και/ή αποτυχημένες απόπειρες εκκίνησης πράξεων πληρωμής, οι οποίες τους παρέχουν τη δυνατότητα εντοπισμού δόλιας ή κακόβουλης χρήσης του λογαριασμού τους.

97. Οι ΠΥΠ θα πρέπει να τηρούν ενήμερους τους χρήστες υπηρεσιών πληρωμών σχετικά με επικαιροποιήσεις των διαδικασιών ασφάλειας οι οποίες τους επηρεάζουν αναφορικά με την παροχή υπηρεσιών πληρωμών.

98. Οι ΠΥΠ θα πρέπει να παρέχουν στους χρήστες υπηρεσιών πληρωμών υποστήριξη σχετικά με όλες τις ερωτήσεις, τα αιτήματα για υποστήριξη και τις γνωστοποιήσεις για ανωμαλίες ή ζητήματα που αφορούν θέματα ασφάλειας σε σχέση με τις υπηρεσίες πληρωμών. Οι χρήστες υπηρεσιών πληρωμών θα πρέπει να ενημερώνονται κατάλληλα σχετικά με τον τρόπο με τον οποίο μπορούν να λαμβάνουν την εν λόγω υποστήριξη.