Πίνακας Περιεχομένων

Κατηγορία		ΣΤΡΑΤΗΓΙΚΗ
STR1		**Μέτρο:** Στρατηγική για την ασφάλεια πληροφοριών **Στόχος Μέτρου:** Να θεσπιστεί στρατηγική ασφάλειας πληροφοριών στην οποία να αναλύονται οι στόχοι και η προσέγγιση υψηλού επιπέδου με σκοπό τον μετριασμό των κινδύνων για την ασφάλεια πληροφοριών. **Περιγραφή Μέτρου:** Καθορισμός του οράματος και της δέσμευσης για την ασφάλεια πληροφοριών σε μια στρατηγική που θα περιγράφει λεπτομερώς συγκεκριμένους στόχους αναφορικά με την ασφάλεια, καθώς και την προσέγγιση για την ασφάλεια και τη διαχείριση του κινδύνου, και τα μέσα για την επικύρωση της αποτελεσματικότητας της στρατηγικής με την υποστήριξη από βασικούς δείκτες επιδόσεων. Η στρατηγική ασφάλειας πληροφοριών αντικατοπτρίζεται στην πολιτική ασφάλειας πληροφοριών, όπως περιγράφεται στο μέτρο [GOV3]. Τα στελέχη γνωρίζουν τη στρατηγική και την πολιτική ασφάλειας πληροφοριών, όπως περιγράφεται στο μέτρο [TA1]. **Πηγή:** C2M2 (Program)
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**
0	1	Ο οργανισμός δεν έχει δομήσει με οποιοδήποτε τρόπο ή εκφράσει με οποιοδήποτε τρόπο την στρατηγική του για την ασφάλεια πληροφοριών.
1	1	Υπάρχει κατεγραμμένη μια στρατηγική για την ασφάλεια πληροφοριών.
1	2	Η στρατηγική περιέχει μια λίστα από στόχους σε σχέση με την ασφάλεια πληροφοριών, σχετικές ενέργειες για υλοποίηση και ένα πλάνο υψηλού επιπέδου (high level) για την υλοποίησή τους.
1	3	Η διαχείριση και η υλοποίηση της συγκεκριμένης στρατηγικής είναι τουλάχιστον ad-hoc.
2	1	Το πλάνο υλοποίησης περιέχει τουλάχιστον στοιχεία σχετικά με το 1) Τι χρειάζεται να υλοποιηθεί, 2) μέχρι πότε χρειάζεται να υλοποιηθεί, 3) σε ποιόν έχει ανατεθεί η υπευθυνότητα παρακολούθησης / ολοκλήρωσης της υλοποίησης, 4) ποιοι πόροι απαιτούνται για την αποτελεσματική υλοποίηση και 5) με ποιον τρόπο και από ποιόν ρόλο θα διενεργηθεί η αξιολόγηση της ορθώς και αποτελεσματικής υλοποίησης.
3	1	Η στρατηγική που υπάρχει κατεγραμμένη, περιγράφει λεπτομερώς συγκεκριμένους στόχους αναφορικά με την ασφάλεια, καθώς και την προσέγγιση για την ασφάλεια και τη διαχείριση του κινδύνου, και τα μέσα για την επικύρωση της αποτελεσματικότητας της στρατηγικής με την υποστήριξη από βασικούς δείκτες επιδόσεων.
3	2	Η στρατηγική ασφάλειας πληροφοριών αντικατοπτρίζεται στην πολιτική ασφάλειας πληροφοριών, όπως περιγράφεται στο μέτρο [GOV3].
3	3	Τα στελέχη γνωρίζουν τη στρατηγική και την πολιτική ασφάλειας πληροφοριών, όπως περιγράφεται στο μέτρο [TA1].
3	4	Οι ενέργειες που έχουν προκύψει για υλοποίηση από την στρατηγική υποστηρίζονται από την διοίκηση με την παροχή πόρων, γνώσεων και χρόνου.
4	1	Έχει δημιουργηθεί και καταγραφεί διαδικασία μέσω της οποίας γίνεται διαχείριση του κύκλου ζωής της στρατηγικής.
4	2	Στα πλαίσια της διαδικασίας προβλέπεται η ανασκόπηση για την καταλληλότητα των σχετικών στοιχείων τουλάχιστον μια φορά το χρόνο και οι αλλαγές που προκύπτουν υλοποιούνται στα πλαίσια της διαδικασίας διαχείρισης αλλαγών.
4	3	Στα πλαίσια της διαδικασίας προβλέπεται ο έλεγχος της συμβατότητας της πολιτικής με τους στόχους του οργανισμού και τις απαιτήσεις του εσωτερικού και εξωτερικού του περιβάλλοντος (context).
4	4	Στα πλαίσια της διαδικασίας προβλέπεται ο τρόπος με το οποίο θα επικυρώνεται η αποτελεσματικότητας των επιμέρους ενεργειών της στρατηγικής.
4	5	Στα πλαίσια της διαδικασίας προβλέπεται η εξαγωγή βασικών δεικτών επιδόσεων άμεσα συνδεδεμένων με τους στόχους του οργανισμού.

5	1	Η στρατηγική για την ασφάλεια πληροφοριών αποτελεί μια υπό-ενότητα της επιχειρησιακής στρατηγικής του οργανισμού.
5	2	Η στρατηγική εντάσσεται στο συνολικό πλαίσιο διακυβέρνησης (governance) του οργανισμού.
5	3	Μέσω της διακυβέρνησης ο οργανισμός δίνει την στρατηγική κατεύθυνση ώστε να καλύπτει τις υποχρεώσεις του (νομικές, κανονιστικές, συμβατικές και άλλες), να διαχειρίζεται με αποτελεσματικό τρόπο τον κίνδυνο, να χρησιμοποιεί αποτελεσματικά τους πόρους του, και να καλύπτει τους σχετικούς του στόχους.
5	4	Οι λειτουργίες της διακυβέρνησης υποστηρίζονται από μια επίσημη δομή επίβλεψης ασφάλειας πληροφοριών (cybersecurity oversight committee).
5	5	Οι λειτουργίες της διακυβέρνησης υποστηρίζονται από ένα σύστημα μέσω του οποίου διενεργούνται σχετικοί έλεγχοι σε τακτική βάση, αποτελεσματικά.
5	6	Οι λειτουργίες της διακυβέρνησης υποστηρίζονται από αναφορές προς την ανώτατη διοίκηση σχετικά με την υλοποίηση της στρατηγικής και την εκπλήρωση των στόχων, για τους υψηλούς κινδύνους και την πορεία των μέτρων αντιμετώπισης.
5	7	Οι λειτουργίες της διακυβέρνησης υποστηρίζονται από αναφορές σχετικά με περιστατικά ασφαλείας ή παραλίγο περιστατικά ασφαλείας.
5	8	Οι λειτουργίες της διακυβέρνησης υποστηρίζονται από αναλύσεις τάσεων (trend analysis) και προτάσεις για βελτίωση
5	9	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	10	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

Κατηγορία		ΔΙΑΚΥΒΕΡΝΗΣΗ
GOV1		**Μέτρο:** Ρόλοι και αρμοδιότητες σχετικά με την ασφάλεια πληροφοριών **Στόχος Μέτρου:** Να καθοριστούν οι ρόλοι και οι αρμοδιότητες σχετικά με την ασφάλεια πληροφοριών εντός του οργανισμού. **Περιγραφή Μέτρου:** Καθορισμός των ρόλων και των αρμοδιοτήτων όσον αφορά την ασφάλεια δικτύων και πληροφοριών για όλα τα στελέχη που ασχολούνται με την επεξεργασία πληροφοριών ή έχουν πρόσβαση σε συστήματα επεξεργασίας πληροφοριών. Οι καθορισμένοι ρόλοι και αρμοδιότητες αντικατοπτρίζονται στην πολιτική ασφάλειας των πληροφοριών [GOV3]. Τα στελέχη πρέπει να είναι επαρκώς ενημερωμένα και να έχουν επίγνωση των ρόλων και των ευθυνών τους όσον αφορά την ασφάλεια δικτύων και πληροφοριών, όπως ορίζεται στα μέτρα [TA1, TA2]. Οι ρόλοι και οι αρμοδιότητες που σχετίζονται με την ασφάλεια των πληροφοριών θα πρέπει να καθορίζονται από τη διοίκηση, ώστε να εξασφαλίζεται η υπευθυνότητα για τις αποφάσεις της διοίκησης που σχετίζονται με την ασφάλεια δικτύων και συστημάτων πληροφοριών. **Πηγή:** C2M2, ISO 27002
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**
0	1	Ο οργανισμός δεν κάποιο συστηματικό τρόπο με τον οποίο να αναγνωρίζει τις εφαρμοστέες νομικές και κανονιστικές υποχρεώσεις όσον αφορά την ασφάλεια δικτύων και πληροφοριών.
1	1	Έχει πραγματοποιηθεί ο καθορισμός των ρόλων και των αρμοδιοτήτων όσον αφορά την ασφάλεια δικτύων και πληροφοριών για όλα τα στελέχη που ασχολούνται με την επεξεργασία πληροφοριών ή έχουν πρόσβαση σε συστήματα επεξεργασίας πληροφοριών με τρόπο ο οποίος δεν είναι συστηματικός και δεν τεκμηριώνεται εγγράφως.
1	2	Δεν έχει πραγματοποιηθεί διαχωρισμός των αντικρουόμενων καθηκόντων και των τομέων ευθύνης.
2	1	Έχει γίνει καταγραφή των ρόλων και αρμοδιοτήτων και έχουν ανατεθεί στο αντίστοιχο προσωπικό.
2	2	Υπάρχει έγκριση από τη διοίκηση του οργανισμού για τους ρόλους και αρμοδιότητες και για την ανάθεσή τους.
2	3	Τα αντικρουόμενα καθήκοντα και οι τομείς ευθύνης διαχωρίζονται για να μειωθούν οι ευκαιρίες για μη εξουσιοδοτημένη ή ακούσια τροποποίηση ή κατάχρηση των περιουσιακών στοιχείων του οργανισμού.
2	4	Έχει οριστεί από τον οργανισμό Υπεύθυνος για την ασφάλεια δικτύων και συστημάτων πληροφοριών.
2	5	Οι ελάχιστες αρμοδιότητες για τον Υπεύθυνο ασφάλειας δικτύων και πληροφοριών που αναφέρονται στη νομοθεσία πληρούνται όλες.
2	6	Ο Υπεύθυνος ασφάλειας δικτύων και πληροφοριών έχει διοριστεί βάσει επαγγελματικών προσόντων και κυρίως βάσει ειδικών γνώσεων στον τομέα της ασφάλειας δικτύων και πληροφοριών και της ικανότητας εκπλήρωσης των καθηκόντων που αναφέρονται στο εδάφιο (3) της σχετικής νομοθεσίας.
2	7	Ο υπεύθυνος ασφάλειας δικτύων και πληροφοριών εκτελεί αποκλειστικά αυτά τα καθήκοντα. (Για μικρούς οργανισμούς, δύναται να εκτελεί και άλλα καθήκοντα μόνο όταν δεν οδηγούν σε σύγκρουση συμφερόντων και λαμβάνοντας υπόψη το επίπεδο κρισιμότητας του φορέα, με την έγκριση της Αρχής.)
2	8	Ο φορέας έχει κοινοποιήσει στην Αρχή τα στοιχεία επικοινωνίας του υπευθύνου ασφάλειας δικτύων και πληροφοριών.
2	9	Ο φορέας διασφαλίζει ότι οι υποψήφιοι για τη θέση του υπεύθυνου ασφάλειας δικτύων και πληροφοριών ελέγχονται επαρκώς, και εξασφαλίζει ότι το εν λόγω πρόσωπο διεκπεραιώνει τα καθήκοντά του δεόντως.

3	1	Οι ρόλοι και οι αρμοδιότητες αντικατοπτρίζονται στην πολιτική ασφάλειας των πληροφοριών [GOV3] και όλα τα στελέχη του οργανισμού έχουν λάβει την απαραίτητη ενημέρωση και επίγνωση των ρόλων και των ευθυνών τους όσον αφορά την ασφάλεια δικτύων και πληροφοριών, όπως ορίζεται στα μέτρα [TA1, TA2].
3	2	Γίνεται ανασκόπηση και ενημέρωση των ρόλων και αρμοδιοτήτων χωρίς αυτό να είναι συστηματικό.
4	1	Πραγματοποιείται ανασκόπηση και ενημέρωση (όπου αυτό χρειάζεται) των ρόλων και των αρμοδιοτήτων τουλάχιστον σε ετήσια βάση ή όταν έχουν υπάρξει κρίσιμες αλλαγές στον οργανισμό που επηρέασαν ρόλους ή αρμοδιότητες. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
4	2	Οι κίνδυνοι που σχετίζονται με αντικρουόμενα καθήκοντα έχουν εντοπισθεί, αξιολογηθεί και αντιμετωπιστεί όπως απαιτείται.
5	1	Οι ανατεθειμένοι ρόλοι και αρμοδιότητες διαχειρίζονται έτσι ώστε να διασφαλίζεται η επάρκεια και ο πλεονασμός της κάλυψης, συμπεριλαμβανομένου του σχεδιασμού διαδοχής.
5	2	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	3	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
GOV2		**Μέτρο:** Συμμόρφωση με νομικές και κανονιστικές υποχρεώσεις **Στόχος Μέτρου:** Να εξασφαλιστεί η συμμόρφωση με όλες τις εφαρμοστέες νομικές και κανονιστικές υποχρεώσεις όσον αφορά την ασφάλεια δικτύων και πληροφοριών. **Περιγραφή Μέτρου:** Δημιουργία και διατήρηση κεντρικού αποθετηρίου, και συμμόρφωση με όλες τις σχετικές νομοθετικές, κανονιστικές και ρυθμιστικές απαιτήσεις, και συμβατικές απαιτήσεις όσον αφορά την ασφάλεια δικτύων και πληροφοριών. **Πηγή:** ISMM (Compliance), ISO 27002 (18.1), NIST 800-53(AU-6, AU-11), C2M2 (Program)
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**
0	1	Ο οργανισμός δεν έχει κάποιο συστηματικό τρόπο με τον οποίο να αναγνωρίζει τις εφαρμοστέες νομικές και κανονιστικές υποχρεώσεις όσον αφορά την ασφάλεια δικτύων και πληροφοριών.
1	1	Έχουν αναγνωρισθεί και καταγραφεί κάποιες νομοθετικές, κανονιστικές και ρυθμιστικές απαιτήσεις, και συμβατικές απαιτήσεις όσον αφορά την ασφάλεια δικτύων και πληροφοριών χωρίς να υπάρχει γνώση της κατάστασης συμμόρφωσης προς αυτές.
1	2	Οι διαδικασίες αναγνώρισης και ελέγχου συμμόρφωσης είναι τουλάχιστο ad-hoc.
2	1	Έχουν αναγνωρισθεί και καταγραφεί στο σύνολό τους νομοθετικές, κανονιστικές και ρυθμιστικές απαιτήσεις, και συμβατικές απαιτήσεις όσον αφορά την ασφάλεια δικτύων και πληροφοριών.
2	2	Έχει ανατεθεί σε ρόλο εσωτερικά ο έλεγχος προς την συμμόρφωση προς τις συγκεκριμένες απαιτήσεις.
3	1	Έχει δημιουργηθεί και διατηρείται κεντρικό αποθετήριο με όλες τις σχετικές νομοθετικές, κανονιστικές και υθμιστικές απαιτήσεις, και συμβατικές απαιτήσεις όσον αφορά την ασφάλεια δικτύων και πληροφοριών.
3	2	Έχει δημιουργηθεί σχετική διαδικασία και διενεργείται εσωτερικός έλεγχος τουλάχιστον ετήσια για την διαπίστωση της συμμόρφωσης με όλες τις σχετικές νομοθετικές, κανονιστικές και ρυθμιστικές απαιτήσεις, και συμβατικές απαιτήσεις όσον αφορά την ασφάλεια δικτύων και πληροφοριών.
4	1	Έχει δημιουργήθεί μια διαδικασία και τηρούνται οι κατάλληλες προβλέψεις ώστε να μπορούν να αναγνωρίζονται έγκαιρα σχετικές νομοθετικές, κανονιστικές και ρυθμιστικές απαιτήσεις, και συμβατικές απαιτήσεις όσον αφορά την ασφάλεια δικτύων και πληροφοριών.
4	2	Το κεντρικό αποθετήριο επικαιροποιείται σε περίπτωση νέων απαιτήσεων ή τροποποίησης υπαρχόντων.

4	3	Τα περιεχόμενα του αποθετηρίου επικοινωνούνται στο αρμόδιο προσωπικό όπως και όταν απαιτείται.
4	4	Σε περίπτωση αναγνώρισης απόκλισης από μία ή περισσότερες απαιτήσεις δημιουργείται καταγεγραμμένο πλάνο ενεργειών συμμόρφωσης. Το πλάνο ενεργειών συμμόρφωσης περιέχει στοιχεία σχετικά με το 1) Τι χρειάζεται να υλοποιηθεί, 2) μέχρι πότε χρειάζεται να υλοποιηθεί, 3) σε ποιόν έχει ανατεθεί η υπευθυνότητα παρακολούθησης / ολοκλήρωσης της υλοποίησης, 4) ποιοι πόροι απαιτούνται για την αποτελεσματική υλοποίηση και 5) με ποιον τρόπο και από ποιόν ρόλο θα διενεργηθεί η αξιολόγηση της ορθώς και αποτελεσματικής υλοποίησης.
4	5	Οι σχετικές πολιτικές και διαδικασίες ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Ο οργανισμός εξουσιοδοτεί τη διενέργεια εξωτερικών επιθεωρήσεων / ελέγχων για τον έλεγχο της συμμόρφωσης με όλες τις σχετικές νομοθετικές, κανονιστικές και ρυθμιστικές απαιτήσεις, και συμβατικές απαιτήσεις όσον αφορά την ασφάλεια δικτύων και πληροφοριών.
5	2	Τα δεδομένα των επιθεωρήσεων, (εσωτερικά και εξωτερικά) προστατεύονται από μη εξουσιοδοτημένη πρόσβαση και διατηρούνται για τουλάχιστον 5 χρόνια, εκτός αν προβλέπεται διαφορετικά από την σχετική νομοθεσία.
5	3	Όπου αυτό είναι εφικτό ο οργανισμός συμμετέχει σε δραστηριότητες και λειτουργίες ώστε να ενημερώνεται για επικείμενες αλλαγές ή νέες προσθήκες απαιτήσεων όσο πιο γρήγορα γίνεται.
5	4	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	5	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
GOV3		**Μέτρο:** Πολιτικές, πρότυπα, κατευθυντήριες γραμμές και διαδικασίες ασφάλειας πληροφοριών. **Στόχος Μέτρου:** Να θεσπιστούν πολιτικές, πρότυπα, κατευθυντήριες γραμμές και διαδικασίες για την ασφάλεια πληροφοριών που να αντικατοπτρίζουν τη στρατηγική ασφάλειας πληροφοριών. **Περιγραφή Μέτρου:** Καθορισμός των μέτρων ασφάλειας πληροφοριών και λεπτομερής περιγραφή της εφαρμογής τους στα πλαίσια μιας πολιτικής ασφάλειας πληροφοριών που θα αντικατοπτρίζει τους στόχους που περιγράφονται στη στρατηγική ασφάλειας πληροφοριών [STR1]. Η πολιτική ασφάλειας των πληροφοριών θα πρέπει να περιλαμβάνει τους ρόλους και τις αρμοδιότητες σε επίπεδο οργάνωσης, όπως ορίζεται στο [GOV1]. Εφαρμογή συγκεκριμένων πολιτικών και διαδικασιών για την ασφάλεια πληροφοριών σε σχέση με συγκεκριμένες επεξεργασίες, συστήματα ή δραστηριότητες, ανάλογα με τις ανάγκες. Καθορισμός επιχειρησιακών κατευθυντήριων γραμμών για την ασφάλεια πληροφοριών και τυποποιημένες διαδικασίες λειτουργίας για συγκεκριμένες δραστηριότητες που σχετίζονται με πληροφορίες ή συστήματα επεξεργασίας πληροφοριών σε επιχειρησιακό επίπεδο. **Πηγή:** ISO 27002
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**
0	1	Δεν έχουν καθοριστεί από τον οργανισμό πολιτικές, οδηγίες και διαδικασίες σε σχέση με την ασφάλεια πληροφοριών.
1	1	Ακολουθείται μία σειρά από διαδικασίες και οδηγίες οι οποίες όμως δεν αντικατοπτρίζουν τις πραγματικές ανάγκες του οργανισμού σε σχέση με την ασφάλεια πληροφοριών.
1	2	Οι πολιτικές και οι διαδικασίες εφαρμόζονται μερικώς και το προσωπικό δεν είναι ή είναι μερικώς ενημερωμένο.
2	1	Έχει δημιουργηθεί μια πολιτική ασφάλειας πληροφοριών στην οποία γίνεται συνοπτική αναφορά και περιγραφή των μέτρων που έχουν ληφθεί.
3	1	Έχει δημιουργηθεί πολιτική ασφάλειας πληροφοριών όπου περιγράφονται αναλυτικά τα μέτρα που έχουν ληφθεί, όπως επίσης και λεπτομερή περιγραφή της εφαρμογής τους.

3	2	Η πολιτική ασφάλειας πληροφοριών αντικατοπτρίζει τους στόχους που περιγράφονται στη στρατηγική ασφάλειας πληροφοριών [STR1]
3	3	Η πολιτική ασφάλειας πληροφοριών περιλαμβάνει τους ρόλους και τις αρμοδιότητες σε επίπεδο οργάνωσης, όπως ορίζεται στο [GOV1].
3	4	Έχουν δημιουργηθεί μία σειρά από πολιτικές, οδηγίες και τυποποιημένες διαδικασίες λειτουργίας οι οποίες και εφαρμόζονται για την ασφάλεια πληροφοριών σε σχέση με συγκεκριμένες επεξεργασίες, συστήματα ή δραστηριότητες, ανάλογα με τις ανάγκες. και το προσωπικό έχει ενημερωθεί και εκπαιδευτεί σχετικά.
3	5	Όλες οι πολιτικές και οι διαδικασίες έχουν εγκριθεί από τη διοίκηση του οργανισμού.
3	6	Το προσωπικό έχει ενημερωθεί και εκπαιδευτεί σχετικά με τις πολιτικές και οι διαδικασίες.
4	1	Όλες οι πολιτικές και διαδικασίες ανασκοπούνται για την καταλληλότητά τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
4	2	Η ανασκόπηση περιλαμβάνει αξιολόγηση ευκαιριών για βελτίωση των πολιτικών, οδηγιών και διαδικασιών και της προσέγγισης του οργανισμού για τη διαχείριση της ασφάλειας των πληροφοριών ως απάντηση σε αλλαγές στο οργανωτικό περιβάλλον, τις επιχειρηματικές συνθήκες, τις νομικές συνθήκες ή το τεχνικό περιβάλλον.
5	1	Ο οργανισμός υλοποιεί αυτοματοποιημένα συστήματα για την διαχείριση της σχετικής τεκμηρίωσης.
5	2	Οι πολιτικές και οι διαδικασίες υλοποιούνται σε ένα μεγάλο βαθμό μέσα από αυτόματες ροές και παρέχεται η δυνατότητα απευθείας ενσωμάτωσης των διαφόρων δεδομένων, των εγκρίσεων και της υλοποίησης.
5	3	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους
5	4	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

Κατηγορία		ΔΙΑΧΕΙΡΙΣΗ ΚΙΝΔΥΝΩΝ
RM1		**Μέτρο:** Μεθοδολογία **Στόχος Μέτρου:** Να θεσπιστεί μεθοδολογία διαχείρισης κινδύνων, η οποία αντικατοπτρίζει τη διαδικασία εκτίμησης κινδύνου του οργανισμού, τα κριτήρια ανάλυσης κινδύνου, τα κριτήρια αποδοχής κινδύνων και την πολιτική ανάληψης κινδύνων. **Περιγραφή Μέτρου:** Θέσπιση μεθοδολογίας για τη διαχείριση κινδύνων μέσω του καθορισμού της διαδικασίας εκτίμησης κινδύνων, των κριτηρίων ανάλυσης κινδύνου (δηλαδή των κριτηρίων επιπτώσεων, των κριτηρίων πιθανότητας, της βαθμολογίας κινδύνου), των κριτηρίων αποδοχής κινδύνων και της πολιτικής ανάληψης κινδύνων από τον οργανισμό. Η μεθοδολογία διαχείρισης κινδύνου θα επιτρέψει στον οργανισμό να αξιολογήσει τους κινδύνους για την ασφάλεια πληροφοριών που αντιμετωπίζει, και να εφαρμόσει τα κατάλληλα μέτρα για την αντιμετώπιση ή τον μετριασμό τους. Ο οργανισμός θα πρέπει να θέσει σε εφαρμογή διαδικασίες και εργαλεία, ανάλογα με την περίπτωση, προκειμένου να στηρίξει τις διαδικασίες διαχείρισης κινδύνων, έχοντας κατ' ελάχιστον ένα μητρώο κινδύνων, ένα σχέδιο αντιμετώπισης κινδύνων και μια δομή διακυβέρνησης της ασφάλειας πληροφοριών στην οποία θα περιγράφονται λεπτομερώς οι ρόλοι και οι αρμοδιότητες. Η οριζόμενη μεθοδολογία διαχείρισης κινδύνων θα πρέπει να επικυρώνεται, να συμφωνείται και να υποστηρίζεται από τη διοίκηση ανώτατου επιπέδου και άλλους σχετικούς φορείς εντός του οργανισμού. **Πηγή:** C2M2 (Risk), NIST 800-53 (PM-9), ISO 27001 6.1
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**
0	1	Ο οργανισμός δεν υλοποιεί ενέργειες για την διαχείριση κινδύνων σχετικά με την ασφάλεια των πληροφοριών και των δικτύων.
1	1	Διενεργούνται σε ad hoc βάση, ή έχουν τουλάχιστον διενεργηθεί μια φορά κατά τα τελευταία 2 χρόνια ανάλυση και αποτίμηση κινδύνων σχετικά με την ασφάλεια των πληροφοριών και των δικτύων.
1	2	Η διαδικασία δεν είναι πλήρως καταγεγραμμένη αλλά αποτυπώνεται μέσα από τα αρχεία που διατηρήθηκαν κατά την υλοποίηση.
2	1	Έχει δημιουργηθεί και καταγραφεί διαδικασία για την διαχείριση κινδύνων ασφάλειας πληροφοριών και δικτύων.
2	2	Η διαδικασία περιέχει κατ' ελάχιστο ρόλους και αρμοδιότητες, κριτήρια για την διενέργεια της αξιολόγηση κινδύνων και τα σχετικά αρχεία που πρέπει να τηρούνται.
2	4	Μέσα από την εφαρμογή της διαδικασίας προκύπτει κατ' ελάχιστο μια προτεραιοποίηση των αναγνωρισμένων κινδύνων.
2	3	Όλες οι σχετικές πληροφορίες σε σχέση με τη διαχείριση των κινδύνων ασφάλειας πληροφοριών έχουν καταγραφεί και η εν λόγω πληροφόρηση παρέχεται στην Αρχή ετήσια ή και κατόπιν αιτήματος.
3	1	Έχει θεσπίστει και καταγράφει μεθοδολογία για τη διαχείριση κινδύνων.
3	2	Η μεθοδολογία περιέχει την διαδικασία εκτίμησης κινδύνων, προσδιορίζει τα κριτήρια ανάλυσης κινδύνου (τα οποία είναι κατ΄ ελάχιστον κριτήρια επιπτώσεων, κριτήρια πιθανότητας, και συναρτήσεις για την εξαγωγή της βαθμολογίας κινδύνου), των κριτηρίων αποδοχής κινδύνων και της πολιτικής ανάληψης κινδύνων από τον οργανισμό.
3	3	Ο ρόλος του ιδιοκτήτη κινδύνων ορίζεται στη μεθοδολογία και περιγράφονται οι ρόλοι και οι αρμοδιότητές τους σε σχέση με την διαχείρισης κινδύνων.
3	4	Η μεθοδολογία διαχείρισης κινδύνου επιτρέπει στον οργανισμό να αξιολογεί τους κινδύνους για την ασφάλεια πληροφοριών που αντιμετωπίζει, και να εφαρμόζει τα κατάλληλα μέτρα για την αντιμετώπιση ή τον μετριασμό τους λαμβάνοντας υπόψη το πλαίσιο λειτουργίας του.

	5	Έχουν τεθεί σε εφαρμογή διαδικασίες και εργαλεία, ανάλογα με την περίπτωση για υποστήριξη των διαδικασιών διαχείρισης κινδύνων, έχοντας κατ' ελάχιστον ένα μητρώο κινδύνων, ένα σχέδιο αντιμετώπισης κινδύνων και μια δομή διακυβέρνησης της ασφάλειας πληροφοριών στην οποία περιγράφονται λεπτομερώς οι ρόλοι και οι αρμοδιότητες.
3	6	Η οριζόμενη μεθοδολογία διαχείρισης κινδύνων επικυρώνεται, συμφωνείται και υποστηρίζεται από τη διοίκηση ανώτατου επιπέδου και άλλους σχετικούς φορείς εντός του οργανισμού.
3	7	Η μεθοδολογία ορίζει ότι εφαρμόζεται (ως μεθοδολογογία) εντός του οργανισμού σε τακτά χρονικά διαστήματα και τουλάχιστον ετησίως.
3	8	Έχει δημιουργηθεί μια διακριτή πολιτική ανάληψης κινδύνων η οποία έχει άμεση σχέση με τους στόχους, το πλαίσιο λειτουργίας και την στρατηγική του οργανισμού και αποτυπώνεται και στα σχετικά κριτήρια αποδοχής κινδύνου.
4	1	Η μεθοδολογία για τη διαχείριση κινδύνων ακολουθεί διεθνείς σχετικές βέλτιστες πρακτικές.
4	2	Η μεθοδολογία αποτυπώνει τα ακόλουθα επιμέρους βήματα για την διαχείριση κινδύνων: Πλαίσιο λειτουργίας, αξιολόγηση κινδύνων (που αποτελείται από αναγνώριση κινδύνων, ανάλυση κινδύνων και αποτίμηση κινδύνων), αντιμετώπιση κινδύνων, καταγραφή και αναφορά των κινδύνων, επικοινωνία, παρακολούθηση και ανασκόπηση κινδύνων.
4	3	Τα κριτήρια επιπτώσεων έχουν προσαρμοστεί και ανταποκρίνονται στις επιχειρησιακές ανάγκες και στόχους του οργανισμού όπως αναφέρονται στην σχετική στρατηγική [STR1], με στόχο να μπορούν να εξυπηρετήσουν την καλύτερη κατανόηση της συμπλήρωσης και των αποτελεσμάτων από το σύνολο του εμπλεκόμενου προσωπικού.
4	4	Ο οργανισμός εξάγει, παρακολουθεί και καταγράφει την επίδοση της διαχείρισης κινδύνων μέσω κατάλληλων μετρητών.
4	5	Η μεθοδολογία είναι συμβατή και τροφοδοτεί στοιχεία στην επιχειρησιακού επιπέδου διεργασία διαχείρισης κινδύνων (Enterprise Risk Management process).
4	6	Έχει οριστεί ένας υπεύθυνος που έχει επαρκή εξουσιοδότηση για την συνολική διαχείριση και παρακολούθηση της μεθοδολογίας.
4	7	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
4	8	Η μεθοδολογία αναγράφει σαφώς την συχνότητα εφαρμογής της μεθοδολογίας και την ανάγκη για επικαιροποίηση σε περίπτωση σημαντικών αλλαγών.
5	1	Η μεθοδολογία για τη διαχείριση κινδύνων περιλαμβάνεται στο πλαίσιο διακυβέρνησης του οργανισμού και είναι συμβατό με την σχετική στρατηγική όπως αναφέρεται στο [STR1].
5	2	Γίνονται εξωτερικές επιθεωρήσεις με αντικείμενο τον σχεδιασμό, την λειτουργία και την βελτίωση της μεθοδολογίας διαχείρισης κινδύνων.
5	3	Σε περίπτωση αναγνώρισης απόκλισης από μια ή περισσότερες απαιτήσεις δημιουργείται καταγεγραμμένο πλάνο ενεργειών συμμόρφωσης.
5	4	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους
5	5	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
5	6	Τα στοιχεία σχετικά με τον τρόπο που οργανισμός διαχειρίζεται τους κινδύνους ασφάλειας πληροφοριών και δικτύων επικοινωνούνται στα διάφορα εμπλεκόμενα μέρη όπως απαιτείται. Σε περίπτωση αλλαγής της κατάστασης των σχετικών κινδύνων, ενημερώνονται αντίστοιχα. (τα εμπλεκόμενα μέρη μπορεί να είναι τόσο εσωτερικά όσο και εξωτερικά του οργανισμού)

RM2	**Μέτρο:** Πλαίσιο **Στόχος Μέτρου:** Να καταρτιστεί κατάλογος στοιχείων ενεργητικού, συστημάτων και διαδικασιών εντός του οργανισμού. **Περιγραφή Μέτρου:** Κατάρτιση καταλόγου στοιχείων ενεργητικού, συστημάτων και διαδικασιών εντός του οργανισμού και καταγραφή των εξαρτήσεων και αλληλεξαρτήσεων μεταξύ αυτών των στοιχείων ενεργητικού, των συστημάτων και των διαδικασιών με σκοπό τη σαφή αποτύπωση του πλαισίου / περιβάλλοντος στο οποίο θα πραγματοποιηθεί η εκτίμηση κινδύνου. Μια σαφής εικόνα του πλαισίου του οργανισμού θα επιτρέψει τον εντοπισμό των κινδύνων εντός του οργανισμού **Πηγή:** C2M2 (Configuration), NIST 800-53 (PM-9), ISO 27001 A.8

Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν έχει κάποιο συγκεκριμένο / οργανωμένο τρόπο για την αναγνώριση στοιχείων ενεργητικού, συστημάτων και διαδικασιών εντός του οργανισμού.
1	1	Τα στοιχεία ενεργητικού καταγράφονται με μη συστηματικό τρόπο. Τηρείται κάποιο αρχείο, χωρίς κεντρική διαχείριση ενώ ενημερώνεται ad-hoc.
2	1	Τηρείται έναν ενιαίο κατάλογο στοιχείων ενεργητικού, συστημάτων και διαδικασιών εντός του οργανισμού στον οποίο δεν περιλαμβάνονται οι αλληλεξαρτήσεις μεταξύ τους.
2	2	Υπάρχει ένας αναγνωρισμένος ιδιοκτήτης του καταλόγου, ο οποίος είναι υπεύθυνος για την τήρηση και επικαιροποίηση των σχετικών δεδομένων.
3	1	Στον κατάλογο στοιχείων ενεργητικού έχουν καταγραφεί οι εξαρτήσεις και αλληλεξαρτήσεις μεταξύ αυτών των στοιχείων ενεργητικού, των συστημάτων και των διαδικασιών με σκοπό τη σαφή αποτύπωση του πλαισίου / περιβάλλοντος στο οποίο πραγματοποιείται η εκτίμηση κινδύνου.
3	2	Ο κατάλογος είναι συμβατός και μπορεί να συμπίπτει (να αποτελεί μέρος ή παράγωγο) με αυτόν που αναφέρεται στο [AM2], με την προϋπόθεση της κάλυψης και των 2 ομάδων απαιτήσεων για τα αντίστοιχα επίπεδα.
3	3	Τηρείται διαδικασία για την διαχείριση των πόρων όπως αναφέρεται στο [AM1], μέσω της οποίας εξασφαλίζεται η έγκαιρη ενημέρωση του καταλόγου σε περίπτωση αλλαγών.
4	1	Χρησιμοποιείται αυτόματο σύστημα για την αναγνώριση και καταγραφή στοιχείων ενεργητικού και συστημάτων εντός του οργανισμού αλλά και εκτός του οργανισμού (hosted in third parties).
4	2	Τα στοιχεία που εξάγονται από το αυτόματο σύστημα συμπληρώνονται με στοιχεία διαδικασιών και δημιουργείται αποτύπωση των σχετικών εξαρτήσεων και αλληλεξαρτήσεων με όσο περισσότερο αυτοματοποιημένο τρόπο γίνεται.
4	3	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Διατήθεται αυτόματο σύστημα και διαδικασίες για τον ελέγχου της ακεραιότητας και εγκυρότητας των στοιχείων του καταλόγου στοιχείων ενεργητικού, συστημάτων και διαδικασιών.
5	2	Σε περίπτωση ανίχνευσης στοιχείου που δεν βρίσκεται καταχωρημένο στον κατάλογο διενεργούνται αυτόματες ενέργειες ενημέρωσης του αρμόδιου προσωπικού για τον έλεγχο και επικαιροποίηση των σχετικών στοιχείων.
5	3	Ειδικά σε περίπτωση στοιχείων ενεργητικού, λαμβάνονται άμεσες ενέργειες περιορισμού μέχρι την υλοποίηση της σχετικής διερεύνησης.
5	4	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	5	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

RM3		**Μέτρο:** Εντοπισμός κινδύνων **Στόχος Μέτρου:** Να εντοπιστούν οι απειλές, ευπάθειες και κίνδυνοι στους οποίους εκτίθενται τα στοιχεία ενεργητικού, τα συστήματα και οι διαδικασίες του οργανισμού. **Περιγραφή Μέτρου:** Προσδιορισμός και κατάρτιση καταλόγου απειλών, ευπαθειών και κινδύνων στους οποίους είναι εκτεθειμένος ο οργανισμός όσον αφορά τα στοιχεία ενεργητικού, τα συστήματα και τις διαδικασίες που προσδιορίζονται στο μέτρο [RM2]. Οι κίνδυνοι που θα εντοπιστούν στα πλαίσια αυτής της διαδικασίας πρέπει να αποτυπώνονται σε μητρώο κινδύνων ώστε να μπορεί ο οργανισμός να παρακολουθεί τις απειλές, τις ευπάθειες και τους κινδύνους στους οποίους είναι εκτεθειμένος. **Πηγή:** C2M2 (RISK), NIST 800-53 (RA-1, RA-5), ISO 27001 6.1., ISO 27005
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**
0	1	Ο οργανισμός δεν υλοποιεί ενέργειες για την αναγνώριση κινδύνων σχετικά με την ασφάλεια των πληροφοριών και των δικτύων.
1	1	Διενεργούνται σε ad hoc βάση, ή έχουν τουλάχιστον διενεργηθεί μια φορά κατά τα τελευταία 2 χρόνια ανάλυση και αποτίμηση κινδύνων σχετικά με την ασφάλεια των πληροφοριών και των δικτύων.
1	2	Η διαδικασία αναγνώρισης κινδύνων δεν είναι πλήρως καταγεγραμμένη αλλά έχει δημιουργηθεί και διατηρείται τουλάχιστον μια λίστα κινδύνων σχετικά με την ασφάλειας των πληροφοριών και των δικτύων.
2	1	Έχει δημιουργηθεί και καταγραφεί διαδικασία για την διαχείριση κινδύνων ασφάλειας πληροφοριών και δικτύων στην οποία αναφέρεται και η αναγνώριση κινδύνων.
2	2	Η διαδικασία περιέχει κατ' ελάχιστο ρόλους και αρμοδιότητες, κριτήρια για την διενέργεια της αναγνώρισης κινδύνων και τα σχετικά αρχεία που πρέπει να τηρούνται.
2	3	Οι κίνδυνοι αναγνωρίζονται ανά στοιχείο που περιέχεται στον ενιαίο κατάλογο στοιχείων ενεργητικού, συστημάτων και διαδικασιών εντός του οργανισμού.
3	1	Ο οργανισμός έχει προσδιορίσει και καταρτίσει κατάλογο απειλών, ευπαθειών και κινδύνων στους οποίους είναι εκτεθειμένος ο οργανισμός όσον αφορά τα στοιχεία ενεργητικού, τα συστήματα και τις διαδικασίες που προσδιορίζονται στο μέτρο [RM2].
3	2	Οι κίνδυνοι που εντοπίζονται στα πλαίσια αυτής της διαδικασίας αποτυπώνονται σε μητρώο κινδύνων ώστε να μπορεί ο οργανισμός να παρακολουθεί τις απειλές, τις ευπάθειες και τους κινδύνους στους οποίους είναι εκτεθειμένος.
3	3	Τα στοιχεία του καταλόγου είναι σύμφωνα με διεθνείς βέλτιστες πρακτικές.
3	4	Για κάθε κίνδυνο αναγνωρίζεται ένας τουλάχιστον ιδιοκτήτης κινδύνου όπως ορίζει η σχετική διαδικασία του [RM1].
3	5	Σε κάθε περίπτωση περιλαμβάνονται κίνδυνοι που προκύπτουν από τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, άνευ αδείας κοινοποίηση ή πρόσβαση σε πληροφορίες που διαβιβάζονται, αποθηκεύονται ή υποβάλλονται κατ’ άλλο τρόπο σε επεξεργασία καθώς και άλλοι κίνδυνοι που παρουσιάζονται οι οποίοι θα μπορούσαν να έχουν επιδράσουν δυνητικά σε ουσιώδεις οικονομικές και κοινωνικές λειτουργίες και υπηρεσίες που παρέχονται από τον ΦΕΒΥ ή ΦΚΥΠ.
4	1	Οι κίνδυνοι έχουν αναγνωριστεί στην βάση του ενημερωμένου καταλόγου στοιχείων ενεργητικού, συστημάτων και διαδικασιών του οργανισμού όπως περιγράφεται στο [RM2].
4	2	Οι κίνδυνοι καλύπτουν όλες τις πιθανές κατηγορίες πηγών κινδύνων (risk sources) ανεξάρτητα από το αν είναι υπό τον έλεγχο του οργανισμού. Ειδικά για τα πολύπλοκα και κρίσιμα σενάρια κινδύνων, η μεθοδολογία επαναλαμβάνεται (iterations - στην αρχή σε high level και στην συνέχεια drilling down σε περισσότερες λεπτομέρειες μέχρι να αναγνωριστεί το ορθό root cause).
4	3	Όπου έχουν γίνει παραδοχές και ομαδοποιήσεις, υπάρχει σχετική καταγραφή που εξηγεί το σκεπτικό και προκύπτει ότι οι κίνδυνοι είναι σχετικοί σε όλα τα επίπεδα σύμφωνα με το πλαίσιο λειτουργίας του οργανισμού.

4	4	Η αναγνώριση κινδύνων είναι βασικό κομμάτι της διαχείρισης κινδύνου και διενεργείται σύμφωνα με την περιοδικότητα που έχει αναγνωριστεί στην σχετική διαδικασία όπως αναφέρεται στο [RM1].
4	5	Όταν τα εμπλεκόμενα μέρη αναγνωρίσουν ότι αδυναμίες, απειλές ή κίνδυνοι δεν είναι πλέον εφαρμόσιμοι, ο σχετικός κατάλογος επικαιροποιείται υποδεικνύοντας ότι η αντίστοιχη εγγραφή δεν είναι πλέον ενεργή. (Η ιστορικότητα αναγνώρισης διατηρείται και τεκμηριώνεται).
4	6	Τα στοιχεία του καταλόγου ενημερώνονται / επικαιροποιούνται / εμπλουτίζονται σε σύνδεση με την διαδικασία καταγραφής και αναφοράς ευπαθειών όπως αναφέρεται στο [VM2].
4	7	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
4	9	Για την αναγνώριση των απειλών, ευπαθειών και κινδύνων στους οποίους είναι εκτεθειμένος ο οργανισμός γίνεται με την συμμετοχή όσο μεγαλύτερου πλήθους εσωτερικών μερών γίνεται.
4	10	Υπάρχει δυνατότητα και διαδικασία γνωστή στο προσωπικό για την παροχή στοιχείων αναγνώρισης απειλών, ευπαθειών και κινδύνων στους οποίους είναι εκτεθειμένος ο οργανισμός από το προσωπικό ad-hoc.
4	11	Γίνεται τακτικός έλεγχος πληρότητας των στοιχείων των καταλόγων έναντι διεθνών έγκυρων πηγών.
5	1	Έγκυρες πληροφορίες Cyber threat intelligence λαμβάνονται έγκαιρα και μεταξύ άλλων χρησιμοποιούνται για την επικαιροποίηση του καταλόγου απειλών, ευπαθειών και κινδύνων στους οποίους είναι εκτεθειμένος ο οργανισμός.
5	2	Τα στοιχεία από τα διδάγματα που έχουν αντληθεί από τα συμβάντα και περιστατικά ασφάλειας πληροφοριών, χρησιμοποιούνται για την ενημέρωση των στοιχείων του καταλόγου (απειλών, ευπαθειών και κινδύνων) σε συμφωνία με τα αναγραφόμενα στο [EIM4].
5	3	Γίνονται τακτικές και εξειδικευμένες συναντήσεις με εσωτερικά και εξωτερικά εμπλεκόμενα μέρη για την υποβοήθηση / εμπλουτισμό και επικαιροποίηση του καταλόγου απειλών, ευπαθειών και κινδύνων στους οποίους είναι εκτεθειμένος ο οργανισμός.
5	4	Τα αποτελέσματα από εσωτερικούς και εξωτερικούς ελέγχους που υποδεικνύουν κενά στην συμμόρφωση του οργανισμού, καταγράφονται ως κίνδυνοι και αναλύονται στον σχετικό κατάλογο.
5	5	Κίνδυνοι που σχετίζονται με την εξάρτηση από άλλες κρίσιμες υποδομές ή τρίτους οργανισμούς περιέχονται στον σχετικό κατάλογο.
5	6	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	7	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

RM4	**Μέτρο:** Ανάλυση κινδύνου **Στόχος Μέτρου:** Να αναλυθούν οι κίνδυνοι για την ασφάλεια πληροφοριών στο πλαίσιο των στοιχείων ενεργητικού ανάλογα με τις διάφορες πιθανότητες και επιπτώσεις. **Περιγραφή Μέτρου:** Ανάλυση των κινδύνων για την ασφάλεια πληροφοριών όσον αφορά τα στοιχεία ενεργητικού, όπως προσδιορίζονται στο [RM2], λαμβάνοντας υπόψη τις διαφορετικές πιθανότητες και τις βαθμολογίες των επιπτώσεων, όπως ορίζονται στο [RM1]. Ο οργανισμός προσδιορίζει τη βαθμολογία κινδύνου προκειμένου να αξιολογήσει την κατάλληλη στρατηγική μετριασμού της [RM5]. Κατά την αξιολόγηση του κατάλληλου επιπέδου ασφάλειας, λαμβάνονται ιδίως υπόψη οι κίνδυνοι που προκύπτουν από τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, άνευ αδείας κοινοποίηση ή πρόσβαση σε πληροφορίες που διαβιβάζονται, αποθηκεύονται ή υποβάλλονται κατ' άλλο τρόπο σε επεξεργασία. Επίσης, λαμβάνονται υπόψη οι κίνδυνοι που παρουσιάζονται οι οποίοι θα μπορούσαν να επιδράσουν δυνητικά σε ουσιώδεις οικονομικές και κοινωνικές λειτουργίες και υπηρεσίες που παρέχονται από τον ΦΕΒΥ ή ΦΚΥΠ. Τα αποτελέσματα της ανάλυσης κινδύνου θα πρέπει να καταγράφονται στο μητρώο κινδύνων του οργανισμού. **Πηγή:** C2M2 (RISK), NIST 800-53 (RA-1, RA-6), ISO 27001 6.1., ISO 27005

Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν υλοποιεί ενέργειες για την ανάλυση κινδύνων σχετικά με την ασφάλεια των πληροφοριών και των δικτύων.
1	1	Διενεργούνται σε ad hoc βάση, ή έχουν τουλάχιστον διενεργηθεί μια φορά κατά τα τελευταία 2 χρόνια ανάλυση κινδύνων σχετικά με την ασφάλεια των πληροφοριών και των δικτύων.
1	2	Η διαδικασία ανάλυσης κινδύνων δεν είναι πλήρως καταγεγραμμένη αλλά τηρείται τουλάχιστον ένα αρχείο που περιέχει τα σχετικά κριτήρια και τα αποτελέσματα της ανάλυσης των κινδύνων.
2	1	Έχει δημιουργηθεί και καταγραφεί διαδικασία για την διαχείριση κινδύνων ασφάλειας πληροφοριών και δικτύων στην οποία αναφέρεται και το κομμάτι της ανάλυσης κινδύνων.
2	2	Η διαδικασία περιέχει κατ' ελάχιστο ρόλους και αρμοδιότητες, κριτήρια για την διενέργεια της ανάλυσης κινδύνων και τα σχετικά αρχεία που πρέπει να τηρούνται.
2	3	Οι κίνδυνοι αναλύονται ανά στοιχείο που περιέχεται στον ενιαίο κατάλογο στοιχείων ενεργητικού, συστημάτων και διαδικασιών εντός του οργανισμού.
3	1	Υλοποιείται ανάλυση των κινδύνων για την ασφάλεια πληροφοριών όσον αφορά τα στοιχεία ενεργητικού, όπως προσδιορίζονται στο [RM2], λαμβάνοντας υπόψη τις διαφορετικές πιθανότητες και τις βαθμολογίες των επιπτώσεων, όπως ορίζονται στο [RM1].
3	2	Ο κίνδυνος προσδιορίζεται και βαθμολογείται για αξιολόγηση της κατάλληλης στρατηγικής μετριασμού του [RM5].
3	3	Κατά την αξιολόγηση του κατάλληλου επιπέδου ασφάλειας, λαμβάνονται ιδίως υπόψη οι κίνδυνοι που προκύπτουν από τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, άνευ αδείας κοινοποίηση ή πρόσβαση σε πληροφορίες που διαβιβάζονται, αποθηκεύονται ή υποβάλλονται κατ' άλλο τρόπο σε επεξεργασία. Επίσης, λαμβάνονται υπόψη οι κίνδυνοι που παρουσιάζονται οι οποίοι θα μπορούσαν να επιδράσουν δυνητικά σε ουσιώδεις οικονομικές και κοινωνικές λειτουργίες και υπηρεσίες που παρέχονται από τον ΦΕΒΥ ή ΦΚΥΠ.
3	4	Τα αποτελέσματα της ανάλυσης κινδύνου καταγράφονται στο μητρώο κινδύνων του οργανισμού.
4	1	Κατά την εκτίμηση της πιθανότητας αλλά και της σχετικής επίπτωσης, λαμβάνεται υπόψη η υλοποίηση ανεξάρτητων και εξαρτημένων γεγονότων (π.χ. ένα δεύτερο γεγονός που μπορεί να υλοποιηθεί επειδή ένα πρώτο έχει συμβεί).
4	2	Αντίστοιχα υλοποιούνται μέθοδοι και προβλέψεις για τον προσδιορισμό cascading κίνδυνοι και οι επιπτώσεις τους.
4	3	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.

4	4	Η ανάλυση των κινδύνων στους οποίους είναι εκτεθειμένος ο οργανισμός γίνεται με την συμμετοχή όσο μεγαλύτερου πλήθους εσωτερικών μερών γίνεται.
4	5	Υπάρχει δυνατότητα και διαδικασία γνωστή στο προσωπικό για την ενημέρωση του αρμόδιου προσωπικού σε περίπτωση αναγνώρισης λάθους ή παράλειψης της ανάλυσης κινδύνων.
4	6	Για τον προσδιορισμό της πιθανότητας αλλά και της επίπτωσης των αναγνωρισμένων κινδύνων, λαμβάνεται υπόψη η υλοποίηση σχετικών (αν υπάρχουν) μέτρων αντιμετώπισης (controls).
5	1	Έγκυρες πληροφορίες Cyber threat intelligence λαμβάνονται έγκαιρα και μεταξύ άλλων χρησιμοποιούνται για την επικαιροποίηση των αποτελεσμάτων της ανάλυσης κινδύνων στους οποίους είναι εκτεθειμένος ο οργανισμός.
5	2	Τα στοιχεία από τα διδάγματα που έχουν αντληθεί από τα συμβάντα και περιστατικά ασφάλειας πληροφοριών, χρησιμοποιούνται για την ενημέρωση των αποτελεσμάτων της ανάλυσης κινδύνων σε συμφωνία με τα αναγραφόμενα στο [EIM4].
5	3	Γίνονται τακτικές και εξειδικευμένες συναντήσεις με εσωτερικά και εξωτερικά εμπλεκόμενα μέρη για την αξιολόγηση της ορθότητας και εγκυρότητας των αποτελεσμάτων της ανάλυσης κινδύνων.
5	4	Τα αποτελέσματα από εσωτερικούς και εξωτερικούς ελέγχους (στο βαθμό που σχετίζονται) χρησιμοποιούνται για την επικαιροποίηση των στοιχείων των αποτελεσμάτων της ανάλυσης κινδύνων.
5	5	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	6	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
5	7	Όπου είναι δυνατό, χρησιμοποιούνται αυτοματοποιημένα εργαλεία και βάσεις δεδομένων τα οποία προσδιορίζουν τις ευπάθειες των διαφόρων στοιχείων, αξιολογούν την ευκολία εκμετάλλευσής τους, καθορίζουν σχετικά σενάρια και διαδρομές επίθεσης και προσδιορίζουν την πιθανότητα υλοποίησης συγκεκριμένων κινδύνων.
5	8	Έχει δημιουργήσει ένα συστηματικό πλαίσιο για τον έλεγχο της αποτελεσματικότητας των μέτρων αντιμετώπισης που έχει υλοποιήσει ο οργανισμός και τα στοιχεία της αποτελεσματικότητας των μέτρων τροφοδοτούν συστηματικά κατάλληλα την ανάλυση κινδύνων.
RM5		**Μέτρο:** Αξιολόγηση κινδύνων **Στόχος Μέτρου:** Να αξιολογηθούν οι κίνδυνοι για την ασφάλεια πληροφοριών με βάση την πολιτική ανάληψης κινδύνων του οργανισμού και να καθοριστούν οι κατάλληλες στρατηγικές αντιμετώπισης. **Περιγραφή Μέτρου:** Καθορισμός κατάλληλων και επαρκών στρατηγικών για την αντιμετώπιση των κινδύνων που αναλύονται σύμφωνα με το [RM4]. Ο οργανισμός λαμβάνει υπόψη τη μείωση του κινδύνου, τη μεταφορά κινδύνου, την αποφυγή του κινδύνου και την αποδοχή (ή τη διατήρηση) κινδύνου ως κατάλληλες στρατηγικές αντιμετώπισης κινδύνων. Κατά την αξιολόγηση των στρατηγικών αντιμετώπισης κινδύνων, ο οργανισμός λαμβάνει υπόψη την πολιτική ανάληψης κινδύνων όπως ορίζεται στο [RM1]. Το αποτέλεσμα της αξιολόγησης κινδύνων θα πρέπει να καταγράφεται στο μητρώο κινδύνων του οργανισμού. **Πηγή:** C2M2 (RISK), NIST 800-53 (RA-1, RA-6), ISO 27001 6.1., ISO 27005
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**
0	1	Ο οργανισμός δεν υλοποιεί ενέργειες για την αξιολόγηση κινδύνων σχετικά με την ασφάλεια των πληροφοριών και των δικτύων.
1	1	Διενεργείται σε ad hoc βάση, ή έχει τουλάχιστον διενεργηθεί μια φορά κατά τα τελευταία 2 χρόνια αξιολόγηση κινδύνων σχετικά με την ασφάλεια των πληροφοριών και των δικτύων.
1	2	Η διαδικασία ανάλυσης κινδύνων δεν είναι πλήρως καταγεγραμμένη αλλά έχει δημιουργηθεί και διατηρείται τουλάχιστον ένα αρχείο που περιέχει τα σχετικά κριτήρια και τα αποτελέσματα της αξιολόγησης των κινδύνων.

2	1	Έχει δημιουργηθεί και καταγραφεί διαδικασία για την διαχείριση κινδύνων ασφάλειας πληροφοριών και δικτύων στην οποία αναφέρεται και το κομμάτι της αξιολόγησης κινδύνων.
2	2	Η διαδικασία περιέχει κατ' ελάχιστο ρόλους και αρμοδιότητες, κριτήρια για την διενέργεια της αξιολόγησης κινδύνων και τα σχετικά αρχεία που πρέπει να τηρούνται.
2	3	Οι κίνδυνοι αξιολογούνται ανά στοιχείο που περιέχεται στον ενιαίο κατάλογο στοιχείων ενεργητικού, συστημάτων και διαδικασιών εντός του οργανισμού.
3	1	Έχουν καθοριστεί κατάλληλες και επαρκείς στρατηγικές για την αντιμετώπιση των κινδύνων που αναλύονται σύμφωνα με το [RM4].
3	2	Λαμβάνεται υπόψη η μείωση του κινδύνου, η μεταφορά κινδύνου, η αποφυγή του κινδύνου και η αποδοχή (ή διατήρηση) κινδύνου ως κατάλληλες στρατηγικές αντιμετώπισης κινδύνων.
3	3	Κατά την αξιολόγηση των στρατηγικών αντιμετώπισης κινδύνων, λαμβάνεται υπόψη η πολιτική ανάληψης κινδύνων όπως ορίζεται στο [RM1].
3	4	Το αποτέλεσμα της αξιολόγησης κινδύνων καταγράφονται στο μητρώο κινδύνων του οργανισμού.
3	5	Οι αποφάσεις σχετικά με τις στρατηγικές που έχουν επιλεγεί ανά περίπτωση τεκμηριώνονται και διατηρούνται.
4	1	Οι πιθανές και επιλεγμένες στρατηγικές ανασκοπούνται περιοδικά από τα κατάλληλα εξουσιοδοτημένα ενδιαφερόμενα μέρη, προκειμένου να εξεταστεί κατά πόσο εξακολουθούν να είναι κατάλληλες και αποτελεσματικές για την διαχείριση των σχετικών κινδύνων για τον οργανισμό.
4	2	Αλλαγές σε σχέση με την τεχνολογία, τις υπηρεσίες ή νέες στρατηγικές συνεργασίες οδηγούν στην ανασκόπηση των σχετικών στρατηγικών και αποφάσεων.
4	3	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
4	4	Ο ιδιοκτήτης του κινδύνου, δίνει την έγγραφη αποδοχή του σχετικά με την αποδοχή του εναπομείναντα κινδύνου και της επιλεγμένης στρατηγικής αντιμετώπισης κινδύνου.
5	1	Κατά το στάδιο του προσδιορισμού των κατάλληλων στρατηγικών, δημιουργείται και διατηρείται σχετική τεκμηρίωση η οποία περιέχει τα υπέρ, τα κατά, καθώς και μια αποτίμηση σε σχέση με το εκτιμώμενο κόστος χρησιμοποιώντας διεθνώς αναγνωρισμένες σχετικές πρακτικές (π.χ. προσδιορισμός ROSI).
5	2	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	3	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
RM6		**Μέτρο:** Αντιμετώπιση κινδύνων **Στόχος Μέτρου:** Να καθοριστούν οι δράσεις για την αντιμετώπιση των κινδύνων για την ασφάλεια πληροφοριών. **Περιγραφή Μέτρου:** Καθορισμός κατάλληλων και επαρκών μέτρων αντιμετώπισης του κινδύνου στα πλαίσια της εφαρμογής της στρατηγικής αντιμετώπισης κινδύνων που καθορίζεται στη διαδικασία αξιολόγησης των κινδύνων, όπως αυτή περιγράφεται στην [RM5]. Κατά τον καθορισμό των μέτρων, ο οργανισμός λαμβάνει υπόψη προληπτικά μέτρα, μέτρα εντοπισμού και μέτρα αντίδρασης από διοικητική, τεχνολογική και φυσική άποψη, προκειμένου να διασφαλίσει, κατά περίπτωση, μια πολυεπίπεδη άμυνα. Κατά τον καθορισμό των δράσεων αντιμετώπισης κινδύνων, ο φορέας εξετάζει τα μέτρα ασφάλειας που περιγράφονται στο Πλαίσιο μέτρων ασφάλειας (το παρόν έγγραφο). Το αποτέλεσμα της αντιμετώπισης κινδύνων θα πρέπει να καταγράφεται στο σχέδιο αντιμετώπισης κινδύνων του οργανισμού. **Πηγή:** C2M2 (RISK), NIST 800-53 (RA-1, RA-6), ISO 27001 6.1., ISO 27005
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**

0	1	Ο οργανισμός δεν υλοποιεί δράσεις και ενέργειες για την αντιμετώπιση κινδύνων σχετικά με την ασφάλεια των πληροφοριών και των δικτύων.
1	1	Διενεργούνται σε ad hoc βάση, ή έχουν τουλάχιστον διενεργηθεί μια φορά κατά τα τελευταία 2 χρόνια ενέργειες / δράσεις για την αντιμετώπιση κινδύνων σχετικά με την ασφάλεια των πληροφοριών και των δικτύων.
1	2	Η διαδικασία αντιμετώπισης κινδύνων δεν είναι πλήρως καταγεγραμμένη αλλά έχει δημιουργηθεί και διατηρείται τουλάχιστον ένα αρχείο που περιέχει τις σχετικές ενέργειες.
2	1	Έχει δημιουργηθεί και καταγραφεί διαδικασία για την διαχείριση κινδύνων ασφάλειας πληροφοριών και δικτύων στην οποία αναφέρεται και το κομμάτι της αντιμετώπισης κινδύνων.
2	2	Η διαδικασία περιέχει κατ' ελάχιστο ρόλους και αρμοδιότητες, κριτήρια για την διενέργεια της αντιμετώπισης κινδύνων και τα σχετικά αρχεία που πρέπει να τηρούνται.
2	3	Υπάρχει αρχείο που περιέχει τις ενέργειες αντιμετώπισης, το οποίο περιέχει τι θα γίνει, μέχρι πότε, ποιος είναι υπεύθυνος και σε ποιο επίπεδο αναμένεται να βρεθεί το επίπεδο στο οποίο θα βρεθεί ο κίνδυνος μετά την αντιμετώπιση.
3	1	Καθορίζονται κατάλληλα και επαρκή μέτρα αντιμετώπισης του κινδύνου στα πλαίσια της εφαρμογής της στρατηγικής αντιμετώπισης κινδύνων που καθορίζεται στη διαδικασία αξιολόγησης των κινδύνων, όπως αυτή περιγράφεται στην [RM5].
3	2	Κατά τον καθορισμό των μέτρων, λαμβάνονται υπόψη προληπτικά μέτρα, μέτρα εντοπισμού και μέτρα αντίδρασης από διοικητική, τεχνολογική και φυσική άποψη, προκειμένου να διασφαλίζεται, κατά περίπτωση, μια πολυεπίπεδη άμυνα.
3	3	Κατά τον καθορισμό των δράσεων αντιμετώπισης κινδύνων, ο φορέας εξετάζει τα μέτρα ασφάλειας που περιγράφονται στην σχετική νομοθεσία της Αρχής (Κ.Δ.Π. 389/2020).
3	4	Το αποτέλεσμα της αντιμετώπισης κινδύνων καταγράφεται στο σχέδιο αντιμετώπισης κινδύνων του οργανισμού.
3	5	Το σχέδιο κινδύνων περιέχει τουλάχιστον τα ακόλουθα για κάθε κίνδυνο: τι θα γίνει, μέχρι πότε, ποιος είναι υπεύθυνος και σε ποιο επίπεδο αναμένεται να βρεθεί το επίπεδο στο οποίο θα βρεθεί ο κίνδυνος μετά την αντιμετώπιση, ποιοι είναι οι πόροι που απαιτούνται, με ποιόν τρόπο θα ελεγχθεί η αποτελεσματικότητα των ενεργειών, ποιος είναι ο ιδιοκτήτης του κινδύνου.
4	1	Διενεργείται περιοδικά έλεγχος της πορείας υλοποίησης των ενεργειών αντιμετώπισης κινδύνου. Το χρονικό διάστημα στο οποίο ο οργανισμός πρέπει να υλοποιήσει τις σχετικές ενέργειες καθορίζεται σύμφωνα με την κρισιμότητα του κινδύνου όπως αποτυπώνεται και στην σχετική διαδικασία.
4	2	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
4	3	Προκειμένου να αξιολογηθεί η πληρότητα των επιλεγμένων μέτρων, γίνεται σε τακτική βάση, σύγκριση με οργανωμένες λίστες ενεργειών (π.χ. ISO 27002 / ISO 27001 Annex A, ISO 27017, ISO 27011 κ.α.).
4	4	Σε περίπτωση που αναγνωριστεί κάποια ενέργεια η οποία μπορεί να υλοποιηθεί, ο οργανισμός προβαίνει σε κατάλληλη αξιολόγηση διενεργώντας τα βήματα της διαχείρισης κινδύνου με πεδίο τους κινδύνους που μπορεί να καλύψει η συγκεκριμένη ενέργεια.
5	1	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	2	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
5	3	Έχει δημιουργηθεί ένα συστηματικό πλαίσιο για τον έλεγχο της αποτελεσματικότητας των μέτρων αντιμετώπισης που έχει υλοποιήσει ο οργανισμός.
5	4	Ο οργανισμός εξουσιοδοτεί την διενέργεια εξωτερικών επιθεωρήσεων / ελέγχων για τον έλεγχο της αποτελεσματικότητας των υλοποιημένων μέτρων.

5	5	Τα στοιχεία της αποτελεσματικότητας των μέτρων τροφοδοτούν συστηματικά κατάλληλα τα βήματα αξιολόγησης και αντιμετώπισης κινδύνων ώστε να γίνουν τροποποιήσεις όπου απαιτείται.

Κατηγορία		ΕΥΑΙΣΘΗΤΟΠΟΙΗΣΗ ΚΑΙ ΕΚΠΑΙΔΕΥΣΗ
ΤΑ1		**Μέτρο:** Ευαισθητοποίηση σχετικά με την ασφάλεια πληροφοριών **Στόχος Μέτρου:** Να θεσπιστεί πρόγραμμα ενημέρωσης σχετικά με την ασφάλεια πληροφοριών για όλα τα στελέχη εντός του οργανισμού, λαμβάνοντας υπόψη τα στοιχεία που περιγράφονται στις πολιτικές, τα πρότυπα, τις κατευθυντήριες γραμμές και τις διαδικασίες ασφάλειας πληροφοριών. **Περιγραφή Μέτρου:** Καθορισμός προγράμματος ευαισθητοποίησης όσον αφορά την ασφάλεια των πληροφοριών, ώστε να υπάρχει επαρκής ευαισθητοποίηση των στελεχών σχετικά με τους ρόλους και τις ευθύνες όσον αφορά την ασφάλεια δικτύων και πληροφοριών, όπως ορίζεται στο [GOV1]. **Πηγή:** CIS, ISO 27002
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**
0	1	Ο οργανισμός δεν έχει θεσπίσει πρόγραμμα ενημέρωσης σχετικά με την ασφάλεια πληροφοριών για τα στελέχη εντός του οργανισμού.
1	1	Έχει δημιουργηθεί ένα πρόγραμμα ενημέρωσης σχετικά με την ασφάλεια πληροφοριών το οποίο δεν πραγματοποιείται συστηματικά.
1	2	Η εκπαίδευση αφορά τις βασικές αρχές για την ασφάλεια πληροφοριών.
2	1	Έχει δημιουργηθεί πρόγραμμα ενημέρωσης σχετικά με την ασφάλεια πληροφοριών το οποίο το παρακολουθούν όλα τα στελέχη του οργανισμού σε συγκεκριμένες περιόδους, ώστε να διασφαλίζεται ότι κατανοούν και επιδεικνύουν τις απαραίτητες συμπεριφορές και δεξιότητες για να διασφαλιστεί η ασφάλεια του οργανισμού.
3	1	Έχει γίνει καθορισμός προγράμματος ευαισθητοποίησης όσον αφορά την ασφάλεια των πληροφοριών, ώστε να υπάρχει επαρκής ευαισθητοποίηση των στελεχών σχετικά με τους ρόλους και τις ευθύνες όσον αφορά την ασφάλεια δικτύων και πληροφοριών, όπως ορίζεται στο [GOV1].
3	2	Το πρόγραμμα ευαισθητοποίησης για την ασφάλεια των πληροφοριών έχει δημιουργηθεί σύμφωνα με τις πολιτικές και τις σχετικές διαδικασίες του οργανισμού, λαμβάνοντας υπόψη τις πληροφορίες του οργανισμού που θα πρέπει να προστατεύονται και τα μέτρα που έχουν εφαρμοστεί για την προστασία των πληροφοριών.
3	3	Το πρόγραμμα ευαισθητοποίησης έχει σχεδιαστεί λαμβάνοντας υπόψη τους ρόλους των εργαζομένων στον οργανισμό και, κατά περίπτωση, τις προσδοκίες του οργανισμού για την ευαισθητοποίηση των εργολάβων.
3	4	Οι δραστηριότητες στο πρόγραμμα ευαισθητοποίησης προγραμματίζονται σε τακτικά χρονικά διαστήματα και τουλάχιστον μια φορά το χρόνο, ώστε οι δραστηριότητες να επαναλαμβάνονται και να καλύπτουν νέους εργαζόμενους και εργολάβους.
3	5	Στην περίπτωση νέου εργαζόμενου η εκπαίδευση πραγματοποιείται αμέσως μετά την πρόσληψη.
4	1	Το πρόγραμμα ευαισθητοποίησης ενημερώνεται τακτικά, ώστε να είναι σύμφωνο με τις οργανωτικές πολιτικές και διαδικασίες και βασίζεται σε διδάγματα που αντλούνται από συμβάντα ασφάλειας πληροφοριών.
4	2	Περιλαμβάνει μια σειρά από δραστηριότητες ευαισθητοποίησης, όπως εκστρατείες (π.χ. μια «ημέρα ασφάλειας πληροφοριών») και έκδοση φυλλαδίων ή ενημερωτικών δελτίων.
4	3	Η αποτελεσματικότητα του προγράμματος αξιολογείται περιοδικά (τουλάχιστον μία φορά το χρόνο) και γίνονται βελτιώσεις ανάλογα με την περίπτωση. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Το πρόγραμμα ευαισθητοποίησης εξετάζει διαφορετικές μορφές εκπαίδευσης και κατάρτισης, π.χ. διαλέξεις ή αυτοδιδασκαλία. Το πρόγραμμα ευαισθητοποίησης περιλαμβάνει συνεχή εκπαίδευση και ευκαιρίες επαγγελματικής ανάπτυξης για το προσωπικό με σημαντικές ευθύνες στην ασφάλεια πληροφοριών.

5	2	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	3	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
ΤΑ2		**Μέτρο:** Ευαισθητοποίηση και εκπαίδευση σε θέματα ασφάλειας πληροφοριών **Στόχος Μέτρου:** Να παρέχει εκπαίδευση προς όλα τα στελέχη του οργανισμού, όπως ορίζεται στο πρόγραμμα ασφάλειας πληροφοριών. **Περιγραφή Μέτρου:** Επαρκής ενημέρωση των στελεχών σχετικά με τους ρόλους και τις αρμοδιότητες τους όσον αφορά την ασφάλεια δικτύων και πληροφοριών, όπως ορίζεται στο [GOV1] μέσω κατάλληλης εκπαίδευσης και κατάρτισης που προσφέρεται με την υποστήριξη της διοίκησης ανώτατου επιπέδου. Οι εκπαιδεύσεις σχετικά με την ασφάλεια πληροφοριών περιλαμβάνουν συγκεκριμένες πληροφορίες σχετικά με τις επιχειρησιακές δραστηριότητες των στελεχών για λογαριασμό του οργανισμού στο πλαίσιο της επεξεργασίας πληροφοριών ή της πρόσβασης σε συστήματα επεξεργασίας πληροφοριών. **Πηγή:** C2M2, ISO 27002, ISO 27003, ENISA
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**
0	1	Ο οργανισμός δεν πραγματοποιεί εκπαιδεύσεις στο προσωπικό σε σχέση με την Ασφάλεια Πληροφοριών.
1	1	Πραγματοποιούνται εκπαιδεύσεις σε σχέση με την ασφάλεια πληροφοριών στο εμπλεκόμενο προσωπικό χωρίς όμως αυτές να υλοποιούνται συστηματικά και χωρίς να περιλαμβάνεται το σύνολο του προσωπικού.
2	1	Πραγματοποιούνται εκπαιδεύσεις συστηματικά σε όλο προσωπικό σε σχέση με την ασφάλεια πληροφοριών χωρίς όμως να υπάρχει πρόγραμμα ενημέρωσης όπως αυτό αναφέρεται στον [ΤΑ1].
2	2	Οι στόχοι σχετικά με την εκπαίδευση του προσωπικού για την ασφάλεια πληροφοριών είναι καθορισμένοι και διατηρούνται.
3	1	Παρέχεται επαρκή ενημέρωση των στελεχών σχετικά με τους ρόλους και τις αρμοδιότητες τους όσον αφορά την ασφάλεια δικτύων και πληροφοριών, όπως ορίζεται στο [GOV1] μέσω κατάλληλης εκπαίδευσης και κατάρτισης που προσφέρεται με την υποστήριξη της διοίκησης ανώτατου επιπέδου.
3	2	Οι εκπαιδεύσεις σχετικά με την ασφάλεια πληροφοριών περιλαμβάνουν συγκεκριμένες πληροφορίες σχετικά με τις επιχειρησιακές δραστηριότητες των στελεχών για λογαριασμό του οργανισμού στο πλαίσιο της επεξεργασίας πληροφοριών ή της πρόσβασης σε συστήματα επεξεργασίας πληροφοριών.
3	3	Ακολουθείται το πρόγραμμα ενημέρωσης σχετικά με την ασφάλεια πληροφοριών όπως αναφέρεται στο [ΤΑ1].
3	4	Διατηρούνται τεκμηριωμένες πληροφορίες σχετικά με τις εκπαιδεύσεις και τα αποτελέσματα αυτών.
3	5	Πραγματοποιούνται αρχικές εκπαίδευσεις όχι μόνο σε νέους υπαλλήλους αλλά και σε όσους μεταφέρονται σε νέες θέσεις ή αναλαμβάνουν νέους ρόλους με διαφορετικές απαιτήσεις ασφάλειας πληροφοριών.
4	1	Πραγματοποιούνται έλεγχοι σε σχέση με την γνώση του προσωπικού όσον αφορά την ασφάλεια πληροφοριών.
4	2	Η αποτελεσματικότητα των εκπαιδεύσεων σε σχέση με ασφάλεια πληροφοριών αξιολογείται περιοδικά, και τουλάχιστον μία φορά το χρόνο, και σύμφωνα με καθορισμένους παράγοντες ενεργοποίησης, όπως αλλαγές συστήματος και εξωτερικά συμβάντα, και γίνονται βελτιώσεις ανάλογα με την περίπτωση.
5	1	Παρέχονται στο προσωπικό συνεδρίες εκπαίδευσης για την απόκτηση αναγνωρισμένων πιστοποιητικών σε σχέση με την ασφάλεια πληροφοριών ή cybersecurity.

5	2	Έχουν δημιουργηθεί επαφές και κανάλια επικοινωνίας με ομάδες και ενώσεις σχετικές με την ασφάλεια πληροφοριών ώστε να παραμένει το προσωπικό ενημερωμένο με τις πιο πρόσφατες συνιστώμενες πρακτικές, τεχνικές και τεχνολογίες ασφάλειας.
5	3	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	4	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

Κατηγορία		ΔΙΑΧΕΙΡΙΣΗ ΤΡΙΤΩΝ ΜΕΡΩΝ ΚΑΙ ΠΡΟΜΗΘΕΥΤΩΝ
TPS1		**Μέτρο:** Δέουσα επιμέλεια για τρίτα μέρη και προμηθευτές **Στόχος Μέτρου:** Να επιδεικνύει τη δέουσα επιμέλεια σχετικά με τρίτα μέρη και προμηθευτές **Περιγραφή Μέτρου:** Επίδειξη δέουσας επιμέλειας κατά τον εντοπισμό και τη σύναψη συμβατικών σχέσεων με τρίτα μέρη και προμηθευτές, λαμβανομένων υπόψη των κινδύνων τρίτων μερών, μεταξύ άλλων, της εξάρτησης από τον εκάστοτε προμηθευτή, της διαχείρισης περιστατικών και της ευθύνης σε σχέση με την ασφάλεια δικτύων και πληροφοριών. Ο οργανισμός επιδεικνύει τη δέουσα επιμέλεια ως προς την ασφάλεια πληροφοριών όταν αναλαμβάνει τη συνεργασία με τρίτα μέρη ιδίως στο πλαίσιο της απόκτησης ή της παράδοσης λογισμικού. **Πηγή:** C2M2, ISO 27002
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**
0	1	Ο οργανισμός δεν λαμβάνει υπόψη του κατά τον εντοπισμό και τη σύναψη συμβατικών σχέσεων με τρίτα μέρη και προμηθευτές θέματα που επηρεάζουν την ασφάλεια πληροφοριών όπως κινδύνους που μπορεί να παρουσιαστούν από τα τρίτα μέρη, κατά πόσο εξαρτάται ο οργανισμός από τον εκάστοτε προμηθευτή και τον τρόπο διαχείρισης των περιστατικών ασφαλείας και της ευθύνης που έχουν οι προμηθευτές και τα τρίτα μέρη.
1	1	Για την επιλογή των προμηθευτών και των τρίτων μερών ο οργανισμός λαμβάνει υπόψη του την ικανότητα και την επάρκεια τους σε σχέση με την ασφάλεια πληροφοριών. Ο τρόπος που πραγματοποιείται είναι ad hoc.
2	1	Εντοπίζονται βασικές εξαρτήσεις και βασικοί κίνδυνοι που προκύπτουν από προμηθευτές και τρίτα μέρη. Ο τρόπος με τον οποίο γίνεται ο εντοπισμός είναι ad hoc και όχι συστηματικά.
2	2	Αναγνωρίζονται ad hoc και όχι συστηματικά τρίτα μέρη ή/και προμηθευτές που έχουν πρόσβαση, έλεγχο ή φύλαξη σε συστήματα ή πληροφορίες που είναι σημαντικά για τον οργανισμό και για την εκτέλεση των εργασιών τους. Δεν αποτυπώνονται σε συμβάσεις.
3	1	Ακολουθείται μια καθορισμένη μέθοδος (διαδικασία) για εντοπισμό κινδύνων που προκύπτουν από προμηθευτές και τρίτα μέρη.
3	2	Ακολουθείται μια καθορισμένη μέθοδος (διαδικασία) για τον εντοπισμό απαιτήσεων σε σχέση με την ασφάλεια πληροφοριών και την εφαρμογή σχετικών μέτρων που προστατεύουν από τους κινδύνους που προκύπτουν από προμηθευτές και τρίτα μέρη.
3	3	Καθορίζεται ο τρόπος πρόσβασης στις πληροφορίες, που επιτρέπεται σε διαφορετικούς τύπους προμηθευτών και τρίτα μέρη, η παρακολούθηση και ο έλεγχος της πρόσβασής τους.
3	4	Οι απαιτήσεις ασφάλειας πληροφοριών αποτυπώνονται σε συμβάσεις με τους προμηθευτές και τρίτα μέρη.
4	1	Οι προμηθευτές και τα τρίτα μέρη βεβαιώνουν περιοδικά την ικανότητά τους να πληρούν τις απαιτήσεις ασφάλειας πληροφοριών που έχουν συμφωνηθεί με τον οργανισμό.
4	2	Όλες οι πολιτικές και διαδικασίες ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Οι απαιτήσεις ασφάλειας για προμηθευτές και τρίτα μέρη περιλαμβάνουν ασφαλές λογισμικό και ασφαλείς απαιτήσεις ανάπτυξης προϊόντων, όπου αυτό είναι εφικτό.
5	2	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	3	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

TPS2	**Μέτρο:** Σχέσεις με τρίτα μέρη και προμηθευτές **Στόχος Μέτρου:** Να διασφαλιστεί η ενσωμάτωση συμβατικών ρητρών ασφάλειας πληροφοριών στις σχέσεις με τρίτα μέρη και προμηθευτές. **Περιγραφή Μέτρου:** Διατήρηση κεντρικού αποθετηρίου προμηθευτών, πωλητών και άλλων τρίτων μερών. Ο οργανισμός θα πρέπει να διασφαλίζει ότι όλες οι σχέσεις με τρίτα μέρη υποστηρίζονται από κατάλληλες συμβατικές ρήτρες, προκειμένου να διασφαλίζεται ότι, μεταξύ άλλων, οι ρόλοι, οι αρμοδιότητες και η ευθύνη σε περίπτωση συμβάντων όσον αφορά την ασφάλεια δικτύων και πληροφοριών είναι δεόντως καταγραμμένα. **Πηγή:** C2M2, ISO 27002

Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν έχει συνάψει συμβάσεις με προμηθευτές ή τρίτα μέρη (προμηθευτές ή τρίτα μέρη που μπορεί να επηρεάσουν την ασφάλεια πληροφοριών).
1	1	Έχουν συναφθεί συμβάσεις με προμηθευτές και τρίτα μέρη χωρίς να περιλαμβάνονται απαιτήσεις ασφαλείας.
2	1	Έχουν συναφθεί συμβάσεις με προμηθευτές και τρίτα μέρη στις οποίες περιλαμβάνονται κάποιες απαιτήσεις ασφαλείας οι οποίες είναι ad hoc και δεν γίνεται συστηματικά για το σύνολο των προμηθευτών που εμπλέκονται σε θέματα σχετικά με την ασφάλεια πληροφοριών.
3	1	Έχει δημιουργηθεί σχετική λίστα που περιλαμβάνει τους προμηθευτές και τα τρίτα μέρη.
3	2	Έχουν προτεραιοποιηθεί οι προμηθευτές και τα τρίτα μέρη σύμφωνα με προκαθορισμένα κριτήρια που έχουν αποφασιστεί και εγκριθεί.
3	3	Ακολουθείταιμια καθορισμένη μέθοδος (διαδικασία) για την αξιολόγηση των προμηθευτών και άλλων τρίτων μερών.
3	4	Εφαρμόζονται πιο αυστηροί έλεγχοι σε σχέση με την ασφάλεια πληροφοριών για προμηθευτές και τρίτα μέρη υψηλότερης προτεραιότητας.
3	5	Περιλαμβάνονται στις συμβάσεις με τους προμηθευτές και τα τρίτα μέρη νομικές και κανονιστικές απαιτήσεις, συμπεριλαμβανομένης της προστασίας δεδομένων, των δικαιωμάτων πνευματικής ιδιοκτησίας και των πνευματικών δικαιωμάτων, και περιγραφή του τρόπου με τον οποίο θα διασφαλίζουν ότι πληρούνται.
3	6	Περιλαμβάνεται στις συμβάσεις με προμηθευτές και τρίτα μέρη ταξινόμηση των πληροφοριών σύμφωνα με το σχήμα ταξινόμησης του οργανισμού όπως επίσης και χαρτογράφηση (mapping) μεταξύ του συστήματος ταξινόμησης του ίδιου του οργανισμού και του σχήματος ταξινόμησης του προμηθευτή.
3	7	Περιλαμβάνονται στις συμβάσεις με προμηθευτές και τρίτα μέρη απαιτήσεις και διαδικασίες διαχείρισης συμβάντων (ειδικά ειδοποίηση και συνεργασία κατά την αποκατάσταση περιστατικών)
3	8	Έχει δημιουργηθεί πολιτική ασφάλειας η οποία και κοινοποιείται στους προμηθευτές και τα τρίτα μέρη.
4	1	Η προτεραιοποίηση των προμηθευτών και άλλων τρίτων μερών ανασκοπείται περιοδικά και σύμφωνα με καθορισμένους παράγοντες ενεργοποίησης, όπως αλλαγές συστήματος και εξωτερικά συμβάντα. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
4	2	Πραγματοποιούνται σε ετήσια βάση επιτόπιες επιθεωρήσεις σε σχέση με την ασφάλεια πληροφοριών για προμηθευτές ή τρίτα μέρη υψηλότερης προτεραιότητας.
4	3	Όλες οι πολιτικές και διαδικασίες ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Γίνεται ανάθεση σε ανεξάρτητο τρίτο μέρος η διεξαγωγή επιθεώρησης σε σχέση με την ασφάλεια πληροφοριών για προμηθευτές ή τρίτα μέρη υψηλότερης προτεραιότητας.

5	2	Οι προμηθευτές και τα τρίτα μέρη συμμορφώνονται πλήρως με τι απαιτήσεις ασφάλειας του οργανισμού.
5	3	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	4	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

Κατηγορία		ΑΣΦΑΛΕΙΑ ΔΕΔΟΜΕΝΩΝ
DS1		**Μέτρο:** Διαχείριση του κύκλου ζωής των πληροφοριών **Στόχος Μέτρου:** Να εξασφαλιστεί η προστασία δεδομένων καθ' όλο τον κύκλο ζωής των πληροφοριών, συμπεριλαμβανομένης της συλλογής, καταχώρησης, οργάνωσης, δομής, αποθήκευσης, προσαρμογής ή μεταβολής, ανάκτησης, αναζήτησης, χρήσης, κοινοποίησης με διαβίβαση, διάδοσης ή κάθε άλλη μορφή διάθεσης, συσχέτισης ή συνδυασμού, περιορισμού, διαγραφής ή καταστροφής. **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση μέτρων ασφάλειας πληροφοριών για την προστασία πληροφοριών καθ' όλη τη διάρκεια του κύκλου ζωής των πληροφοριών. Κύκλος ζωής των πληροφοριών θεωρούνται ως όλα τα στάδια που σχετίζονται με την επεξεργασία των πληροφοριών, ενώ η επεξεργασία αφορά κάθε πράξη, ή σειρά πράξεων, που πραγματοποιείται σε δεδομένα προσωπικού χαρακτήρα, ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, είτε με αυτοματοποιημένα μέσα είτε όχι, όπως η συλλογή, καταχώριση, οργάνωση, δομή, αποθήκευση, προσαρμογή ή μεταβολή, ανάκτηση, αναζήτηση, χρήση, κοινοποίηση με διαβίβαση, διάδοση ή κάθε άλλη μορφή διάθεσης, συσχέτιση ή συνδυασμός, περιορισμός, διαγραφή ή καταστροφή. **Πηγή:** ENISA (PII MEASURES), CNIL
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**
0	1	Ο οργανισμός δεν έχει κάποια διαδικασία ή άλλο μέσο για την αναγνώριση και εφαρμογή μέτρων για την προστασίας δεδομένων καθ' όλο τον κύκλο ζωής των πληροφοριών τους.
1	1	Εφαρμόζονται κάποια μέτρα για την προστασία των πληροφοριών του αλλά δεν είναι οργανωμένος ο τρόπος αναγνώρισης των πληροφοριών και των μέτρων που χρειάζεται να εφαρμοστούν.
2	1	Έχει δημιουργηθεί διαδικασία για την διαχείριση του συνολικού κύκλου ζωής των πληροφοριών του οργανισμού (προσωπικά και μη προσωπικά δεδομένα).
2	2	Η διαδικασία περιλαμβάνει μια μεθοδολογία / προσέγγιση ή τρόπο για την αναγνώριση των πληροφοριών που επεξεργάζονται από τον οργανισμό στα πλαίσια των λειτουργιών του.
2	3	Οι πληροφορίες (τουλάχιστον σε επίπεδο κατηγοριών π.χ. λειτουργικές διαδικασίες, χρηματοοικονομικά δεδομένα, απλά προσωπικά δεδομένα προσωπικού κ.α.) καταγράφονται σε έναν κατάλογο (ο κατάλογος μπορεί να είναι ο ίδιος ή να συσχετίζεται ή να παράγεται από τον ενιαίο κατάλογο στοιχείων ενεργητικού, συστημάτων και διαδικασιών εντός του οργανισμού όπως αναφέρεται στο [RM2].
2	4	Υπάρχει ένας αναγνωρισμένος ιδιοκτήτης του καταλόγου, ο οποίος είναι υπεύθυνος για την τήρηση και επικαιροποίηση των σχετικών δεδομένων.
2	5	Για κάθε κατηγορία πληροφορίας έχει αναγνωριστεί το επίπεδο διαβάθμισης όπως αναφέρεται στο [DS2].
2	6	Ο χειρισμός των πληροφοριών γίνεται σύμφωνα σχετικές γραπτές οδηγίες οι οποίες αναφέρουν οδηγίες και περιορισμούς σε σχέση με τον τρόπο χειρισμού των πληροφοριών καθ' όλο τον κύκλο ζωής (από την δημιουργία / συλλογή μέχρι και την καταστροφή).
2	7	Κατ' ελάχιστο τα μέτρα για την καταστροφή κρίσιμων ή ευαίσθητων πληροφοριών περιλαμβάνουν 1) software-based overwriting για τα επαναχρησιμοποιούμενα μέσα αποθήκευσης ή φυσική καταστροφή για τα υπόλοιπα, 2) shredding χαρτιών και 3) προβλέψεις σε συμβάσεις με τρίτα μέρη αντίστοιχων μέτρων όπου απαιτούνται.
2	8	Για τα δεδομένα που βρίσκονται σε μεταφορά ή ανταλλάσσονται τα μέτρα πρέπει να συμφωνούν αντίστοιχα με το [DS4].

3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται μέτρα ασφάλειας πληροφοριών για την προστασία πληροφοριών καθ' όλη τη διάρκεια του κύκλου ζωής των πληροφοριών. (Κύκλος ζωής των πληροφοριών θεωρείται ως όλα τα στάδια που σχετίζονται με την επεξεργασία των πληροφοριών, ενώ η επεξεργασία αφορά κάθε πράξη, ή σειρά πράξεων, που πραγματοποιείται σε δεδομένα προσωπικού χαρακτήρα, ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, είτε με αυτοματοποιημένα μέσα είτε όχι, όπως η συλλογή, καταχώριση, οργάνωση, δομή, αποθήκευση, προσαρμογή ή μεταβολή, ανάκτηση, αναζήτηση, χρήση, κοινοποίηση με διαβίβαση, διάδοση ή κάθε άλλη μορφή διάθεσης, συσχέτιση ή συνδυασμός, περιορισμός, διαγραφή ή καταστροφή.)
3	2	Ο χειρισμός των πληροφοριών γίνεται σύμφωνα σχετικές γραπτές οδηγίες οι οποίες αναφέρουν οδηγίες και περιορισμούς σε σχέση με τον τρόπο χειρισμού των πληροφοριών καθ' όλο τον κύκλο ζωής (από την δημιουργία / συλλογή μέχρι και την καταστροφή).
3	3	Κατ' ελάχιστο τα μέτρα για την καταστροφή πληροφοριών περιλαμβάνουν 1) multiple passes of software-based overwriting για τα επαναχρησιμοποιούμενα μέσα αποθήκευσης ή φυσική καταστροφή για τα υπόλοιπα, 2) cross cut shredding χαρτιών και 3) προβλέψεις σε συμβάσεις με τρίτα μέρη αντίστοιχων μέτρων όπου απαιτούνται.
3	4	Για τα δεδομένα που βρίσκονται σε μεταφορά ή ανταλλάσσονται τα μέτρα πρέπει να συμφωνούν αντίστοιχα με το [DS4].
3	5	Για τα κρίσιμα ή ευαίσθητα δεδομένα που βρίσκονται σε ηρεμία (data at rest), εφαρμόζεται κρυπτογραφία σε συμφωνία με την σχετική πολιτική του [AM5].
3	6	Ο οργανισμός έχει ορίσει μια περίοδο διατήρησης των δεδομένων για όλες τις κατηγορίες δεδομένων και εφαρμόζει τις σχετικές προβλέψεις.
4	1	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
4	2	Για τα δεδομένα προσωπικού χαρακτήρα εφαρμόζονται κατάλληλα μέτρα κατά την μετάδοση (in transit) αλλά και όσο είναι σε ηρεμία.
4	3	Σε περίπτωση που δεν είναι δυνατή η εφαρμογή κρυπτογράφησης, αναγνωρίζεται ως κίνδυνος και γίνεται σχεδιασμός και υλοποίηση άλλων μέτρων για την εξασφάλιση του επιθυμητού επίπεδου ασφαλείας.
4	4	Έχουν σχεδιαστεί κατάλληλες διαδικασίες, πολιτικές για την συμμόρφωση προς τις νομικές και κανονιστικές απαιτήσεις σε σχέση με την προστασία δεδομένων προσωπικού χαρακτήρα.
4	5	Η διαχείριση κινδύνου έχει προσαρμοστεί ώστε να περιλαμβάνει την αναγνώριση, αποτίμηση και αξιολόγηση κινδύνων διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων από την επεξεργασία των δεδομένων τους από τον οργανισμό.
4	6	Υλοποιούνται κατάλληλα τεχνικά και οργανωτικά μέτρα σύμφωνα με τα αποτελέσματα της αξιολόγησης κινδύνων. Ειδικά για την διαγραφή των δεδομένων έχει καταγραφεί μια διαδικασία για την ασφαλή διαγραφή δεδομένων η οποία περιέχει ρόλους, αρμοδιότητες, μεθοδολογίες, κριτήρια και εργαλεία χρησιμοποιούνται για την διαγραφή των δεδομένων κάθε επιπέδου διαβάθμισης σύμφωνα με το [DS2].
4	7	Η διαδικασία προβλέπει επίσης τα μέτρα που εφαρμόζονται όταν μεταφέρονται στοιχεία (πόροι) σε εξωτερικά μέση (π.χ. λόγω λήξης συμβολαίου ενοικίασης, για λόγους επισκευής κλπ.).
4	8	Σε περίπτωση χρησιμοποιείται τρίτο μέρος για την διαγραφή ή καταστροφή, υπάρχουν σχετικές προβλέψεις και όροι που εξασφαλίζουν την ορθή και αποτελεσματική εφαρμογή των σχετικών κανόνων στο σχετικό συμβόλαιο.
4	9	Σε περίπτωση που τα δεδομένα αποθηκεύονται σε τρίτα μέρη (π.χ. Cloud services) δίνονται συγκεκριμένες δεσμεύσεις και αποδείξεις από την μεριά του τρίτου μέρους για την υλοποίηση των συγκεκριμένων ρυθμίσεων. Σε διαφορετική περίπτωση λαμβάνονται άλλα αντισταθμιστικά μέτρα.
4	10	Εφαρμόζονται αυτόματα ή ημιαυτόματα μέσα για την εφαρμογή της περιόδου διατήρησης των δεδομένων.

5	1	Έχει εφαρμοστεί αυτόματο σύστημα για την προστασία των πληροφοριών από διαρροές (DLP).
5	2	Έχουν γίνει οι κατάλληλες ρυθμίσεις σε συμφωνία με το σχήμα διαβάθμισης πληροφοριών και τις οδηγίες για τον χειρισμό των πληροφοριών [DS2].
5	3	Κάθε νέο μέσο ή στοιχείο, κρυπτογραφείται με αυτοματοποιημένο τρόπο όπου αυτό είναι δυνατό, πριν ή κατά την εισαγωγή του στον οργανισμό.
5	4	Για την διαγραφή δεδομένων, σε περίπτωση που αυτή υλοποιείται μέσω λογισμικού, χρησιμοποιούνται επιπλέον μέτρα σε φυσικό επίπεδο (π.χ. degaussing).
5	5	Σε περίπτωση που χρησιμοποιείται τρίτο μέρος για την διαγραφή ή καταστροφή, η ενέργεια αυτή γίνεται στο χώρο του οργανισμού για να αποφευχθούν κίνδυνοι που σχετίζονται με την μεταφορά των δεδομένων. Αν αυτό δεν είναι εφικτό, εφαρμόζονται συγκεκριμένα μέτρα για την αποφυγή του σχετικού κινδύνου (π.χ. κλειδωμένα containers, live feed, παρουσία προσωπικού κλπ.).
5	6	Εφαρμόζονται αυτόματα μέτρα για την εφαρμογή της περιόδου διατήρησης των δεδομένων.
5	7	Στα πλαίσια των ελέγχων που αναφέρονται στο [GOV2] περιλαμβάνονται και έλεγχοι για την τήρηση του διαστήματος διατήρησης των πληροφοριών.
5	8	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	9	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
DS2		**Μέτρο:** Ταξινόμηση και επισήμανση πληροφοριών **Στόχος Μέτρου:** Να εξασφαλιστεί ότι τα δεδομένα ταξινομούνται και επισημαίνονται κατά τρόπο ώστε να αντικατοπτρίζεται η ευαισθησία τους ώστε να εξασφαλίζεται η κατάλληλη επεξεργασία τους **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση μιας πολιτικής ταξινόμησης και επισήμανσης που διασφαλίζει την ταξινόμηση και επισήμανση των πληροφοριών, σύμφωνα με την εμπιστευτικότητα και την ευαισθησία τους. Εξέταση ενδεχομένου εφαρμογής συστημάτων ταξινόμησης και επισήμανσης με βάση τις διεθνείς και βιομηχανικές βέλτιστες πρακτικές, όπως το πρωτόκολλο «Traffic Light Protocol». Τουλάχιστον, ο οργανισμός θα πρέπει να γίνεται διάκριση μεταξύ των δημόσιων, ιδιωτικών και διαβαθμισμένων πληροφοριών. **Πηγή:** CIS (1.3 Data protection), ENISA (SO 23 – Security of data at rest), NIST 800-53 (MP-3)
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**
0	1	Ο οργανισμός δεν έχει κάποια διαδικασία ή άλλο μέσο για την ταξινόμηση και επισήμανση των πληροφοριών τους.
1	1	Αναγνωρίζονται κάποια δεδομένα ως πιο κρίσιμα ή ευαίσθητα αλλά δεν υπάρχει κάποια συγκεκριμένη καταγραφή.
2	1	Έχουν αναγνωριστεί τουλάχιστον 2 κατηγορίες πληροφοριών (εσωτερικές και δημόσιες) και υπάρχει σήμανση τουλάχιστον σε μια από τις δυο κατηγορίες.
2	2	Ο χειρισμός των πληροφοριών γίνεται σύμφωνα με σχετικές γραπτές οδηγίες οι οποίες αναφέρουν οδηγίες και περιορισμούς σε σχέση με τον τρόπο χειρισμού των πληροφοριών καθ' όλο τον κύκλο ζωής (από την δημιουργία / συλλογή μέχρι και την καταστροφή).
3	1	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται πολιτική ταξινόμησης και επισήμανσης που διασφαλίζει την ταξινόμηση και επισήμανση των πληροφοριών, σύμφωνα με την εμπιστευτικότητα και την ευαισθησία τους.
3	2	Η πολιτική επιβάλει κατ΄ ελάχιστο την διάκριση όσον αφορά τις πληροφορίες: Δημόσια, Ιδιωτική και Διαβαθμισμένη.
3	3	Ο χειρισμός των πληροφοριών γίνεται σύμφωνα με σχετικές γραπτές οδηγίες οι οποίες αναφέρουν οδηγίες και περιορισμούς σε σχέση με τον τρόπο χειρισμού των πληροφοριών καθ' όλο τον κύκλο ζωής όπως αναφέρεται στο [DS1].

4	1	Έχει δημιουργηθεί διαδικασία σχετικά με την ταξινόμηση και την επισήμανση των πληροφοριών στην οποία αποτυπώνεται ο τρόπος με τον οποίο γίνεται η διαβάθμιση και η επισήμανση της πληροφορίας.
4	2	Χρησιμοποιείται αυτοματοποιημένος τρόπος (π.χ. λογισμικό) για την επισήμανση και διαχείριση των πληροφοριών σύμφωνα με το σχήμα που έχει εφαρμοστεί.
4	3	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Η διαδικασία ταξινόμησης και επισήμανσης, προβλέπει ότι με την είσοδο ενός εγγράφου / πληροφορίας στον οργανισμό, αναγνωρίζεται ο ιδιοκτήτης και κατατάσσεται και επισημαίνεται σύμφωνα με τα αναγνωρισμένα κριτήρια με την χρήση κατάλληλων εργαλείων. Το ίδιο ισχύει και για πληροφορίες οι οποίες δημιουργούνται από τον οργανισμό, οι οποίες και αυτές κατατάσσονται και επισημαίνονται την στιγμή της δημιουργίας.
5	2	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	3	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
5	4	Διενεργούνται έλεγχοι για την συμμόρφωση προς τις απαιτήσεις ταξινόμησης και επισήμανσης.
DS3		**Μέτρο:** Εφεδρικά αντίγραφα και ανάκτηση δεδομένων **Στόχος Μέτρου:** Να καταστεί δυνατή η αποκατάσταση των πληροφοριών στο πλαίσιο συμβάντων και περιστατικών ασφάλειας. **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση διαδικασίας εφεδρικών αντιγράφων και ανάκτησης δεδομένων, προκειμένου να διασφαλίζεται η έγκαιρη και αποτελεσματική αποκατάσταση δεδομένων μετά την ύπαρξη ενός συμβάντος ή περιστατικού, ή κατόπιν αιτήματος. Οι διαδικασίες εφεδρικών αντιγράφων και ανάκτησης δεδομένων θα πρέπει να δοκιμάζονται επαρκώς και συχνά, προκειμένου να διασφαλίζεται η ορθή και αξιόπιστη λειτουργία όλων των υποστηρικτικών διαδικασιών και συστημάτων. Τα συστήματα και οι υποδομές υποστήριξης, που επιτρέπουν την εφεδρεία και την αποκατάσταση δεδομένων, θα πρέπει να είναι γεωγραφικά διεσπαρμένες (αποθήκευση σε άλλη τοποθεσία) προκειμένου να προστατεύονται από φυσικούς κινδύνους ασφάλειας. **Πηγή:**
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**
0	1	Ο οργανισμός δεν λαμβάνει αντίγραφα ασφαλείας με οποιαδήποτε μορφή.
1	1	Λαμβάνονται για κάποιες πληροφορίες αντίγραφα ασφαλείας αλλά αυτό γίνεται σε ad-hoc βάση και χωρίς συγκεκριμένο / καταγεγραμμένο τρόπο.
2	1	Τηρούνται αντίγραφα ασφαλείας που καλύπτουν το σύνολο του ενιαίο κατάλογο στοιχείων ενεργητικού, συστημάτων και διαδικασιών εντός του οργανισμού.
2	2	Υπάρχει ένας αναγνωρισμένος υπεύθυνος για την λειτουργία και τήρηση των αντιγράφων ασφαλείας.
3	1	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται διαδικασία εφεδρικών αντιγράφων και ανάκτησης δεδομένων, προκειμένου να διασφαλίζεται η έγκαιρη και αποτελεσματική αποκατάσταση δεδομένων μετά την ύπαρξη ενός συμβάντος ή περιστατικού, ή κατόπιν αιτήματος.
3	2	Οι διαδικασίες εφεδρικών αντιγράφων και ανάκτησης δεδομένων δοκιμάζονται επαρκώς και συχνά, προκειμένου να διασφαλίζεται η ορθή και αξιόπιστη λειτουργία όλων των υποστηρικτικών διαδικασιών και συστημάτων.
3	3	Τα συστήματα και οι υποδομές υποστήριξης, που επιτρέπουν την εφεδρεία και την αποκατάσταση δεδομένων, είναι γεωγραφικά διεσπαρμένες (αποθήκευση σε άλλη τοποθεσία) προκειμένου να προστατεύονται από φυσικούς κινδύνους ασφάλειας.
3	4	Τα αντίγραφα ασφαλείας λαμβάνουν το σύνολο της πληροφορίας ή τις αλλαγές της σε ημερήσια βάση τουλάχιστον.

4	1	Η υλοποίηση της διαδικασίας εφεδρικών αντιγράφων και ανάκτησης δεδομένων υποστηρίζεται από κατάλληλο αδειοδοτημένο (όπου απαιτείται) λογισμικό.
4	2	Τα αρχεία εφεδρικών αντιγράφων κρυπτογραφούνται με την χρήση αλγορίθμων όπως προβλέπεται από το [AM1].
4	3	Έχει προβλεφθεί ώστε να υπάρχει δυνατότητα πρόσβασης και ανάκτησης των δεδομένων όπως απαιτείται από τα εφεδρικά αντίγραφα (π.χ. υπάρχει δυνατότητα λήψης, εγκατάστασης ή χρήσης του λογισμικού αντιγράφων ασφαλείας και υπάρχει διαθεσιμότητα των σχετικών κλειδιών).
4	4	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
4	5	Η συχνότητα λήψης αντιγράφων ασφαλείας τουλάχιστον για τα κρίσιμα συστήματα είναι ανά 8 ώρες.
4	6	Έχει δημιουργηθεί ένα σχήμα διατήρησης εφεδρικών αντιγράφων σε επίπεδο ημέρας / εβδομάδας / μήνα και έτους.
5	1	Έχουν εφαρμοστεί λύσεις συγχρονισμού (replication) σε εναλλακτικό χώρο για τα κρίσιμα συστήματα όπως αυτά έχουν αναγνωριστεί σύμφωνα με την ανάλυση επιχειρησιακών επιπτώσεων και τα σχετικά σχέδια επιχειρησιακής συνέχειας και ανάκαμψης από καταστροφή.
5	2	Μια φορά το χρόνο τουλάχιστον γίνεται πλήρης λειτουργική δοκιμή της κατάστασης συγχρονισμού και της δυνατότητας λειτουργίας του οργανισμού από την εναλλακτική τοποθεσία.
5	3	Τηρούνται χωριστά εφεδρικά αντίγραφα και σε τρίτη ασφαλή τοποθεσία, για να μπορεί να προστατευτεί ο οργανισμός και από επιθέσεις κυβερνοεκβιασμού.
5	4	Η συχνότητα λήψης των συγκεκριμένων αντιγράφων είναι κατάλληλη σύμφωνα με το πλαίσιο λειτουργίας, τους στόχους και την στρατηγική του οργανισμού.
5	5	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	6	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
DS4		**Μέτρο:** Μεταφορές και ανταλλαγή πληροφοριών **Στόχος Μέτρου:** Να εφαρμοστούν επαρκή μέτρα στο πλαίσιο της διαβίβασης και ανταλλαγής πληροφοριών εσωτερικά ή με τρίτα μέρη, προκειμένου να διασφαλιστεί η ασφαλής μεταφορά δεδομένων. **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση διαδικασιών μεταφοράς και ανταλλαγής πληροφοριών προκειμένου να διασφαλίζεται η προστασία των πληροφοριών κατά τη μεταφορά ή την ανταλλαγή τους εσωτερικά ή με τρίτα μέρη. Η μεταφορά και ανταλλαγή πληροφοριών θα πρέπει να λαμβάνει υπόψη τις κανονιστικές και νομοθετικές απαιτήσεις, όπως ορίζονται στο [GOV2], για παράδειγμα κατά την επεξεργασία πληροφοριών στο πλαίσιο διεθνών διαβιβάσεων δεδομένων. **Πηγή:** C2M2 (Architecture), ISO 27001, OWASP API, OWASP ASVS
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**
0	1	Ο οργανισμός δεν έχει κάποια διαδικασία ή άλλο μέσο για την αναγνώριση και εφαρμογή μέτρων για την προστασία δεδομένων κατά την μεταφορά ή ανταλλαγή τους.
1	1	Έχουν τεθεί σε συγκεκριμένα σημεία κάποια μέτρα για την προστασία των δεδομένων κατά την ανταλλαγή ή μεταφορά τους. Τα μέτρα δεν καλύπτουν το σύνολο των τρόπων ανταλλαγής ή μεταφοράς.
2	1	Έχουν αναγνωριστεί τουλάχιστον 2 κατηγορίες πληροφοριών (εσωτερικές και δημόσιες) και υπάρχει σήμανση τουλάχιστον σε μια από τις δυο κατηγορίες.

2	2	Έχουν αναγνωρισθεί οι τρόποι με τους οποίους μπορεί να γίνει ανταλλαγή των εσωτερικών πληροφοριών και έχουν καταγραφεί σε σχετικές γραπτές οδηγίες.
2	3	Σε περίπτωση που δίνεται πρόσβαση στις πληροφορίες αυτές σε τρίτα μέρη, χρησιμοποιούνται ενότητες μόνο που μπορούν να παρέχουν κατάλληλες διαβεβαιώσεις και εγγυήσεις για την προστασία των δεδομένων σε όλο τον κύκλο ζωής τους.
2	4	Οι γραπτές οδηγίες χειρισμού επικοινωνούνται στο τρίτο μέρος ώστε να συμμορφωθεί.
2	5	Σε περίπτωση αδυναμίας συμμόρφωσης, ο οργανισμός αναγνωρίζει τον σχετικό κίνδυνο και εισάγει κατάλληλα αντισταθμιστικά μέτρα.
3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται διαδικασίες μεταφοράς και ανταλλαγής πληροφοριών προκειμένου να διασφαλίζεται η προστασία των πληροφοριών κατά τη μεταφορά ή την ανταλλαγή τους εσωτερικά ή με τρίτα μέρη.
3	2	Η μεταφορά και ανταλλαγή πληροφοριών λαμβάνει υπόψη τις κανονιστικές και νομοθετικές απαιτήσεις, όπως ορίζονται στο [GOV2], για παράδειγμα κατά την επεξεργασία πληροφοριών στο πλαίσιο διεθνών διαβιβάσεων δεδομένων.
3	3	Ειδικά για τα κρίσιμα ή ευαίσθητα δεδομένα, υλοποιείται κρυπτογράφηση κατά την ανταλλαγή ή μεταφορά. Παραδείγματα τέτοιας υλοποίησης περιλαμβάνει (Transport Layer Security (TLS) and Open Secure Shell (OpenSSH) κα.).
3	4	Τα δεδομένα που μεταφέρονται με φυσικά μέσα, πρώτα κρυπτογραφούνται κατάλληλα και μετά αποστέλλονται.
3	5	Τα κλειδιά κρυπτογράφησης μεταφέρονται χωριστά, με άλλο μέσο (ή τρόπο) χωρίς επισήμανση της χρήσης τους.
3	6	Για σύγχρονη μεταφορά χρησιμοποιούνται πρωτόκολλα όπως είναι οι πιο πρόσφατες σταθερές εκδόσεις πρωτοκόλλων όπως είναι το SFTP ή HTTPS.
4	1	Εφαρμόζονται μηχανισμοίγια την εξασφάλιση της ακεραιότητας και αυθεντικότητας της πληροφορίας που ανταλλάσσεται.
4	2	Οι σχετικές πληροφορίες ανταλλάσσονται χρησιμοποιώντας ψηφιακές υπογραφές.
4	3	Τηρείται μητρώο με τις πληροφορίες που ανταλλάσσονται (κρίσιμες ή ευαίσθητες), καταγράφονται τα μέτρα που εφαρμόστηκαν και οι σχετικές εγγυήσεις από τα σχετικά μέρη.
4	4	Όταν χρησιμοποιούνται προσωρινές τοποθεσίες αποθήκευσης, αυτές ελέγχονται στον προδιαγεγραμμένο χρόνο και οι πληροφορίες διαγράφονται με ασφάλεια.
4	5	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
4	6	Ειδικά για τα ευαίσθητα προσωπικά δεδομένα, εφαρμόζονται μηχανισμοί data masking για την επιπλέον προστασία τους (όπου μπορεί να εφαρμοστεί).
4	7	Για την ανταλλαγή πληροφοριών μέσω APIs, γίνεται κατάλληλος σχεδιασμός, παραμετροποίηση, υλοποίηση και λειτουργίας ώστε να συμμορφώνεται με το επίπεδο ασφάλειας του οργανισμού.
4	8	Βέλτιστες διεθνείς πρακτικές (π.χ. API OWASP Top Ten) εφαρμόζονται.
4	9	Η εμπιστευτικότητα των δεδομένων εξασφαλίζεται είτε με κρυπτογράφηση σε επίπεδο καναλιού είτε με κρυπτογράφηση σε επίπεδο δεδομένων όταν γίνεται μεταφορά σε διαφορετικά δίκτυα ακόμα και εντός του ίδιου του οργανισμού.
5	1	Έχει εφαρμοστεί αυτόματο σύστημα για την προστασία των πληροφοριών από διαρροές (π.χ. Host Based Data Loss Prevention).
5	2	Έχουν γίνει οι κατάλληλες ρυθμίσεις σε συμφωνία με το σχήμα διαβάθμισης πληροφοριών και τις οδηγίες για τον χειρισμό των πληροφοριών [DS2].
5	3	Το σύστημα καλύπτει όλες τις πληροφορίες που επεξεργάζονται ή ανταλλάσσονται εντός του οργανισμού περιλαμβανομένων αυτών που βρίσκονται σε τρίτα μέρη.
5	4	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	5	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

5	6	Γίνονται τακτικοί έλεγχοι για την παρακολούθηση της εφαρμογής και συμμόρφωσης των διαδικασιών από το σχετικό προσωπικό.
5	7	Αντίστοιχοι έλεγχοι υλοποιούνται και σε τεχνικό επίπεδο (π.χ. Penetration tests) ή σε περίπτωση λογισμικού / APIs, security assessments στηριζόμενες σε διεθνείς βέλτιστες πρακτικές (π.χ. Application Security Verification Standard OWASP).
5	8	Σε περίπτωση αναγνώρισης κάποιας απόκλισης ενεργοποιείται άμεσα η διαδικασία ανταπόκρισης περιστατικών ασφαλείας. [EIM1]
DS5		**Μέτρο:** Πρόληψη απώλειας δεδομένων και διαρροής δεδομένων **Στόχος Μέτρου:** Να εξασφαλιστεί η προστασία των δεδομένων από εκούσια ή ακούσια απώλεια και διαρροή δεδομένων. **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση εύλογων μέτρων για τη μείωση του κινδύνου απώλειας δεδομένων και διαρροής δεδομένων, λαμβάνοντας τα κατάλληλα τεχνικά και οργανωτικά μέτρα για πρόληψη. Τα μέτρα πρόληψης, απώλειας ή διαρροής δεδομένων θα πρέπει να λαμβάνουν υπόψη εξωτερικούς και εσωτερικούς φορείς απειλής που θα μπορούσαν δυνητικά να αποκαλύψουν διαβαθμισμένες ή ευαίσθητες πληροφορίες. Θα πρέπει να εφαρμόζονται επαρκή μέτρα ελέγχου πρόσβασης για διεπαφή με τα μέτρα πρόληψης για την απώλεια δεδομένων και διαρροή δεδομένων. Οι πολιτικές για την ανταλλαγή και κοινοποίηση δεδομένων θα πρέπει να είναι βάσει του ρόλου του χρήστη, όπως ορίζεται στο [IAM1]. Κατά τον καθορισμό των μέτρων πρόληψης για την απώλεια και τη διαρροή δεδομένων, ο οργανισμός θα πρέπει να εξετάζει την ταξινόμηση, την προστασία και την παρακολούθηση των πληροφοριών. **Πηγή:**
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**
0	1	Ο οργανισμός δεν έχει κάποια διαδικασία ή μέτρα για την προστασία των δεδομένων από εκούσια ή ακούσια απώλεια και διαρροή δεδομένων.
1	1	Έχουν τεθεί σε συγκεκριμένα σημεία κάποια μέτρα για την προστασία των δεδομένων από εκούσια ή ακούσια απώλεια και διαρροή δεδομένων.
2	1	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται μια πολιτική ελέγχου πρόσβασης για όλα τα δεδομένα στα πλαίσια του ενιαίου καταλόγου στοιχείων σύμφωνα με το [IAM1].
2	2	Για κάθε επίπεδο πληροφορίας σύμφωνα με το [DS2], έχουν επιλεγεί και μέτρα που αποσκοπούν στην προστασία έναντι διαρροών μέσω της χρήσης μεταφερόμενων αποθηκευτικών μέσων [DS1], μέσω της αποστολής πληροφοριών [DS4].
2	3	Μέτρα για την προστασία των δικτύων ακολουθούν τα αναγραφόμενα του [NS1].
3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται εύλογα μέτρα για τη μείωση του κινδύνου απώλειας δεδομένων και διαρροής δεδομένων, λαμβάνοντας τα κατάλληλα τεχνικά και οργανωτικά μέτρα για πρόληψη.
3	2	Τα μέτρα πρόληψης, απώλειας ή διαρροής δεδομένων λαμβάνουν υπόψη εξωτερικούς και εσωτερικούς φορείς απειλής που μπορούν δυνητικά να αποκαλύψουν διαβαθμισμένες ή ευαίσθητες πληροφορίες.
3	3	Εφαρμόζονται επαρκή μέτρα ελέγχου πρόσβασης για διεπαφή με τα μέτρα πρόληψης για την απώλεια δεδομένων και διαρροή δεδομένων.
3	4	Οι πολιτικές για την ανταλλαγή και κοινοποίηση δεδομένων είναι βάσει του ρόλου του χρήστη, όπως ορίζεται στο [IAM1].
3	5	Κατά τον καθορισμό των μέτρων πρόληψης για την απώλεια και τη διαρροή δεδομένων, ο οργανισμόςεξετάζει την ταξινόμηση, την προστασία και την παρακολούθηση των πληροφοριών.
3	6	Διενεργείται εκπαίδευση στο προσωπικό σχετικά με τους τρόπους επίθεσης (π.χ. phishing) οι οποίοι μπορεί να οδηγήσουν σε απώλεια δεδομένων.
4	1	Η πρόσβαση σε γνωστά μέσα για την μεταφορά δεδομένων και σε μη εταιρικά συστήματα ανταλλαγής μηνυμάτων απαγορεύεται.

4	2	Η μεταφορά δεδομένων σε USB απαγορεύεται. Σε περίπτωση που δεν μπορεί να απαγορευτεί καθολικά, οι εξαιρέσεις διαχειρίζονται με κατάλληλα οργανωτικά και τεχνικά μέτρα ώστε να εξασφαλίζεται ότι υπάρχει έλεγχος του είδους της πληροφορίας που μεταφέρεται, της αιτιολόγησης της μεταφοράς, της εξουσιοδότησης της μεταφοράς και της εφαρμογής κατάλληλων κρυπτογραφικών μέτρων προστασίας.
4	3	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Εφαρμόζεται αυτόματο σύστημα για την προστασίας των πληροφοριών από διαρροές (π.χ. Host Based Data Loss Prevention).
5	2	Έχουν γίνει οι κατάλληλες ρυθμίσεις σε συμφωνία με το σχήμα διαβάθμισης πληροφοριών και τις οδηγίες για τον χειρισμό των πληροφοριών [DS2].
5	3	Το σύστημα καλύπτει όλες τις πληροφορίες που επεξεργάζονται ή ανταλλάσσονται εντός του οργανισμού περιλαμβανομένων αυτών που βρίσκονται σε τρίτα μέρη.
5	4	Οποιεσδήποτε ανωμαλίες αναγνωρίζονται επί των κανονικών traffic patterns καταγράφεται και αντιμετωπίζεται σύμφωνα με την διαδικασία διαχείρισης περιστατικών ασφαλείας [EIM1].
5	5	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	6	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

Κατηγορία		ΔΙΑΧΕΙΡΙΣΗ ΑΛΛΑΓΩΝ
CM1		**Μέτρο:** Διαχείριση αλλαγών **Στόχος Μέτρου:** Να διασφαλιστεί ότι οι αλλαγές στις διαδικασίες και τα συστήματα πληροφοριών εφαρμόζονται με ασφάλεια, χωρίς να θίγεται το απόρρητο, η ακεραιότητα, η διαθεσιμότητα ή η αυθεντικότητα των πληροφοριών. **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση διαδικασιών διαχείρισης αλλαγών για τον έλεγχο και τη διαχείριση αλλαγών σε συστήματα, εφαρμογές και άλλα υποστηρικτικά στοιχεία ενεργητικού στο πλαίσιο της επεξεργασίας πληροφοριών. Κατά τον καθορισμό της διαδικασίας διαχείρισης αλλαγών, ο οργανισμός πρέπει να προνοεί αιτήσεις αλλαγής, προκειμένου να λαμβάνονται υπόψη οι αλλαγές που ζητούνται από τους συμμετέχοντες. Η διαδικασία διαχείρισης αλλαγών θα πρέπει να επιτρέπει στον οργανισμό να αξιολογεί τους κινδύνους στο πλαίσιο αιτημάτων αλλαγών και να σχεδιάζει αλλαγές λαμβάνοντας υπόψη κατάλληλα μέτρα ασφάλειας. Η διαδικασία διαχείρισης αλλαγών θα πρέπει να περιλαμβάνει την προετοιμασία και την επαλήθευση των αλλαγών. **Πηγή:**
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**
0	1	Ο οργανισμός δεν εφαρμόζει κάποια διαχείριση ή έλεγχο επί των αλλαγών.
1	1	Ο οργανισμός υλοποιεί κάποιο έλεγχο πάνω σε κάποιες αλλαγές που κάνει σε κρίσιμα συστήματα.
1	2	Οι καταγραφές είναι περιστασιακές και η διαχείριση των αλλαγών είναι ad-hoc.
2	1	Υπάρχει μια διαδικασία για την διαχείριση των αλλαγών στα κρίσιμα συστήματα.
2	2	Η διαδικασία διαχείρισης αλλαγών είναι καταγεγραμμένη και έχει αναγνωρίσει συγκεκριμένους ρόλους που είναι υπεύθυνοι για την έγκριση των αλλαγών.
3	1	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται διαδικασία διαχείρισης αλλαγών για τον έλεγχο και τη διαχείριση αλλαγών σε συστήματα, εφαρμογές και άλλα υποστηρικτικά στοιχεία ενεργητικού στο πλαίσιο της επεξεργασίας πληροφοριών.
3	2	Κατά τον καθορισμό της διαδικασίας διαχείρισης αλλαγών,προνοούνται αιτήσεις αλλαγής, προκειμένου να λαμβάνονται υπόψη οι αλλαγές που ζητούνται από τους συμμετέχοντες.
3	3	Η διαδικασία διαχείρισης αλλαγών επιτρέπει στον οργανισμό να αξιολογεί τους κινδύνους στο πλαίσιο αιτημάτων αλλαγών και να σχεδιάζει αλλαγές λαμβάνοντας υπόψη κατάλληλα μέτρα ασφάλειας.
3	4	Ειδικά για κρίσιμα συστήματα, σε κάθε περίπτωση διενέργειας αλλαγής, αυτή γίνεται αφού έχει υλοποιηθεί η εγκατάσταση σε δοκιμαστικό / παρόμοιο σύστημα χαμηλού κινδύνου.
3	5	Η διαδικασία διαχείρισης αλλαγών περιλαμβάνει την προετοιμασία και την επαλήθευση των αλλαγών.
3	6	Η διαδικασία διαχείρισης των αλλαγών υποστηρίζεται από κάποιο εργαλείο (π.χ. ticketing) το οποίο επιτρέπει την ιχνηλάτηση των αλλαγών.
3	7	Εχουν δημιουργηθεί κατηγορίες αλλαγών (λαμβάνοντας υπόψη τον σχετικό κίνδυνο) και έχει προδιαγραφεί ο τρόπος (βήματα και εγκρίσεις) που γίνεται η διαχείριση της κάθε κατηγορίας. (Συγκεκριμένα, οδηγία για την κατάταξη των αλλαγών σε κατηγορίες κρισιμότητας και προτεραιότητας, καθορίζονται οι ενέργειες αιτιολόγησης, ανάλυσης, δοκιμής, υπαναχώρησης και επιβεβαίωσης που γίνονται πριν να υλοποιηθεί η αλλαγή σε παραγωγικό σύστημα, καθορίζονται οι ρόλοι οι οποίοι εμπλέκονται στον σχεδιασμό, έλεγχο, υλοποίηση και έγκριση της αλλαγής και τα σχετικά αρχεία που τηρούνται).
3	8	Η διαδικασία διαχείρισης αλλαγών περιέχει επίσης προβλέψεις και τρόπο χειρισμού για επείγουσες αλλαγές.
3	9	Όλοι οι εμπλεκόμενοι ενημερώνονται σχετικά με τις λεπτομέρειες τις εκάστοτε αλλαγής.

3	10	Η διαδικασία διαχείρισης αλλαγών περιλαμβάνει σχέδιο roll-back για τις περιπτώσεις που οι αλλαγές είναι ανεπιτυχείς ή όταν έχει προκύψει κάποιο γεγονός που δεν επιτρέπει την επιτυχή ολοκλήρωση της αλλαγής.
3	11	Τα τρίτα μέρη ενημερώνονται για σημαντικές αλλαγές σε κρίσιμα συστήματα που επηρεάζουν τις προσφερόμενες υπηρεσίες.
4	1	Έχει δημιουργηθεί σχετική επιτροπή για τον έλεγχο και την έγκριση των αλλαγών, εξασφαλίζοντας ότι δεν υπάρχει σύγκρουση συμφερόντων ανάμεσα στα άτομα που αιτούνται την αλλαγή, υλοποιούν την αλλαγή και εγκρίνουν την αλλαγή.
4	2	Πραγματοποιούνται δοκιμές στην εφαρμογή της διαδικασίας διαχείρισης αλλαγών ώστε να βεβαιώνεται ότι οι αλλαγές κρίσιμων συστημάτων γίνονται πάντα με προκαθορισμένο τρόπο.
4	3	Δίνεται ιδιαίτερη βαρύτητα σε αλλαγές που προκύπτουν σε παραγωγικό περιβάλλον, και ειδικά κατά τη μεταφορά ενός συστήματος από την ανάπτυξη στο λειτουργικό περιβάλλον.
4	4	Γίνεται ανασκόπηση σε τακτική βάση οι αλλαγές που διενεργούνται στα συστήματα (με αφετηρία την αλλαγή στο σύστημα αλλά και με αφετηρία την τεκμηρίωση της αλλαγής) για τον έλεγχο της τήρησης της διαδικασίες διαχείρισης αλλαγών.
4	5	Η διαδικασία διαχείρισης αλλαγών λαμβάνει εισερχόμενα από το σύνολο των λειτουργιών του οργανισμού όπως αναφέρεται σε διάφορα controls του παρόντος πλαισίου.
4	6	Η διαδικασία διαχείρισης αλλαγών συνδέεται άμεσα με την διαδικασία διαχείρισης διαμόρφωσης όπως αναφέρεται στο [CM2].
5	1	Τηρείται αυτοματοποιημένο σύστημα για την διαχείριση των αλλαγών, το οποίο έχει την δυνατότητα να συνδέσει σε ποιο στοιχείο γίνεται η αλλαγή, να δημιουργήσει αιτήσεις αλλαγών, να δρομολογήσει τις αλλαγές ακολουθώντας προκαθορισμένο πρόγραμμα, να λαμβάνει σαν εισερχόμενο την ανάλυση κινδύνων για την αλλαγή (περιλαμβανομένων κινδύνων για την ασφάλεια), να την κατατάσσει σε κατηγορίες, να επιλέγει εγκριτική ροή με βάση την κατηγορία κινδύνου και την προτεραιότητα, να καταγράφει τις σχετικές εγκρίσεις, να περιέχει τις ενέργειες που έγιναν για την υλοποίηση, ενημέρωση, έλεγχο, δοκιμή της αλλαγής, να περιέχει το σχέδιο roll back και άλλες συναφείς πληροφορίες.
5	2	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	3	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
CM2		**Μέτρο:** Διαχείριση διαμόρφωσης (configuration) **Στόχος Μέτρου:** Να εντοπίζονται, να διατηρούνται και να επαληθεύονται οι πληροφορίες για τα στοιχεία ενεργητικού και τις διαμορφώσεις του οργανισμού. **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση διαδικασιών διαχείρισης διαμόρφωσης για τον έλεγχο και τη διαχείριση των διαμορφώσεων των στοιχείων ενεργητικού που υποστηρίζουν δίκτυα και συστήματα πληροφοριών. Ο οργανισμός τηρεί μητρώο των διαμορφώσεων που ισχύουν για τα εν λόγω στοιχεία ενεργητικού. Οι οργανισμοί καθορίζουν και καταγράφουν τις σχέσεις ανάμεσα στις διαμορφώσεις των στοιχείων ενεργητικού με σκοπό τον προσδιορισμό των αλληλεξαρτήσεων και τη διασφάλιση της κατάλληλης διαχείρισης της αλλαγής όσον αφορά την τροποποίηση των διαμορφώσεων. **Πηγή:** PNNL, NIST 800-53, ENISA
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**
0	1	Ο οργανισμός δεν διαχειρίζεται με κάποιο τρόπο την διαμόρφωση των στοιχείων του.
1	1	Γίνεται παραμετροποίηση κρίσιμων συστημάλλων αλλά συνήθως πριν την υλοποίηση κύριων αλλαγών λαμβάνεται ένα αντίγραφο της διαμόρφωσης.
		Ο τρόπος λήψης των αντιγράφων διαμόρφωσης και διαχείρισης δεν είναι συστηματικός.
2	1	Έχει καταγραφεί μια διαδικασία για την διαχείριση των αλλαγών στα κρίσιμα συστήματα και έχουν αναγνωρισθεί συγκεκριμένοι ρόλοι που είναι υπεύθυνοι για την έγκριση των αλλαγών.

2	2	Στα πλαίσια της διαχείρισης αλλαγών καταγράφονται και αλλαγές που έχουν να κάνουν με την παραμετροποίηση κρίσιμων συστημάτων (π.χ. αλλαγή βασικών κανόνων του firewall κ.α.).
3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται διαδικασίες διαχείρισης διαμόρφωσης για τον έλεγχο και τη διαχείριση των διαμορφώσεων των στοιχείων ενεργητικού που υποστηρίζουν δίκτυα και συστήματα πληροφοριών.
3	2	Οι σχέσεις ανάμεσα στις διαμορφώσεις των στοιχείων ενεργητικού με σκοπό τον προσδιορισμό των αλληλεξαρτήσεων και τη διασφάλιση της κατάλληλης διαχείρισης της αλλαγής όσον αφορά την τροποποίηση των διαμορφώσεων καθορίζονται και καταγράφονται.
3	3	Τηρείται μητρώο διαμορφώσεων που ισχύουν για τα εν λόγω στοιχεία ενεργητικού. Με τον όρο διαμόρφωση ορίζεται το σύνολο των παραμέτρων τα οποία μπορούν να αλλαχθούν σε υλισμικό, λογισμικό ή firmware και τα οποία μπορεί να επηρεάσουν την ασφάλεια ή / και την λειτουργικότητα ενός συστήματος.
3	4	Τα ελάχιστα στοιχεία που περιέχονται εντός του μητρώου είναι τα ακόλουθα: registry settings, permission settings σε επίπεδο αρχείων, φακέλων αλλά και άλλων πόρων, ρυθμίσεις που σχετίζονται με ανοικτές θύρες, ενεργοποιημένες ή αποκλεισμένες υπηρεσίες ή πρωτόκολλα, επιτρεπτές ή αποκλεισμένες συνδέσεις.
3	5	Για κάθε αλλαγή μέσα από το ticketing σύστημα που μπορεί να επηρεάσει την διαμόρφωση (baseline configuration) φαίνεται σε κάθε περίπτωση το στοιχείο το οποίο υφίσταται την αλλαγή.
3	6	Ως βασικό βήμα, προβλέπεται η διενέργεια αντιγράφου ασφαλείας της παραμετροποίησης του στοιχείου και αποθήκευση σε προστατευμένο σημείο, με υπόδειξη της αντιστοιχία με την συγκεκριμένη αλλαγή.
3	7	Οι ασφαλείς διαμορφώσεις ακολουθούν τις προδιαγραφές του [SS3].
4	1	Διενεργούνται σωτερικές ή και εξωτερικές επιθεωρήσεις με αντικείμενο την πληρότητα και την ακεραιότητα των διαμορφώσεων των στοιχείων.
4	2	Στα πλαίσια των ελέγχων ιχνηλατούνται αλλαγές με εκκίνηση το documentation μιας αλλαγής (προκειμένου να εξακριβωθεί ότι υπάρχει αρχείο διαμόρφωσης που συσχετίζεται με αυτήν την αλλαγή καθώς και έλεγχοι σύγκρισης της υπάρχουσας διαμόρφωσης προς το διατηρούμενο αρχείο διαμόρφωσης ανά περίπτωση.
4	3	Έχουν προσδιοριστεί στα πλαίσια των σχετικών διαδικασιών το χρονικό διάστημα διατήρησης του ιστορικού διαμόρφωσης.
4	4	Οι διαμορφώσεις προστατεύονται σύμφωνα με το υψηλότερο επίπεδο διαβάθμισης πληροφοριών όπως αναφέρεται στο [DS2] και άρα εφαρμόζεται και αυστηρός έλεγχος πρόσβασης.
4	5	Στοιχεία από περιστατικά ασφαλείας ή από ενημερώσεις σχετικά με αδυναμίες και σημεία βελτίωσης, λαμβάνονται ως εισερχόμενα στην διαδικασία διαχείρισης διαμόρφωσης και ενεργοποιούν σχετικές αλλαγές.
4	6	Έχει προβλέφθεί μια διαδικασία εξαίρεσης από την εφαρμογή συγκεκριμένων secure baselines όπως προβλέπεται.
4	7	Εφαρμόζονται εργαλεία system configuration management, τα οποία επιβάλλουν και ανανεώνουν αυτόματα τις ρυθμίσεις παραμέτρων στα συστήματα, σε προκαθορισμένο χρόνο ή σε περίπτωση περιστατικού ή συμβάντος. Τέτοια εργαλεία μπορεί να είναι το Active Directory Group Policy Objects για συστήματα Microsoft Windows και το Puppet για UNIX συστήματα.
4	8	Οι αλλαγές στα αρχεία αυτά διαχειρίζονται μέσω της διαδικασίας διαχείρισης αλλαγών [CM1]. (Αλλαγές πρέπει να γίνονται για την επικαιροποίηση των updates / patches, στην αλλαγή ρυθμίσεων βάσει στοιχείων περιστατικών ή ενημέρωσης από άλλα αξιόπιστα ενδιαφερόμενα μέρη κ.α.).
4	9	Σε περίπτωση που υπάρχει κάποιο πρόβλημα με κάποιο στοιχείο, αντικαθίσταται με καθαρή υλοποίηση από το αρχείο (baseline).
4	10	Κάθε στοιχείο εντός του δικτύου του οργανισμού είναι μοναδικά αναγνωρίσιμο και περιέχεται μέσα στον ενιαίο κατάλογο στοιχείων ενεργητικού όπως αναφέρεται στο [DS1/RM2].

4	11	Αντίστοιχες διαδικασίες και οδηγίες υπάρχουν και για διαφορετικού είδους λογισμικά όπως είναι εφαρμογές, βάσεις δεδομένων κ.α.
4	12	Εφεδρικά αντίγραφα ασφαλείας λαμβάνονται για τα αρχεία των διαμορφώσεων σύμφωνα με την σχετική πολιτική.
4	13	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Χρησιμοποιούνται αυτοματοποιημένα εργαλεία για την επαλήθευση των βασικών διαμορφώσεων των στοιχείων ενεργητικού ώστε να εντοπίζονται αλλαγές.
5	2	Οι αλλαγές αυτές καταγράφονται και ενημερώνεται ο υπεύθυνος ασφάλειας δικτύων και πληροφοριών και ενεργοποιείται η διαδικασία διαχείρισης περιστατικών ασφαλείας.
5	3	Διατηρούνται τα προηγούμενα αρχεία (baselines) για λόγους ιστορικότητας και δυνατότητας roll back σε περίπτωση ανάγκης.
5	4	Τηρούνται αρχεία (baseline) και για τα συστήματα που χρησιμοποιούνται για την ανάπτυξη και δοκιμή, διακριτά από αυτά που χρησιμοποιούνται για την παραγωγή.
5	5	Διενεργούνται έλεγχοι και δοκιμές για την αξιολόγηση της ανθετικότητας των baseline αρχείων. Σε περίπτωση που διαπιστωθούν αδυναμίες, λαμβάνονται άμεσα μέτρα και ακολουθείται η διαδικασία διαχείρισης αλλαγών.
5	6	Οι συσκευές οι οποίες συνδέονται απομακρυσμένα στα συστήματα ελέγχονται απομακρυσμένα σχετικά τη διαμόρφωση τους, το λογισμικό που έχουν εγκατεστημένο και το επίπεδο ενημέρωσης.
5	7	Οι συσκευές οι οποίες συνδέονται στα συστήματα και αφορούν τρίτα μέρη, ο οργανισμός τους έχει κοινοποιήσει το ελάχιστα αποδεκτό επίπεδο ασφάλειας που έχουν υλοποιήσει και πραγματοποιεί ελέγχους ασφαλείας προτού δοθεί πρόσβαση στα συστήματα του οργανισμού.
5	8	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	9	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

Κατηγορία		ΔΙΑΧΕΙΡΙΣΗ ΣΤΟΙΧΕΙΩΝ ΕΝΕΡΓΗΤΙΚΟΥ
AM1		**Μέτρο:** Διαχείριση του κύκλου ζωής στοιχείων ενεργητικού **Στόχος Μέτρου:** Να διασφαλιστεί ότι τα στοιχεία ενεργητικού είναι ασφαλή καθ' όλη τη διάρκεια του κύκλου ζωής τους, συμπεριλαμβανομένης της προμήθειας, της ανάπτυξης, της συντήρησης και της διάθεσης τους. **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση μέτρων ασφάλειας πληροφοριών στο πλαίσιο του σχεδίου διαχείρισης του κύκλου ζωής των στοιχείων ενεργητικού, προκειμένου να διασφαλίζεται ότι η ασφάλεια των πληροφοριών είναι αναπόσπαστο κομμάτι αυτού του κύκλου ζωής, δηλαδή την προμήθεια, την εγκατάσταση, τη συντήρηση και τη διάθεση. Η διαχείριση του κύκλου ζωής των πληροφοριών, όπως περιγράφεται στο μέτρο [DS1], θα πρέπει να αποτελεί μέρος του σχεδίου διαχείρισης του κύκλου ζωής των στοιχείων ενεργητικού. Το σχέδιο διαχείρισης του κύκλου ζωής των στοιχείων ενεργητικού πρέπει να περιγράφει όλες τις διαδικασίες για τον χειρισμό των πληροφοριών σύμφωνα με την πολιτική ταξινόμησης και επισήμανσης των δεδομένων, όπως περιγράφεται στο μέτρο [DS2]. **Πηγή:**
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**
0	1	Ο οργανισμός δεν έχει κάποιο δομημένο τρόπο με τον οποίο να διαχειρίζεται τους πόρους (στοιχεία ενεργητικού) καθ΄ όλη τη διάρκεια του κύκλου ζωής τους.
1	1	Οι διαδικασίες σχετικά με την απόκτηση και απομάκρυνση στοιχείων ενεργητικού διενεργούνται τουλάχιστον με τρόπο ad hoc και σύμφωνα με τις γνώσεις του εμπλεκόμενου προσωπικού.
	2	Ο έλεγχος αλλαγών περιορίζεται μόνο στα κρίσιμα στοιχεία ενεργητικού.
2	1	Υπάρχει μια καταγεγραμμένη διαδικασία η οποία περιγράφει τον τρόπο με τον οποίο διαχειρίζονται τα στοιχεία ενεργητικού κατά τη διάρκεια του κύκλου ζωής τους.
2	2	Η συγκεκριμένη διαδικασία περιλαμβάνει ενέργειες που διενεργούνται από σχετικά εξουσιοδοτημένους ρόλους για την: προμήθεια, την εγκατάσταση, τη συντήρηση και τη διάθεση.
2	3	Σχετικοί ρόλοι και αρμοδιότητες έχουν ανατεθεί στο προσωπικό. Οι αλλαγές στα στοιχεία ενεργητικού γίνονται τουλάχιστον με τρόπο ad-hoc και διατηρείται βασική τεκμηριωμένη πληροφορία.
3	1	Υπάρχει μια καταγεγραμμένη διαδικασία η οποία περιγράφει τον τρόπο με τον οποίο διαχειρίζονται τα στοιχεία ενεργητικού κατά τη διάρκεια του κύκλου ζωής τους.
3	2	Η συγκεκριμένη διαδικασία περιλαμβάνει ενέργειες που διενεργούνται από σχετικά εξουσιοδοτημένους ρόλους για την: προμήθεια, την εγκατάσταση, τη συντήρηση και τη διάθεση.
3	3	Στα πλαίσια της διαδικασίας περιλαμβάνονται και στοιχεία ασφάλειας πληροφοριών ώστε να διασφαλίζεται ότι η ασφάλεια των πληροφοριών είναι αναπόσπαστο κομμάτι αυτού του κύκλου ζωής, δηλαδή την προμήθεια, την εγκατάσταση, τη συντήρηση και τη διάθεση.
3	4	Η διαχείριση του κύκλου ζωής των πληροφοριών, όπως περιγράφεται στο μέτρο [DS1], αποτελεί μέρος του σχεδίου διαχείρισης του κύκλου ζωής των στοιχείων ενεργητικού.
3	5	Η διαδικασία διαχείρισης του κύκλου ζωής των στοιχείων ενεργητικού περιγράφει όλες τις επιμέρους διαδικασίες για τον χειρισμό των πληροφοριών σύμφωνα με την πολιτική ταξινόμησης και επισήμανσης των δεδομένων, όπως περιγράφεται στο μέτρο [DS2].
3	6	Αλλαγές στα στοιχεία ενεργητικού γίνονται σύμφωνα με την διαδικασία διαχείρισης αλλαγών [CM1].
3	7	Στα πλαίσια του σχεδίου περιγράφονται και τα κριτήρια που χρησιμοποιεί ο οργανισμός προκειμένου να κατανέμει τους πόρους σε κατηγορίες κρισιμότητας.
3	8	Προδιαγραφές ασφαλείας, κατάλληλες για την επικείμενη χρήση του στοιχείου ενεργητικού προδιαγράφονται πριν την προμήθεια.

4	1	Καθορίζονται ανά κατηγορία στοιχείου ενεργητικού και ανά κατηγορία κρισιμότητας, οι ελάχιστες διαδικασίες συντήρησης για τα στοιχεία ενεργητικού.
4	2	Τουλάχιστον μια φορά το χρόνο διενεργείται έλεγχος για την αναγνώριση κατά πόσο το σχέδιο διαχείρισης του κύκλου ζωής των στοιχείων ενεργητικού εφαρμόζεται ορθά και αποτελεσματικά. Από τον έλεγχο προκύπτει επίσης κατά πόσο υπάρχουν επαρκείς πόροι (άνθρωποι, εξοπλισμός, εργαλεία, χρήματα κ.α.) για την αποτελεσματική λειτουργία του σχεδίου.
4	3	Σε περίπτωση που προκύψει απόκλιση ως αποτέλεσμα του ελέγχου, καταγράφεται άμεσα και δρομολογούνται σχετικές διορθωτικές ενέργειες.
4	4	Οι κατηγορίες κρισιμότητας των πόρων χρησιμοποιούνται και είναι συμβατές προς αυτές που χρησιμοποιούνται κατά τη διάρκεια της διαχείρισης διακινδύνευσης.
4	5	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
4	6	Τα δεδομένα καταστρέφονται με ασφάλεια πριν ο εξοπλισμός επαναχρησιμοποιηθεί ή όταν ολοκληρώσει τον κύκλο ζωής του.
5	1	Τα κομμάτια του εξοπλισμού που έχουν την δυνατότητα να διατηρούν δεδομένα, καταστρέφονται φυσικά στο τέλος του κύκλου ζωής τους σύμφωνα με τα προβλεπόμενα του [DS1].
5	2	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	3	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
AM2		**Μέτρο:** Καταγραφή των στοιχείων ενεργειακού και ιδιοκτησία **Στόχος Μέτρου:** Να διασφαλιστεί ότι τα στοιχεία ενεργητικού καταγράφονται σε κατάλογο και ότι η ιδιοκτησία καθορίζεται με σκοπό την επίτευξη της ιχνηλασιμότητας και της ευθύνης για τα στοιχεία. **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση καταλόγου καταγραφής των στοιχείων ενεργητικού, προκειμένου να διασφαλίσει ότι ο οργανισμός έχει σαφή, ακριβή και ενημερωμένη κατάσταση των στοιχείων (π.χ. υλισμικό, λογισμικό, πληροφορίες) που διατηρεί. Ο κατάλογος θα πρέπει να προσδιορίζει τον ιδιοκτήτη των στοιχείων αυτών. Ο κατάλογος θα πρέπει επίσης να επιτρέπει στον οργανισμό να παρακολουθεί όλα τα στοιχεία ενεργητικού για τα οποία θα πρέπει να εφαρμόζει και να διατηρεί μέτρα ασφάλειας πληροφοριών. **Πηγή:**
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**
0	1	Ο οργανισμός δεν έχει κάποιο συγκεκριμένο / οργανωμένο τρόπο για την αναγνώριση στοιχείων ενεργητικού εντός του οργανισμού.
1	1	Δεν καταγράφονται με συστηματικό τρόπο τα στοιχεία ενεργητικού.
1	2	Τηρείται κάποιο αρχείο, χωρίς κεντρική διαχείριση ενώ ενημερώνεται ad-hoc.
2	1	Τηρείται ένας ενιαίος κατάλογος στοιχείων ενεργητικού. (Δεν περιλαμβάνονται όμως αλληλεξαρτήσεις μεταξύ τους).
2	2	Υπάρχει ένας αναγνωρισμένος ιδιοκτήτης του καταλόγου, ο οποίος είναι υπεύθυνος για την τήρηση και επικαιροποίηση των σχετικών δεδομένων.
3	1	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται ένας κατάλογος καταγραφής των στοιχείων ενεργητικού, προκειμένου να διασφαλίσει ότι ο οργανισμός έχει σαφή, ακριβή και ενημερωμένη κατάσταση των στοιχείων (π.χ. υλισμικό, λογισμικό, πληροφορίες) που διατηρεί.
3	2	Ο κατάλογος προσδιορίζει τον ιδιοκτήτη των στοιχείων αυτών.

3	3	Ο κατάλογος επίσης να επιτρέπει στον οργανισμό να παρακολουθεί όλα τα στοιχεία ενεργητικού για τα οποία εφαρμόζει και διατηρεί μέτρα ασφάλειας πληροφοριών, τουλάχιστον με χειροκίνητο τρόπο.
3	4	Στον κατάλογο συμπεριλαμβάνονται η περιγραφή της αποδεκτής χρήσης, της λειτουργίας και της τοποθεσίας των στοιχείων, προκειμένου να υπάρχει πλήρης απογραφή των στοιχείων αυτών.
4	1	Χρησιμοποιείται αυτόματο σύστημα για την αναγνώριση και καταγραφή στοιχείων ενεργητικού και συστημάτων εντός του οργανισμού αλλά και εκτός του οργανισμού (hosted in third parties).
4	2	Τα στοιχεία που εξάγονται από το αυτόματο σύστημα συμπληρώνονται με στοιχεία διαδικασιών και δημιουργείται αποτύπωση των σχετικών εξαρτήσεων και αλληλεξαρτήσεων με όσο περισσότερο αυτοματοποιημένο τρόπο γίνεται.
4	3	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
4	4	Έχει δημιουργηθεί κατάλογος με μη εξουσιοδοτημένες εφαρμογές και κατηγορίες εκτελέσιμων αρχείων και διασφαλίζεται ότι απαγορεύεται η εκτέλεσή τους στα στοιχεία του οργανισμού (application blacklisting).
5	1	Διατίθεται αυτόματο σύστημα και διαδικασίες για τον έλεγχο της ακεραιότητας και εγκυρότητας των στοιχείων του καταλόγου στοιχείων ενεργητικού, συστημάτων και διαδικασιών.
5	2	Σε περίπτωση ανίχνευσης στοιχείου που δεν βρίσκεται καταχωρημένο στον κατάλογο διενεργούνται αυτόματες ενέργειες ενημέρωσης του αρμόδιου προσωπικού για τον έλεγχο και επικαιροποίηση των σχετικών στοιχείων.
5	3	Ειδικά σε περίπτωση στοιχείων ενεργητικού, λαμβάνονται άμεσες ενέργειες περιορισμού μέχρι την υλοποίηση της σχετικής διερεύνησης.
5	4	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	5	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
AM3		**Μέτρο:** Παρακολούθηση στοιχείων ενεργητικού **Στόχος Μέτρου:** Να διασφαλιστεί ότι τα στοιχεία ενεργητικού είναι υπό παρακολούθηση για επιθέσεις, ανωμαλίες και απειλές κατά της ασφάλειας, προκειμένου να ενεργοποιηθούν οι διαδικασίες για την αντιμετώπιση συμβάντων και περιστατικών. **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση δυνατοτήτων παρακολούθησης των στοιχείων ενεργητικού, ώστε ο οργανισμός να είναι σε θέση να εντοπίζει ανωμαλίες σε σχέση με κανονικές συνθήκες (π.χ. τοποθεσία, χρήση) και/ή τη λειτουργία των στοιχείων αυτών. Ο οργανισμός θα πρέπει να αναφέρει στην πολιτική αποδεκτής χρήσης, όπως περιγράφεται στο [HRS6], τι συνιστά αποδεκτή χρήση και/ή λειτουργία των στοιχείων ενεργητικού. Ο οργανισμός θα μπορούσε επίσης να εξετάσει την συμπερίληψη της περιγραφής της αποδεκτής χρήσης, της λειτουργίας και της τοποθεσίας των στοιχείων στον κατάλογο των στοιχείων ενεργητικού, όπως περιγράφεται στο [AM2], προκειμένου να υπάρχει πλήρης απογραφή των στοιχείων αυτών. Όταν εντοπίζονται ανωμαλίες, θα πρέπει να ενεργοποιούνται διαδικασίες διαχείρισης συμβάντων και περιστατικών προκειμένου ο οργανισμός να είναι ανθεκτικός στην παρουσία ανωμαλιών. **Πηγή:** C2M2 (Situation), PNNL, NIST 800-53, ISO 27001
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**
0	1	Ο οργανισμός δεν παρακολουθεί τα στοιχεία ενεργητικού του.
1	1	Διενεργείται αρακολούθηση σε ένα μέρος των στοιχείων ενεργητικού του, η οποία δεν είναι πλήρης ή συστηματική.
2	1	Για τα κρίσιμα στοιχεία ενεργητικού, όπως αυτά αποτυπώνονται στον σχετικό κατάλογο [AM2 / RM2], έχει ενεργοποιηθεί παρακολούθηση.

2	2	Η παρακολούθηση περιλαμβάνει κατ' ελάχιστο τις ενέργειες των ατόμων, αντικειμένων και οντοτήτων όταν αποκτούν πρόσβαση ή χρησιμοποιούν τα στοιχεία ενεργητικού, τα γεγονότα που μπορεί να διαταράξουν την ομαλή λειτουργία μιας δραστηριότητας, τις αλλαγές των στοιχείων ενεργητικού που οδηγούν σε διαφοροποίηση από το security baseline, στοιχεία ενεργητικού που συνδέονται (μη-αναμενόμενα) στα δίκτυα του οργανισμού και οποιαδήποτε άλλη ύποπτη δραστηριότητα.
3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται δυνατότητες παρακολούθησης των στοιχείων ενεργητικού, ώστε ο οργανισμός να είναι σε θέση να εντοπίζει ανωμαλίες σε σχέση με κανονικές συνθήκες (π.χ. τοποθεσία, χρήση) και/ή τη λειτουργία των στοιχείων αυτών.
3	2	Αναφέρεται στην πολιτική αποδεκτής χρήσης, όπως περιγράφεται στο [HRS6], τι συνιστά αποδεκτή χρήση και/ή λειτουργία των στοιχείων ενεργητικού.
3	3	Συμπεριλαμβάνεται στην περιγραφή της αποδεκτής χρήσης, η λειτουργία και η τοποθεσία των στοιχείων στον κατάλογο των στοιχείων ενεργητικού όπως αναφέρεται στο [AM2], προκειμένου να υπάρχει πλήρης απογραφή των στοιχείων αυτών.
3	4	Όταν εντοπίζονται ανωμαλίες, ενεργοποιούνται διαδικασίες διαχείρισης συμβάντων και περιστατικών προκειμένου ο οργανισμός να είναι ανθεκτικός στην παρουσία ανωμαλιών.
3	5	Τα αποτελέσματα της παρακολούθησης (logs) περιέχουν κατ' ελάχιστο τις ακόλουθες πληροφορίες: ημερομηνία, ώρα, source address & destination address (όπου αυτό εφαρμόζεται), τύπος καταγραφής, και όποια άλλη πληροφορία μπορεί να δοθεί επιπλέον ως επεξήγηση.
3	6	Εχει προσδιορίστει το είδος της παρακολούθησης που είναι ενεργοποιημένο ανά στοιχείο ενεργητικού (π.χ. System, Security, Application κ.α.), η έκταση της παρακολούθησης σε επίπεδο γεγονότος (π.χ. types of events: audit success, audit failure, login success, object access success, warning, ….), το χρονικό διάστημα διατήρησης των σχετικών εγγραφών (π.χ. 3 μήνες) και η τοποθεσία αποθήκευσης (π.χ. στην συσκευή, σε syslog server, σε άλλο αποθηκευτικό μέσο κ.α.). Τα παραπάνω έχουν εξαχθεί λαμβάνοντας υπόψη το πλαίσιο λειτουργίας του οργανισμού, την στρατηγική και τους στόχους ασφάλειας πληροφοριών όπως αναφέρεται στο [STR1] και το κείμενο νομοθετικό και κανονιστικό πλαίσιο.
4	1	Έχει διενεργηθεί ανάλυση ώστε να προσδιορίσούν οι ανάγκες σε χώρο και υπολογιστική ισχύ για να μπορεί να γίνει η αποθήκευση και διαχείριση των σχετικών δεδομένων παρακολούθησης χωρίς προβλήματα ανά σύστημα.
4	2	Τα δεδομένα της παρακολούθησης ανασκοπούνται ημερησίως με χειροκίνητο ή ημιαυτόματο τρόπο με σκοπό την αναγνώριση πιθανών ανωμαλιών, τάσεων, επερχόμενων επιθέσεων ή πραγματικών επιθέσεων.
4	3	Τουλάχιστον δυο πηγές συγχρονισμού ρολογιού έχουν οριστεί ώστε να εξασφαλίζεται ότι τα στοιχεία της παρακολούθησης έχουν την σωστή χρονοσήμανση.
4	4	Ο συγχρονισμός αφορά όλα τα κρίσιμα στοιχεία ενεργητικού (κατ' ελάχιστον όλοι οι servers και ο εξοπλισμός δικτύου).
4	5	Διενεργείται έλεγχος στα στοιχεία της παρακολούθησης σχετικά με την περίληψη στοιχείων που αναφέρονται στο ML3 (παραπάνω επίπεδο, 3).
4	6	Μέσω κατάλληλων τεχνικών μέτρων, γίνεται παρακολούθηση της κατάστασης των στοιχείων ενεργητικού όπως προβλέπεται από το [AM6].
4	7	Σε περίπτωση που οι δυνατότητες παρακολούθησης αποτυγχάνουν, τότε λαμβάνονται κατάλληλες ενέργειες ώστε να τίθεται εκτός λειτουργίας το συγκεκριμένο στοιχείο μέχρις ότου διερευνηθεί πλήρως ο λόγος της αποτυχίας (Δεν εφαρμόζεται για στοιχεία τα οποία έχουν άμεση σχέση με την διαχείριση της ασφάλειας).
4	8	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Έχει τεθεί σε λειτουργία σύστημα SIEM το οποίο συγκεντρώνει τα στοιχεία παρακολούθησης από το σύνολο των στοιχείων ενεργητικού του οργανισμού.

5	2	Έχουν παραμετροποιηθεί κανόνες και έχουν δημιουργηθεί ενημερώσεις (notifications & alerts) στο κατάλληλο προσωπικό σε περίπτωση ενεργοποίησης κάποιου κανόνα.
5	3	Για την δημιουργία των κανόνων έχουν ληφθεί υπόψη βασικές μέθοδοι επίθεσης. Κατ' ελάχιστον οι κανόνες έχουν παραμετροποιηθεί για να ενημερώνουν 1)σε περίπτωση που ένας λογαριασμός έχει προστεθεί σε ομάδα προνομιακών λογαριασμών ή αν έχουν αναβαθμιστεί τα δικαιώματα υπάρχοντος λογαριασμού ή αν έχει δημιουργηθεί νέος λογαριασμός με δικαιώματα προνομιακής πρόσβασης 2) σε περίπτωση που για κάποιο λογαριασμό με προνομιακό δικαίωμα πρόσβασης έχει αλλάξει ο κωδικός πρόσβασης ή άλλο μυστικό στοιχείο αυθεντικοποίησης 3) αν η σύνδεση έχει γίνει από τοποθεσία η οποία δεν έχει προβλεφθεί από τους σχετικούς κανόνες του οργανισμού, 4) σε περίπτωση (π.χ. >3) αποτυχημένων προσπαθειών πρόσβασης από την ίδια πηγή σε σχετικά μικρό χρονικό διάστημα, 5) σε περίπτωση αποτυχημένων προσπαθειών πρόσβασης από τον ίδιο λογαριασμό σε διαφορετικά μηχανήματα, 6) όταν διενεργείται κάποια σάρωση δικτύου, 7) όταν δημιουργείται κάποιος DHCP εντός του δικτύου 8) όταν ανιχνεύεται κάποια επίθεση που αντιστοιχεί σε κάποιο από τα OWASP Top 10, 9) σε περίπτωση που έχουν δημιουργηθεί alerts για τα IPS / IDS που έχει υλοποιήσει ο οργανισμός, 10) σε περίπτωση που έχουν δημιουργηθεί alerts από το DLP, 11) περιπτώσεις που έχουν διενεργηθεί αλλαγές σε οποιαδήποτε εγγραφή παρακολούθησης περιλαμβανομένης και της διαγραφής του ή της απενεργοποίησης της σχετικής ικανότητας.
5	4	Ο χώρος στον οποίο αποθηκεύονται τα στοιχεία παρακολούθησης είναι προστατευμένος και write only. Σε περίπτωση που αυτό δεν είναι εφικτό, χρησιμοποιούνται χωριστά μηχανήματα στα οποία η πρόσβαση είναι αυστηρά καθορισμένη όπως προβλέπεται και από το [IAM2].
5	5	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	6	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
AM4		**Μέτρο:** Διαχείριση διαθεσιμότητας **Στόχος Μέτρου:** Να διασφαλιστεί η διαθεσιμότητα δικτύων και συστημάτων πληροφοριών με την επίτευξη επαρκούς διαθεσιμότητας πόρων, εφεδρείας και συστημάτων / διαδικασιών υψηλής διαθεσιμότητας. **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση διαδικασιών διαχείρισης της διαθεσιμότητας προκειμένου να διασφαλίζεται ότι παρέχεται το επιθυμητό επίπεδο των επιχειρησιακών υπηρεσιών από τον οργανισμό. Ο οργανισμός θα πρέπει να διασφαλίζει ανά πάσα στιγμή τη διαθεσιμότητα των πόρων (π.χ. χώροι, προσωπικό, συστήματα πληροφορικής, κ.λπ.). Όπως περιγράφεται στο μέτρο [NS6], ο οργανισμός θα πρέπει να εγγυάται την εφεδρεία και την υψηλή διαθεσιμότητα όλων των συστημάτων πληροφορικής, προκειμένου να διασφαλίζεται η έγκαιρη και αποτελεσματική ανάκτηση των δεδομένων μετά την ύπαρξη ενός συμβάντος ή περιστατικού, ή κατόπιν αιτήματος. Ο οργανισμός θα πρέπει να δημιουργήσει εφεδρικά αντίγραφα των πληροφοριών που περιγράφονται στο [DS3]. **Πηγή:**
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**
0	1	Ο οργανισμός δεν έχει λάβει μέτρα για την εξασφάλιση της διαθεσιμότητας των δικτύων και συστημάτων πληροφορικής.
1	1	Υπάρχει κάποιος εξοπλισμός σε εφεδρεία που μπορεί να χρησιμοποιηθεί σε περίπτωση αστοχίας ενός στοιχείου ενεργητικού αλλά δεν καλύπτεται το σύνολο του κρίσιμου εξοπλισμού.
2	1	Έχουν αναγνωρίσθει τα κρίσιμα στοιχεία ενεργητικού.
2	2	Για τα συγκεκριμένα στοιχεία υπάρχει τουλάχιστον ένα ακόμα στοιχείο σε εφεδρεία (μπορεί να είναι το ίδιο ή αντίστοιχης ικανότητας).
2	3	Τα στοιχεία αυτά περιέχονται μέσα στον ενιαίο κατάλογο στοιχείων ενεργητικού.

3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται διαδικασίες διαχείρισης της διαθεσιμότητας προκειμένου να διασφαλίζεται ότι παρέχεται το επιθυμητό επίπεδο των επιχειρησιακών υπηρεσιών από τον οργανισμό.
3	2	Διασφαλείζεται ανά πάσα στιγμή η διαθεσιμότητα των πόρων (π.χ. χώροι, προσωπικό, συστήματα πληροφορικής, κ.λπ.).
3	3	Όπως περιγράφεται στο μέτρο [NS6], ο οργανισμός εγγυάται την εφεδρεία και την υψηλή διαθεσιμότητα όλων των συστημάτων πληροφορικής, προκειμένου να διασφαλίζεται η έγκαιρη και αποτελεσματική ανάκτηση των δεδομένων μετά την ύπαρξη ενός συμβάντος ή περιστατικού, ή κατόπιν αιτήματος.
3	4	Δημιουργούνται εφεδρικά αντίγραφα των πληροφοριών που περιγράφονται στο [DS3].
3	5	Κατ΄ ελάχιστο ο εξοπλισμός διαθέτει εφεδρείες σε σχέση με την ενέργεια, την χωρητικότητα, το δίκτυο και τον τρόπο διασύνδεσης.
3	6	Δεν υπάρχει κρίσιμος εξοπλισμός που δεν έχει εφεδρικό εντός του ίδιου χώρου σε ενεργή ή και ανενεργή λειτουργία.
3	7	Υπάρχει εξοπλισμός σε δευτερεύον σημείο, ο οποίος έχει σχετικά μελετηθεί ώστε να μπορεί να χρησιμοποιηθεί για να ανακάμψουν οι βασικές δραστηριότητες του οργανισμού ενός συγκεκριμένου χρονικού διαστήματος και σε συγκεκριμένο επίπεδο.
4	1	Μέσω κατάλληλων τεχνικών μέτρων, γίνεται παρακολούθηση της κατάστασης των στοιχείων ενεργητικού συνεχώς. (Συγκεκριμένα γίνεται παρακολούθηση αν τα στοιχεία ενεργητικού του οργανισμού τόσο στον βασικό όσο και στον εφεδρικό χώρο ανταποκρίνονται και βρίσκονται σε καλή κατάσταση λειτουργίας).
4	2	Σε περίπτωση που κάποιο σύστημα ενεργητικού έχει αναγνωριστεί ότι δεν είναι διαθέσιμο (alert), το κατάλληλο προσωπικό ειδοποιείται για την διερεύνηση και την χειροκίνητη μετάβαση στο εφεδρικό σύστημα (αν απαιτείται).
4	3	Έχει προβλεφθεί ώστε να υπάρχει δυνατότητα πρόσβασης και ανάκτησης των δεδομένων όπως απαιτείται από τα εφεδρικά αντίγραφα (π.χ. υπάρχει δυνατότητα λήψης, εγκατάστασης ή χρήσης του λογισμικού αντιγράφων ασφαλείας και υπάρχει διαθεσιμότητα των σχετικών κλειδιών) όπως προβλέπεται από το [DS3].
4	4	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Εφαρμόζονται λύσεις συγχρονισμού (replication) σε εναλλακτικό χώρο για τα κρίσιμα συστήματα όπως αυτά έχουν αναγνωριστεί σύμφωνα με την ανάλυση επιχειρησιακών επιπτώσεων και τα σχετικά σχέδια επιχειρησιακής συνέχειας και ανάκαμψης από καταστροφή.
5	2	Σε περίπτωση αστοχίας ή μη διαθεσιμότητας του πρωτεύοντος εξοπλισμού γίνονται αυτόματες ενέργειες για την ενεργοποίηση του δευτερεύοντος.
5	3	Μια φορά το χρόνο τουλάχιστον γίνεται πλήρης λειτουργική δοκιμή της κατάστασης συγχρονισμού και της δυνατότητας λειτουργίας του οργανισμού από την εναλλακτική τοποθεσία.
5	4	Τηρούνται χωριστά εφεδρικά αντίγραφα και σε τρίτη ασφαλή τοποθεσία, για να μπορεί να προστατευτεί ο οργανισμός και από επιθέσεις κυβερνοεκβιασμού σύμφωνα με τα προβλεπόμενα του [DS3].
5	5	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	6	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

AM5	**Μέτρο:** Κρυπτογραφία **Στόχος Μέτρου:** Να διασφαλιστεί η εμπιστευτικότητα, ακεραιότητα και αυθεντικότητα των πληροφοριών με την υιοθέτηση κατάλληλων κρυπτογραφικών λύσεων. **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση πολιτικής σχετικά με τη χρήση κρυπτογραφικών μέτρων, προκειμένου να διασφαλίζονται η εμπιστευτικότητα, η ακεραιότητα και η αυθεντικότητα των δεδομένων κατά την αποθήκευση, τη χρήση και τη μεταφορά. Η πολιτική κρυπτογράφησης θα πρέπει να λαμβάνει υπόψη την εφαρμογή κρυπτογραφικών μέτρων σε όλα τα στάδια του κύκλου ζωής των πληροφοριών και να εξετάζει εφαρμογές, συστήματα, εξοπλισμό δικτύου και διαύλους επικοινωνίας. **Πηγή:** CSA CCM v4., ANSII guidelines, NIST 800-53, NIST 800-57, CIS

Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν υλοποιεί κρυπτογραφία σε καμια της μορφή και εφαρμογή.
1	1	Χρησιμοποιούνται λύσεις κρυπτογραφίας σε μεμονωμένες περιπτώσεις για κάποιους πόρους χωρίς να υπάρχει κάποιος συνολικός σχεδιασμός ή έλεγχος.
2	1	Εφαρμόζεται κρυπτογραφία στα δεδομένα ή σε ολόκληρες συσκευές που έχουν αναγνωριστεί ως κρίσιμες στον σχετικό ενιαίο κατάλογο πόρων.
2	2	Επίσης εφαρμόζεται κρυπτογράφηση σε αφαιρούμενα μεταφορικά μέσα όπου αυτά χρησιμοποιούνται και σε end point devices.
3	1	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται πολιτική σχετικά με τη χρήση κρυπτογραφικών μέτρων, προκειμένου να διασφαλίζονται η εμπιστευτικότητα, η ακεραιότητα και η αυθεντικότητα των δεδομένων κατά την αποθήκευση, τη χρήση και τη μεταφορά.
3	2	Η πολιτική κρυπτογράφησης λαμβάνει υπόψη την εφαρμογή κρυπτογραφικών μέτρων σε όλα τα στάδια του κύκλου ζωής των πληροφοριών και εξετάζει εφαρμογές, συστήματα, εξοπλισμό δικτύου και διαύλους επικοινωνίας.
3	3	Κατ΄ ελάχιστον εφαρμόζονται τα ακόλουθα: SHA-256, SHA-512 or SHA-341 ως hash function, HMAC με SHA-256, bcrypt, scrypt ή PBKDF2 για την αποθήκευση κωδικών πρόσβασης, AES ή AES-CBC για συμμετρική κρυπτογράφηση; RSA-OAEP όπως ορίζεται στο PKCS#1 v2.1 για ασύμμετρη κρυπτογράφηση και για υπογραφές, RSA-SSA-PSS όπως ορίζεται στο PKCS#1 v2.1.
3	4	Σε κάθε περίπτωση χρησιμοποιούνται κατάλληλα κλειδιά. Ειδικά για AES τα κλειδιά θα είναι 128 bits και για τους αλγόριθμους που στηρίζονται στο RSA, τα modules και τα secret exponents πρέπει να είναι τουλάχιστον 2048 bits ή 3072 bits, με public exponents, για την κρυπτογράφηση τουλάχιστον μεγαλύτερο από 65536.
3	5	Για την μεταφορά δεδομένων και την προστασία των δεδομένων σε ηρεμία εφαρμόζονται τα αντίστοιχα των [DS2] και [DS4].
4	1	Χρησιμοποιείται λογισμικό ή κρυπτογραφικές βιβλιοθήκες οι οποίες έχουν ελεγχθεί από έγκυρα τρίτα μέρη.
4	2	Επιπλέον χρησιμοποιούνται λύσεις που είναι σχετικά πιστοποιημένες (όπου αυτό υπάρχει), λογισμικό όπως VeraCrypt software, για την δημιουργία encrypted containers, το GNU Privacy Guard software, που επιτρέπει την εφαρμογή ασύμμετρης κρυπτογραφίας.
4	3	Κανενός τύπου Wi-Fi enabled εξοπλισμός δεν παραμετροποιείται ώστε να λαμβάνει ή να μοιράζεται κλειδιά κρυπτογράφησης.
4	4	Τα κλειδιά κρυπτογράφησης προστατεύονται ως πληροφορία του υψηλότερου επίπεδου διαβάθμισης όπως αναφέρεται στο [DS2] και υπόκειται σε αυστηρό έλεγχο πρόσβασης.
4	5	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Τηρείται αυτόματο σύστημα για την παρακολούθηση και διαχείριση των πιστοποιητικών και άλλων μέσων κρυπτογράφησης.

5	2	Στις περιπτώσεις που ο οργανισμός διαχειρίζεται (περιλαμβανομένης και της έκδοσης) κρυπτογραφικά κλειδιά, χρησιμοποιείται σύστημα διαχείρισης που του επιτρέπει την δημιουργία, μοναδική χρήση, περιτροπή, ανάκληση, καταστροφή, ενεργοποίηση, απενεργοποίηση, αρχειοθέτηση κλειδιών.
5	3	Υπάρχουν διαδικασίες άμεσης ανταπόκρισης σε περίπτωση που υποκλαπεί ή διαρρεύσει ένα κλειδί κρυπτογράφησης για άμεσα περιορισμό του σχετικού κινδύνου.
5	4	Οι βέλτιστες διεθνείς πρακτικές τόσο για on-premise όσο και για cloud συστήματα που αναφέρονται στο CSA CCM v4.0 στο αντικείμενο του CEK εφαρμόζονται.
5	5	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	6	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
ΑΜ6		**Μέτρο:** Διαχείριση χωρητικότητας **Στόχος Μέτρου:** Να εξασφαλιστεί η κατάλληλη χωρητικότητα και επίδοση των υπηρεσιών των συστημάτων και διαδικασιών πληροφοριών. **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση διαδικασίας διαχείρισης της χωρητικότητας προκειμένου να διασφαλιστεί ότι η χωρητικότητα και οι επιδόσεις των συστημάτων πληροφορικής του οργανισμού δεν επηρεάζονται αρνητικά από αυξημένα επίπεδα ζήτησης υπηρεσιών. Η διαδικασία διαχείρισης χωρητικότητας θα πρέπει να περιλαμβάνει τη διαχείριση της επιχειρησιακής ικανότητας, προκειμένου να διασφαλίζεται ότι οι επιχειρησιακές ανάγκες μετατρέπονται σε απαιτήσεις χωρητικότητας, διαχείριση της χωρητικότητας υπηρεσιών ώστε να γίνεται σωστή διαχείριση της χωρητικότητας των υποσυστημάτων πληροφορικής και ένα μηχανισμό υποβολής εκθέσεων διαχείρισης χωρητικότητας. **Πηγή:**
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**
0	1	Ο οργανισμός δεν διαχειρίζεται με κάποιο τρόπο την χωρητικότητα των συστημάτων πληροφορικής.
1	1	Γίνεται παρακολούθηση κάποιων στοιχείων για κάποιους πόρους τουλάχιστον σε ad-hoc βάση και χωρίς κάποια συγκεκριμένη οργάνωση.
2	1	Έχει αναγνωρίσθει μια σειρά από κρίσιμους πόρους (όπως αυτοί περιέχονται στον ενιαίο κατάλογο στοιχείων ενεργητικού) για τους οποίους γίνεται παρακολούθηση των στοιχείων χωρητικότητας.
2	2	Για τα συγκεκριμένα στοιχεία ενεργητικού έχουν προσδιοριστεί τα βασικά στοιχεία παρακολούθησης (κατ' ελάχιστο: δίσκος, μνήμη, επεξεργαστής, bandwidth) και έχουν παραμετροποιηθεί σχετικοί κανόνες.
3	1	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται διαδικασία διαχείρισης της χωρητικότητας προκειμένου να διασφαλιστεί ότι η χωρητικότητα και οι επιδόσεις των συστημάτων πληροφορικής του οργανισμού δεν επηρεάζονται αρνητικά από αυξημένα επίπεδα ζήτησης υπηρεσιών.
3	2	Η διαδικασία διαχείρισης χωρητικότητας περιλαμβάνει τη διαχείριση της επιχειρησιακής ικανότητας, (προκειμένου να διασφαλίζεται ότι οι επιχειρησιακές ανάγκες μετατρέπονται σε απαιτήσεις χωρητικότητας), διαχείριση της χωρητικότητας υπηρεσιών (ώστε να γίνεται σωστή διαχείριση της χωρητικότητας των υποσυστημάτων πληροφορικής) και ένα μηχανισμό υποβολής εκθέσεων διαχείρισης χωρητικότητας.
3	3	Για τα κρίσιμα στοιχεία ενεργητικού του οργανισμού αλλά και τις βασικές λειτουργίες γίνεται αυτόματη παρακολούθηση της διαθεσιμότητας τους.
3	4	Διενεργείται system tuning & monitoring για την εξασφάλιση της βέλτιστης δυνατής επίδοσης σε επίπεδο χωρητικότητας.
4	1	Για τα κρίσιμα στοιχεία ενεργητικού του οργανισμού αλλά και τις βασικές λειτουργίες έχουν διεξαχθεί μελέτες για τον σχεδιασμό των κατάλληλων πόρων σε βάθος 5ετίας.

4	2	Οι μελέτες στηρίζονται πάνω σε ιστορικά και πρόσφατα στοιχεία ενώ λαμβάνουν υπόψη τις τάσεις, τα μελλοντικά σχέδια και τους στόχους του οργανισμού όπως αναφέρονται στο [STR1].
4	3	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
4	4	Τα στοιχεία που παρακολουθούνται είναι εγκαταστάσεις, εξοπλισμός, άτομα, γραφεία και άλλα.
5	1	Συνεχής παρακολούθηση της κατάστασης σε σχέση με την χωρητικότητα των συστημάτων.
5	2	Εξάγονται στοιχεία και αναφορές σχετικά με την επίδοση και αναθεωρείται ο σχετικός σχεδιασμός όπως απαιτείται σύμφωνα με τα στοιχεία πραγματικής χρήσης και τάσεων.
5	3	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	4	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
5	5	Διενεργούνται stress tests για την επιβεβαίωση της αποτελεσματικότητας των σχετικών προβλέψεων.

Κατηγορία		ΔΙΑΧΕΙΡΙΣΗ ΤΑΥΤΟΤΗΤΑΣ ΚΑΙ ΠΡΟΣΒΑΣΗΣ
IAM1		**Μέτρο:** Έλεγχος πρόσβασης βάσει ρόλου **Στόχος Μέτρου:** Να επαληθευτεί της η αυθεντικότητα και εξουσιοδότηση χρηστών, με βάση το ελάχιστο προνόμιο και τους οργανωτικούς ρόλους και αρμοδιότητες. **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση μέτρων διαχείρισης ταυτότητας και πρόσβασης τα οποία εξετάζουν μέτρα πρόσβασης με βάση το ρόλο, με σκοπό να παρέχουν τεχνικά και οργανωτικά μέσα για την επιβολή της αρχής του ελάχιστου προνομίου και να διαχειρίζονται αντίστοιχα τους προνομιούχους χρήστες. Ο έλεγχος πρόσβασης βάσει ρόλου θα πρέπει να διασφαλίζει ότι χορηγούνται επαρκείς άδειες σε χρήστες με βάση τις αρμοδιότητες τους που συνδέονται με αντίστοιχους ρόλους. Ο έλεγχος πρόσβασης βάσει ρόλου θα πρέπει να γίνεται σύμφωνα με τις διαδικασίες ασφάλειας των ανθρώπινων πόρων, όπως ορίζεται στο [HRS1], προκειμένου να διασφαλιστεί ότι οι ρόλοι πρόσβασης είναι ευθυγραμμισμένοι με τους ρόλους και αρμοδιότητες των στελεχών στο πλαίσιο του οργανισμού. **Πηγή:**
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**
0	1	Ο οργανισμός δεν διαχειρίζεται καθόλου την πρόσβαση στα συστήματά του.
1	1	Ο οργανισμός έχει συστήματα για την διαχείριση πρόσβασης στα συστήματα του.
1	2	Η διαχείριση της πρόσβασης δεν είναι οργανωμένη και συντονισμένη κεντρικά.
2	1	Υπάρχει μια πολιτική ελέγχου πρόσβασης η οποία καλύπτει όλα τα στοιχεία ενεργητικού και τα κτήρια του οργανισμού όπως εμφανίζονται στον ενιαίο κατάλογο στοιχείων ενεργητικού σύμφωνα με το [AM2].
2	2	Η πολιτική ελέγχου πρόσβασης καλύπτει την πρόσβαση σε εφαρμογές, δίκτυα, πόρους και κτήρια.
3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται μέτρα διαχείρισης ταυτότητας και πρόσβασης τα οποία εξετάζουν μέτρα πρόσβασης με βάση το ρόλο, με σκοπό να παρέχουν τεχνικά και οργανωτικά μέσα για την επιβολή της αρχής του ελάχιστου προνομίου και να διαχειρίζονται αντίστοιχα τους προνομιούχους χρήστες.
3	2	Ο έλεγχος πρόσβασης βάσει ρόλου διασφαλίζει ότι χορηγούνται επαρκείς άδειες σε χρήστες με βάση τις αρμοδιότητες τους που συνδέονται με αντίστοιχους ρόλους.
3	3	Ο έλεγχος πρόσβασης βάσει ρόλουγίνεται σύμφωνα με τις διαδικασίες ασφάλειας των ανθρώπινων πόρων, όπως ορίζεται στο [HRS1], προκειμένου να διασφαλιστεί ότι οι ρόλοι πρόσβασης είναι ευθυγραμμισμένοι με τους ρόλους και αρμοδιότητες των στελεχών στο πλαίσιο του οργανισμού.
3	4	Οι ιδιοκτήτες των πόρων προσδιορίζουν τα κατάλληλα δικαιώματα πρόσβασης και τους κανόνες πρόσβασης για τους ρόλους που πρέπει να έχουν πρόσβαση στους πόρους υπό την ευθύνη τους.
3	5	Ο προσδιορισμός στηρίζεται στην κρισιμότητα του πόρου, την ανάγκη πρόσβασης, την αρχή της ελάχιστης πρόσβασης και τα αποτελέσματα της ανάλυσης κινδύνου.
3	6	Ισχύουν οι ακόλουθες βασικές αρχές : 1) Οι λειτουργίες ασφαλείας είναι περιορισμένες στον ελάχιστο αριθμό χρηστών που είναι απαραίτητες για να εξασφαλίσουν την ασφάλεια των συστημάτων, 2) Αν ένας ρόλος δεν χρειάζεται να έχει πρόσβαση σε μια πληροφορία, τότε δεν πρέπει να έχει πρόσβαση, 3) Τηρείται διαχωρισμός καθηκόντων όπου είναι αυτό δυνατό.
3	7	Η πολιτική ελέγχου πρόσβασης περιγράφει ποιος (groups / entities / users / systems / services κλπ) μπορεί να έχει πρόσβαση σε ποια πληροφορία/ οντότητα / αντικείμενο / σύστημα /υπηρεσία / δίκτυο κ.α. και σε ποιο επίπεδο.
3	8	Διατηρείται μητρώο σχετικών λογαριασμών και οντοτήτων.
4	1	Γίνεται ανάθεση δικαιωμάτων βάσει ρόλου.
4	2	Υπάρχει μια ευθυγράμμιση μεταξύ των επιχειρηματικών ρόλων και των προφίλ ελέγχου πρόσβασης.

4	3	Η πολιτική περιλαμβάνει τη σχετική νομοθεσία και τυχόν συμβατικές υποχρεώσεις σχετικά με τον περιορισμό της πρόσβασης σε δεδομένα ή υπηρεσίες.
4	4	Διενεργείται τακτικός έλεγχος δικαιωμάτων πρόσβασης.
4	5	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Υπάρχει αυτοματοποιημένο σύστημα το οποίο ελέγχει την ύπαρξη λογαριασμών ή οντοτήτων εντός του οργανισμού που δεν είναι explicitly εξουσιοδοτημένος για συγκεκριμένες ενέργειες.
5	2	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	3	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
IAM2		**Μέτρο:** Έλεγχος εξωτερικής πρόσβασης **Στόχος Μέτρου:** Να εξασφαλιστούν επαρκή μέτρα στο πλαίσιο της εξωτερικής πρόσβασης σε οργανωτικούς πόρους. **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση μέτρων ελέγχου πρόσβασης για εξωτερική και εξ αποστάσεως πρόσβαση σε οργανωτικούς πόρους. Ο οργανισμός θα πρέπει να διασφαλίζει τη δυνατότητα απομακρυσμένης πρόσβασης στο δίκτυο με τη χρήση εικονικών ιδιωτικών δικτύων (VPN) και την πρόσβαση σε εξ αποστάσεως εφαρμογές μέσω της χρήσης εξωτερικών εφαρμογών διεπαφών. Ο οργανισμός εφαρμόζει επαρκή μέτρα διαχείρισης ταυτότητας και πρόσβασης, ώστε να αντικατοπτρίζει την πολιτική ασφάλειας πληροφοριών, όπως ορίζεται στο [GOV3], και τον ειδικό έλεγχο πρόσβασης βάσει ρόλου, όπως ορίζεται στο μέτρο [IAM1]. **Πηγή:**
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**
0	1	Ο οργανισμός δεν διαχειρίζεται με συγκεκριμένο οργανωμένο τρόπο την εξωτερική πρόσβαση σε όλους τους πόρους. Υπάρχει εξωτερική πρόσβαση σε κάποια συστήματα του οργανισμού αλλά ο τρόπος πρόσβασης δεν είναι καθορισμένος και δεν ακολουθεί μια συγκεκριμένη πολιτική.
1	1	Η εξωτερική πρόσβαση σε πόρους του οργανισμού δίνεται μετά από σχετική έγκριση από εξουσιοδοτημένο υπεύθυνο.
1	2	Ο υπεύθυνος τηρεί λίστα με τις εξωτερικές προσβάσεις που έχουν δοθεί ανά σύστημα.
1	3	Μπορεί για κάθε εξωτερική πρόσβαση να υπάρχει διαφορετικός τρόπος πρόσβασης και να εφαρμόζονται διαφορετικά μέτρα.
2	1	Υπάρχει πολιτική για την διαχείριση της εξωτερικής πρόσβασης σε πόρους του οργανισμού.
2	2	Υπάρχει σαφής ιδιοκτήτης της πολιτικής και έχουν καθοριστεί τα βήματα που ακολουθούνται για την ενεργοποίηση εξωτερικής πρόσβασης σε πόρους του οργανισμού.
2	3	Προκειμένου να αποδοθεί εξωτερική πρόσβαση στους πόρους, ακολουθείται διαδικασία έγκρισης από τον αναγνωρισμένο ιδιοκτήτη του πόρου.
3	1	Οι εξωτερικές προσβάσεις σε πόρους του οργανισμού είναι περιορισμένες και υπόκεινται σε αυστηρές διαδικασίες διαχείρισης και ελέγχου πρόσβασης.
3	2	Οι ρόλοι στους οποίους δίνεται το δικαίωμα εξωτερικής πρόσβασης είναι συγκεκριμένοι, διακριτοί και εξουσιοδοτημένοι κατάλληλα από τους ιδιοκτήτες των πόρων ή άλλους κατάλληλους ρόλους (που έχει ορίσει ο οργανισμός με βάσει την δομή και λειτουργία του).
3	3	Για την εξωτερική πρόσβασης χρησιμοποιείται πάντα κρυπτογράφηση.
3	4	Οι εξωτερικές συνδέσεις παρακολουθούνται (logged) αυτόματα από κατάλληλο σύστημα.
4	1	Η πρόσβαση υλοποιείται με MFA.
4	2	Η εξωτερική πρόσβαση γίνεται μέσα από συγκεκριμένες καθορισμένες πύλες πρόσβασης με υλοποιημένα αυστηρά πρωτόκολλα ασφαλείας.

4	3	Σε περίπτωση εξωτερικής πρόσβασης, πριν την διενέργεια της σύνδεσης, η συσκευή ελέγχεται για την συμμόρφωσή της με συγκεκριμένες πολιτικές ασφαλείας του οργανισμού (π.χ. antimalware, USB, firewall, password, applications κ.α.).
4	4	Οι ενέργειες πρόσβασης καταγράφονται (logged) ανεξάρτητα του επιπέδου χρήστη.
4	5	Ελέγχονται σε τακτά χρονικά διαστήματα οι καταγραφές (logs) για την επιβεβαίωση της συμμόρφωσης με την πολιτική ελέγχου πρόσβασης και την ανίχνευση πιθανών αποκλίσεων.
4	6	Αν είναι δυνατό, η διαδικασία αυτά υλοποιείται αυτόματα.
4	7	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Web application firewalls χρησιμοποιούνται για ολες τις εφαρμογές στις οποίες γίνεται πρόσβαση από το Web ή είναι κρίσιμες για τον οργανισμό.
5	2	Απευθείας απόμακρυσμένη πρόσβαση σε κρίσιμους πόρους δεν επιτρέπεται.
5	3	Έχει δημιουργηθεί κατάλληλη αρχιτεκτονική, με κατάλληλους διαχωρισμούς, ώστε να μπορεί να υπάρχει δυνατότητα πρόσβασης σε κρίσιμους πόρους σε περίπτωση ανάγκης χωρίς να επηρεάζεται η ασφάλεια του πόρου.
5	4	Ελέγχονται σε τακτά χρονικά διαστήματα οι καταγραφές (logs) για την επιβεβαίωση της συμμόρφωσης με την πολιτική ελέγχου πρόσβασης και την ανίχνευση πιθανών αποκλίσεων.
5	5	Κατάλληλοι συσχετισμοί / κανόνες και alerts έχουν υλοποιηθεί μέσα στα συστήματα, για την έγκαιρη ενημέρωση του οργανισμού.
5	6	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	7	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
IAM3		**Μέτρο:** Διαχείριση προνομιούχων χρηστών **Στόχος Μέτρου:** Να εξασφαλιστούν επαρκή μέτρα για τους χρήστες που έχουν προνομιακή πρόσβαση σε οργανωτικούς πόρους, συστήματα και δίκτυα. **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση μέτρων για τη διασφάλιση της ορθής διαχείρισης των προνομιούχων χρηστών, και ενεργοποίηση τους μόνο όταν χρειάζεται. Ο οργανισμός διασφαλίζει ότι στους χρήστες δεν χορηγούνται προνομιακά δικαιώματα εξ ορισμού και ότι εφαρμόζονται κατάλληλα τεχνικά και οργανωτικά μέτρα για τη διασφάλιση της προστασίας των προνομιακών δικαιωμάτων των χρηστών από κακόβουλες πράξεις ή από άλλες αρνητικές συμπεριφορές ή προθέσεις. Ο οργανισμός διασφαλίζει ότι τα συστήματα και οι εφαρμογές δεν λειτουργούν εξ ορισμού με προνομιακά δικαιώματα χρήστη, προκειμένου να μετριάζεται ο κίνδυνος της κλιμάκωσης προνομίων. **Πηγή:**
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**
0	1	Ο οργανισμός δεν έχει έλεγχο επί της διαδικασίας παραχώρησης προνομιακών δικαιωμάτων πρόσβασης σε πόρους, συστήματα και δίκτυα.
1	1	Για τους κρίσιμους πόρους, ο οργανισμός έχει περιορίσει το πλήθος των χρηστών που έχουν προνομιακή πρόσβαση σε πόρους, συστήματα και δίκτυα.
2	1	Έχει υλοποιηθεί συγκεκριμένη πολιτική ή και διαδικασία με την οποία γίνεται απόδοση προνομιακών δικαιωμάτων πρόσβασης στους χρήστες.
2	2	Τηρείται λίστα με όλους τους λογαριασμούς (χρηστών / service acccounts κλπ) που έχουν προνομιακή πρόσβαση σε πόρους, συστήματα και δίκτυα.
3	1	Έχειι καταγραφεί πολιτική ή διαδικασία για την διαχείριση της προνομιακής πρόσβασης σε πόρους, συστήματα και δίκτυα.
3	2	Η πολιτική ή διαδικασία είναι συμβατή με τις επιχειρησιακές ανάγκες του οργανισμού και την πολιτική ελέγχου πρόσβασης του οργανισμού.

3	3	Τα δικαιώματα προνομιακής πρόσβασης αποδίδονται μόνο σε χρήστες σύμφωνα με την σχετική ανάγκη (need to use basis & event by event basis).
3	4	Οι χρήστες που έχουν δικαιώματα προνομιακής πρόσβασης είναι διαφορετικοί από αυτούς που χρησιμοποιούνται για τις καθημερινές επιχειρησιακές δραστηριότητες.
4	1	Για τους λογαριασμούς που έχουν προνομιακή πρόσβαση σε πόρους, συστήματα και δίκτυα, υλοποιείται παρακολούθηση (logging) και εξασφαλίζεται ότι οι σχετικές καταγραφές δεν μπορούν να τροποιηθούν, απενεργοποιηθούν, διαγραφούν ή αλλοιωθούν από τους λογαριασμούς αυτούς.
4	2	Για τους λογαριασμούς με προνομιακή πρόσβαση υλοποιείται MFA, είτε οι πόροι βρίσκονται on-site είτε φιλοξενούνται από τρίτα μέρη.
4	3	Τηρείται λίστα με όλους τους λογαριασμούς (χρηστών / service acccounts κλπ) που έχουν προνομιακή πρόσβαση σε πόρους, συστήματα και δίκτυα.
4	4	Η λίστα περιέχει κατ΄ ελάχιστο τα ακόλουθα: πόρος, λογαριασμός, τύπος προνομιακής πρόσβασης, ημερομηνία εκχώρησης, ιδιοκτήτη πόρου, ημερομηνία ανασκόπησης, σκοπός.
4	5	Διενεργείται, τουλάχιστον κάθε τρίμηνο, ανασκόπηση των προνομιακών δικαιωμάτων για επικύρωση ότι όλοι οι ενεργοί λογαριασμοί είναι εξουσιοδοτημένοι.
4	6	Οι κωδικοί πρόσβασης των λογαριασμών προνομιακής πρόσβασης είναι γνωστοί μόνο στον ανατεθειμένο ιδιοκτήτη τους.
4	7	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Οι λογαριασμοί με προνομιακή πρόσβαση έχουν καθορισμένη πολιτική για την αλλαγή των κωδικών πρόσβασης.
5	2	Γενικοί λογαριασμοί προνομιακής πρόσβασης δεν χρησιμοποιούνται (εκτός από συγκεκριμένες περιπτώσεις στις οποίες δεν υπάρχει άλλη επιλογή).
5	3	Οι κωδικοί πρόσβασης για γενικούς λογαριασμούς προνομιακής πρόσβασης προστατεύονται και είναι προσβάσιμοι μόνο σε περίπτωση που απαιτείται σε συγκεκριμένα εξουσιοδοτημένα άτομα.
5	4	Η χρήση γενικών λογαριασμών προνομιακής πρόσβασης παρακολουθείται (logged) ενώ υπάρχει αυτόματο σύστημα το οποίο ενημερώνει το εξουσιοδοτημένο προσωπικό σχετικά με την χρήση του.
5	5	Τέτοιες περιπτώσεις διαχειρίζονται ως πιθανά περιστατικά ασφαλείας και ενεργοποιείται η αντίστοιχη διαδικασία διαχείρισης περιστατικών ασφαλείας.
5	6	Σε περίπτωση ανάγκης χρήσης γενικών λογαριασμών προνομιακής πρόσβασης, ακολουθείται η διαδικασία διαχείρισης αλλαγών (έκτακτων ή προγραμματισμένων) και δεν χρησιμοποιούνται μέχρι να ολοκληρωθεί η σχετική εξουσιοδότηση.
5	7	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	8	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

IAM4	**Μέτρο:** Ισχυρά μέτρα για επαλήθευση ταυτότητας **Στόχος Μέτρου:** Να εξασφαλιστεί ότι γίνεται επαλήθευση της ταυτότητας των εξουσιοδοτημένων ατόμων με ασφάλεια και με τη χρήση μέτρων ισχυρής επαλήθευσης ταυτότητας. **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση ισχυρών μέτρων ελέγχου πρόσβασης και επαλήθευσης της ταυτότητας, προκειμένου να διασφαλίζεται ότι τα εξουσιοδοτημένα άτομα αναγνωρίζονται δεόντως και γίνεται επαλήθευση της ταυτότητας τους κατά την επεξεργασία οργανωτικών πόρων. Ο οργανισμός πρέπει να εξετάσει την επαλήθευση μέσω πολλών παραγόντων προκειμένου να αποδείξει την ταυτότητά ενός ατόμου. Η διαδικασία αυτή πρέπει να περιλαμβάνει τουλάχιστον δύο από τις ακόλουθες αρχές: παροχή ταυτότητας με την κατοχή συγκεκριμένου στοιχείου (π.χ. κλειδί ή άλλο μέσο εξακρίβωσης της ταυτότητας), με τη γνώση ενός στοιχείου (π.χ. κωδικός ή φράση πρόσβασης, ή άλλο μυστικό), με βιομετρικά ή μορφολογικά χαρακτηριστικά (π.χ. σάρωση ίριδας, αποτύπωμα δακτύλου ή οπτική επαλήθευση ταυτότητας από ένα αξιόπιστο μέρος, όπως έναν φρουρό ασφαλείας). **Πηγή:**

Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν έχει υλοποιήσει κάποια συγκεκριμένη / οργανωμένη πολιτική για τον τρόπο με τον οποίο γίνεται η επαλήθευση της ταυτότητας των λογαριασμών πρόσβασης.
1	1	Γίνεται αυθεντικοποίηση της πρόσβασης στα περισσότερα συστήματα του οργανισμού αλλά υπάρχουν και κάποιες λειτουργίες (κυρίως εντός δικτύου του οργανισμού) που δεν απαιτείται αυθεντικοποίηση.
2	1	Η επιλογή των μηχανισμών αυθεντικοποίησης (επαλήθευσης της ταυτότητας των εξουσιοδοτημένων ατόμων) γίνεται ως αποτέλεσμα σχετικής διαδικασίας ανάλυσης διακινδύνευσης. (Διαφορετικής κρισιμότητας συστήματα μπορεί να απαιτούν διαφορετικού επιπέδου μέτρα επαλήθευσης ταυτότητας.)
2	2	Η ταυτότητα όλων των χρηστών, διεργασιών, πόρων επαληθεύεται ως προαπαιτούμενο για την παραχώρηση πρόσβασης.
3	1	Έχει καταγραφεί πολιτική ή διαδικασία για την διαχείριση του επαλήθευσης ταυτότητας.
3	2	Η πολιτική ή διαδικασία είναι συμβατή με τις επιχειρησιακές ανάγκες του οργανισμού και την πολιτική ελέγχου πρόσβασης του οργανισμού. (μπορεί να αποτελεί και μέρος της τελευταίας).
3	3	Η πολιτική περιέχει τις κατηγορίες μηχανισμών αυθεντικοποίησης που μπορούν να χρησιμοποιούνται ανά κρισιμότητα συστήματος (π.χ. Single-Sign-On, two-factor authentication, multi-factor authentication κ.α.) τόσο για τους πόρους όσο και για τα δίκτυα (περιλαμβανομένων των remote & wifi) και τις άλλες λειτουργίες (εφαρμογές κ.α.).
3	4	Οι χρήστες και τα συστήματα έχουν μοναδικά αναγνωριστικά και αυθεντικοποιούνται πριν την πρόσβασή στους στις υπηρεσίες και τα συστήματα.
3	5	Το σύστημα αυθεντικοποίησης επικυρώνει την πληροφορία αυθεντικοποίησης αφού ολοκληρωθεί η εισαγωγή όλης της πληροφορίας.
3	6	Το σύστημα αυθεντικοποίησης είναι προστατευμένο έναντι brute force log-on attempts και καταγράφει τις επιτυχημένες και αποτυχημένες προσπάθειες.
3	7	Η πρόσβαση υλοποιείται όπου είναι δυνατό με MFA (σε συμφωνία και με τις άλλες σχετικές απαιτήσεις IAM).
3	8	Εξατέζεται η επαλύθευση μέσω πολλών παραγόντων προκειμένου να αποδειχθεί η ταυτότητά ενός ατόμου.
3	9	Η διαδικασία αυτή περιλαμβάνει τουλάχιστον δύο από τις ακόλουθες αρχές: παροχή ταυτότητας με την κατοχή συγκεκριμένου στοιχείου (π.χ. κλειδί ή άλλο μέσο εξακρίβωσης της ταυτότητας), με τη γνώση ενός στοιχείου (π.χ. κωδικός ή φράση πρόσβασης, ή άλλο μυστικό), με βιομετρικά ή μορφολογικά χαρακτηριστικά (π.χ. σάρωση ίριδας, αποτύπωμα δακτύλου ή οπτική επαλήθευση ταυτότητας από ένα αξιόπιστο μέρος, όπως έναν φρουρό ασφαλείας).

4	1	Οι προκαθορισμένοι λογαριασμοί (λειτουργιών ή κατασκευαστών) απενεργοποιούνται ή μετονομάζονται όπου αυτό είναι δυνατό.
4	2	Για κάθε έναν από τους μηχανισμούς αυθεντικοποίησης έχει προδιαγραφεί και καταγραφεί ο τρόπος λειτουργίας.
4	3	Ειδικά για την περίπτωση χρήσης κωδικών πρόσβασης, υπάρχει καταγεγραμμένη πολιτική κωδικών πρόσβασης με συγκεκριμένες προβλέψεις για πολυπλοκότητα κωδικών, μοναδικότητα / επαναχρησιμοποίηση κωδικών, προσωρινών κωδικών, invalid logon attempts κ.α.
4	4	Οι κωδικοί πρόσβασης προστατεύονται όπου και αν βρίσκονται μέσω κρυπτογράφησης.
4	5	Σε περίπτωση χρήσης άλλων ή επιπλέον μηχανισμών (π.χ. authenticators, one time passwords κλπ), προσδιορίζεται ακριβώς το επίπεδο ασφαλείας των συγκεκριμένων μηχανισμών ανά περίπτωση και συμφωνεί με τα αποτελέσματα της ανάλυσης διακινδύνευσης.
4	6	Ο έλεγχος ταυτότητας είναι replay resistant (Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.)
4	7	Οι πληροφορίες ανταπόκρισης από τα συστήματα ελέγχου ταυτότητας είναι τέτοιες που δεν παρέχουν πληροφορίες που μπορεί να εκμεταλλευτούν από κακόβουλους χρήστες.
4	8	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Ο οργανισμός χρησιμοποιεί port level access control, ακολουθόντας τα πρότυπα 802.1x, και ελέγχει ποιες συσκευές μπορούν να αυθεντικοποιούνται στο δίκτυο.
5	2	Το σύστημα για την αυθεντικοποίηση συνδέεται με τα δεδομένα της φυσικής λίστας πόρων (hardware asset inventory) ώστε να εξασφαλίζεται ότι μόνο εξουσιοδοτημένες συσκευές μπορούν να συνδεθούν στο δίκτυο.
5	3	Ανασκοπήσεις των καταγραφών (logs) που προκύπτουν από την λειτουργία των συστημάτων ελέγχου ταυτότητας γίνονται αυτόματα και ενημερώνεται το εξουσιοδοτημένο προσωπικό σε περίπτωση ανίχνευσης κάποιου κινδύνου ή τάσης.
5	4	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	5	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
IAM5		**Μέτρο:** Διαχείριση διαπιστευτηρίων **Στόχος Μέτρου:** Να διασφαλιστεί ασφαλής διαχείριση διαπιστευτηρίων για πρόσβαση σε εταιρικούς πόρους, και ότι επαληθεύεται η ταυτότητα των χρηστών με ασφάλεια για χρήση υπηρεσιών του οργανισμού. **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση διαδικασιών διαχείρισης διαπιστευτηρίων για να εξασφαλίζεται η κατάλληλη διαχείριση των μέσων ταυτοποίησης και επαλήθευσης με τα οποία οι χρήστες μπορούν να έχουν πρόσβαση σε οργανωτικούς πόρους. Ο οργανισμός θα πρέπει να εξετάσει τη χρήση ομαδοποιημένων διαπιστευτηρίων (π.χ. single sign-on) προκειμένου να βελτιώσει την εμπειρία του χρήστη σε θέματα ταυτοποίησης και πρόσβασης. Ο οργανισμός πρέπει να εξετάσει τη διαχείριση διαπιστευτηρίων για τους χρήστες, τα συστήματα και τα δίκτυα προκειμένου να διασφαλίσει τον έλεγχο της πρόσβασης καθ' όλη τη διάρκεια του κύκλου ζωής πληροφοριών, όπως ορίζεται στο μέτρο [DS1]. **Πηγή:**
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**
0	1	Δεν υπάρχει δομημένος / οργανωμένος τρόπος για την διαχείριση διαπιστευτηρίων για πρόσβαση σε πόρους, συστήματα και δίκτυα. Μπορεί ανά περίπτωση κάποια συστήματα να έχουν κωδικούς πρόσβασης αλλά δεν υπόκειται σε κάποια πολιτική.
1	1	Η πρόσβαση σε κρίσιμους πόρους προστατεύεται με χρήση διαπιστευτηρίων.
1	2	Τα διαπιστευτήρια είναι τουλάχιστον 8 χαρακτήρων για τους απλούς χρήστες και τουλάχιστον 14 για τους χρήστες προνομιακής πρόσβασης.

2	1	Η επιλογή των μηχανισμών αυθεντικοποίησης (επαλήθευσης της ταυτότητας των εξουσιοδοτημένων ατόμων) γίνεται ως αποτέλεσμα σχετικής διαδικασίας ανάλυσης διακινδύνευσης. (Διαφορετικής κρισιμότητας συστήματα μπορεί να απαιτούν διαφορετικού επιπέδου μέτρα επαλήθευσης ταυτότητας.)
2	2	Η ταυτότητα όλων των χρηστών, διεργασιών, πόρων επαληθεύεται ως προαπαιτούμενο για την παραχώρηση πρόσβασης.
3	1	Έχει δημιουργηθεί μια καταγεγραμμένη διαδικασία διαχείρισης διαπιστευτηρίων και εξασφαλίζεται η κατάλληλη διαχείριση των μέσων ταυτοποίησης και επαλήθευσης με τα οποία οι χρήστες έχουν πρόσβαση σε οργανωτικούς πόρους.
3	2	Οι απαιτήσεις προστασίας των διαπιστευτηρίων από τους χρήστες έχουν επικοινωνηθεί από τον οργανισμό σε όλο το εμπλεκόμενο προσωπικό.
3	3	Ειδικές ενέργειες διενεργούνται για τον έλεγχο της αποτελεσματικότητας της συγκεκριμένης επικοινωνίας.
3	4	Η συμμόρφωση των χρηστών με τις σχετικές οδηγίες και την πολιτική είναι υποχρεωτική.
3	5	Σε περίπτωση χρήσης κωδικών πρόσβασης, οι κωδικοί είναι πολύπλοκοι, αλλάζουν με κάποια περιοδικότητα, δεν χρησιμοποιούνται σε πολλαπλά συστήματα και αποθηκεύονται κρυπτογραφημένοι.
3	6	Το σύστημα προστατεύεται έναντι πολλαπλών προσπαθειών αποτυχημένης πρόσβασης.
4	1	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
4	2	Υλοποιήθηκε χρήση ομαδοποιημένων διαπιστευτηρίων (π.χ. single sign-on) προκειμένου να βελτιωθεί η εμπειρία του χρήστη σε θέματα ταυτοποίησης και πρόσβασης.
4	3	Υλοποιήθηκε ένα διαδραστικό σύστημα για την εξασφάλιση της αυτόματης συμμόρφωσης των διαπιστευτηρίων με την σχετική πολιτική.
4	4	Σε περίπτωση χρήσης MFA, προσδιορίζεται ο τύπος της μεθόδου αυθεντικοποίησης και η σχετική του ασφάλεια.
5	1	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	2	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
IAM6		**Μέτρο:** Ιχνηλασιμότητα και έλεγχος **Στόχος Μέτρου:** Να διασφαλιστεί η μη-άρνηση ανιχνευσιμότητας των ενεργειών των χρηστών που εκτελούνται στο πλαίσιο των οργανωτικών πόρων, ώστε να είναι δυνατή η ανίχνευση και η διερεύνηση εκούσιων ή ακούσιων δραστηριοτήτων που έχουν αρνητικό αντίκτυπο **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση μέτρων διαχείρισης ταυτότητας και πρόσβασης για τη διασφάλιση της χρονολογικής ιχνηλασιμότητας και της ικανότητας ελέγχου, ώστε να ανατίθεται ευθύνη στους χρήστες που εκτελούν εντολές σε συστήματα επεξεργασίας πληροφοριών. Ο φορέας εξετάζει μέτρα που διασφαλίζουν τη μη- άρνηση από χρήστες. Ο οργανισμός πρέπει να εξετάζει τη δυνατότητα ιχνηλασιμότητας και ελέγχου στο πλαίσιο της διαχείρισης ταυτότητας και πρόσβασης που ισχύει για τα συστήματα, τις εφαρμογές και τα δίκτυα. **Πηγή:**
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**
0	1	Δεν υπάρχει οργάνωση στην παρακολούθηση των ενεργειών των χρηστών. Τα συστήματα μπορεί ανά περίπτωση να δημιουργούν κάποιες εγγραφές παρακολούθησης ενεργειών αλλά δεν ορίζονται τα χαρακτηριστικά τους και δεν ελέγχονται χειροκίνητα ή αυτόματα.

1	1	Τα συστήματα δημιουργούν, ανά περίπτωση, κάποιες εγγραφές παρακολούθησης ενεργειών, μετά από σχετική παρέμβαση του εξουσιοδοτημένου ιδιοκτήτη πόρου (ή του authorized custodian - π.χ. IT) σε ad hoc βάση.
2	1	Έχει δημιουργηθεί μια καταγεγραμμένη πολιτική, η οποία ορίζει σε ποια συστήματα γίνεται παρακολούθηση και καταγραφή ενεργειών (logs).
2	2	Η έκταση της παρακολούθησης και καταγραφής ενεργειών προκύπτει από τα αποτελέσματα σχετικής ανάλυσης διακινδύνευσης που διενεργείται με ευθύνη των ιδιοκτητών πόρων.
2	3	Τα βασικά χαρακτηριστικά που καθορίζονται είναι: είδος καγραφής, χρονικό διάστημα διατήρησης, μέσο διατήρησης.
2	4	Καταγραφή ενεργειών που σχετίζονται με την ασφάλεια είναι ενεργοποιημένη κατ΄ελάχιστο στα κρίσιμα συστήματα.
3	1	Καταγραφή ενεργειών που σχετίζονται με την ασφάλεια είναι ενεργοποιημένη σε όλα τα συστήματα.
3	2	Οι εξωτερικές συνδέσεις παρακολουθούνται (logged) αυτόματα από κατάλληλο σύστημα.
3	3	Το σύστημα αυθεντικοποίησης καταγράφει τις επιτυχημένες και απότυχημένες προσπάθειες.
3	4	Στις σχετικές καταγραφές δεν φαίνεται το password ή άλλο μυστικό στοιχείο αυθεντικοποίησης που έχει χρησιμοποιηθεί / εισαχθεί σε κάθε περίπτωση προσπάθειας πρόσβασης.
4	1	Οι ενέργειες πρόσβασης καταγράφονται (logged) ανεξάρτητα του επιπέδου χρήστη.
4	2	Ελέγχονται σε τακτά χρονικά διαστήματα οι καταγραφές (logs) για την επιβεβαίωση της συμμόρφωσης με την πολιτική ελέγχου πρόσβασης και την ανίχνευση πιθανών απόκλίσεων. Όπου είναι δυνατό, η διαδικασίαυλοποιείται αυτόματα.
4	3	Για τους λογαριασμούς που έχουν προνομιακή πρόσβασης σε πόρους, συστήματα και δίκτυα, υλοποιείται παρακολούθηση (logging) και εξασφαλίζεται ότι οι σχετικές καταγραφές δεν μπορούν να τροποιηθούν, απενεργοποιηθούν, διαγραφούν ή αλλοιωθούν από τους λογαριασμούς αυτούς.
4	4	Το χρονικό διάστημα διατήρησης των σχετικών καταγραφών είναι τουλάχιστον για 3 μήνες ανά σύστημα. Σε περίπτωση που αυτό δεν είναι τεχνικά εφικτό, υπάρχει ένας μηχανισμός για την δημιουργία εξαίρεσης από την σχετική πολιτική.
4	5	Η έγκριση της εξαίρεσης ακολουθεί την διαδικασία ελέγχου αλλαγών.
4	6	Η αίτηση για εξαίρεση αναφέρει τους τρόπους με τους οποίους ο σχετικός κίνδυνος μειώνεται μέσω άλλων αντισταθμιστικών μέτρων.
4	7	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Κατάλληλα παραμετροποιημενα συστήματα intrusion detection/prevention και anomaly detection systems έχουν υλοποιηθεί.
5	2	Οι σχετικές καταγραφές διατηρούνται κατ' ελάχιστον ένα έτος.
5	3	Ειδικά κάποιες κατηγορίες (π.χ. χρήση λογαριασμών προνομιακής πρόσβασης σε κρίσιμα συστήματα)αρχειοθετούνται για μεγαλύτερο χρονικό διάστημα, λαμβάνοντας υπόψη και τις απαιτήσεις σχετικής νομοθεσίας όπου υπάρχει.
5	4	Η πρόσβαση στα συστήματα αυτά είναι ελεγχόμενη και περιορισμένη.
5	5	Τα δεδομένα καταγραφών χαρακτηρίζονται εμπιστευτικά σύμφωνα με το σχέση διαβάθμισης πληροφοριών του οργανισμού και χειρίζονται αντίστοιχα.
5	6	Αντίγραφα ασφαλείας των δεδομένων καταγραφών λαμβάνονται σύμφωνα με τις προδιαγραφές της σχετικής πολιτικής αντιγράφων ασφαλείας, της αξιολόγησης διακινδύνευσης και της κρισιμότητας του πόρου.
5	7	Ελέγχονται αυτόματα σε τακτά χρονικά διαστήματα οι καταγραφές (logs) για την επιβεβαίωση της συμμόρφωσης με την πολιτική ελέγχου πρόσβασης και την ανίχνευση πιθανών αποκλίσεων.
5	8	Κατάλληλοι συσχετισμοί / κανόνες και alerts έχουν υλοποιηθεί μέσα στα συστήματα για την έγκαιρη ενημέρωση του οργανισμού.

5	9	Η χρήση γενικών λογαριασμών προνομιακής πρόσβασης παρακολουθείται (logged) ενώ υπάρχει αυτόματο σύστημα το οποίο ενημερώνει το εξουσιοδοτημένο προσωπικό σχετικά με την χρήση του. Τέτοιες περιπτώσεις διαχειρίζονται ως πιθανά περιστατικά ασφαλείας και ενεργοποιείται η αντίστοιχη διαδικασία διαχείρισης περιστατικών ασφαλείας.
5	10	Ανασκοπήσεις των καταγραφών (logs) που προκύπτουν από την λειτουργία των συστημάτων ελέγχου ταυτότητας γίνονται αυτόματα και ενημερώνεται το εξουσιοδοτημένο προσωπικό σε περίπτωση ανίχνευσης κάποιου κινδύνου ή τάσης.
5	11	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	12	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
IAM7		**Μέτρο:** Διαχείριση του κύκλου ζωής της ταυτότητας **Στόχος Μέτρου:** Να διασφαλιστεί ότι οι ρόλοι και η έγκριση της ταυτότητας αντικατοπτρίζουν τον κύκλο ζωής της ταυτότητας του χρήστη. **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση επαρκών μέτρων διαχείρισης ταυτότητας και πρόσβασης καθ' όλη τη διάρκεια του κύκλου ζωής της ταυτότητας, που περιλαμβάνει μεταξύ άλλων, παροχή, επαλήθευση της ταυτότητας, έγκριση και αφαίρεση ταυτοτήτων. Οι έλεγχοι για τη διαχείριση του κύκλου ζωής της ταυτότητας θα πρέπει να ενσωματωθούν στις διαδικασίες ασφάλειας περί ανθρώπινων πόρων, όπως ορίζεται στο μέτρο [HRS1], προκειμένου να διασφαλιστεί ότι οι ρόλοι πρόσβασης ευθυγραμμίζονται με τον κύκλο ζωής της εργοδότησης των στελεχών μέσα στον οργανισμό. **Πηγή:**
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**
0	1	Δεν υπάρχει ένας οργανωμένος / δομημένος τρόπος με τον οποίο γίνεται η διαχείριση των χρηστών. Υπάρχουν ανά σύστημα λογαριασμοί πρόσβασης και εκχωρούνται σε χρήστες αλλά δεν υπάρχει κάποια βασική δομή, έλεγχος ή δυνατότητα επιβεβαίωσης για τους λογαριασμούς.
1	1	Η δημιουργία λογαριασμών και η παραχώρησης πρόσβασης σε πόρους του οργανισμού δίνεται μετά από σχετική έγκριση από εξουσιοδοτημένο υπεύθυνο.
1	2	Ο υπεύθυνος τηρεί λίστα με τους λογαριασμούς που έχουν δημιουργηθεί ανά σύστημα.
1	3	Αντίστοιχα σε περίπτωση αποχώρησης, γίνονται κατάλληλες ενέργειες κατάργησης / απενεργοποίησης λογαριασμών από το σχετικά εξουσιοδοτημένο προσωπικό.
2	1	Υπάρχει πολιτική / διαδικασία για την δημιουργία λογαριασμών και την διαχείριση της πρόσβασης σε πόρους του οργανισμού. (Η πολιτική / διαδικασία καλύπτει τόσο στην εγγραφή όσο και την απεγράφη λογαριασμών (registration and deregistration)).
2	2	Υπάρχει σαφής ιδιοκτήτης της πολιτικής και έχουν καθοριστεί τα βήματα που ακολουθούνται για την ενεργοποίηση λογαριασμών και πρόσβασης σε πόρους του οργανισμού.
2	3	Προκειμένου να αποδοθεί πρόσβαση στους πόρους, ακολουθείται διαδικασία έγκρισης από τον αναγνωρισμένο ιδιοκτήτη του πόρου.
2	4	Για κάθε σχετική με λογαριασμούς και δικαιώματα πρόσβασης κίνηση τηρείται η αντίστοιχη καταγραφή.
2	5	Τηρείται μια κεντρική λίστα με τους λογαριασμούς χρηστών στα συστήματα του οργανισμού.
2	6	Υπάρχει αντίστοιχα λίστα και με τα δικαιώματα των λογαριασμών.
3	1	Υπάρχει καταγεγραμμένη πολιτική / διαδικασία για την διαχείριση των λογαριασμών εντός των συστημάτων, των πόρων και των δικτύων.
3	2	Η πολιτική / διαδικασία περιέχει ενέργειες που γίνονται για την δημιουργία, τροποποίηση, ανασκόπηση, απενεργοποίηση και διαγραφή των λογαριασμών.
3	3	Η διαδικασία αναγνωρίζει συγκεκριμένους ρόλους εντός του οργανισμού που διενεργούν τις αντίστοιχες ενέργειες.

3	4	Σύμφωνα με τις απαιτήσεις και τον τρόπο λειτουργίας έχει καθοριστεί ένα σύνολο ρόλων, οι οποίοι στην συνέχεια έχουν συσχετιστεί με δικαιώματα πρόσβασης σε πόρους, συστήματα και δίκτυα.
3	5	Κατά τη διάρκεια της εγγραφής ενός νέου λογαριασμού, στην σχετική αίτηση περιλαμβάνεται: το είδος του λογαριασμού (απλός, προνομιακός, άλλες κατηγορίες σύμφωνα με τις ανάγκες του οργανισμού), ο ιδιοκτήτης του λογαριασμού, η ημερομηνία ενεργοποίησης, ο ρόλος, η διάρκεια (όπου εφαρμόζεται).
3	6	Οι λειτουργίες που αφορούν την διαχείριση λογαριασμών είναι ενσωματωμένες και ευθυγραμμισμένες με τις διαδικασίες ασφάλειας περί ανθρωπίνων πόρων όπως περιγράφονται στο HRS1, ώστε εξασφαλίζεται ότι οι ρόλοι πρόσβασης και οι λογαριασμοί είναι ευθυγραμμισμένοι με τον κύκλο ζωής της εργοδότηρηση των αντίστοιχων οντοτήτων (προσωπικό, εξωτερικοί συνεργάτες κλπ).
3	7	Κάθε φορά που γίνεται αλλαγή (υποβάθμιση, αναβάθμιση, μετακίνηση) ατόμου σε θέση εργασίας, ενεργοποιείται και αλλαγή / ανασκόπηση των δικαιωμάτων πρόσβασης.
3	8	Η ανασκόπηση των λογαριασμών χρηστών γίνεται τουλάχιστον ad-hoc και χειροκίνητα.
4	1	Οι λογαριασμοί που υπάρχουν στα διάφορα συστήματα ανασκοπούνται κατ' ελάχιστο μια φορά το τρίμηνο και μετά από μεγάλες αλλαγές.
4	2	Λογαριασμοί οι οποίοι είναι ανενεργοί για περισσότερες από 90 ημέρες απενεργοποιούνται.
4	3	Οι διαδικασίες για την απενεργοποίηση ή κατάργηση λογαριασμών είναι όσο γίνεται πιο αυτόματες.
4	4	Σε περίπτωση που αναγνωριστεί κάποια απόκλιση, καταγράφεται άμεσα και ενεργοποιείται η διαδικασία ανταπόκρισης σε περιστατικά ασφαλείας.
4	5	Όπου είναι δυνατό,οι λογαριασμοί απενεργοποιούνται μετά από αλλαγή των συνθηματικών πρόσβασης και αφαίρεσης των σχετικών δικαιωμάτων. Σε περίπτωση που αυτό δεν είναι εφικτό, διαγράφονται. (Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor. Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.)
4	6	Οι διαδικασίες της απόδοσης αλλά και της ανασκόπησης λογαριασμών και δικαιωμάτων αφορούν τόσο την λογική όσο και την φυσική πρόσβαση. Λογαριασμοί που ανήκαν ή είχαν αποδοθεί προηγούμενα, δεν εκχωρούνται σε άλλους χρήστες.
4	7	Για κάθε ενέργεια αλλαγής που σχετίζεται με τον κύκλο ζωής ενός λογαριασμού, τηρείται σχετικό ιστορικό και ακριβές timestamp.
4	8	Οι ενέργειες που διενεργούνται στα πλαίσια της διαχείρισης λογαριασμών, υλοποιούνται από ρόλους και άτομα που δεν θα έχουν σύγκρουση συμφερόντων.
4	9	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Η διαδικασία ανασκόπησης και διαχείρισης λογαριασμών είναι αυτοματοποιημένη και συνεχής.
5	2	Τηραούνται τα κατάλληλα τεχνικά μέτρα ώστε το σύνολο του κύκλου ζωής ενός λογαριασμού λειτουργεί με ελάχιστη ανθρώπινη παρέμβαση.
5	3	Τουλάχιστον μια φορά το τρίμηνο, διενεργείται τεχνική αξιολόγηση της απότελεσματικότητας λειτουργίας του αυτοματοποιημένου μηχανισμού διαχείρισης λογαριασμών.
5	4	Οι ενέργειες που διενεργούνται για τους σχετικούς ελέγχους, υλοποιούνται από ρόλους και άτομα που δεν έχουν σύγκρουση συμφερόντων.
5	5	Οι διαδικασίες αφορούν το σύνολο των συστημάτων, δικτύων, πόρων του οργανισμού.
5	6	Σε περίπτωση που δεν μπορεί να ενταχθεί κάποιο σύστημα, δίκτυο ή πόρος στην αυτόματη διαδικασία, υπάρχει μηχανισμός για την δημιουργία εξαίρεσης από την σχετική διαδικασία.
5	7	Η έγκριση της εξαίρεσης ακολουθεί την διαδικασία ελέγχου αλλαγών.
5	8	Η αίτηση για εξαίρεση αναφέρει τους τρόπους με τους οποίους ο σχετικός κίνδυνος μειώνεται μέσω άλλων αντισταθμιστικών μέτρων. .

5	9	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	10	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

Κατηγορία		ΔΙΑΧΕΙΡΙΣΗ ΕΥΠΑΘΕΙΩΝ ΚΑΙ ΕΝΗΜΕΡΩΣΕΩΝ ΑΣΦΑΛΕΙΑΣ
VM1		**Μέτρο:** Ανίχνευση και εντοπισμός ευπαθειών **Στόχος Μέτρου:** Να διασφαλιστεί ότι οι ευπάθειες συστημάτων είναι γνωστές στον οργανισμό, προκειμένου να τύχουν κατάλληλου χειρισμού. **Περιγραφή Μέτρου:** Κατάρτιση, εφαρμογή και διατήρηση σχεδίου και προσέγγισης βάσει του κινδύνου για τη δοκιμή εφαρμογών, συστημάτων και δικτύων για ευπάθειες και αδυναμίες, οι οποίες θα μπορούσαν να τύχουν εκμετάλλευσης από απειλές. Ο οργανισμός θα πρέπει να εξετάζει την ανίχνευση για τον εντοπισμό ευπαθειών που προκύπτουν από νέες ή τροποποιημένες διαδικασίες ή συστήματα στα πλαίσια επεξεργασίας πληροφοριών. Οι ευπάθειες πρέπει να ανιχνεύονται και να εντοπίζονται στο πλαίσιο των απειλών κατά της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών. Ο οργανισμός θα πρέπει να εξετάζει το ενδεχόμενο διενέργειας δοκιμών διείσδυσης, ως μέσο για την ανίχνευση και τον εντοπισμό ευπαθειών. Τα αποτελέσματα των προσπαθειών ανίχνευσης και εντοπισμού ευπαθειών θα πρέπει να καταγράφονται όπως περιγράφεται στο μέτρο [VM2]. **Πηγή:**
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**
0	1	Ο οργανισμός δεν υλοποιεί καμία ενέργεια για την ανίχνευση και εντοπισμό ευπαθειών.
1	1	Υλοποιούνται διορθωτικές ενέργειες έναντι ευπαθειών με reactive και τουλάχιστον ad-hoc τρόπο και συνήθως όχι πρωτοβουλία του οργανισμού (π.χ. εφαρμογή αυτοματοποιημένων security updates).
2	1	Έχουν ενεργοποιηθεί μηχανισμοί και δημιουργηθεί επαφές για την λήψη έγκαιρης πληροφόρησης για την ανίχνευσης και εντοπισμό των ευπαθειών στα κρίσιμα συστήματα.
3	1	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται σχέδιο και προσέγγιση βάσει του κινδύνου για τη δοκιμή εφαρμογών, συστημάτων και δικτύων για ευπάθειες και αδυναμίες, οι οποίες μπορούν να τύχουν εκμετάλλευσης από απειλές.
3	2	Εξετάζεται η ανίχνευση για τον εντοπισμό ευπαθειών που προκύπτουν από νέες ή τροποποιημένες διαδικασίες ή συστήματα στα πλαίσια επεξεργασίας πληροφοριών.
3	3	Οι ευπάθειες ανιχνεύονται και εντοπίζονται στο πλαίσιο των απειλών κατά της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών.
3	4	Τα αποτελέσματα των προσπαθειών ανίχνευσης και εντοπισμού ευπαθειών καταγράφονται όπως περιγράφεται στο μέτρο [VM2].
4	1	Έχουν υοθετηθεί αυτοματοποιημένες μεθόδοι και εργαλεία για την ανίχνευση και εντοπισμό ευπαθειών.
4	2	Η ανίχνευση και εντοπισμός ευπαθειών στο εσωτερικό του οργανισμού γίνεται τουλάχιστον ανά τρίμηνο, είναι authenticated ή και unauthenticated ενώ τα εργαλεία είναι συμβατά με διεθνείς βέλτιστες πρακτικές όπως είναι το SCAP.
4	3	Η ανίχνευση και εντοπισμός ευπαθειών στα συστήματα του οργανισμού που είναι εκτεθειμένα εξωτερικά, διενεργούνται τουλάχιστον μια φορά το μήνα, ενώ τα εργαλεία είναι συμβατά με διεθνείς βέλτιστες πρακτικές όπως είναι το SCAP.
4	4	Η καταγραφή των ευπαθειών γίνεται σύμφωνα με το [VM2] ενώ η αντιμετώπισή τους γίνεται σύμφωνα με το [VM3].
4	5	Ο οργανισμός έχει εγγραφεί σε υπηρεσίες διαμοιρασμού πληροφοριών σχετικά με τις ευπάθειες προκειμένου να παραμένει ενήμερος για νέα θέματα. Πληροφορίες οι οποίες έχουν ληφθεί με αυτόν τον τρόπο, χρησιμοποιούνται για τον καλύτερο σχεδιασμό και λειτουργία της διαδικασίας και των μηχανισμών ανίχνευσης και εντοπισμού ευπαθειών.
4	6	Τα στοιχεία ευπαθειών αποτελούν εισερχόμενο στην διαδικασία της διαχείρισης κινδύνων.
4	7	Χρησιμοποιούνται έγκυρες πηγές αναγνώρισης ευπαθειών προκειμένου να υπάρχει πρόσβαση σε στοιχεία επαλήθευσης και κατηγοριοποίησης.

4	8	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Ο οργανισμός συμμετέχει και λαμβάνει έγκυρες πληροφορίες Cyber threat intelligence οι οποίες μεταξύ άλλων χρησιμοποιούνται για την επικαιροποίηση του καταλόγου απειλών, ευπαθειών και κινδύνων στους οποίους είναι εκτεθειμένος ο οργανισμός σύμφωνα με το [RM3] και το [VM2].
5	2	Διενεργείται από εξωτερικό ανεξάρτητο μέρος αξιολόγηση ευπαθειών (vulnerability assessment) σε τακτά χρονικά διαστήματα, καλύπτοντας όλα τα κρίσιμα συστήματα του οργανισμού σύμφωνα με την σχετική ανάλυση κρισιμότητας όπως προβλέπεται στο [DS2].
5	3	Διενεργούνται δοκιμές διείσδυσης, ως μέσο για την ανίχνευση και τον εντοπισμό ευπαθειών.
5	4	Τα δεδομένα των vulnerability assessments χρησιμοποιούνται ως σημείο εκκίνησης για την καλύτερη στόχευση των ενεργειών παρείσδυσης.
5	5	Οι δοκιμές παρείσδυσης διενεργούνται εσωτερικά, κατ΄ ελάχιστο μια φορά το χρόνο, σύμφωνα με τον σχετικό σχεδιασμό. Τέτοιου είδους δοκιμές μπορεί να είναι white box ή grey box.
5	6	Λαμβάνοντας υπόψη το πλαίσιο λειτουργίας του οργανισμού, τους στόχους ασφαλείας, την στρατηγική ασφαλείας, τις νομοθετικές, κανονιστικές και συμβατικές απαιτήσεις, καταρτίζεται οργανωμένο σχέδιο (πρόγραμμα) δοκιμών παρείσδυσης.
5	7	Το σχέδιο περιλαμβάνει το πεδίο εφαρμογής των δοκιμών (π.χ. δικτύου, web applications, APIs, hosted υπηρεσίες, μέτρα φυσικής πρόσβασης κα.), τους περιορισμούς (π.χ. τις ώρες που μπορεί να διενεργηθεί, το προσωπικό που πρέπει να ενημερωθεί κ.α), τα είδη των δοκιμών που θα διενεργηθούν και τις σχετικές μεθοδολογίες και πρότυπα, την συχνότητα διενέργειας, τον στόχο, τους ρόλους και αρμοδιότητες, το είδος της τεκμηρίωσης που θα διατηρηθεί και θα παραδοθεί στον οργανισμό, τα σημεία επαφής και ένα πλάνο άμεσων ενεργειών σε περίπτωση ευρήματος.
5	8	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	9	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
VM2		**Μέτρο:** Καταγραφή και αναφορά ευπαθειών **Στόχος Μέτρου:** Να διασφαλιστεί ότι οι ευπάθειες καταγράφονται και υποβάλλονται σε σχετικές εκθέσεις, ώστε να είναι δυνατή η λήψη τεκμηριωμένων αποφάσεων από τη διοίκηση όσον αφορά τον χειρισμό τους. **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση διαδικασιών για την καταγραφή και την αναφορά των ευπαθειών που έχουν εντοπιστεί, ώστε να είναι δυνατή η αποκατάσταση και η ενημέρωση συστημάτων και διαδικασιών για τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών. Η καταγραφή ευπαθειών και η υποβολή σχετικών εκθέσεων θα πρέπει να είναι το αποτέλεσμα των προσπαθειών ανίχνευσης και εντοπισμού ευπαθειών, όπως περιγράφεται στο μέτρο [VM1]. Ο οργανισμός πρέπει να εξετάζει το ενδεχόμενο συμπερίληψης στοιχείων για ευπάθειες υψηλού κινδύνου σε γενικές εκθέσεις προς τη διοίκηση, ώστε να εξασφαλίζεται η εκ των άνω προς τα κάτω επίγνωση των ευπαθειών με δυνητικές επιπτώσεις και να προσδιορίζονται τα κατάλληλα μέτρα για την αποκατάσταση και την εφαρμογή διορθωτικών συστημάτων και διαδικασιών, όπως περιγράφεται στο μέτρο [VM3]. **Πηγή:**
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**
0	1	Ο οργανισμός δεν υλοποιεί καμία ενέργεια για την ανίχνευση, εντοπισμό, καταγραφή και αναφορά ευπαθειών.
1	1	Υλοποιούνται διορθωτικές ενέργειες έναντι ευπαθειών με reactive και τουλάχιστον ad-hoc τρόπο και συνήθως όχι με δική του πρωτοβουλία (π.χ. εφαρμογή αυτοματοποιημένων security updates), και χωρίς κάποια συγκεκριμένη καταγραφή.

2	1	Έχουν ενεργοποιηθεί μηχανισμοί και δημιουργήθεί επαφές για την λήψη έγκαιρης πληροφόρησης για την ανίχνευση και εντοπισμό των ευπαθειών στα κρίσιμα συστήματα.
2	2	Τα στοιχεία των ευπαθειών καταγράφονται σε σχετικά αρχεία και επικοινωνούνται εσωτερικά στον οργανισμό.
3	1	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται διαδικασία για την καταγραφή και την αναφορά των ευπαθειών που έχουν εντοπιστεί, ώστε να είναι δυνατή η αποκατάσταση και η ενημέρωση συστημάτων και διαδικασιών για τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών.
3	2	Η καταγραφή ευπαθειών και η υποβολή σχετικών εκθέσεων είναι το αποτέλεσμα των προσπαθειών ανίχνευσης και εντοπισμού ευπαθειών, όπως περιγράφεται στο μέτρο [VM1].
3	3	Εξετάζεται το ενδεχόμενο συμπερίληψης στοιχείων για ευπάθειες υψηλού κινδύνου σε γενικές εκθέσεις προς τη διοίκηση, ώστε να εξασφαλίζεται η εκ των άνω προς τα κάτω επίγνωση των ευπαθειών με δυνητικές επιπτώσεις και να προσδιορίζονται τα κατάλληλα μέτρα για την αποκατάσταση και την εφαρμογή διορθωτικών συστημάτων και διαδικασιών, όπως περιγράφεται στο μέτρο [VM3].
3	4	Καταγράφονται οι σχετικές ευπάθειες στον κατάλογο απειλών, ευπαθειών και κινδύνων όπως αναφέρεται στο [RM3].
3	5	Αξιολογείται το επίπεδο της ευπάθειας λαμβάνοντας υπόψη την δυνατότητα εκμετάλλευσης (exploitability) την πιθανή επίπτωση της ευπάθειας ανά περίπτωση και ανά κατηγορία στοιχείων ενεργητικού (λαμβάνοντας υπόψη και τα σχετικά μέτρα π.χ. μέτρα σε επίπεδο δικτύου, μέτρα σε επίπεδο στοιχείου ενεργητικού κ.α.).
4	1	Όταν τα εμπλεκόμενα μέρη αναγνωρίσουν ότι αδυναμίες, απειλές ή κίνδυνοι δεν είναι πλέον εφαρμόσιμοι, ο σχετικός κατάλογος επικαιροποιείται υποδεικνύοντας ότι η αντίστοιχη εγγραφή δεν είναι πλέον ενεργή. (Η ιστορικότητα αναγνώρισης διατηρείται και τεκμηριώνεται). Η ενημέρωση των στοιχείων μπορεί να προκύψει από διαφορετικές πηγές όπως αναφέρονται στα [RM3], [VM1].
4	2	Χρησιμοποιούνται έγκυρες πηγές αναγνώρισης ευπαθειών προκειμένου να υπάρχει πρόσβαση σε στοιχεία επαλήθευσης και κατηγοριοποίησης.
4	3	Η κατηγοριοποίηση των ευπαθειών γίνεται σύμφωνα με τις διεθνείς βέλτιστες πρακτικές (π.χ. CVSS).
4	4	Στον κατάλογο ευπαθειών καταγράφονται κατ΄ ελάχιστο ο πόρος ενεργητικού, η ευπάθεια, η απειλή (ή απειλές) που μπορεί να εκμεταλλευτούν την συγκεκριμένη ευπάθεια, ο κίνδυνος που θα δημιουργηθεί, η δυνατότητα εκμετάλλευσης, καθώς και το μέγεθος της ευπάθειας.
4	5	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Χρησιμοποιούνται διεθνείς βέλτιστες πρακτικές και εργαλεία (π.χ. Structured Threat Information Expression (STIX™) και εργαλεία όπως είναι το MISP Threat Sharing Platform) για την δομημένη καταγραφή στοιχείων threat intelligence και την δομημένη υποδοχή ή αποστολή της σχετικής πληροφορίας.
5	2	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	3	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

VM3	**Μέτρο:** Αποκατάσταση ευπαθειών και ενημερώσεις ασφάλειας **Στόχος Μέτρου:** Να εξασφαλιστεί η αποκατάσταση των ευπαθειών συστημάτων και η εφαρμογή ενημερώσεων ασφαλείας, κατόπιν απόφασης της διοίκησης **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση διαδικασιών για την αποκατάσταση ευπαθειών και την εισαγωγή ενημερώσεων ασφάλειας για ευπάθειες που εντοπίζονται σε συστήματα, εφαρμογές και στοιχεία δικτύου, και τα οποία απαιτούν μετριασμό ως αποτέλεσμα της αξιολόγησης της διοίκησης. Η αποκατάσταση ευπαθειών και οι ενημερώσεις ασφάλειας πρέπει να είναι το αποτέλεσμα απόφασης της διοίκησης με βάση την καταγραφή ευπαθειών και την υποβολή σχετικών εκθέσεων, όπως περιγράφεται στο μέτρο [VM2]. **Πηγή:** C2M2 (THREAT, ASSET), NIST 800-53 (SA-22), ISO 27001, ISO 27002

Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν υλοποιεί καμία ενέργεια για την αποκατάσταση ευπαθειών.
1	1	Υλοποιούνται διορθωτικές ενέργειες έναντι ευπαθειών με reactive και τουλάχιστον ad-hoc τρόπο και συνήθως όχι με δική του πρωτοβουλία (π.χ. εφαρμογή αυτοματοποιημένων security updates), και χωρίς κάποια συγκεκριμένη καταγραφή.
2	1	Έχουν ενεργοποιηθεί ή εφαρμόζονται πολιτικές για την αποκατάσταση ευπαθειών μόνο στα κρίσιμα συστήματα.
2	2	Δεν γίνεται αυτόματη εγκατάσταση ενημερώσεων. Εξουσιοδοτημένο προσωπικό, ελέγχει πρώτα τις ενημερώσεις και στην συνέχεια διενεργεί τις σχετικές εγκαταστάσεις.
3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται διαδικασίες για την αποκατάσταση ευπαθειών και την εισαγωγή ενημερώσεων ασφάλειας για ευπάθειες που εντοπίζονται σε συστήματα, εφαρμογές και στοιχεία δικτύου, και τα οποία απαιτούν μετριασμό ως αποτέλεσμα της αξιολόγησης της διοίκησης.
3	2	Η αποκατάσταση ευπαθειών και οι ενημερώσεις ασφάλειας είναι το αποτέλεσμα απόφασης της διοίκησης με βάση την καταγραφή ευπαθειών και την υποβολή σχετικών εκθέσεων, όπως περιγράφεται στο μέτρο [VM2].
3	3	Η εφαρμογή ενεργειών για την αποκατάσταση ευπαθειών ακολουθεί την διαδικασία διαχείρισης αλλαγών όπως αναφέρεται στο [CM1].
3	4	Στα πλαίσια των σχετικών διαδικασιών έχει προσδιοριστεί ο τρόπος ανταπόκρισης του οργανισμού σε ευπάθειες συγκεκριμένης κρισιμότητας ανά κατηγορία στοιχείων όπως αυτά αποτυπώνονται στον ενιαίο κατάλογο στοιχείων ενεργητικού [DS2].
3	5	Ο τρόπος αποκατάστασης αναφέρεται στο είδος των ενεργειών που γίνονται αυτόματα, χωρίς κάποια δοκιμή αλλά και στο είδος των ενεργειών που γίνονται αφού έχουν δοκιμαστεί. (Ειδικά για κρίσιμα συστήματα, σε κάθε περίπτωση η εισαγωγή κάποιας ενημέρωσης γίνεται αφού έχει υλοποιηθεί η εγκατάσταση σε δοκιμαστικό / παρόμοιο σύστημα χαμηλού κινδύνου).
3	6	Η σχετική διαδικασία έχει την έγκριση της διοίκησης
3	7	Η διαδικασία παρακολούθησης σε αυτές τις περιπτώσεις ακολουθεί την διαδικασία διαχείρισης αλλαγών [CM1].
4	1	Εφαρμόζονται οι τεχνικές που αναφέρονται στο [VM1] και [VM2] για την ανίχνευση, εντοπισμό και καταγραφή των ευπαθειών.
4	2	Τηρείται σύστημα μέσα από το οποίο ελέγχεται η κατάσταση των διαφόρων στοιχείων ενεργητικού έναντι στις εντοπισμένες ευπάθειες και κατά πόσο έχουν ενσωματωθεί οι τελευταίες ενημερώσεις ασφαλείας.
4	3	Σε περίπτωση που υπάρχουν νέες εκδόσεις προγραμμάτων ή άλλων στοιχείων,εκκινούνται δραστηριότητες για την αξιολόγηση του κόστους / οφέλους της μετάβασης στην νέα έκδοση.
4	4	Ο οργανισμός κατά κανόνα φροντίζει να βρίσκεται στην τελευταία δοκιμασμένη και σταθερή έκδοση των προγραμμάτων που χρησιμοποιεί.

4	5	Λογισμικό ή εξοπλισμός για το οποίο έχει παρέλθει ο κύκλος ζωής του (after end of life) δεν επιτρέπεται εντός του οργανισμού. Σε περίπτωση που δεν γίνεται διαφορετικά, η συγκεκριμένη περίπτωση αναγνωρίζεται ως κίνδυνος και σχεδιάζονται κατάλληλα αντισταθμιστικά μέτρα για την αντιμετώπιση του σχετικού κινδύνου ακολουθώντας τις προδιαγραφές των [RM1-6].
4	6	Όλες οι αναγνωρισμένες ευπάθειες με υψηλή βαθμολογία κρισιμότητας ακολουθούν και καταγράφονται σύμφωνα με την διαδικασία διαχείρισης αλλαγών [CM1].
4	7	Υλοποιούνται λύσεις antimalware με δυνατότητες αναγνώρισης αδυναμιών και φίλτρα anti-exploitation.
4	8	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Μετά την εφαρμογή των μέτρων για την αντιμετώπιση μιας ευπάθειας (μέτρα μπορεί να είναι μια ενημέρωση αλλά ανάλογα με τις ιδιαιτερότητες της ευπάθειας μπορεί να είναι και άλλες ενέργειες διαφορετικής φύσης), ελέγχεται η αποτελεσματικότητα της υλοποίησης των ενεργειών έναντι της ευπάθειας / απειλής.
5	2	Οι τρόποι για την αξιολόγηση της αποτελεσματικότητας αναφέρονται στην καταγραφή της διαχείρισης αλλαγής και μπορεί να είναι διαφορετικών τύπων περιλαμβανομένων δοκιμών, αναλύσεων, advanced threat hunting, active defense κ.α.
5	3	Σε περίπτωση που τα αποτελέσματα της αξιολόγησης της αποτελεσματικότητας είναι αρνητικά, γίνονται κατάλληλες διορθωτικές ενέργειες.
5	4	Οι απαιτήσεις αφορούν λογισμικό τρίτων, ανοικτό λογισμικό ή και λογισμικό που έχει αναπτυχθεί από τον ίδιο τον οργανισμό. Για το τελευταίο ισχύουν και τα στοιχεία του [AS1].
5	5	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	6	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

Κατηγορία		ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΟΥ
NS1		**Μέτρο:** Ασφάλεια Περιμέτρου **Στόχος Μέτρου:** Να διασφαλιστεί ότι η διεπαφή του τοπικού δικτύου με το εξωτερικό δίκτυο προστατεύεται από επιθέσεις, απειλές και άλλες εκούσιες ή ακούσιες ενέργειες με δυνητικά αρνητικές επιπτώσεις. **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση κατάλληλων μέτρων ασφάλειας δικτύου με σκοπό την προστασία της περιμέτρου του δικτύου από εξωτερικές απειλές και τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών που βρίσκονται στο εσωτερικό δίκτυο. Ο οργανισμός θα πρέπει να λαμβάνει υπόψη ότι η ασφάλεια περιμέτρου αποτελεί ένα μόνο συγκεκριμένο επίπεδο σε μια πολυεπίπεδη αρχιτεκτονική άμυνας. Για την προστασία από επιθέσεις στο δίκτυο, ο οργανισμός λαμβάνει υπόψη τις ειδικές για τον οργανισμό, απειλές και τις ειδικές για τον τομέα, απειλές και κινδύνους για το δίκτυο. Ο οργανισμός λαμβάνει υπόψη τα τείχη προστασίας και τα συστήματα ανίχνευσης και πρόληψης εισβολής, όπως περιγράφονται στο μέτρο [NS7]. Ο οργανισμός λαμβάνει εύλογα μέτρα για να διασφαλίσει ότι η κίνηση δεδομένων φιλτράρεται με βάση τις πολιτικές ασφάλειας του οργανισμού. **Πηγή:** C2M2, NIST 800-53, CIS, ISO 27002
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**
0	1	Ο οργανισμός δεν εφαρμόζει καθόλου μέτρα για την προστασία της (λογικής) περιμέτρου του οργανισμού.
1	1	Υπάρχει ένας firewall ο οποίος λειτουργεί ως σημείο διεπαφής ανάμεσα στο τοπικό δίκτυο και το εξωτερικό δίκτυο.
1	2	Οι ρυθμίσεις του συγκεκριμένου firewall είναι στοιχειώδεις ή δεν υπάρχει τακτικός και ουσιαστικός έλεγχος και διαχείριση.
2	1	Έχει σχεδιαστεί και υλοποιηθεί μια αρχιτεκτονική δικτύου για την εξασφάλιση του επιθυμητού επιπέδου ασφαλείας δικτύου λαμβάνοντας υπόψη τις πρακτικές και τα μέτρα που αναφέρονται στα [NS2] – [NS7].
2	2	Έχει αποτυπωθεί η αρχιτεκτονική σε διάγραμμα δικτύου, και παρέχει ικανή πληροφορία σχετικά με την διασύνδεση, τον τρόπο λειτουργίας και τα διάφορα επίπεδα προστασίας.
2	3	Έχει αναγνωρισθεί ο εξοπλισμός που εκτελεί δραστηριότητες ασφάλειας σε κάθε επίπεδο.
2	4	Για τον εξοπλισμό που βρίσκεται στην περίμετρο, έχουν εφαρμοστεί πολιτικές και κανόνες ασφαλείας υιοθετώντας αρνητική λογική (όλα κλειστά και ανοίγονται μόνο αν απαιτείται), λογική των ελάχιστων υπηρεσιών (υπηρεσίες που δεν χρειάζονται (περιττές) είναι απενεργοποιημένες), ελεγχόμενη πρόσβαση (σύμφωνα με το [IAM1] και παρακολούθηση των ενεργειών (και τήρηση αρχείων καταγραφής) σύμφωνα με το [IAM2].
2	5	Κατ' ελάχιστο είναι απενεργοποιημένα τα : α) η εισερχόμενη από και εξερχόμενη προς το εξωτερικό δίκτυο επικοινωνία στις παρακάτω θύρες: TCP 445 (SMB), UDP 137 (NetBIOS Name Resolution), UDP 138 (NetBIOS Datagram Service) και TCP 139 (NetBIOS Session Service), β) οι εισερχόμενες SMB συνδέσεις στην TCP θύρα 445 σε όσα στοιχεία δεν φιλοξενούν κοινόχρηστο περιεχόμενο (shares), γ)οι εκδόσεις SMBv1 και v2 στο εσωτερικό δίκτυο,
2	6	Αλλαγές που διενεργούνται στον εξοπλισμό που βρίσκονται στην περίμετρο ακολουθούν την διαδικασία διαχείρισης αλλαγών σύμφωνα με το [CM1].
2	7	Έχουν υλοποιηθεί host-based firewalls ή port filtering tools τα οποία έχουν είτε explicit είτε implicit κανόνα που κάνει drop όλη την κίνηση με εξαίρεση τις υπηρεσίες, τα πρωτόκολλα και τις θύρες που είναι ειδικώς (explicitly) εξουσιοδοτημένα.
3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται μέτρα ασφάλειας δικτύου με σκοπό την προστασία της περιμέτρου του δικτύου από εξωτερικές απειλές και τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών που βρίσκονται στο εσωτερικό δίκτυο.

3	2	Έχει υλοποιήσει μια πολυεπίπεδη αρχιτεκτονική άμυνας, στην οποία ασφάλεια περιμέτρου αποτελεί ένα μόνο συγκεκριμένο επίπεδο.
3	3	Κατά τον σχεδιασμό των κανόνων και των μηχανισμών ασφαλείας που έχουν υιοθετηθεί έχουν ληφθεί υπόψη τα αποτελέσματα της αξιολόγησης κινδύνου καθώς και τις ειδικές για τον οργανισμό, απειλές και τις ειδικές για τον τομέα, απειλές και κινδύνους για το δίκτυο.
3	4	Έχει ορισθεί ένα σύνολο πολιτικών ασφαλείας για την εξασφάλιση ότι η κίνηση φιλτράρεται σε επιθυμητό επίπεδο.
3	5	Υλοποιείται διαχωρισμός δικτύων όπως προβλέπεται στο [NS2]. Σε κάθε περίπτωση στοιχεία τα οποία χρειάζεται να είναι προσβάσιμα από το εξωτερικό δίκτυο, είναι διαχωρισμένα από το εσωτερικό δίκτυο.
3	6	Οι συνδέσεις σε εξωτερικά δίκτυα ή συστήματα γίνονται μόνο από τις διαχειριζόμενες διεπαφές των στοιχείων που έχουν αναγνωριστεί στην λογική περίμετρο (σύμφωνα με την υλοποιημένη αρχιτεκτονική).
3	7	Στα switches είναι ενεργοποιημένη η υπηρεσία port security, ενώ οι θύρες που δεν χρησιμοποιούνται είναι απενεργοποιημένες.
3	8	Στους routers τα interfaces και τα πρωτόκολλα δρομολόγησης είναι απενεργοποιημένα.
3	9	Για την πρόσβαση στο διαχειριστικό περιβάλλον των στοιχείων που απαρτίζουν την περίμετρο χρησιμοποιείται MFA.
3	10	Πρωτόκολλα όπως SMB, SNTP και άλλα τα οποία μπορούν να χρησιμοποιηθούν για την μεταφορά στοιχείων, μηνυμάτων και καταστάσεων χρησιμοποιούνται μόνο αν απαιτείται και μετά από κατάλληλη ανάλυση και παραμετροποίηση. Σχετικά στοιχεία διατηρούνται μέσα από την διαδικασία ελέγχου αλλαγών.
3	11	Έχει καταγραφεί και εφαρμόζει μια πολιτική ασφάλειας δικτύων που περιέχει κατ' ελάχιστο ρόλους και αρμοδιότητες, βασικές αρχές που διέπουν τον σχεδιασμό της αρχιτεκτονικής δικτύου του οργανισμού, βασικές διαδικασίες που σχετίζονται με την διαχείρισης δικτύου, τα σχετικά αρχεία που τηρούνται, τα αρχεία καταγραφής και το χρονικό διάστημα διατήρησής τους και τα μέτρα ασφαλείας που εφαρμόζονται.
3	12	Έχει αποτυπωθεί η αρχιτεκτονική σε διάγραμμα δικτύου, και παρέχει αναλυτική πληροφορία σχετικά τα διάφορα επίπεδα της αρχιτεκτονικής, τα στοιχεία που αποτελούν το κάθε επίπεδο, τα βασικά χαρακτηριστικά τους, πιθανά μοναδικά σημεία αστοχίας, τα σημεία στα οποία είναι ενεργοποιημένη η παρακολούθηση.
3	13	Τα διαγράμματα διαχειρίζονται ως πληροφορία του υψηλότερου επιπέδου διαβάθμισης πληροφοριών (όπως αναφέρεται στο [DS2]).
3	14	Εφεδρικά αντίγραφα ασφαλείας λαμβάνονται για τα αρχεία διαμόρφωσης (configuration files) των εν λόγω στοιχείων σύμφωνα με την σχετική πολιτική του οργανισμού και έκτακτα πριν από κάθε αλλαγή. Το ιστορικό των αντιγράφων διατηρείται.
3	15	Το σύνολο της δικτυακής κυκλοφορίας από και προς το διαδίκτυο περνά από αυθεντικοποιημένο διακομιστή μεσολάβησης επιπέδου εφαρμογής (application layer (web) proxy server), ο οποίος έχει ρυθμιστεί να απαγορεύει μη εξουσιοδοτημένες συνδέσεις.
3	16	Για την πρόσβαση από απόσταση, χρησιμοποιείται VPN (Virtual Private Network) και η σύνδεση γίνεται σε υποδομή AAA (Authentication, Authorization and Accounting) του οργανισμού. (Είναι υποχρεωτική η αυθεντικοποίηση του χρήστη στο κατάλληλο σημείο για την πρόσβαση σε άλλα στοιχεία εντός του οργανισμού).
4	1	Η απομακρυσμένη πρόσβαση χρηστών στο εσωτερικό δίκτυο του γίνεται μέσω VPN (Virtual Private Network), με χρήση αυθεντικοποίησης δύο παραγόντων (2-factor authentication) και των πιο πρόσφατων αλγόριθμων κρυπτογράφησης.
4	2	Οι εργασίες του διαχειριστικού προσωπικού πληροφορικής (administrative tasks) διενεργούνται από στοιχεία που χρησιμοποιούνται αποκλειστικά για αυτό το σκοπό. Κατάλληλα μέτρα για τον διαχωρισμό τους εφαρμόζονται σύμφωνα με το [NS2].
4	3	Υλοποιείται Host-based Intrusion Detection σύμφωνα με τις προδιαγραφές του [NS7].

4	4	Σε όλες τα στοιχεία τα οποία χρησιμοποιούνται εντός του οργανισμού για την προστασία της περιμέτρου αλλά και των άλλων επιπέδων της αρχιτεκτονικής ασφαλείας, εφαρμόζεται παρακολούθηση και καταγραφή σύμφωνα με τα αναγραφόμενα του [AM3]. Ακολούθως γίνεται συλλογή των στοιχείων και ανταπόκριση όπως απαιτείται σύμφωνα με το [AM3] και το [EIM1].
4	5	Είναι ενεργοποιημένη η παρακολούθηση ανάμεσα σε διαφορετικά τμήματα του δικτύου (segments) όπως απαιτείται.
4	6	Σε κάθε σταθμό εργασίας (end-point) αλλά και κάθε άλλο στοιχείου (όπου είναι αυτό δυνατό) είναι ενεργοποιημένο ή υλοποιημένο firewall το οποίο να εμποδίζει κάθε δικτυακή σύνδεση από και προς τη συσκευή με εξαίρεση τις θύρες και υπηρεσίες που απαιτούνται με βάση τις επιχειρησιακές ανάγκες.
4	7	Έχουν υλοποιηθεί σχετικές παραμετροποιήσεις ώστε να αναγνωρίζονται TCP sessions τα οποία διαρκούν ασυνήθιστα μεγάλα χρονικά διαστήματα.
4	8	Οι proxy servers παρακολουθούν και καταγράφουν τα TCP sessions και είναι παραμετροποιημένα ώστε να φιλτράρουν και να εμποδίζουν την πρόσβαση σε συγκεκριμένα URLs, domains, IPs σύμφωνα με τους κανόνες του οργανισμού και τον σχετικό κίνδυνο.
4	9	Έχει προσδιοριστεί ένα μέγιστο χρονικό διάστημα σύνδεσης ανά session και έχουν εφαρμοστεί οι κατάλληλοι τεχνικοί κανόνες και εργαλεία ώστε να τερματίζονται οι συνδέσεις είτε όταν έχει παρέλθει εκείνη η διάρκεια είτε μετά από συγκεκριμένο χρονικό διάστημα αδράνειας. (Η διάρκεια μπορεί να μεταβάλλεται με βάση της κρισιμότητα της πληροφορίας και άλλες συνθήκες).
4	10	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Εφαρμόζονται αρχές Zero trust αρχιτεκτονικής δικτύου σύμφωνα με διεθνείς βέλτιστες πρακτικές (π.χ. NIST 800-207).
5	2	Κατ΄ελάχιστο ικανοποιούνται οι ακόλουθες αρχές: α) Όλα τα δεδομένα και τα συστήματα αποτελούν στοιχεία (πόρους) του οργανισμού, β) Όλες οι επικοινωνίες προστατεύονται ανεξάρτητα από την τοποθεσία δικτύου στην οποία βρίσκονται, γ) Πρόσβαση σε στοιχεία του οργανισμού δίνεται μόνο αν αυστηρά χρειάζεται και σε per-session βάση, δ) Η πρόσβαση στα στοιχεία καθορίζεται από μια δυναμική πολιτική που μπορεί να καθορίζεται από διάφορες παραμέτρους περιλαμβανομένων συμπεριφοράς και περιβαλλοντικούς, ε) Τα μετρά για την ακεραιότητα και την επίδοση / επίπεδο ασφάλειας των στοιχείων παρακολουθούνται, ζ) εφαρμόζονται δυναμικές αυθεντικοποίησης και εξουσιοδότησης, πριν δοθεί η πρόσβαση, η) συλλέγεται όση περισσότερη πληροφορία γίνεται για την τρέχουσα κατάσταση των στοιχείων, της υποδομής δικτύων και των επικοινωνιών και χρησιμοποιείται αυτή η πληροφόρηση για βελτιώση του επιπέδου ασφάλειας.
5	3	Εφαρμόζονται δικτυακά συστήματα ανίχνευσης και πρόληψης εισβολών (network intrusion detection / prevention systems) για την ανίχνευση και πρόληψη επιθέσεων σε κάθε τμήμα / υποδίκτυο του Οργανισμού (π.χ. Network Intrusion Detection System (NIDS) ή αντίστοιχα cloud service provider (CSP) service με τις κατάλληλες εγγυήσεις.)
5	4	Υλοποιείται δίοδος δεδομένων (data diode) σε μορφή hardware, που επιβάλλει τη ροή δεδομένων μόνο προς μία κατεύθυνση με σκοπό την προστασία κρίσιμης πληροφορίας σε τμήματα / υποδίκτυα υψηλών απαιτήσεων ασφάλειας.

5	5	Λαμβάνονται μέτρα για την αποφυγή μη εξουσιοδοτημένης μεταφοράς πληροφορίας (unauthorized exfiltration). Μέτρα που ανήκουν σε αυτή την κατηγορία είναι: 1) προσδιορισμός και περιορισμός σε συγκεκριμένα πρωτόκολλα και τρόπους επικοινωνίας 2) παρακολούθηση πιθανής αποστολής μηνυμάτων από στοιχεία του οργανισμού (π.χ. beaconing) 3) υλοποίηση εργαλείων και προσπάθειας για την αναγνώριση πιθανών περιπτώσεων στεγανογραφίας 4) αποσύνδεση της πρόσβασης σε εξωτερικές διεπαφές όταν δεν χρησιμοποιούνται 5) υλοποίηση ανάλυσης κίνησης για την αναγνώριση της κανονικής / μη κανονικής συμπεριφοράς του συστήματος 6) ανάλυση σε επίπεδο packet headers κ.α. (τέτοιες λύσεις σε ένα βαθμό υλοποιούνται μέσα από deep packet inspection firewalls ή XML gateways.
5	6	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	7	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
NS2		**Μέτρο:** Διαχωρισμός και τμηματοποίηση του δικτύου **Στόχος Μέτρου:** Να εξασφαλιστεί ο διαχωρισμός του λογικού δικτύου, σύμφωνα με τις επιχειρηματικές λειτουργίες, και να απόφευχθεί η εξάπλωση κακόβουλων στοιχείων. **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση κατάλληλου διαχωρισμού και τμηματοποίησης του δικτύου, προκειμένου να διασφαλιστεί - λογικός ή/και φυσικός - διαχωρισμός των δικτύων πληροφοριών. Κατά τον σχεδιασμό, την εφαρμογή και τη διατήρηση των μέτρων διαχωρισμού και τμηματοποίησης του δικτύου, ο οργανισμός λαμβάνει υπόψη τους διάφορους τομείς λειτουργικής δραστηριότητας του οργανισμού. Ο οργανισμός λαμβάνει υπόψη τη φύση και την έκταση των δεδομένων που υποβάλλονται σε επεξεργασία στο πλαίσιο συγκεκριμένων επιχειρηματικών δραστηριοτήτων, προκειμένου να διασφαλίζεται επαρκής διαχωρισμός. Ο οργανισμός θα πρέπει να εξετάσει το ενδεχόμενο να υιοθετήσει εικονική τοπική δικτύωση (VLAN) κατά το σχεδιασμό του διαχωρισμού και της αρχιτεκτονικής του δικτύου σε τμήματα. Ο οργανισμός θα πρέπει να εξετάζει τουλάχιστον τον διαχωρισμό των τομέων έρευνας και ανάπτυξης, της διοίκησης, της κεντρικής υποδομής πληροφοριών και των δημόσια διαθέσιμων (στο διαδίκτυο) εφαρμογών και συστημάτων. **Πηγή:** NIST 800-53 (SC-3), ISO 27001, ISO 27002, PNNL
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**
0	1	Ο οργανισμός δεν εφαρμόζει καθόλου μέτρα για την προστασία της (λογικής) περιμέτρου του οργανισμού.
1	1	Έχει ένα firewall που λειτουργεί ως σημείο διεπαφής ανάμεσα στο τοπικό δίκτυο και το εξωτερικό δίκτυο.
1	2	Οι ρυθμίσεις του συγκεκριμένου firewall είναι στοιχειώδεις ή δεν υπάρχει τακτικός και ουσιαστικός έλεγχος και διαχείριση από την μεριά του οργανισμού. (Ο διαχωρισμός που υλοποιείται αφορά μόνο το εσωτερικό δίκτυο από το εξωτερικό).
2	1	Έχει σχεδιαστεί και υλοποιηθεί μια αρχιτεκτονική δικτύου για την εξασφάλιση του επιθυμητού επιπέδου ασφαλείας δικτύου για τον οργανισμό λαμβάνοντας υπόψη τις πρακτικές και τα μέτρα που αναφέρονται στα [NS2] – [NS7].
2	2	Έχει αποτυπωθεί η αρχιτεκτονική σε διάγραμμα δικτύου, και παρέχει ικανή πληροφορία σχετικά με την διασύνδεση, τον τρόπο λειτουργίας και τα διάφορα επίπεδα προστασίας.
2	3	Κρίσιμα συστήματα προστατεύονται από περισσότερα του ενός επίπεδα.
3	1	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται κατάλληλος διαχωρισμός και τμηματοποίηση του δικτύου, προκειμένου να διασφαλιστεί - λογικός ή/και φυσικός (όπου αυτό είναι εφικτό) - διαχωρισμός των δικτύων πληροφοριών.
3	2	Κατά τον σχεδιασμό, την εφαρμογή και τη διατήρηση των μέτρων διαχωρισμού και τμηματοποίησης του δικτύου, ο οργανισμός λαμβάνονται υπόψη οι διάφοροι τομείς λειτουργικής δραστηριότητας του οργανισμού.

3	3	Λαμβάνεται υπόψη η φύση και η έκταση των δεδομένων που υποβάλλονται σε επεξεργασία στο πλαίσιο συγκεκριμένων επιχειρηματικών δραστηριοτήτων, προκειμένου να διασφαλίζεται επαρκής διαχωρισμός.
3	4	Έχει δημιουργηθεί ένας ενιαίος κατάλογος στοιχείων ενεργητικού όπως αναφέρεται στο [RM2] και έχει γίνει μια σχετική διαβάθμιση σε σχέση με την κρισιμότητά τους όπως αναφέρεται στο [DS2].
3	5	Τα κρίσιμα συστήματα βρίσκονται διαχωρισμένα ώστε να μπορούν να εφαρμόζονται επιπλέον μέτρα προστασίας, υψηλότερου επιπέδου διαχείριση πρόσβασης και παρακολούθηση. Για τα τμήματα αυτά, γίνεται φιλτράρισμα της δικτυακής κίνησης (traffic filtering) μεταξύ των τμημάτων / υποδικτύων για να περιοριστεί η ροή της πληροφορίας στην απολύτως απαραίτητη για τις επιχειρησιακές ανάγκες του οργανισμού.
4	1	Έχει υιοθετηθεί εικονική τοπική δικτύωση (VLAN) κατά το σχεδιασμό του διαχωρισμού και της αρχιτεκτονικής του δικτύου σε τμήματα. Τα VLANs έχουν σχεδιαστεί και υλοποιηθεί λαμβάνοντας υπόψη τις ανάγκες κάθε τμήματος, τους στόχους ασφαλείας, την κρισιμότητα των δεδομένων και άλλα κριτήρια που ο οργανισμός κρίνει ως απαιραίτητα.
4	2	Κατ'ελάχιστο είναι διαχωρισμένοι οι τομείς έρευνας και ανάπτυξης, διοίκησης, κεντρικής υποδομής πληροφοριών και των δημόσια διαθέσιμων (στο διαδίκτυο) εφαρμογών και συστημάτων.
4	3	Οι διαχειριστικές εργασίες πληροφορικής (administrative tasks) διενεργούνται από στοιχεία που χρησιμοποιούνται αποκλειστικά για αυτό το σκοπό. Τυπικά, τα συγκεκριμένα στοιχεία είναι φυσικά ή λογικά διαχωρισμένα από τα υπόλοιπα και δεν έχουν πρόσβαση απευθείας στο διαδίκτυο – ακολουθούνται οι κανόνες του διαχωρισμού και της τμηματοποίησης του δικτύου.
4	4	Διενεργούνται τακτικοί έλεγχοι και δοκιμές για την επιβεβαίωση ότι υλοποιούνται οι σχετικοί κανόνες και υπάρχει ο επιθυμητός διαχωρισμός σε όλα τα επίπεδα.
4	5	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Εφαρμόζονται αρχές Zero trust αρχιτεκτονικής δικτύου σύμφωνα με διεθνείς βέλτιστες πρακτικές (π.χ. NIST 800-207).
5	2	Υλοποιείται διαχωρισμός ανάμεσα στις λειτουργίες ασφάλειας από τις υπόλοιπες με την δημιουργία περιβάλλοντος απομόνωσης (isolation boundary). Αυτό υλοποιείται με τον πιο πρόσφορο τρόπο και μπορεί να κυμαίνεται από την χρήση security kernels via processor rings ή processor modes, ή διαχωρισμό του κώδικα ανάμεσα σε security και non security functions στο δυνατό βαθμό .
5	3	Όπου είναι δυνατό,υλοποιείται φυσικός διαχωρισμός ανάμεσα στα αναγνωρισμένα επίπεδα (αντί απλά για λογικό).
5	4	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	5	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

NS3	**Μέτρο:** Προστασία από άρνηση παροχής υπηρεσιών **Στόχος Μέτρου:** Να διασφαλιστεί η προστασία των οργανωτικών πόρων από επιθέσεις άρνησης παροχής υπηρεσιών, και ότι δεν επηρεάζονται οι νόμιμες δραστηριότητες παροχής υπηρεσιών. **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση επαρκούς προστασίας από άρνηση παροχής υπηρεσιών και διανεμημένη άρνηση παροχής υπηρεσιών, προκειμένου να διασφαλίζεται η έγκαιρη και ποιοτική παροχή της υπηρεσίας σε εξουσιοδοτημένους και επικυρωμένους χρήστες και να διατηρείται σταθερό επίπεδο παραγωγικότητας. Κατά τον σχεδιασμό των σχετικών μέτρων προστασίας, ο οργανισμός θα πρέπει να εξετάσει την ενσωμάτωση ικανοτήτων για τον εντοπισμό νόμιμων χρηστών και εφαρμογών έναντι κακόβουλων προσπαθειών πρόσβασης σε πόρους. Ο οργανισμός θα πρέπει να λαμβάνει υπόψη μέτρα εφεδρείας και υψηλής διαθεσιμότητας, όπως περιγράφονται στο μέτρο [NS6], προκειμένου να εξασφαλίζεται η απρόσκοπτη λειτουργία σε περίπτωση απειλής κατά της διαθεσιμότητας πληροφοριών και υπηρεσιών. **Πηγή:** NIST 800-53, PNNL

Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν εφαρμόζει καθόλου μέτρα για την προστασία της (λογικής) περιμέτρου του οργανισμού.
1	1	Υπάρχει ένας firewall ο οποίος λειτουργεί ως σημείο διεπαφής ανάμεσα στο τοπικό δίκτυο και το εξωτερικό δίκτυο.
1	2	Οι ρυθμίσεις του συγκεκριμένου firewall είναι στοιχειώδεις ή δεν υπάρχει τακτικός και ουσιαστικός έλεγχος και διαχείριση από την μεριά του οργανισμού.
1	3	Δεν υπάρχουν ειδικές τεχνικές ρυθμίσεις ή μέτρα που έχουν εφαρμοστεί για την προστασία από άρνηση παροχής υπηρεσιών.
2	1	Στα πλαίσια του [RM2] διενεργείται ανάλυση στην οποία κατανοείται ποια είναι τα στοιχεία ενεργητικού που χρησιμοποιούνται προκειμένου να μπορούν να δώθούν οι σχετικές υπηρεσίες.
2	2	Για κάθε ένα από τα κρίσιμα στοιχεία ενεργητικού (όπως αυτά έχουν αναγνωριστεί στο [DS2]), έχουν αναγνωρισθεί και καταγραφεί οι τρόποι με τους οποίους μπορεί να υπερφορτωθεί, καθώς και τα όρια (σε bandwidth, επεξεργαστική ισχύ και αποθηκευτικό χώρο) πέρα από τα οποία η διαθεσιμότητα του στοιχείου διακινδυνεύεται.
2	3	Κίνδυνοι που σχετίζονται με την απώλεια της διαθεσιμότητας των κρίσιμων στοιχείων ενεργητικού περιλαμβάνονται μέσα στην ανάλυση και αξιολόγηση κινδύνων.
2	4	Τα κρίσιμα συστήματα προστατεύονται από περισσότερα του ενός επίπεδα.
3	1	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται επαρκή προστασία από άρνηση παροχής υπηρεσιών και διανεμημένη άρνηση παροχής υπηρεσιών, προκειμένου να διασφαλίζεται η έγκαιρη και ποιοτική παροχή της υπηρεσίας σε εξουσιοδοτημένους και επικυρωμένους χρήστες και να διατηρείται σταθερό επίπεδο παραγωγικότητας.
3	2	Έχουν εφαρμοστεί μέτρα για την εξουσιοδότηση και αυθεντικοποίηση των λογαριασμών που αποκτούν πρόσβαση στον οργανισμό. Δεν επιτρέπεται μη αυθεντικοποιημένη πρόσβαση, όπως αναφέρεται και στο [IAM1].
3	3	Έχει ενεργοποιηθεί παρακολούθηση και καταγραφή ενεργειών σύμφωνα με το [IAM6].
3	4	Λαμβάνονται υπόψη μέτρα εφεδρείας και υψηλής διαθεσιμότητας, όπως περιγράφονται στο μέτρο [NS6] και στο [AM4] προκειμένου να εξασφαλίζεται η απρόσκοπτη λειτουργία σε περίπτωση απειλής κατά της διαθεσιμότητας πληροφοριών και υπηρεσιών.
3	5	Εφαρμόζεται η χρήση του domain registrar locking για να εμποδίσει άρνηση παροχής υπηρεσιών λόγω μη εξουσιοδοτημένης διαγραφής, μεταφοράς ή αλλοίωσης της εγγραφής του domain του.
3	6	Υλοποιείται διαχωρισμός δικτύων όπως προβλέπεται στο [NS2].
3	7	Σε κάθε περίπτωση στοιχεία τα οποία χρειάζεται να είναι προσβάσιμα από το εξωτερικό δίκτυο (και είναι πιθανότερο να στοχοποιηθούν), είναι διαχωρισμένα από το εσωτερικό δίκτυο.

3	8	Χρησιμοποιείται λογισμικό (custom / open / proprietary) το οποίο έχει, κατ' ελάχιστο, λάβει μέτρα προστασίας από προεπιλογή και κατά το σχεδιασμό έναντι των OWASP TOP 10 (για web applications, APIs) και άλλων αντίστοιχων βέλτιστων πρακτικών για τις λοιπές εφαρμογές (OWASP ASVS).
4	1	Υλοποιούνται συστήματα παρακολούθησης της διαθεσιμότητας των κρίσιμων υπηρεσιών του και των στοιχείων ενεργητικού σύμφωνα με το [AM4], που έχουν την δυνατότητα να ανιχνεύουν επιθέσεις άρνησης παροχής υπηρεσιών και να στέλνουν ειδοποίηση σε πραγματικό χρόνο.
4	2	Ειδικά για οργανισμούς που παρέχουν υπηρεσίες μέσω του διαδικτύου, λαμβάνονται ειδικά μέτρα σε σχέση με την υπηρεσία DNS. Ο οργανισμός έχει 2 τουλάχιστον εξυπηρετητές DNS. Οι δυο εξυπηρετητές είναι προστατευμένοι (φυσικά και λογικά) και βρίσκονται σε διαφορετικές τοποθεσίες. Μεταξύ των δυο DNS γίνονται μεταφορές ζώνης τουλάχιστον μια φορά στις 24 ώρες και υλοποιούνται μέτρα για την ανθεκτικότητα έναντι επιθέσεων.
4	3	Η χρήση source routing απαγορεύεται.
4	4	Τα διάφορα κρίσιμα συστήματα έχουν την δυνατότητα να διαχειρίζονται την πλεονάζουσα χωρητικότητα (π.χ. bandwidth, memory κ.α.) προκειμένου να μειώσουν τις επιπτώσεις από μια επίθεση τέτοιου είδους.
4	5	Σε περίπτωση που γίνει αντιληπτή μια σχετική προσπάθεια, το εξουσιοδοτημένο προσωπικό ενημερώνεται άμεσα και να διενεργεί ενέργειες αντιμετώπισης σύμφωνα με το [EIM1].
4	6	Διενεργείται έλεγχος στα στοιχεία της παρακολούθησης σχετικά με την περίληψη στοιχείων που αναφέρονται στο ML3. Μέσω κατάλληλων τεχνικών μέτρων, γίνεται παρακολούθηση της κατάστασης των στοιχείων ενεργητικού όπως προβλέπεται από το [AM6].
4	7	Έχουν τεθεί συγκεκριμένοι κανόνες με όρια (thresholds) για την κατανάλωση συγκεκριμένων δυνατοτήτων των στοιχείων ενεργητικού (π.χ. bandwidth, memory, disk, κ.α.) ώστε να ενημερώνεται άμεσα το διαχειριστικό προσωπικό.
4	8	Το προσωπικό διενεργεί άμεσα αναλύσεις και εξάγει στοιχεία τάσεων ώστε να καθοριστεί ο λόγος για την σχετική συμπεριφορά και ενεργοποιεί την διαδικασία διαχείρισης περιστατικών ασφαλείας σύμφωνα με το [EIM1].
4	9	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Η φιλοξενία της δημόσιας πρόσβασης εφαρμογών δίνεται σε εξωτερικό αναγνωρισμένο και υψηλής ασφάλειας παρεχόμενης υπηρεσίας cloud υπηρεσιών (π.χ. τουλάχιστον score 10 στα πλαίσια στου CSA), μετά από ενδελεχή αξιολόγηση και αναζήτηση χαρακτηριστικών όσον αφορά στην ικανότητά του να ανθίσταται σε επιθέσεις άρνησης παροχής υπηρεσιών. Στις σχετικές συμβάσεις λαμβάνονται μέτρα και εγγυήσεις όπως προβλέπεται στην [TPS1].
5	2	Ειδικευμένος πάροχος cloud υπηρεσιών ασφάλειας (security as a service) έχει αναλάβει την παροχή υπηρεσιών προστασίας των δημόσιας πρόσβασης εφαρμογών από κατανεμημένες επιθέσεις άρνησης παροχής υπηρεσιών(π.χ. τουλάχιστον score 10 στα πλαίσια στου CSA), μετά από ενδελεχή αξιολόγηση και αναζήτηση χαρακτηριστικών όσον αφορά στην ικανότητά του να ανθίσταται σε επιθέσεις άρνησης παροχής υπηρεσιών. Στις σχετικές συμβάσεις λαμβάνονται μέτρα και εγγυήσεις όπως προβλέπεται στην [TPS1].
5	3	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	4	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

NS4	**Μέτρο:** Ασφαλή πρωτόκολλα επικοινωνίας **Στόχος Μέτρου:** Να διασφαλιστούν κατάλληλα πρωτοκόλλα επικοινωνίας προκειμένου να επιτευχθεί ασφαλής επικοινωνία μεταξύ των πόρων του δικτύου **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση ασφαλών πρωτοκόλλων για τη διευκόλυνση της διακίνησης πληροφοριών μεταξύ σημείων δικτύου, εφαρμογών και συστημάτων, προκειμένου να διασφαλίζεται η εμπιστευτικότητα και η ακεραιότητα των πληροφοριών κατά τη μεταφορά τους, και να αποτρέπονται επιθέσεις και απειλές στο δίκτυο, όπως για παράδειγμα υποκλοπές επικοινωνιών. Ο οργανισμός εξετάζει τα πλέον σύγχρονα πρωτόκολλα επικοινωνίας κατά τη διασφάλιση της μεταφοράς και ανταλλαγής πληροφοριών μέσω δικτύων επικοινωνίας. Ο οργανισμός πρέπει να λαμβάνει υπόψη μέτρα ασφάλειας που υποστηρίζονται από κρυπτογραφικά μέσα, όπως αυτά ορίζονται στο μέτρο [AM5] για την ασφάλεια των επικοινωνιών, χρησιμοποιώντας τεχνολογίες όπως το Hypertext Transfer Protocol Secure (HTTPS), το Internet Protocol security (IPsec), το Transport Layer Security (TLS) / Secure Sockets Layer (SSL), ανάλογα με το επιδιωκόμενο επίπεδο τεχνολογίας **Πηγή:**

Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν εφαρμόζει καθόλου μέτρα για την προστασία της (λογικής) περιμέτρου του οργανισμού.
1	1	Υπάρχει ένας firewall ο οποίος λειτουργεί ως σημείο διεπαφής ανάμεσα στο τοπικό δίκτυο και το εξωτερικό δίκτυο.
1	2	Οι ρυθμίσεις του συγκεκριμένου firewall είναι στοιχειώδεις ή δεν υπάρχει τακτικός και ουσιαστικός έλεγχος και διαχείριση από την μεριά του οργανισμού σε σχέση με τα επιτρεπόμενα και χρησιμοποιούμενα πρωτόκολλα επικοινωνίας.
2	1	Έχουν αναγνωρισθεί οι διαδικασίες μέσω των οποίων γίνεται ανταλλαγή πληροφοριών υψηλής κρισιμότητας (π.χ. passwords) και χρησιμοποιούνται πρωτόκολλα και τρόποιεπικοινωνίας που υλοποιούν κρυπτογράφηση.
2	2	Σε τέτοιες περιπτώσεις άλλα πρωτόκολλα τα οποία δεν υποστηρίζουν ενεργά ισχυρή κρυπτογράφηση χρησιμοποιούνται σε συνδυασμό με δεύτερο μέτρο (π.χ. telnet, virtual network computing, remote desk protocol πάνω από SSL ή Internet Protocol Security (IPsec)).
3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται ασφαλή πρωτόκολλα για τη διευκόλυνση της διακίνησης πληροφοριών μεταξύ σημείων δικτύου, εφαρμογών και συστημάτων, προκειμένου να διασφαλίζεται η εμπιστευτικότητα και η ακεραιότητα των πληροφοριών κατά τη μεταφορά τους, και να αποτρέπονται επιθέσεις και απειλές στο δίκτυο, όπως για παράδειγμα υποκλοπές επικοινωνιών.
3	2	Εξετάζονται τα πλέον σύγχρονα πρωτόκολλα επικοινωνίας κατά τη διασφάλιση της μεταφοράς και ανταλλαγής πληροφοριών μέσω δικτύων επικοινωνίας.
3	3	Λαμβάνονται υπόψη μέτρα ασφάλειας που υποστηρίζονται από κρυπτογραφικά μέσα, όπως αυτά ορίζονται στο μέτρο [AM5] για την ασφάλεια των επικοινωνιών, χρησιμοποιώντας τεχνολογίες όπως το Hypertext Transfer Protocol Secure (HTTPS), το Internet Protocol security (IPsec), το Transport Layer Security (TLS) / Secure Sockets Layer (SSL), ανάλογα με το επιδιωκόμενο επίπεδο τεχνολογίας
3	4	Ειδικά για τα κρίσιμα ή ευαίσθητα δεδομένα, υλοποιείται κρυπτογράφηση κατά την ανταλλαγή ή μεταφορά. Παραδείγματα τέτοιας υλοποίησης περιλαμβάνει (Transport Layer Security (TLS) and Open Secure Shell (OpenSSH) κα.).
3	5	Τα δεδομένα που μεταφέρονται με φυσικά μέσα, πρώτα κρυπτογραφούνται κατάλληλα και μετά αποστέλλονται. Τα κλειδιά κρυπτογράφησης μεταφέρονται χωριστά, με άλλο μέσο (ή τρόπο) χωρίς επισήμανση της χρήσης τους.
3	6	Για σύγχρονη μεταφορά χρησιμοποιούνται πρωτόκολλα των πιο πρόσφατων σταθερών εκδόσεων πρωτοκόλλων όπως είναι το SFTP ή HTTPS.

3	7	Χρησιμοποιείται secure routing protocols ή static routes προκειμένου να μην φαίνεται η εσωτερική δομή του.
3	8	Γίνονται ανασκόπηση και αναλύονται τα διάφορα συστήματα και στοιχεία προκειμένου να αναγνωρίζονται ποια πρωτοκόλλα, πόρτες και υπηρεσίες απαιτούνται για την ορθή και αποτελεσματική λειτουργία τους. Οτιδήποτε δεν προκύπτει ότι απαιτείται απενεργοποιείται. (Αυτό αφορά και πρωτόκολλα και μεθόδους όπως είναι το Bluetooth, FTP, peer-to-peer κ.α.)
4	1	Για την ανταλλαγή πληροφοριών μέσω APIs, γίνεται κατάλληλος σχεδιασμός, παραμετροποίηση, υλοποίηση και λειτουργίας ώστε να συμμορφώνεται με το επίπεδο ασφάλειας του οργανισμού.
4	2	Εφαρμόζονται βέλτιστες διεθνείς πρακτικές (π.χ. API OWASP Top Ten) .
4	3	Η εμπιστευτικότητα των δεδομένων εξασφαλίζεται είτε με κρυπτογράφηση σε επίπεδο καναλιού είτε με κρυπτογράφηση σε επίπεδο δεδομένων όταν γίνεται μεταφορά σε διαφορετικά δίκτυα ακόμα και εντός του ίδιου οργανισμού.
4	4	Για την κίνηση προς το εξωτερικό του οργανισμού (outgoing web, FTP, SSL) γίνεται δρομολόγηση μέσω (τουλάχιστον) ενός proxy σε ένα DMZ δίκτυο. Ο proxy υποστηρίζει παρακολούθηση των TCP sessions, και αποκλείει πρόσβαση σε συγκεκριμένα URLs, domain names και IPs.
4	5	Έχει απενεργοποιηθεί η αποστολή στοιχείων ανατροφοδότησης (τουλάχιστον όσο αφορά πληροφορία που δεν έχει ήδη ο αιτών) σε περίπτωση που γίνεται κάποιο λάθος επικύρωσης (feedback to senders on protocol format validation failure).
4	6	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Έχουν ενεργοποιηθεί περιορισμοί σε σχέση με το VOIP.
5	2	Συγκεκριμένα, χρήση VOIP γίνεται μόνο για συγκεκριμένες εξουσιοδοτημένες χρήσεις και μόνο μέσω συγκεκριμένων dedicated τμημάτων του δικτύου.
5	3	Υλοποιούνται ρυθμίσεις για την προστασία της σχετικής λειτουργίας και την εξασφάλιση υψηλού επιπέδου ασφάλειας επικοινωνιών.
5	4	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	5	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
NS5		**Μέτρο:** Έλεγχος πρόσβασης στο δίκτυο **Στόχος Μέτρου:** Να εξασφαλιστεί ότι η πρόσβαση στο λογικό δίκτυο από εξωτερικά και εσωτερικά συστήματα ασφαλίζεται κατάλληλα, ώστε μόνο τα εξουσιοδοτημένα πρόσωπα να μπορούν να έχουν πρόσβαση σε οργανωτικούς πόρους. **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση μέτρων ελέγχου πρόσβασης στο δίκτυο, ώστε να διασφαλίζεται η λογική πρόσβαση στο δίκτυο του οργανισμού και στους πόρους πληροφοριών, και να αποτρέπεται η μη εξουσιοδοτημένη πρόσβαση. Ο οργανισμός θα πρέπει να εξετάζει συγκεκριμένα τεχνικά και οργανωτικά μέτρα, όπως τους μηχανισμούς επαλήθευσης ταυτότητας για πρόσβαση στο δίκτυο, προκειμένου να διευκολύνει τη λειτουργία του εν λόγω μέτρου. Ο οργανισμός θα πρέπει να εξετάζει το ενδεχόμενο ελέγχου πρόσβασης στο δίκτυο για ενσύρματη, ασύρματη και άλλου είδους σύνδεση με το δίκτυο. Ο οργανισμός θα πρέπει να εξετάσει το ενδεχόμενο ενσωμάτωσης του ελέγχου της πρόσβασης στο δίκτυο με κεντρικά διαπιστευτήρια και με διαδικασίες διαχείρισης της ταυτότητας και της πρόσβασης, όπως ορίζεται στο μέτρο [IAM5]. **Πηγή:**
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**
0	1	Ο οργανισμός δεν διαχειρίζεται καθόλου την πρόσβαση στα συστήματά του (λογικά ή φυσικά).
1	1	Υπάρχουν συστήματα για την διαχείριση πρόσβασης στο δίκτυό.
1	2	Η διαχείριση της πρόσβασης δεν είναι οργανωμένη και συντονισμένη κεντρικά.

2	1	Υπάρχει μια πολιτική ελέγχου πρόσβασης η οποία καλύπτει όλα τα στοιχεία ενεργητικού και τα κτήρια του οργανισμού όπως εμφανίζονται στον ενιαίο κατάλογο στοιχείων ενεργητικού σύμφωνα με το [AM2].
2	2	Η πολιτική ελέγχου πρόσβασης καλύπτει την πρόσβαση σε εφαρμογές, δίκτυα, πόρους και κτήρια.
3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται μέτρα ελέγχου πρόσβασης στο δίκτυο, ώστε να διασφαλίζεται η λογική πρόσβαση στο δίκτυο του οργανισμού και στους πόρους πληροφοριών, και να αποτρέπεται η μη εξουσιοδοτημένη πρόσβαση.
3	2	Υλοποιούνται συγκεκριμένα τεχνικά και οργανωτικά μέτρα, όπως τους μηχανισμούς επαλήθευσης ταυτότητας για πρόσβαση στο δίκτυο, προκειμένου να διευκολύνται η λειτουργία του εν λόγω μέτρου.
3	3	Υλοποιούνται μέτρα για τον έλεγχο πρόσβασης στο δίκτυο για ενσύρματη, ασύρματη και άλλου είδους σύνδεση με το δίκτυο.
3	4	Σε περίπτωση παροχής πρόσβασης σε ασύρματα δίκτυα για δημόσια πρόσβαση, αυτά είναι διαχωρισμένα από το υπόλοιπο δίκτυο.
3	5	Σε κάθε περίπτωση οι διαδικασίες που αναφέρονται στο [IAM1] ισχύουν.
4	1	Η ασύρματη δικτυακή κυκλοφορία κρυπτογραφείται με τον αλγόριθμο Advanced Encryption Standard (AES) με χρήση κλειδιού μήκους 256 bits.
4	2	Χρησιμοποιείται ασύρματο σύστημα ανίχνευσης εισβολών (wireless intrusion detection system, WIDS) για την ανίχνευση μη εγκεκριμένων ασύρματων σημείων πρόσβασης (wireless access points) συνδεδεμένων στο δίκτυο.
4	3	Για την πρόσβαση μέσω ασύρματου δικτύου χρησιμοποιούνται κατάλληλα πρωτοκόλλα αυθεντικοποίησης όπως είναι extensible authentication protocol-transport layer security.
4	4	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Απενεργοποιείται η ασύρματη πρόσβαση σε διάφορα στοιχεία που έχουν την συγκεκριμένη δυνατότητα αλλά δεν απαιτείται για την σωστή και αποτελεσματική τους λειτουργία.
5	2	Υλοποιούνται σχετικές τεχνικές διαδικασίες και εργαλεία για την εξουσιοδότηση της χρήσης ασύρματων δικτύων ενώ υπάρχει αυστηρή πολιτική για το ποιος χρήστης έχει δικαίωμα να παραμετροποιεί wireless networking capabilities.
5	3	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	4	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
NS6		**Μέτρο:** Εφεδρεία και υψηλή διαθεσιμότητα **Στόχος Μέτρου:** Να εξασφαλιστεί της η διαθεσιμότητα πληροφοριών και δικτύων πληροφοριών με την επίτευξη επαρκούς διαθεσιμότητας πόρων, εφεδρικού εξοπλισμού, συστημάτων και συνδέσεων υψηλής διαθεσιμότητας. **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση επαρκών μέτρων για να διασφαλίζεται ένα εύλογο επίπεδο εφεδρείας και υψηλής διαθεσιμότητας, ιδίως για τα συστήματα, τις υπηρεσίες και τις εφαρμογές ζωτικής σημασίας που επεξεργάζονται διαβαθμισμένες ή/και επιχειρησιακές πληροφορίες. Ο οργανισμός πρέπει να εξετάζει το ενδεχόμενο εφεδρείας και υψηλής διαθεσιμότητας σε όλα τα επίπεδα τεχνολογίας, μεταξύ άλλων, αποθήκευσης, επικοινωνίας και επεξεργασίας. Ο οργανισμός λαμβάνει υπόψη τεχνολογίες εφεδρείας και υψηλής διαθεσιμότητας όπως είναι τα συστήματα εναλλακτικής σύνδεσης ή εφεδρείας, Redundant Arrays of Independent Disks (RAID), και εγκαταστάσεις αποθήκευσης δεδομένων σε cold, warm και hot. **Πηγή:**
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**

0	1	Ο οργανισμός δεν έχει λάβει μέτρα για την εξασφάλιση της διαθεσιμότητας των δικτύων και συστημάτων πληροφορικής.
1	1	Υπάρχει κάποιος εξοπλισμός σε εφεδρεία που μπορεί να χρησιμοποιηθεί σε περίπτωση αστοχίας ενός στοιχείου ενεργητικού αλλά δεν καλύπτει το σύνολο του κρίσιμου εξοπλισμού.
2	1	Έχουν αναγνωρισθεί τα κρίσιμα στοιχεία ενεργητικού.
2	2	Για τα συγκεκριμένα στοιχεία υπάρχει τουλάχιστον ένα ακόμα στοιχείο σε εφεδρεία (μπορεί να είναι το ίδιο ή αντίστοιχης ικανότητας).
2	3	Τα στοιχεία αυτά περιέχονται μέσα στον ενιαίο κατάλογο στοιχείων ενεργητικού.
3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται επαρκή μέτρα για να διασφαλίζεται ένα εύλογο επίπεδο εφεδρείας και υψηλής διαθεσιμότητας, ιδίως για τα συστήματα, τις υπηρεσίες και τις εφαρμογές ζωτικής σημασίας που επεξεργάζονται διαβαθμισμένες ή/και επιχειρησιακές πληροφορίες.
3	2	Εξασφαλίζεται εφεδρεία και υψηλή διαθεσιμότητα σε όλα τα επίπεδα τεχνολογίας, μεταξύ άλλων, αποθήκευσης, επικοινωνίας και επεξεργασίας.
3	3	Λαμβάνονται υπόψη τεχνολογίες εφεδρείας και υψηλής διαθεσιμότητας όπως είναι τα συστήματα εναλλακτικής σύνδεσης ή εφεδρείας, Redundant Arrays of Independent Disks (RAID), και εγκαταστάσεις αποθήκευσης δεδομένων σε cold, warm και hot.
3	4	Κατ΄ ελάχιστο ο εξοπλισμός που βρίσκεται στον οργανισμό διαθέτει εφεδρείες σε σχέση με την ενέργεια, την χωρητικότητα, το δίκτυο και τον τρόπο διασύνδεσης. Δεν υπάρχει κρίσιμος εξοπλισμός που δεν έχει εφεδρικό εντός του ίδιου χώρου σε ενεργή ή και ανενεργή λειτουργία.
3	5	Υπάρχει εξοπλισμός σε δευτερεύον σημείο, ο οποίος έχει σχετικά μελετηθεί ώστε να μπορεί να χρησιμοποιηθεί για να ανακάμψουν οι βασικές δραστηριότητες του οργανισμού ενός συγκεκριμένου χρονικού διαστήματος και σε συγκεκριμένο επίπεδο.
3	6	Τηρούνται εφεδρικά αντίγραφα ασφαλείας όπως αναφέρονται στο [DS3].
3	7	Έχουν τεθεί συγκεκριμένοι κανόνες με όρια (thresholds) για την κατανάλωση συγκεκριμένων δυνατοτήτων των στοιχείων ενεργητικού (π.χ. bandwidth, memory, disk, κ.α.) ώστε να ενημερώνεται άμεσα το διαχειριστικό προσωπικό. Το προσωπικό διενεργεί άμεσα αναλύσεις και εξάγει στοιχεία τάσεων ώστε να καθοριστεί ο λόγος για την σχετική συμπεριφορά και ενεργοποιεί την διαδικασία διαχείρισης περιστατικών ασφαλείας σύμφωνα με το [EIM1].
4	1	Έχει υλοποιηθεί ο σχεδιασμός και τα μέτρα που απαιτούνται για την ορθή και αποτελεσματική λειτουργία του Σχεδίου επιχειρησιακής συνέχειας και του Σχεδίου αποκατάστασης από καταστροφή όπως αναφέρονται στα [BCR1-4].
4	2	Υπάρχει τουλάχιστον μια δεύτερη εγκατάσταση αποθήκευσης δεδομένων με τον κρίσιμο εξοπλισμό σε κατάσταση που μπορεί να χαρακτηριστεί ως warm.
4	3	Υπάρχουν εφεδρικά καλώδια (δικτύου, ρεύματος, και ότι άλλο απαιτείται) από διαφορετικές (φυσικά διαχωρισμένες) οδεύσεις, λαμβάνοντας υπόψη τους σχετικούς κινδύνους.
4	4	Διενεργούνται δοκιμές για την αξιολόγηση της ύπαρξης και δυνατότητας ορθής και αποτελεσματικής λειτουργίας του εν λόγω εξοπλισμού αν απαιτηθεί. Σε περίπτωση αναγνώρισης προβλημάτων, αυτά διορθώνονται άμεσα και τηρούνται καταγραφές σύμφωνα με την διαδικασία διαχείρισης αλλαγών [CM1].
4	5	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Υπάρχει τουλάχιστον μια δεύτερη εγκατάσταση αποθήκευσης δεδομένων με τον κρίσιμο εξοπλισμό σε κατάσταση που μπορεί να χαρακτηριστεί ως hot.
5	2	Οι διαδικασίες για την μετάβαση μεταξύ των δυο εγκαταστάσεων είναι αυτόματες με την ελάχιστη δυνατή ανθρώπινη παρέμβαση. (Οι σχετικές εγκαταστάσεις αποθήκευσης και λειτουργίας ακολουθούν διεθνείς βέλτιστες πρακτικές για την διαθεσιμότητα και ανθεκτικότητα – π.χ. επιπέδου τουλάχιστον Tier III Uptime institute.)
5	3	Διενεργούνται δοκιμές για την αξιολόγηση της ύπαρξης και δυνατότητας ορθής και αποτελεσματικής λειτουργίας του εν λόγω εξοπλισμού όταν απαιτηθεί.

5	4	Σε περίπτωση αναγνώρισης προβλημάτων, αυτά διορθώνονται άμεσα και να τηρούνται καταγραφές σύμφωνα με την διαδικασία διαχείρισης αλλαγών [CM1].
5	5	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	6	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
NS7		**Μέτρο:** Ανίχνευση και πρόληψη εισβολών **Στόχος Μέτρου:** Να διασφαλιστεί η ανίχνευση και η πρόληψη από εξωτερικές απόπειρες εισβολής και επιθέσεις ασφάλειας. **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση επαρκών μέτρων για τον εντοπισμό και την πρόληψη εισβολών στο δίκτυο και τους πόρους του οργανισμού. Ο οργανισμός θα πρέπει να λαμβάνει υπόψη τα συστήματα ανίχνευσης εισβολών (IDS) και τα συστήματα πρόληψης εισβολών (IPS) για τον μετριασμό του κινδύνου απόπειρας εξωτερικής εισβολής. Ο οργανισμός εξετάζει το ενδεχόμενο δημιουργίας κονσόλας διαχείρισης για την παρακολούθηση του δικτύου με στόχο την καταχώρηση όλων των απόπειρών εισβολής για περαιτέρω ανάλυση. Στα πλαίσια σχεδιασμού των διαδικασιών ανίχνευσης και πρόληψης εισβολών, ο οργανισμός πρέπει να εξετάσει το ενδεχόμενο αυτόματης ενεργοποίησης μοχλών για την αντιμετώπιση συμβάντων, όπως ορίζεται στο [EIM2]. Ο οργανισμός πρέπει να λαμβάνει υπόψη τις λύσεις για τη διαχείριση συμβάντων και περιστατικών ασφάλειας (SIEM) για την υποστήριξη των διαδικασιών πρόληψης και ανίχνευσης εισβολών. **Πηγή:**
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**
0	1	Ο οργανισμός δεν εφαρμόζει καθόλου μέτρα για την προστασία της (λογικής) περιμέτρου του οργανισμού.
1	1	Υπάρχει ένας firewall ο οποίος λειτουργεί ως σημείο διεπαφής ανάμεσα στο τοπικό δίκτυο και το εξωτερικό δίκτυο.
1	2	Οι ρυθμίσεις του συγκεκριμένου firewall είναι στοιχειώδεις ή δεν υπάρχει τακτικός και ουσιαστικός έλεγχος και διαχείριση από την μεριά του οργανισμού.
2	1	Για τα κρίσιμα στοιχεία ενεργητικού, όπως αυτά αποτυπώνονται στον σχετικό κατάλογο [AM2 / RM2], έχει ενεργοποιηθεί μη αυτοματοποιημένη παρακολούθηση.
2	2	Η παρακολούθηση περιλαμβάνει κατ' ελάχιστο τις ενέργειες των ατόμων, αντικειμένων και οντοτήτων όταν αποκτούν πρόσβαση ή χρησιμοποιούν τα στοιχεία ενεργητικού, τα γεγονότα που μπορεί να διαταράξουν την ομαλή λειτουργία μιας δραστηριότητας, τις αλλαγές των στοιχείων ενεργητικού που οδηγούν σε διαφοροποίηση από το security baseline, στοιχεία ενεργητικού που συνδέονται (μη-αναμενόμενα) στα δίκτυα του οργανισμού και οποιαδήποτε άλλη ύποπτη δραστηριότητα.
3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται επαρκή μέτρα για τον εντοπισμό και την πρόληψη εισβολών στο δίκτυο και τους πόρους του οργανισμού.
3	2	Έχουν υλοποιηθεί και διατηρούνται συστήματα ανίχνευσης εισβολών (IDS) και συστήματα πρόληψης εισβολών (IPS) για τον μετριασμό του κινδύνου απόπειρας εξωτερικής εισβολής.
3	3	Σε περίπτωση αναγνώρισης μη τυπικής (anomalous) συμπεριφορά, ενεργοποιείται η διαδικασία ανταπόκρισης περιστατικών ασφαλείας και απομονώνονται τα σχετικά στοιχεία μέχρι να διερευνηθεί πλήρως η κατάσταση.
3	4	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται δυνατότητες παρακολούθησης των στοιχείων ενεργητικού, ώστε ο οργανισμός να είναι σε θέση να εντοπίζει ανωμαλίες σε σχέση με κανονικές συνθήκες (π.χ. τοποθεσία, χρήση) και/ή τη λειτουργία των στοιχείων αυτών σύμφωνα με το [AM3].
4	1	Χρησιμοποιείται κονσόλα διαχείρισης για την παρακολούθηση του δικτύου με στόχο την καταχώρηση όλων των απόπειρών εισβολής για περαιτέρω ανάλυση.

4	2	Στα πλαίσια σχεδιασμού των διαδικασιών ανίχνευσης και πρόληψης εισβολών, υλοποιείται αυτόματη ενεργοποίηση μοχλών για την αντιμετώπιση συμβάντων, όπως ορίζεται στο [EIM2].
4	3	Χρησιμοποιείται ασύρματο σύστημα ανίχνευσης εισβολών (wireless intrusion detection system, WIDS) για την ανίχνευση μη εγκεκριμένων ασύρματων σημείων πρόσβασης (wireless access points) συνδεδεμένων στο δίκτυο του οργανισμού.
4	4	Έχει υλοποιηθεί IDS εντός της DMZ για ανάλυση της πληροφορίας που ανταλλάσσεται με το εξωτερικό δίκτυο.
4	5	Έχουν υλοποιηθεί IDS sensors στο εξωτερικό δίκτυο αλλά και σε δίκτυα που είναι εκτεθειμένα, για πιο άμεσο εντοπισμό σχετικών επιθέσεων με την χρήση υπογραφών, ανάλυσης κυκλοφορίας ή και άλλων μηχανισμών.
4	6	Η πληροφορία που εξάγεται από τα διάφορα εργαλεία και επίπεδα παρακολούθησης και καταγραφής ενεργειών αναλύεται και τα συμπεράσματα χρησιμοποιούνται στην εκπαίδευση των σχετικών εργαλείων με σκοπό την μείωση των false positives, την μείωση των false negatives και το γενικό fine tuning τους.
4	7	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Έχει τεθεί σε λειτουργία σύστημα SIEM το οποίο συγκεντρώνει τα στοιχεία παρακολούθησης από το σύνολο των στοιχείων ενεργητικού του οργανισμού.
5	2	Έχουν παραμετροποιηθεί κανόνες και έχουν δημιουργηθεί ενημερώσεις (notifications & alerts) στο κατάλληλο προσωπικό σε περίπτωση ενεργοποίησης κάποιου κανόνα. Για την δημιουργία των κανόνων έχουν ληφθεί υπόψη βασικές μέθοδοι επίθεσης.
5	3	Το SIEM λειτουργεί κατ΄ ελάχιστον σύμφωνα με τους κανόνες και τις άλλες προδιαγραφές που αναφέρονται στο [AM3].
5	4	Έχει υλοποιηθεί network based IPS, τα οποία σε συνεργασία με τα IDS, αποτρέπουν συγκεκριμένη κίνηση, συμπεριφορά ή άλλο.
5	5	Τα IPS είναι παραμετροποιημένα (όπως και οι άλλες συσκευές δικτύου όπως αναφέρονται στο [NS1] να παρακολουθούν και να καταγράφουν όλη την κίνηση.
5	6	Έχει δημιουργηθεί μια διασύνδεση ανάμεσα στο IDS και στα εργαλεία ελέγχου πρόσβασης ώστε να μπορούν να ενεργοποιηθούν άμεσα μηχανισμοί για την λήψη κατάλληλων ενεργειών απαγόρευσης πρόσβασης σε περίπτωση σχετικής επίθεσης.
5	7	Το SIEM είναι παραμετροποιημένο ώστε να στέλνει ενημερώσεις σε κατάλληλα εξουσιοδοτημένες και εκπαιδευμένες ομάδες ατόμων, σε περίπτωση αναγνώρισης κάποιου πιθανού security related event.
5	8	Το SIEM συνδυάζει την πληροφορία που έρχεται από διαφορετικές πηγές (όχι μόνο από το IDS/IPS) προκειμένου να δώσει τα βέλτιστα δυνατά αποτελέσματα (σχετικά συστήματα είναι: firewalls, routers, anti-virus software, servers κ.α.). Αν είναι δυνατό, ο οργανισμός επεκτείνει τις πηγές πληροφορίας του SIEM και σε δεδομένα από την φυσική παρακολούθηση ή από την εφοδιαστική αλυσίδα.
5	9	Έχει ανατεθεί σε κατάλληλο εσωτερικό ή εξωτερικό προσωπικό η παρακολούθηση 24x7x365 των σχετικών εργαλείων και στοιχείων, για όσο πιο έγκαιρη προειδοποίηση και όσο πιο άμεση ανταπόκριση γίνεται.
5	10	Διενεργούνται δοκιμές για τον έλεγχο των εργαλείων IDS, IPS και SIEM καθώς και της ετοιμότητας και ικανότητας του σχετικού προσωπικού σε τακτική βάση.
5	11	Έχουν ληφθεί υπόψη κατά το σχεδιασμό και την υλοποίηση των συγκεκριμένων εργαλείων (θέση στο δίκτυο, τύπος του εργαλείου, είδη κανόνων κ.α.) οι ανάγκες για παρακολούθηση και οι ανάγκες για προστασία (π.χ. encryption).
5	12	Υλοποιούνται μέτρα για τον έλεγχο της πληροφορίας που εξέρχεται από το δίκτυό του όπως αναφέρεται στο [NS1].
5	13	Αναγνωρίζονται Indicators of Compromise για ανταπόκριση με μεγαλύτερη ταχύτητα και μειώση της επίπτωσης μιας σχετικής επίθεσης στον οργανισμό.

5	14	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	15	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

Κατηγορία		ΑΣΦΑΛΕΙΑ ΣΥΣΤΗΜΑΤΩΝ
SS1		**Μέτρο:** Καταπολέμηση κακόβουλου λογισμικού **Στόχος Μέτρου:** Να διασφαλιστεί ότι δεν θα επηρεαστούν οργανωτικοί πόροι από κακόβουλο λογισμικό και κώδικα. **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση επαρκών μέτρων για την προστασία των συστημάτων από μολύνσεις από κακόβουλο λογισμικό και κώδικα, προκειμένου να διασφαλίζεται η εμπιστευτικότητα, η ακεραιότητα, η διαθεσιμότητα και η αυθεντικότητα των πληροφοριών. Ο οργανισμός εξετάζει σειρά μέτρων για την καταπολέμηση κακόβουλου λογισμικού, μεταξύ άλλων, λειτουργικά συστήματα, συστήματα και υπηρεσίες δικτύου, λειτουργικά συστήματα εξοπλισμού δικτύου, τερματικά σημεία χρηστών και κινητές συσκευές, καθώς και φορητές συσκευές περιεχομένου. Ο οργανισμός πρέπει να διασφαλίζει ότι τα μέτρα καταπολέμησης του κακόβουλου λογισμικού βασίζονται σε ενημερωμένα δεδομένα με σκοπό τον εντοπισμό και την επίλυση απειλών από κακόβουλο λογισμικό. **Πηγή:**
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**
0	1	Ο οργανισμός δεν έχει υλοποιήσει κανένα μέτρο για την προστασία από κακόβουλο λογισμικό / κώδικα.
1	1	Έχει εγκατασταθεί και χρησιμοποιείται λογισμικό για την προστασία από κακόβουλο λογισμικό / κώδικα σε κάποια από τα end-point devices.
1	2	Η εγκατάσταση του λογισμικού προστασίας δεν είναι συστηματική και δεν υπάρχει κεντρικός έλεγχος.
2	1	Έχει εγκατασταθεί και χρησιμοποιείται λογισμικό για την προστασία από κακόβουλο λογισμικό / κώδικα σε όλα τα end-point devices.
3	1	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται διαδικασία / πολιτική και μέτρα για την προστασία των συστημάτων από μολύνσεις από κακόβουλο λογισμικό και κώδικα, προκειμένου να διασφαλίζεται η εμπιστευτικότητα, η ακεραιότητα, η διαθεσιμότητα και η αυθεντικότητα των πληροφοριών.
3	2	Εφαρμόζεται μια σειρά μέτρων για την καταπολέμηση κακόβουλου λογισμικού, μεταξύ άλλων, λειτουργικά συστήματα, συστήματα και υπηρεσίες δικτύου, λειτουργικά συστήματα εξοπλισμού δικτύου, τερματικά σημεία χρηστών και κινητές συσκευές, καθώς και φορητές συσκευές περιεχομένου.
3	3	Διασφαλίζεται ότι τα μέτρα καταπολέμησης του κακόβουλου λογισμικού βασίζονται σε ενημερωμένα δεδομένα με σκοπό τον εντοπισμό και την επίλυση απειλών από κακόβουλο λογισμικό.
3	4	Το λογισμικό προστασίας είναι παραμετροποιημένο με τέτοιο τρόπο ώστε να: (α) Διενεργεί αυτόματα scan (autoprotect) σε οποιοδήποτε εισερχόμενο
3	5	(β) Διενεργεί scan και να μπλοκάρει συνημμένα ηλεκτρονικών επικοινωνιών που περιέχουν κακόβουλο κώδικα ή τύπους αρχείων που ενέχουν αυξημένο κίνδυνο
3	6	(γ) Διενεργεί τακτικούς ελέγχους στα σημεία αποθήκευσης πληροφοριών για την αναγνώριση αρχείων ή άλλων στοιχείων που σχετίζονται με κακόβουλο κώδικα
3	7	(δ) Μην επιτρέπει την αυτόματη έναρξη λογισμικών (auto-run) από διάφορα μέσα
3	8	(ε) Ειδοποιεί το χρήστη σε περίπτωση αναγνώρισης κάποιας απειλής
3	9	(ζ) Διενεργεί αυτόματα ενέργειες για την διαγραφή ή απομόνωση της απειλής
3	10	(η) Διενεργεί αυτόματα ενημερώσεις τόσο των υπογραφών όσο και της λειτουργικότητας
3	11	Υλοποιείται προστασία τόσο σε επίπεδο συσκευής όσο και σε επίπεδο δικτύου (π.χ. σχετικές υλοποιήσεις σε επίπεδο firewall, proxy κλπ).
3	12	Διενεργούνται εκπαιδεύσεις σε θέματα που σχετίζονται με την προστασία από malware, τεχνικές επίθεσης, phishing & social engineering.

4	1	Χρησιμοποιούνται αυτόματα και κεντρικοποιημένα συστήματα για την συνεχή παρακολούθησης σε σχέση με την προστασία από κακόβουλο κώδικα / λογισμικό όλων των στοιχείων. (workstations, servers, mobile devices, firewalls, IPS κλπ). Τα κεντρικά συστήματα παρέχουν την δυνατότητα στο εξουσιοδοτημένο προσωπικό να βλέπουν την κατάσταση προστασίας από κακόβουλο κώδικά / λογισμικό για όλα τα στοιχεία (ανεξάρτητα του είδους και του λειτουργικού συστήματος). Σε περίπτωση που κάποιο στοιχείο δεν λαμβάνει ενημερώσεις θα πρέπει να γίνονται κατάλληλες ενέργειες.
4	2	Υλοποιούνται λύσεις antimalware με δυνατότητες αναγνώρισης αδυναμιών και φίλτρα anti-exploitation.
4	3	Όπου που υπάρχει αναγνώριση σχετικής απειλής εμφανίζεται σχετικό μήνυμα τόσο στο σημείο αναγνώρισης όσο και κεντρικά και το κατάλληλο προσωπικό ενημερώνεται άμεσα ώστε να υλοποιηθούν οι απαραίτητες ενέργειες. Σε κάθε περίπτωση τα εργαλεία είναι παραμετροποιημένα με default ενέργειες σε περίπτωση ανίχνευσης απειλής (π.χ. quarantine, delete) και σε σχετικούς συνδυασμούς σε περίπτωση αποτυχίας.
4	4	Υλοποιούνται δοκιμές και ασκήσεις για τον έλεγχο της αποτελεσματικότητας της σχετικής εκπαίδευσης και την ετοιμότητα και ανθεκτικότητα του προσωπικού έναντι των σχετικών απειλών.
4	5	Υλοποιούνται μηχανισμοί anti-tampering protection ώστε να μην μπορεί να γίνει απενεργοποίηση της σχετικής προστασίας από μη εξουσιοδοτημένα άτομα.
4	6	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Τηρείται και εφαρμόζεται λίστα με επιτρεπόμενο λογισμικό.
5	2	Διενεργούνται σε τακτική βάση έλεγχοι ακεραιότητας των δεδομένων (integrity monitoring) για την αναγνώριση πιθανών μη εξουσιοδοτημένων αλλαγών και την ύπαρξη σχετικών απειλών εντός του οργανισμού.
5	3	Διασφαλίζεται (με οργανωτικά ή τεχνικά μέσα) ότι ακόμα και όταν στοιχεία βρίσκονται εκτός δικτύου, υπάρχει δυνατότητα λήψης των σχετικών ενημερώσεων και πολιτικών ασφαλείας με ασφάλεια.
5	4	Διενεργούνται δοκιμές για την αξιολόγηση της αποτελεσματικότητας των λύσεων προστασίας από κακόβουλο κώδικα/ λογισμικό.
5	5	Εξετάζεται ειδικά η προστασία από επίκαιρες απειλές, με την χρήση μηχανισμών ανίχνευσης που δεν στηρίζονται στην ταυτοποίηση υπογραφών (signature based).
5	6	Ειδικά για κρίσιμα συστήματα και πριν την ενσωμάτωση νέου λογισμικού ή αλλαγής, γίνεται ανάλυση σε επίπεδο ασφάλειας (π.χ. δοκιμές ανάλυσης κώδικα για ανίχνευση παράνομων διεργασιών μέσα σε ελεγχόμενο περιβάλλον κ.α.)
5	7	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	8	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

SS2	**Μέτρο:** Θωράκιση συστημάτων και συσκευών και βασικές απαιτήσεις ασφάλειας **Στόχος Μέτρου:** Να ελαχιστοποιηθεί, στο μέτρο του δυνατού, η επιφάνεια επίθεσης των συστημάτων πληροφοριών, μέσω της μείωσης της λειτουργικότητας και των χαρακτηριστικών τους. **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση διαδικασίας για τη θωράκιση συστημάτων και συσκευών με βάση καθορισμένες βασικές απαιτήσεις ασφάλειας, ώστε να αποτρέπεται η μη εξουσιοδοτημένη πρόσβαση και χρήση των πόρων και των υπηρεσιών του συστήματος. Ο οργανισμός εξετάζει τα λειτουργικά συστήματα, τις εφαρμογές και κάθε άλλο λογισμικό που είναι εγκατεστημένο σε συσκευές που εμπίπτουν στο πεδίο εφαρμογής της διαδικασίας θωράκισης. Ο οργανισμός πρέπει να εξετάζει τις κατευθυντήριες γραμμές και τα έγγραφα για τη θωράκιση συστημάτων που παρέχονται από τους προμηθευτές λογισμικού και υλισμικού, καθώς και τις κατευθυντήριες γραμμές και τις βέλτιστες πρακτικές που δημοσιεύονται από ομάδες συστημάτων τεχνολογίας, ρυθμιστικές αρχές και άλλες διεθνείς βέλτιστες πρακτικές ή πλαίσια. Ο οργανισμός πρέπει να λαμβάνει υπόψη, τουλάχιστον, τα default configurations και την κατάργηση των μη αναγκαίων προκαθορισμένων λογαριασμών, την εξασφάλιση ενιαίων πρωτογενών λειτουργιών ανά διακομιστή για την αποφυγή λειτουργιών με διαφορετικά επίπεδα ασφάλειας στον ίδιο εξυπηρετητή, παρέχοντας μόνο τις απαραίτητες υπηρεσίες, τα πρωτόκολλα και τους daemons, χρησιμοποιώντας παραμέτρους για την ασφάλεια του συστήματος με στόχο την πρόληψη της κατάχρησης, και την αφαίρεση κάθε περιττής λειτουργίας, όπως των scripts, των drivers, των χαρακτηριστικών και των υποσυστημάτων, προκειμένου να ελαχιστοποιηθεί η επιφάνεια επίθεσης του συστήματος. Ο οργανισμός θα πρέπει να εξετάσει το ενδεχόμενο εφαρμογής τείχων προστασίας στο επίπεδο συστημάτων (firewalls), προκειμένου να αποτρέπονται οι επιπτώσεις από κακόβουλο κώδικα στην ασφάλεια των πληροφοριών που αποθηκεύονται στο τελικό σημείο. **Πηγή:**

Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν εφαρμόζει μέτρα για την αναγνώριση και εφαρμογή ελάχιστου προφίλ ασφαλείας για τα στοιχεία.
1	1	Διενεργούνται βασικές λειτουργίες για την παραμετροποίηση συσκευών.
1	2	Οι απαιτήσεις ασφαλείας ενσωματώνονται μερικώς και ad-hoc.
2	1	Έχουν αναγνωρισθεί βασικά στοιχεία που πρέπει να είναι περιορισμένα σε συγκεκριμένες κατηγορίες στοιχείων.
2	2	Τα στοιχεία αυτά ενσωματώνονται είτε κατά την εγκατάσταση είτε κατόπιν αυτής.
3	1	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται διαδικασία για τη θωράκιση συστημάτων και συσκευών με βάση καθορισμένες βασικές απαιτήσεις ασφάλειας, ώστε να αποτρέπεται η μη εξουσιοδοτημένη πρόσβαση και χρήση των πόρων και των υπηρεσιών του συστήματος.
3	2	Τα λειτουργικά συστήματα, οι εφαρμογές και κάθε άλλο λογισμικό που είναι εγκατεστημένο σε συσκευές που εμπίπτουν στο πεδίο εφαρμογής της διαδικασίας θωράκισης εξετάζεται.
3	3	Εξετάζονται οι κατευθυντήριες γραμμές και τα έγγραφα για τη θωράκιση συστημάτων που παρέχονται από τους προμηθευτές λογισμικού και υλισμικού, καθώς και οι κατευθυντήριες γραμμές και οι βέλτιστες πρακτικές που δημοσιεύονται από ομάδες συστημάτων τεχνολογίας, ρυθμιστικές αρχές και άλλες διεθνείς βέλτιστες πρακτικές ή πλαίσια.
3	4	Λαμβάνονται υπόψη, τουλάχιστον, τα default configurations και η κατάργηση των μη αναγκαίων προκαθορισμένων λογαριασμών, την εξασφάλιση ενιαίων πρωτογενών λειτουργιών ανά διακομιστή για την αποφυγή λειτουργιών με διαφορετικά επίπεδα ασφάλειας στον ίδιο εξυπηρετητή, παρέχοντας μόνο τις απαραίτητες υπηρεσίες, τα πρωτόκολλα και τους daemons, χρησιμοποιώντας παραμέτρους για την ασφάλεια του συστήματος με στόχο την πρόληψη της κατάχρησης, και την αφαίρεση κάθε περιττής λειτουργίας, όπως των scripts, των drivers, των χαρακτηριστικών και των υποσυστημάτων, προκειμένου να ελαχιστοποιηθεί η επιφάνεια επίθεσης του συστήματος, σύμφωνα με τις απαιτήσεις [IAM1].

3	5	Εξετάζεται το ενδεχόμενο εφαρμογής τείχων προστασίας στο επίπεδο συστημάτων (firewalls), προκειμένου να αποτρέπονται οι επιπτώσεις από κακόβουλο κώδικα στην ασφάλεια των πληροφοριών που αποθηκεύονται στο τελικό σημείο σύμφωνα με τις απαιτήσεις του [NS1].
3	6	Εγκατάσταση λογισμικού γίνεται από ειδικά εξουσιοδοτημένο προσωπικό.
4	1	Για κάθε λειτουργικό σύστημα έχει δημιουργηθεί ένα αρχείο (ανάλογα με τον τρόπο με τον οποίο γίνεται το deployment – container, vm, image κλπ) που αντιστοιχεί στην πιο επίκαιρη, σταθερή και ασφαλή παραμετροποίηση του.
4	2	Η παραμετροποίηση ακολουθεί τις προτάσεις του κατασκευαστή ή άλλων αξιόπιστων πηγών και έχει το επιθυμητό επίπεδο θωράκισης (hardened).
4	3	Οι βασικές αρχές που έχουν αναφερθεί στα σχετικά [IAM1], [NS1], [AM1-4] εφαρμόζονται. Κατ' ελάχιστον καλύπτονται τα στοιχεία του ML3 καθώς και τα ακόλουθα: μη χρησιμοποιούμενες θύρες, θύρες που χρησιμοποιούνται για διαγνωστικούς σκοπούς, μη επιθυμητά πρωτόκολλα, απενεργοποίηση μη χρησιμοποιούμενων λογαριασμών, υλοποίηση λύσεων προστασίας από κακόβουλο λογισμικό, ενεργοποίηση λογισμικού firewall, IDS και IPS όπου αυτά βρίσκουν εφαρμογή κ.α.
4	4	Γίνεται διαχείριση των αλλαγών στα αρχεία αυτά μέσω της διαδικασίας διαχείρισης αλλαγών [CM1]. (Αλλαγές πρέπει να γίνονται για την επικαιροποίηση των updates / patches, στην αλλαγή ρυθμίσεων βάσει στοιχείων περιστατικών ή ενημέρωσης από άλλα αξιόπιστα ενδιαφερόμενα μέρη κ.α.). Σε περίπτωση που υπάρχει κάποιο πρόβλημα με κάποιο στοιχείο, αντικαθίσταται με καθαρή υλοποίηση από το αρχείο (baseline).
4	5	Κάθε στοιχείο εντός του δικτύου του οργανισμού είναι μοναδικά αναγνωρίσιμο και περιέχεται μέσα στον ενιαίο κατάλογο στοιχείων ενεργητικού όπως αναφέρεται στο [DS1/RM2].
4	6	Αντίστοιχες διαδικασίες και οδηγίες υπάρχουν και για διαφορετικού είδους λογισμικά όπως είναι εφαρμογές, βάσεις δεδομένων κ.α.
4	7	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Τηρείται και εφαρμόζεται λίστα με επιτρεπόμενο λογισμικό για κάθε περίπτωση λογισμικού που αναγνωρισμένα υποστηρίζει τις επιχειρησιακές λειτουργίες του οργανισμού.
5	2	Για κάθε λογισμικό (περιλαμβανομένου και του λειτουργικού) έχουν αναγνωριστεί και καταγραφεί οι επιτρεπτές εκδόσεις σε συμφωνία με τους στόχους του οργανισμού και τον σχετικό κίνδυνο.
5	3	Όσα στοιχεία έχουν έμμεσα ή άμεσα πρόσβαση σε πληροφορία, είναι απενεργοποιημένα τα: peer-to-peer wireless network capabilities και το wireless peripheral access to devices (περιλαμβανομένου του Bluetooth) – εκτός των περιπτώσεων που έχει υλοποιηθεί τεχνικός τρόπος ώστε να γίνεται σύνδεση με συγκεκριμένες – εξουσιοδοτημένες από τον οργανισμό συσκευές.
5	4	Τα προηγούμενα αρχεία (baselines) διατηρούνται για λόγους ιστορικότητας και δυνατότητας roll back σε περίπτωση ανάγκης.
5	5	Τηρούνται αρχεία (baseline) και για τα συστήματα που χρησιμοποιούνται για την ανάπτυξη και δοκιμή, διακριτά από αυτά που χρησιμοποιούνται για την παραγωγή.
5	6	Διενεργούνται έλεγχοι και δοκιμές για την αξιολόγηση της ανθετικότητας των baseline αρχείων. Σε περίπτωση που διαπιστωθούν αδυναμίες, λαμβάνονται άμεσα μέτρα και ακολουθείται η διαδικασία διαχείρισης αλλαγών.
5	7	Διενεργούνται τακτικοί έλεγχοι για τον έλεγχο της συμμόρφωσης της παραμετροποίησης και της λειτουργίας των στοιχείων προς τις αναγνωρισμένες βέλτιστες πρακτικές θωράκισης. Μέτρα λαμβάνονται άμεσα και διαχειρίζονται μέσα από την διαδικασία διαχείρισης αλλαγών ή / και την διαχείριση περιστατικών ασφαλείας όπως απαιτείται.
5	8	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.

5	9	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
SS3		**Μέτρο:** Ασφάλεια κινητών συσκευών **Στόχος Μέτρου:** Να εξασφαλιστεί η κατάλληλη ασφάλεια των κινητών συσκευών που έχουν πρόσβαση σε οργανωτικούς πόρους. **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση μέτρων ασφάλειας κινητών συσκευών προκειμένου να διασφαλίζεται η εμπιστευτικότητα, η ακεραιότητα, η διαθεσιμότητα και η αυθεντικότητα των κινητών συστημάτων που χρησιμοποιούνται από τα στελέχη για να συνδέονται, αλληλοεπιδρούν ή επεξεργάζονται οργανωτικά στοιχεία υποδομής και πόρους. Ο οργανισμός πρέπει να εξετάζει τη διαχείριση κινητών συσκευών, μέτρα ασφαλούς αποθήκευσης και κρυπτογράφησης, όπως ορίζονται στο μέτρο [DS5], ισχυρή επαλήθευση ταυτότητας, όπως ορίζεται στο μέτρο [IAM4], και μέτρα ασφαλούς επικοινωνίας και δικτύωσης, όπως ορίζονται στο μέτρο [NS4]. Ο φορέας διασφαλίζει την επαρκή προστασία των κινητών συσκευών και των πληροφοριών που διατηρούνται σε κινητές συσκευές έναντι κλοπής και απώλειας. Ο οργανισμός πρέπει να εξετάζει τη δυνατότητα εξ αποστάσεως καθαρισμού και του εντοπισμού της γεωγραφικής θέσης. **Πηγή:**
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**
0	1	Ο οργανισμός δεν λαμβάνει μέτρα για την ασφάλεια κινητών συσκευών.
1	1	Λαμβάνονται κάποια μέτρα για την ασφάλεια κινητών συσκευών, χωρίς αυτά να είναι συνολικά, σε όλες τις συσκευές ή οργανωμένα.
2	1	Έχουν αναγνωρισθεί στα πλαίσια του ενιαίου καταλόγου στοιχείων όπως αναφέρεται στο [DS2/RM2] τα στοιχεία που είναι μεταφερόμενες – κινητές συσκευές.
2	2	Έχουν αναγνωρισθεί οι κίνδυνοι όπως προβλέπεται από τα [RM1/RM3] που σχετίζονται με την ύπαρξη και λειτουργία μεταφερόμενων / κινητών συσκευών.
2	3	Για αυτά τα στοιχεία εφαρμόζεται κρυπτογράφηση σε επίπεδο συσκευής (σύμφωνα με τα αναγραφόμενα του [AM5].
3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται μέτρα ασφάλειας κινητών συσκευών προκειμένου να διασφαλίζεται η εμπιστευτικότητα, η ακεραιότητα, η διαθεσιμότητα και η αυθεντικότητα των κινητών συστημάτων που χρησιμοποιούνται από τα στελέχη για να συνδέονται, αλληλοεπιδρούν ή επεξεργάζονται οργανωτικά στοιχεία υποδομής και πόρους.
3	2	Εξετάζονται η διαχείριση κινητών συσκευών, μέτρα ασφαλούς αποθήκευσης και κρυπτογράφησης, όπως ορίζονται στο μέτρο [DS5], ισχυρή επαλήθευση ταυτότητας, όπως ορίζεται στο μέτρο [IAM4], και μέτρα ασφαλούς επικοινωνίας και δικτύωσης, όπως ορίζονται στο μέτρο [NS4].
3	3	Διασφαλίζεται η επαρκή προστασία των κινητών συσκευών και των πληροφοριών που διατηρούνται σε κινητές συσκευές έναντι κλοπής και απώλειας.
3	4	Αλλαγές στις συσκευές υλοποιούνται από εξουσιοδοτημένους χρήστες σύμφωνα με την διαδικασία [IAM1].
4	1	Εφαρμόζεται σύστημα για την διαχείριση φορητών συσκευών (MDM). Η παραμετροποίηση του MDM δίνει στον οργανισμό την δυνατότητα: να αναγνωρίζει την συσκευή, την τοποθεσία της συσκευής, τον αναγνωρισμένο χρήστη της συσκευής, να εφαρμόζει τις πολιτικές του οργανισμού σε σχέση με την ασφάλεια (αποθήκευση δεδομένων, κρυπτογράφηση, δυνατότητα διασύνδεσης, επιτρεπόμενο λογισμικό, επιτρεπόμενα πρωτόκολλα, υπηρεσίες και θύρες και να διενεργεί άμεσες ενέργειες ασφαλούς διαγραφής σε περίπτωση που αυτό κρίνεται απαραίτητο.
4	2	Υπάρχει σχετική συμμόρφωση της συγκεκριμένης πρακτικής με την κείμενη νομοθεσία και κανονισμούς για την προστασία δεδομένων προσωπικού χαρακτήρα.

4	3	Όπου απαιτείται για την αποτελεσματική λειτουργία του οργανισμού δίνεται η απο απόσταση ανάθεση προνομιακών δικαιωμάτων και στην οποία εφαρμόζονται τεχνικά μέτρα (οι συγκεκριμένες εφαρμογές στηρίζονται σε ένα event based authorization χωρίς να υπάρχει αποκάλυψη προνομιακών κωδικών πρόσβασης σε μη εξουσιοδοτημένες οντότητες).
4	4	Η εξ αποστάσεως δυνατότητα καθορίζει και εντοπίζει τη γεωγραφικής θέση.
4	5	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Έχει διενεργηθεί ανάλυση και έχουν προσδιορισθεί οι κατασκευαστές και οι συσκευές που προμηθεύονται και χρησιμοποιούνται στον οργανισμό.
5	2	Όπου είναι εφικτό, διενεργούνται σχετικές επικοινωνίες με τις εν λόγω εταιρίες ώστε η προμήθεια των συσκευών να γίνεται με secure out-of-the box configuration (προ παραμετροποιημένο λαμβάνοντας υπόψη τις απαιτήσεις ασφαλείας).
5	3	Διενεργούνται σε τακτική βάση έλεγχοι για την συμμόρφωση των φορητών συσκευών προς τις απαιτήσεις του οργανισμού.
5	4	Διενεργούνται έλεγχοι και δοκιμές για τον προσδιορισμό της αποτελεσματικότητας των εφαρμοζόμενων μέτρων ανά περίπτωση. Σε περίπτωση απόκλισης λαμβάνονται άμεσες ενέργειες οι οποίες διαχειρίζονται μέσα από την διαδικασία διαχείρισης αλλαγών ή αντιμετώπισης περιστατικών ασφαλείας όπως απαιτείται.
5	5	Κάθε νέο μέσο ή στοιχείο, κρυπτογραφείται με αυτοματοποιημένο τρόπο όπου αυτό είναι δυνατό, πριν ή κατά την εισαγωγή του στον οργανισμό.
5	6	Για την διαγραφή δεδομένων, σε περίπτωση που αυτή υλοποιείται μέσω λογισμικού, χρησιμοποιούνται επιπλέον μέτρα σε φυσικό επίπεδο (π.χ. degaussing). (όπως προβλέπεται στο [DS1]).
5	7	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	8	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
SS4		**Μέτρο:** Διαχείριση διαμόρφωσης εφαρμογών **Στόχος Μέτρου:** Να διασφαλιστεί η κατάλληλη διαχείριση των εφαρμογών που χρησιμοποιούνται για την πρόσβαση ή επεξεργασία οργανωτικών πόρων. **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση μέτρων διαχείρισης της διαμόρφωσης εφαρμογών με σκοπό την πρόληψη της μη επιτρεπόμενης και κακόβουλης εγκατάστασης, της διαμόρφωσης ή της τροποποίησης εφαρμογών και του λογισμικού σε οργανωτικά στοιχεία και συσκευές. Ο οργανισμός πρέπει να εξετάσει το ενδεχόμενο δημιουργίας κεντρικής διεπαφής για τη διαχείριση και διαμόρφωση εφαρμογών ώστε να εξασφαλίζεται ότι όλες οι οργανωτικές συσκευές υπόκεινται σε κεντρική διαχείριση, ενώ η διαμόρφωση και οι ενημερώσεις λογισμικού μπορούν να προωθηθούν στις τελικές συσκευές. Αυτή η κεντρική διεπαφή διαχείρισης πρέπει να επιτρέπει στον οργανισμό να θεσπίζει κατάλογο ορισμένων επιτρεπόμενων ή μη επιτρεπόμενων τύπων εφαρμογών. **Πηγή:**
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**
0	1	Ο οργανισμός δεν εφαρμόζει κάποια μέτρα ή έλεγχο για την εγκατάσταση εφαρμογών.
1	1	Εφαρμόζονται κάποια μέτρα για την εγκατάσταση εφαρμογών στα κρίσιμα συστήματα όπως είναι οι servers.
1	2	Τα μέτρα επιλέγονται και εφαρμόζονται σε ad-hoc βάση.
2	1	Για τα κρίσιμα στοιχεία ενεργητικού, όπως αυτά αποτυπώνονται στον σχετικό κατάλογο [AM2 / RM2], έχει ενεργοποιηθεί παρακολούθηση.

2	2	Έχει δημιουργηθεί μια πολιτική ελέγχου πρόσβασης η οποία καλύπτει όλα τα στοιχεία ενεργητικού και τα κτήρια του οργανισμού όπως εμφανίζονται στον ενιαίο κατάλογο στοιχείων ενεργητικού σύμφωνα με το [AM2].
2	3	Δεν υπάρχει η δυνατότητα σε όλους τους χρήστες να κάνουν αλλαγές ή να εγκαθιστούν λογισμικού σε κρίσιμα συστήματα του οργανισμού.
3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται μέτρα διαχείρισης της διαμόρφωσης εφαρμογών με σκοπό την πρόληψη της μη επιτρεπόμενης και κακόβουλης εγκατάστασης, της διαμόρφωσης ή της τροποποίησης εφαρμογών και του λογισμικού σε οργανωτικά στοιχεία και συσκευές.
3	2	Για κάθε στοιχείο λογισμικού έχει αναγνωριστεί ιδιοκτήτης ο οποίος σε συνεργασία με το λοιπό τεχνικό προσωπικό, προσδιορίζει τους ρόλους για τους οποίους απαιτείται πρόσβαση (στο λογισμικό) καθώς και το επίπεδο της πρόσβασης.
3	3	Αλλαγές στις συσκευές υλοποιούνται από εξουσιοδοτημένους χρήστες σύμφωνα με την διαδικασία [IAM1].
4	1	Έχει δημιουργηθεί κεντρική διεπαφή για τη διαχείριση και διαμόρφωση εφαρμογών ώστε να εξασφαλίζεται ότι όλες οι οργανωτικές συσκευές υπόκεινται σε κεντρική διαχείριση, ενώ η διαμόρφωση και οι ενημερώσεις λογισμικού μπορούν να προωθηθούν στις τελικές συσκευές.
4	2	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Τηρείται και εφαρμόζεται λίστα με επιτρεπόμενο λογισμικό για κάθε περίπτωση λογισμικού που αναγνωρισμένα υποστηρίζει τις επιχειρησιακές λειτουργίες του οργανισμού μέσω της κεντρικής διεπαφή διαχείρισης.
5	2	Για κάθε λογισμικό (περιλαμβανομένου και του λειτουργικού) έχουν αναγνωριστεί και καταγραφεί οι επιτρεπτές εκδόσεις σε συμφωνία με τους στόχους του οργανισμού και τον σχετικό κίνδυνο.
5	3	Τηρούνται λίστες και μέτρα για τα επιτρεπόμενα components λογισμικού.
5	4	Διενεργούνται τακτικοί έλεγχοι για τον έλεγχο της συμμόρφωσης της παραμετροποίησης και της λειτουργίας των στοιχείων προς τις αναγνωρισμένες βέλτιστες πρακτικές θωράκισης.
5	5	Όπου απαιτείται τα μέτρα που λαμβάνονται είναι άμεσα και διαχειρίζονται μέσα από την διαδικασία διαχείρισης αλλαγών ή / και την διαχείριση περιστατικών ασφαλείας όπως απαιτείται.
5	6	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	7	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

Κατηγορία		ΑΣΦΑΛΕΙΑ ΕΦΑΡΜΟΓΩΝ
AS1		**Μέτρο:** Ασφαλής κύκλος ζωής ανάπτυξης λογισμικού **Στόχος Μέτρου:** Να διασφαλιστούν επαρκή μέτρα ασφάλειας στο πλαίσιο των δραστηριοτήτων ανάπτυξης λογισμικού που αναπτύσσει ο οργανισμός **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση ασφαλών πρακτικών ανάπτυξης λογισμικού σε παραδοσιακές διαδικασίες κύκλου ζωής ανάπτυξης λογισμικού, ώστε να διασφαλίζεται ότι η ασφάλεια είναι ενσωματωμένη στο σχεδιασμό στο πλαίσιο των δραστηριοτήτων ανάπτυξης εφαρμογών και λογισμικού. Ο οργανισμός πρέπει να εξετάσει το ενδεχόμενο εφαρμογής, τουλάχιστον, μιας αξιολόγησης κινδύνου στο αρχικό στάδιο του έργου, διενέργειας δοκιμών ασφάλειας και εξέτασης κώδικα στα στάδια ανάπτυξης του έργου, και διενέργεια αξιολόγησης ασφάλειας και ασφαλούς διαμόρφωσης στην παράδοση του έργου. Ο οργανισμός πρέπει να διασφαλίζει ότι εφαρμόζονται κατάλληλα μέτρα για τον διαχωρισμό των περιβαλλόντων ανάπτυξης λογισμικού από το επιχειρησιακό περιβάλλον παραγωγής. Ο οργανισμός διασφαλίζει ότι τα δεδομένα που χρησιμοποιούνται για τη διενέργεια δοκιμών είναι ανώνυμα και δεν συνδέονται με εμπιστευτικές και ευαίσθητες πληροφορίες στο πλαίσιο αναπτυξιακών δραστηριοτήτων. **Πηγή:**
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**
0	1	Ο οργανισμός δεν λαμβάνει μέτρα για την ασφαλή ανάπτυξη λογισμικού.
1	1	Κατά την ανάπτυξη λογισμικού τίθονται περιοδικά και όχι με συστηματικό τρόπο κάποιες προδιαγραφές ασφαλείας και κάποιες σχετικές δοκιμές.
2	1	Δημιουργείται χωριστό έργο (project) για ανάπτυξη λογισμικού που πρέπει να διενεργηθεί (όχι για κάθε component αλλά για κάθε έργο).
2	2	Έχει δημιουργηθεί μια διαδικασία διαχείρισης του κύκλου ανάπτυξης λογισμικού (SDLC).
2	3	Στα αρχικά βήματα του κύκλου ζωής, περιλαμβάνεται η αναγνώριση απαιτήσεων ασφαλείας.
2	4	Στα τελευταία βήματα της ανάπτυξης και πριν την εφαρμογή στην παραγωγή έχουν προβλεφθεί και γίνονται δοκιμές για την αποδοχή του συστήματος έναντι των κριτηρίων και απαιτήσεων ποιότητας, λειτουργικότητας και ασφάλειας.
3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται ασφαλείς πρακτικές ανάπτυξης λογισμικού σε παραδοσιακές διαδικασίες κύκλου ζωής ανάπτυξης λογισμικού, ώστε να διασφαλίζεται ότι η ασφάλεια είναι ενσωματωμένη στο σχεδιασμό στο πλαίσιο των δραστηριοτήτων ανάπτυξης εφαρμογών και λογισμικού.
3	2	Εφαρμόζονται κατάλληλα μέτρα για τον διαχωρισμό των περιβαλλόντων ανάπτυξης λογισμικού από το επιχειρησιακό περιβάλλον παραγωγής.
3	3	Τα δεδομένα που χρησιμοποιούνται για τη διενέργεια δοκιμών είναι ανώνυμα και δεν συνδέονται με εμπιστευτικές και ευαίσθητες πληροφορίες στο πλαίσιο αναπτυξιακών δραστηριοτήτων.
3	4	Στη περίπτωση που η ανάπτυξη εφαρμογών δίνεται σε τρίτα μέρη, δίνονται τουλάχιστον προδιαγραφές ασφαλείας που χρειάζεται να ικανοποιεί η εφαρμογή και ζητούνται επαρκείς εγγυήσεις, διαβεβαιώσεις και στοιχεία ότι καλύπτονται πριν την αποδοχή ή την λειτουργία τους.
3	5	Έχει δημιουργηθεί μια σειρά από οδηγίες (υποχρεωτικής εφαρμογής) για την ασφαλή ανάπτυξη λογισμικού. Οι οδηγίες είναι εξειδικευμένες ανά γλώσσα ή περιβάλλον ανάπτυξης και είναι σύμφωνες με τις διεθνείς βέλτιστες πρακτικές και τις οδηγίες του αντίστοιχου vendor.
3	6	Διενεργείται risk assessment ή threat profiling κατά τη διάρκεια του σχεδιασμού ενός λογισμικού. Κατάλληλα μέτρα ασφαλείας ενσωματώνονται στην εφαρμογή σύμφωνα με τα αποτελέσματα των διαδικασιών αυτών.
3	7	Αλλαγές στο λογισμικό ελέγχονται μέσα από την διαδικασία διαχείρισης αλλαγών [CM1].
3	8	Δεξιότητες και γνώσεις σχετικά με την ασφαλή ανάπτυξη λογισμικού αναγνωρίζονται στις σχετικές θέσεις εργασίας ως προαπαιτούμενο.

3	9	Έχουν ενταχθεί απαιτήσεις για ασφάλεια και ιδωτικότητα από προεπιλογή και από σχεδιασμό σύμφωνα με τις απαιτήσεις κανονισμών, νομοθεσίας και βέλτιστων σχετικών πρακτικών.
4	1	Διενεργείται, τουλάχιστον, μια αξιολόγηση κινδύνου στο αρχικό στάδιο του έργου, δοκιμές ασφάλειας και εξέταση κώδικα στα στάδια ανάπτυξης του έργου, και αξιολόγηση ασφάλειας και ασφαλούς διαμόρφωσης στην παράδοση του έργου.
4	2	Στην εκκίνηση του σχεδιασμού το περιβάλλον καθορίζεται το περιβάλλον στο οποίο γίνεται η ανάπτυξη.
4	3	Το περιβάλλον καθορίζεται σύμφωνα με τις απαιτήσεις ασφαλείας του λογισμικού προς ανάπτυξη αλλά και την προσδοκώμενη χρήση του (intended use).
4	4	Το περιβάλλον ανάπτυξης αποτελείται από την γλώσσα προγραμματισμού, το χρησιμοποιούμενο framework, τα εργαλεία ανάπτυξης, τα εργαλεία δοκιμών και τα εργαλεία διαχείρισης και αποθήκευσης του κώδικα. Σε κάθε περίπτωση επιλέγεται και η έκδοση των εν λόγω στοιχείων, λαμβάνοντας υπόψη τις δυνατότητες αλλά και τις ανοιχτές αδυναμίες σύμφωνα με έγκυρες σχετικές πηγές.
4	5	Τα αποτελέσματα των δοκιμών διατηρούνται και ενεργοποιούν και διαδικασίες διόρθωσης όπως απαιτείται σύμφωνα με την διαδικασία διαχείρισης αλλαγών [CM1].
4	6	Υπάρχει πλήρης διαχωρισμός καθηκόντων ανάμεσα στο προσωπικό το οποίο διενεργεί την ανάπτυξη, το προσωπικό που διενεργεί τις δοκιμές και το προσωπικό που είναι υπεύθυνο για την παραγωγική λειτουργία των συστημάτων.
4	7	Στη περίπτωση που το λογισμικό λαμβάνεται από τρίτο μέρος, εξετάζεται ότι η διαδικασία ανάπτυξης καλύπτει τις απαιτήσεις που θα είχε ο οργανισμός αν υλοποιούσε μόνος του την ανάπτυξη. Επίσης, εξετάζεται η ιστορικότητα (σε σχέση με περιστατικά, με ενημερώσεις, με ανοιχτές ευπάθειες) του τρίτου μέρους και οι διαδικασίες για ανταπόκριση σε αναγνωρισμένες ευπάθειες.
4	8	Αντίστοιχες διαδικασίες και οδηγίες υπάρχουν και για διαφορετικού είδους λογισμικά όπως είναι εφαρμογές, βάσεις δεδομένων κ.α.
4	9	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Εντάσσονται αυτόματα εργαλεία για static analysis του κώδικα σε επίπεδο ασφάλειας κατά την ανάπτυξη του λογισμικού.
5	2	Διενεργούνται συγκεκριμένα τεστ, τα οποία γίνονται σε κάθε περίπτωση ανάπτυξης ή αλλαγής με αυτόματους ή ημιαυτόματους τρόπους με την χρήση κατάλληλων εργαλείων. Ειδικά για κρίσιμα συστήματα και πριν την ενσωμάτωση νέου λογισμικού ή αλλαγής, γίνεται ανάλυση σε επίπεδο ασφάλειας (π.χ. δοκιμές ανάλυσης κώδικα για ανίχνευση παράνομων διεργασιών μέσα σε ελεγχόμενο περιβάλλον κ.α.)
5	3	Σε περίπτωση που είναι εφικτό, ο οργανισμόςδέχεται εξωτερικό έλεγχο ή και πιστοποίηση από ανεξάρτητο εργαστήριο για την ασφάλεια του λογισμικού, πριν την εφαρμογή στην παραγωγή και χρήση του.
5	4	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	5	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

Κατηγορία		ΑΣΦΑΛΕΙΑ ΑΝΘΡΩΠΙΝΩΝ ΠΟΡΩΝ
HRS1		**Μέτρο:** Κύκλος ζωής της εργοδότησης **Στόχος Μέτρου:** Να υλοποιούνται επαρκή μέτρα για την εξασφάλιση ότι τα στελέχη που εργάζονται για λογαριασμό του οργανισμού, τα οποία έχουν πρόσβαση σε οργανωτικούς πόρους, υποστηρίζουν την πολιτική ασφάλειας πληροφοριών και τους στόχους του οργανισμού. **Περιγραφή Μέτρου:** Κατάρτιση, εφαρμογή και διατήρηση σχεδίου για να διασφαλιστεί ότι η ασφάλεια πληροφοριών είναι ενσωματωμένη καθ' όλη τη διάρκεια του κύκλου ζωής της εργοδότησης (δηλαδή πριν, κατά τη διάρκεια και μετά την εργοδότηση των εργαζομένων) και να καταβάλει κάθε εύλογη προσπάθεια προκειμένου να διασφαλίσει ότι οι εργαζόμενοι κατανοούν τις ευθύνες τους σε σχέση με την ασφάλεια πληροφοριών. Το σχέδιο περιλαμβάνει κατάλληλα μέτρα ασφάλειας πληροφοριών σε κάθε φάση της εργοδότησης, π.χ. έλεγχοι ιστορικού πριν την πρόσληψη, κατάρτιση και ευαισθητοποίηση των εργαζομένων, ενσωμάτωση επαρκών προνοιών στις συμβάσεις εργασίας, κατάρτιση πολιτικής αποδεκτή ς χρήσης, επιστροφή των συσκευών των εργαζομένων που περιέχουν κρίσιμες πληροφορίες, και αφαίρεση της πρόσβασης σε συστήματα και εφαρμογές σύμφωνα με τον κύκλο ζωής της διαχείρισης ταυτότητας, όπως ορίζεται στο μέτρο [IAM7]. **Πηγή:** 27002, PNNL
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**
0	1	Ο οργανισμός δεν λαμβάνει μέτρα ώστε να διασφαλίσει ότι η ασφάλεια πληροφοριών είναι ενσωματωμένη καθ' όλη τη διάρκεια του κύκλου ζωής της εργοδότησης.
1	1	Διενεργείται επαλήθευση των υποχρεωτικών ακαδημαϊκών και επαγγελματικών προσόντων μέσω της λήψης και της εξέτασης των σχετικών εγγράφων.
1	2	Τα αποτελέσματα του ελέγχου τα οποία αφορούν προσωπικά δεδομένα, προστατεύονται σύμφωνα με το υψηλότερο επίπεδο ταξινόμησης.
2	1	Διενεργούνται έλεγχοι ιστορικού για βασικό προσωπικό και εξωτερικούς εργολάβους, όταν χρειάζεται και επιτρέπεται από το νόμο.
2	2	Ζητούνται σχετικές αναφορές που επαληθεύουν την ύπαρξη των επιθυμητών χαρακτηριστικών που έχει δηλώσει ο υποψήφιος.
2	3	Έχει θεσπιστεί μία βασική διαδικασία σχετικά με τον έλεγχο ιστορικού για τους υποψήφιους υπαλλήλους.
3	1	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται μια διαδικασία που διασφαλίζει ότι η ασφάλεια πληροφοριών είναι ενσωματωμένη καθ' όλη τη διάρκεια του κύκλου ζωής της εργοδότησης και καταβάλει κάθε εύλογη προσπάθεια προκειμένου να διασφαλίσει ότι οι εργαζόμενοι κατανοούν τις ευθύνες τους σε σχέση με την ασφάλεια πληροφοριών.
3	2	Η διαδικασία περιλαμβάνει κατάλληλα μέτρα ασφάλειας πληροφοριών σε κάθε φάση της εργοδότησης, π.χ. έλεγχοι ιστορικού πριν την πρόσληψη, κατάρτιση και ευαισθητοποίηση τους.
4	1	Έχει θεσπιστεί διαδικασία ελέγχων επαλήθευσης που περιγράφει λεπτομερώς τα κριτήρια και τους περιορισμούς για τους ελέγχους επαλήθευσης, π.χ. ποιος είναι κατάλληλος για τον έλεγχο ατόμων και πώς, πότε και γιατί διενεργούνται έλεγχοι επαλήθευσης.
4	2	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Υπάρχει συνεργασία με τρίτο μέρος το οποίο έχει αναλάβει να υλοποιεί τους ελέγχους ιστορικού και σύμφωνα με τις απαιτήσεις της σχετικής νομοθεσίας.
5	2	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	3	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

HRS2		**Μέτρο:** Παρακολούθηση εργαζομένων **Στόχος Μέτρου:** Να εξασφαλιστεί ότι τα στελέχη που εργάζονται για λογαριασμό του οργανισμού συμμορφώνονται με την πολιτική ασφάλειας πληροφοριών και τηρούν τις ευθύνες ασφάλειας τους καθ' όλη τη διάρκεια του κύκλου ζωής της απασχόλησης. **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση σχεδίου για την παρακολούθηση της συμμόρφωσης των εργαζομένων με τις υποχρεώσεις και τις ευθύνες τους όσον αφορά την ασφάλεια πληροφοριών, καθ' όλη τη διάρκεια του κύκλου ζωής της απασχόλησης. **Πηγή:**
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**
0	1	Ο οργανισμός δεν εφαρμόζει μέτρα σχετικά με την παρακολούθηση της συμμόρφωσης των εργαζομένων με τις υποχρεώσεις και τις ευθύνες τους όσον αφορά την ασφάλεια πληροφοριών, καθ' όλη τη διάρκεια του κύκλου ζωής της απασχόλησης.
1	1	Είναι δυνατό και αναγνωρίζεται ότι υπάρχει κάποια μη συμμόρφωση προσωπικού σε σχέση με πολιτικές, διαδικασίες ή μέτρα κατά τη διάρκεια σχετικής διερεύνησης περιστατικού ασφαλείας.
2	1	Έχει γίνει καταγραφή των ρόλων και αρμοδιοτήτων και έχουν ανατεθεί στο αντίστοιχο προσωπικό.
2	2	Το προσωπικό έχει ενημερωθεί σχετικά με τις σχετικές υποχρεώσεις του.
2	3	Γίνονται κάποιοι έλεγχοι ad-hoc για τον έλεγχο της συμμόρφωσης του προσωπικού προς τις σχετικές υποχρεώσεις.
3	1	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται διαδικασία για την παρακολούθηση της συμμόρφωσης των εργαζομένων με τις υποχρεώσεις και τις ευθύνες τους όσον αφορά την ασφάλεια πληροφοριών, καθ' όλη τη διάρκεια του κύκλου ζωής της απασχόλησης.
3	2	Σχετικοί έλεγχοι περιλαμβάνουν και δοκιμές που σχετίζονται με τον έλεγχο της αποτελεσματικότητας της εκπαίδευσης του προσωπικού όπως αναφέρεται στο [DS5] και [SS1].
4	1	Έχουν δημιουργηθεί συγκεκριμένα πλάνα ελέγχου (εσωτερικά και εξωτερικά) που περιλαμβάνουν (στο πεδίο εφαρμογής τους) και ελέγχους συμμόρφωσης του προσωπικού προς τις πολιτικές, διαδικασίες και μέτρα ασφαλείας του οργανισμού.
4	2	Τα στοιχεία των ελέγχων αναλύονται και εξάγονται συμπεράσματα για την συμμόρφωση του ανθρώπινου δυναμικού προς τις σχετικές απαιτήσεις. Σε περίπτωση που έχει αναγνωριστεί κάποια απόκλιση, γίνεται ενεργοποίηση της διαδικασίας ανταπόκρισης περιστατικών ασφαλείας [EIM1] και την διαδικασία για τα πειθαρχικά μέτρα [HRS3].
4	3	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Έχουν εφαρμοστεί αυτοματοποιημένα μέτρα για τον έλεγχο της συμμόρφωσης του προσωπικού με τις πολιτικές, διαδικασίες και μέτρα ασφαλείας του οργανισμού (όπου είναι αυτό εφικτό). (π.χ. υλοποίηση MDM για την διαχείριση και εφαρμογή πολιτικών στις κινητές συσκευές, υλοποίηση DLP για τον έλεγχο της διαχείρισης της πληροφορίας εντός του οργανισμού, παρακολούθηση και καταγραφή ενεργειών – logs τα οποία συγκεντρώνονται και αναλύονται κ.α.).
5	2	Τα στοιχεία από τα αυτοματοποιημένα εργαλεία, καθώς και τα στοιχεία των άλλων ελέγχων που προβλέπονται αναλύονται και εξάγονται συμπεράσματα για την συμμόρφωση του ανθρώπινου δυναμικού προς τις σχετικές απαιτήσεις. Σε περίπτωση που έχει αναγνωριστεί κάποια απόκλιση, γίνεται ενεργοποίηση της διαδικασίας ανταπόκρισης περιστατικών ασφαλείας [EIM1] και την διαδικασία για τα πειθαρχικά μέτρα [HRS3].
5	3	Συλλέγονται στοιχεία για την συμμόρφωση του προσωπικού προς τις απαιτήσεις και προδιαγραφές των διαδικασιών και των πολιτικών του οργανισμού σε συμφωνία με την κείμενη νομοθεσία.
5	4	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.

5	5	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
HRS3		**Μέτρο:** Πειθαρχικά μέτρα και επιβολή **Στόχος Μέτρου:** Να εξασφαλιστεί ότι τα στελέχη που εργάζονται για λογαριασμό του οργανισμού, είναι υπεύθυνα για τις εκούσιες ή ακούσιες δραστηριότητες που επηρεάζουν τους στόχους ασφάλειας πληροφοριών του οργανισμού. **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση σειράς πειθαρχικών μέτρων προκειμένου να διασφαλιστεί η συμμόρφωση των στελεχών με τις υποχρεώσεις και τις ευθύνες τους όσον αφορά την ασφάλεια πληροφοριών και την ανάληψη δράσης σε περίπτωση παραβίασης των υποχρεώσεων και των ευθυνών αυτών. Ο οργανισμός πρέπει να εξετάσει το ενδεχόμενο θέσπισης επίσημης διαδικασίας επιβολής κυρώσεων για στελέχη που δεν συμμορφώνονται με τις υποχρεώσεις και τις ευθύνες τους στον τομέα της ασφάλειας πληροφοριών. Η μη συμμόρφωση με τις υποχρεώσεις και τις ευθύνες όσον αφορά την ασφάλεια πληροφοριών εντοπίζεται μέσω των διαδικασιών παρακολούθησης των εργαζομένων [HRS2]. **Πηγή:** 27002
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**
0	1	Ο οργανισμός δεν υλοποιεί μέτρα και δεν έχει δημιουργήσει διαδικασία επιβολής κυρώσεων προκειμένου να διασφαλιστεί η συμμόρφωση των στελεχών με τις υποχρεώσεις και τις ευθύνες τους όσον αφορά την ασφάλεια πληροφοριών και την ανάληψη δράσης σε περίπτωση παραβίασης των υποχρεώσεων και των ευθυνών αυτών.
1	1	Στις περιπτώσεις πειθαρχικού παραπτώματος σε σχέση με την ασφάλεια πληροφοριών, το εμπλεκόμενο προσωπικό απομακρύνεται χωρίς να υπάρχει κάποια διαδικασία καταγεγραμμένη και κοινοποιημένη.
2	1	Έχει θεσπίστει πειθαρχική διαδικασία για τη λήψη μέτρων κατά των εργαζομένων που έχουν διαπράξει παραβίαση της ασφάλειας των πληροφοριών.
2	2	Η διαδικασία δεν έχει κοινοποιηθεί στο σύνολο του προσωπικού.
3	1	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται σειρά πειθαρχικών μέτρων μέσω πειθαρχικής διαδικασίας προκειμένου να διασφαλιστεί η συμμόρφωση των στελεχών με τις υποχρεώσεις και τις ευθύνες τους όσον αφορά την ασφάλεια πληροφοριών και την ανάληψη δράσης σε περίπτωση παραβίασης των υποχρεώσεων και των ευθυνών αυτών.
3	2	Η πειθαρχική διαδικασία διασφαλίζει τη σωστή και δίκαιη μεταχείριση των εργαζομένων που είναι ύποπτοι για παραβιάσεις της ασφάλειας των πληροφοριών.
3	3	Η πειθαρχική διαδικασία προβλέπει μια σταδιακή απάντηση που λαμβάνει υπόψη παράγοντες όπως η φύση και η σοβαρότητα της παράβασης και ο αντίκτυπός της στην επιχείρηση, είτε πρόκειται για πρώτο ή επαναλαμβανόμενο παράπτωμα είτε όχι, είτε ο παραβάτης ήταν κατάλληλα εκπαιδευμένος είτε όχι, σχετική νομοθεσία, επιχειρηματικές συμβάσεις και άλλους παράγοντες όπως απαιτείται.
3	4	Έχει κοινοποιηθεί η πειθαρχική διαδικασία στο σύνολο του προσωπικού.
3	4	Έχει εξεταστεί το ενδεχόμενο θέσπισης επίσημης διαδικασίας επιβολής κυρώσεων για στελέχη που δεν συμμορφώνονται με τις υποχρεώσεις και τις ευθύνες τους στον τομέα της ασφάλειας πληροφοριών.
3	5	Η μη συμμόρφωση με τις υποχρεώσεις και τις ευθύνες όσον αφορά την ασφάλεια πληροφοριών εντοπίζεται μέσω των διαδικασιών παρακολούθησης των εργαζομένων [HRS2].
4	1	Έχει θεσπίστει επίσημη διαδικασία επιβολής κυρώσεων για στελέχη που δεν συμμορφώνονται με τις υποχρεώσεις και τις ευθύνες τους στον τομέα της ασφάλειας πληροφοριών.
4	2	Η μη συμμόρφωση με τις υποχρεώσεις και τις ευθύνες όσον αφορά την ασφάλεια πληροφοριών εντοπίζεται μέσω των διαδικασιών παρακολούθησης των εργαζομένων [HRS2].
4	3	Η διαδικασία επιβολής κυρώσεων έχει κοινοποιηθεί στο σύνολο του προσωπικού του οργανισμού.

4	4	Η πειθαρχική διαδικασία περιλαμβάνει επίσης θετικές κυρώσεις για αξιοσημείωτη συμπεριφορά όσον αφορά την ασφάλεια των πληροφοριών.
4	5	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Συλλέγονται στοιχεία για την συμμόρφωση του προσωπικού προς τις απαιτήσεις και προδιαγραφές των διαδικασιών και των πολιτικών του οργανισμού σε συμφωνία με την κείμενη νομοθεσία.
5	2	Τα στοιχεία της παρακολούθησης όπως αναφέρεται στο [HRS2] ενεργοποιούν την διαδικασία των πειθαρχικών μέτρων.
5	3	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	4	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
HRS4		**Μέτρο:** Εξωτερικοί συνεργάτες **Στόχος Μέτρου:** Να εξασφαλιστεί ότι οι εξωτερικοί συνεργάτες που εργάζονται για λογαριασμό του οργανισμού τηρούν την πολιτική ασφάλειας πληροφοριών και τους στόχους ασφάλειας του οργανισμού. **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση μέτρων για την ασφάλεια πληροφοριών σε σχέση με το εξωτερικό εργατικό δυναμικό, π.χ. με τους αναδόχους συμβάσεων, προκειμένου να διασφαλίζεται η δέουσα προστασία των πληροφοριών που ανταλλάσσονται με εξωτερικούς συνεργάτες. **Πηγή:** 27002
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**
0	1	Ο οργανισμός δεν έχει θεσπίσει και δεν εφαρμόζει μέτρα για την ασφάλεια πληροφοριών σε σχέση με το εξωτερικό εργατικό δυναμικό.
1	1	Στους εξωτερικούς συνεργάτες αναφέρονται βασικά μέτρα σε σχέση με την ασφάλεια πληροφοριών που δεν αποτυπώνονται σε συμβάσεις μεταξύ των 2 μερών.
2	1	Περιλαμβάνονται μέτρα στις συμβατικές συμφωνίες με βασικά εξωτερικά μέρη και όχι στο σύνολο, σε σχέση με την ασφάλεια πληροφοριών.
2	2	Στις συμβατικές συμφωνίες περιέχονται οι νομικές ευθύνες και δικαιώματα του αναδόχου, π.χ. σχετικά με τους νόμους περί πνευματικών δικαιωμάτων ή τη νομοθεσία περί προστασίας δεδομένων.
3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται για την ασφάλεια πληροφοριών σε σχέση με το εξωτερικό εργατικό δυναμικό προκειμένου να διασφαλίζεται η δέουσα προστασία των πληροφοριών που ανταλλάσσονται με εξωτερικούς συνεργάτες.
3	2	Στις συμβατικές συμφωνίες υπάρχει σχετικό παράρτημα που ενημερώνει τους εξωτερικούς συνεργάτες σχετικά με την πολιτική ασφάλειας πληροφοριών του οργανισμού και την υποχρέωση για την τήρηση αυτής.
3	3	Ο οργανισμός συνάπτει συμβατική συμφωνία με το εκάστοτε εξωτερικό εργατικό δυναμικό που περιλαμβάνει μέτρα σε σχέση με την ασφάλεια πληροφοριών.
3	4	Οι συμβατικές συμφωνίες περιέχουν μια σαφή δήλωση ότι όλοι οι εργολάβοι στους οποίους παρέχεται πρόσβαση σε εμπιστευτικές πληροφορίες υπογράφουν συμφωνία εμπιστευτικότητας ή μη αποκάλυψης προτού τους δοθεί πρόσβαση σε εγκαταστάσεις επεξεργασίας πληροφοριών. Το NDA θα μπορούσε να είναι μέρος της συμβατικής συμφωνίας.
3	5	Η συμβατική συμφωνία περιλαμβάνει τις ευθύνες για την ταξινόμηση των πληροφοριών και τη διαχείριση οργανωτικών περιουσιακών στοιχείων που σχετίζονται με πληροφορίες, εγκαταστάσεις επεξεργασίας πληροφοριών και υπηρεσίες πληροφοριών που διαχειρίζεται ο ανάδοχος, καθώς και τις ευθύνες του αναδόχου για τη διαχείριση πληροφοριών που λαμβάνονται από άλλες εταιρείες ή εξωτερικά μέρη.

4	1	Έχει θεσπιστεί συγκεκριμένη διαδικασία σε σχέση με το εξωτερικό εργατικό δυναμικό.
4	2	Η συμβατική συμφωνία περιέχει ενέργειες που πρέπει να γίνουν εάν ο ανάδοχος αγνοήσει τις απαιτήσεις ασφάλειας του οργανισμού.
4	3	Στις συμβατικές συμφωνίες υπάρχει σχετικό παράρτημα που ενημερώνει τους εξωτερικούς συνεργάτες σχετικά με τους στόχους ασφάλειας του οργανισμού και την υποχρέωση για την τήρηση τους.
4	4	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Ένας κώδικας δεοντολογίας χρησιμοποιείται για να δηλώσει τις ευθύνες ασφάλειας πληροφοριών του αναδόχου σχετικά με το απόρρητο, την προστασία δεδομένων, τη δεοντολογία, την κατάλληλη χρήση του εξοπλισμού και των εγκαταστάσεων του οργανισμού, καθώς και αξιόπιστες πρακτικές που αναμένει ο οργανισμός. Ένα εξωτερικό μέρος, με το οποίο συνδέεται ένας ανάδοχος, μπορεί να κληθεί να συνάψει συμβατικές ρυθμίσεις για λογαριασμό του συμβαλλόμενου ατόμου.
5	2	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	3	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
HRS5		**Μέτρο:** Προστασία από απειλές που προέρχονται από εσωτερικά πρόσωπα **Στόχος Μέτρου:** Να εξασφαλιστεί η προστασία από απειλές κατά της ασφάλειας δικτύων και πληροφοριών από το εσωτερικό του οργανισμού. **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση κατάλληλων μέτρων για την πρόληψη, τον εντοπισμό και την παρακολούθηση των επιθέσεων από εσωτερικά πρόσωπα, από άγνοια, αμέλεια, ή κακόβουλες ή επαγγελματικές προθέσεις. Ο οργανισμός πρέπει να εκπαιδεύει και να ευαισθητοποιεί τους εργαζόμενους σχετικά με τις πρακτικές ασφάλειας των πληροφοριών εντός του οργανισμού, σύμφωνα με το μέτρο [TA2], να διενεργεί επαρκή έλεγχο των υποψηφίων σύμφωνα με το μέτρο [HRS1], και να παρακολουθεί τους εργαζόμενους [HRS2], ώστε να μειώνεται η πιθανότητα να υπάρξουν εσωτερικές επιθέσεις. **Πηγή:**
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**
0	1	Ο οργανισμός δεν παίρνει κάποιο μέτρο για την προστασία από απειλές που προέρχονται από εσωτερικά πρόσωπα.
1	1	Όπου υπάρχει κάποια μη συμμόρφωση προσωπικού σε σχέση με πολιτικές, διαδικασίες ή μέτρα κατά τη διάρκεια σχετικής διερεύνησης περιστατικού ασφαλείας, αυτή αναγνωρίζεται. Σε αυτή την περίπτωση λαμβάνονται μέτρα για την ανταπόκριση στο συγκεκριμένο περιστατικό.
1	2	Διενεργείται, σε ad hoc βάση, ή έχει τουλάχιστον μια φορά κατά τα τελευταία 2 χρόνια διενεργηθεί αναγνώριση κινδύνων σχετικά με την ασφάλεια των πληροφοριών και των δικτύων.
1	3	Η διαδικασία αναγνώρισης κινδύνων δεν είναι πλήρως καταγεγραμμένη αλλά έχει δημιουργηθεί και διατηρηθεί τουλάχιστον μια λίστα κινδύνων σχετικά με την ασφάλειας των πληροφοριών και των δικτύων.
2	1	Έχει δημιουργηθεί και καταγραφεί μια διαδικασία για την διαχείριση κινδύνων ασφάλειας πληροφοριών και δικτύων στην οποία αναφέρεται και το κομμάτι της αναγνώρισης κινδύνων.
2	2	Η διαδικασία περιέχει κατ' ελάχιστο ρόλους και αρμοδιότητες, κριτήρια για την διενέργεια της αναγνώρισης κινδύνων και τα σχετικά αρχεία που πρέπει να τηρούνται.
2	3	Οι κίνδυνοι αναγνωρίζονται ανά στοιχείο που περιέχεται στον ενιαίο κατάλογο στοιχείων ενεργητικού, συστημάτων και διαδικασιών εντός του οργανισμού.
2	4	Έχουν αναγνωρισθεί και κάποιοι κίνδυνοι που σχετίζονται με απειλές που προέρχονται από εσωτερικά πρόσωπα.

3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται κατάλληλα μέτρα για την πρόληψη, τον εντοπισμό και την παρακολούθηση των επιθέσεων από εσωτερικά πρόσωπα, από άγνοια, αμέλεια, ή κακόβουλες ή επαγγελματικές προθέσεις.
3	2	Οι εργαζόμενοι εκπαιδεύονται και ευαισθητοποιούνται σχετικά με τις πρακτικές ασφάλειας των πληροφοριών εντός του οργανισμού, σύμφωνα με το μέτρο [TA2], διενεργείται επαρκής έλεγχος των υποψηφίων σύμφωνα με το μέτρο [HRS1], και οι εργαζόμενοι παρακολουθούνται [HRS2], ώστε να μειώνεται η πιθανότητα να υπάρξουν εσωτερικές επιθέσεις.
4	1	Οι κίνδυνοι καλύπτουν όλες τις πιθανές κατηγορίες πηγών κινδύνων (risk sources) ανεξάρτητα από το αν είναι υπό τον έλεγχο του οργανισμού.
4	2	Έχουν κατ' ελάχιστο αναγνωριστεί πηγές κινδύνων που σχετίζονται με τον ανθρώπινο παράγοντα.
4	3	Επίσης περιλαμβάνονται απειλές όπως remote spying, theft of equipment, theft of information or media, retrieval of recycled or discarded media, data input from untrustworthy sources, incorrect use of devices, illegal processing of data, sending or distributing of malware, abuse of rights κ.α.
4	4	Αντίστοιχα περιλαμβάνονται αδυναμίες όπως είναι ελλιπείς πόροι προσωπικού, προσωπικό που διενεργεί ενέργειες με conflict of interest / απουσία διαχωρισμού καθηκόντων, έλλειψη παρακολούθησης και εποπτείας, μερικός ορισμός πολιτικών, αδυναμία εφαρμογής τεχνικών μέτρων επιβολής πολιτικών και διαδικασιών, κ.α.
4	5	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Τα στοιχεία από την παρακολούθηση του προσωπικού όπως αναφέρεται στο [HRS2] και τα στοιχεία από την διαχείριση περιστατικών ασφαλείας όπως αναφέρεται στο [EIM1] τροφοδοτούν την διαδικασία διαχείρισης διακινδύνευσης. Συγκεκριμένα, ελέγχεται αν υπάρχει σχετικός κίνδυνος που χρειάζεται να επικαιροποιηθεί ή αν δεν υπάρχει, να γίνει η σχετική προσθήκη ακολουθώντας το σύνολο της διαδικασίας όπως αναφέρεται στο [RM1-RM4]. Σε κάθε περίπτωση διενεργείται διαδικασία διάγνωσης για τους λόγους για τους οποίους δεν είχε αναγνωριστεί σωστά ή ελλιπώς κάποιος κίνδυνος. Σε περίπτωση που έχει αναγνωριστεί κάποια συστηματική απόκλιση ή παράλειψη διενεργείται εκ νέου η διαδικασία διαχείρισης διακινδύνευσης είτε συνολικά είτε στο μέρος που άμεσα ή έμμεσα επηρεάζεται.
5	2	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	3	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
HRS6		**Μέτρο:** Συμφωνίες εργοδότησης και αποδεκτή χρήση **Στόχος Μέτρου:** Να διασφαλιστεί ότι οι ευθύνες που αφορούν την ασφάλεια πληροφοριών και την αποδεκτή χρήση των στοιχείων ενεργητικού, ενσωματώνονται στις συμφωνίες εργοδότησης και στις διαδικασίες έναρξης απασχόλησης, για την επίτευξη υπευθυνότητας και ευαισθητοποίησης. **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση μιας αποδεκτής πολιτικής χρήσης, η οποία προσδιορίζει τις χρήσεις που ο οργανισμός θεωρεί αποδεκτές χρήσεις των συστημάτων πληροφοριών που τίθενται στη διάθεση των στελεχών, ώστε να εξασφαλίζεται ότι τα στελέχη γνωρίζουν τι αναμένεται από αυτούς όσον αφορά τη χρήση, π.χ., ηλεκτρονικών υπολογιστών και κινητών συσκευών. Ο οργανισμός θα πρέπει να εξετάζει το ενδεχόμενο να ελέγχει την επίγνωση σχετικά με την πολιτική αποδεκτής χρήσης. Ο οργανισμός θα πρέπει επίσης να συνάπτει επαρκείς συμφωνίες εργοδότησης, στις οποίες να αναφέρονται με σαφήνεια οι υποχρεώσεις και οι ευθύνες του εργαζομένου όσον αφορά την ασφάλεια πληροφοριών. **Πηγή:**
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**

0	1	Ο οργανισμός δεν έχει θεσπίσει πολιτική αποδεκτής χρήσης η οποία προσδιορίζει τις χρήσεις που ο οργανισμός θεωρεί αποδεκτές χρήσεις των συστημάτων πληροφοριών που τίθενται στη διάθεση των στελεχών, ώστε να εξασφαλίζεται ότι τα στελέχη γνωρίζουν τι αναμένεται από αυτούς όσον αφορά τη χρήση.
1	1	Το προσωπικό ενημερώνεται για την αποδεκτή χρήση των πόρων ή/και των πληροφοριών χωρίς όμως αυτό να είναι καταγεγραμμένο και να υλοποιείται συστηματικά.
2	1	Έχουν προσδιορισθεί και εφαρμόζονται βασικούς κανόνες για την αποδεκτή χρήση πληροφοριών και περιουσιακών στοιχείων που σχετίζονται με πληροφορίες κρίσιμες για τον οργανισμό.
2	2	Στα βασικά στοιχεία περιέχονται τα ακόλουθα: (α) Περιορισμοί σε σχέση με τον τρόπο πλοήγησης στο διαδίκτυο
2	3	(β) Χρήση των υπολογιστών και άλλων πόρων που έχουν εκχωρηθεί για την διενέργεια εταιρικών εργασιών
2	4	(γ) Απαγόρευση της χρήσης των υπολογιστών και άλλων πόρων που έχουν εκχωρηθεί για την διενέργεια εταιρικών εργασιών για προσωπική χρήση
3	1	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται μία πολιτική αποδεκτής χρήσης η οποία προσδιορίζει τις χρήσεις που ο οργανισμός θεωρεί αποδεκτές χρήσεις των συστημάτων πληροφοριών που τίθενται στη διάθεση των στελεχών, ώστε να εξασφαλίζεται ότι τα στελέχη γνωρίζουν τι αναμένεται από αυτούς όσον αφορά τη χρήση.
3	2	Συνάπτονται επαρκείς συμφωνίες εργοδότησης, στις οποίες αναφέρονται με σαφήνεια οι υποχρεώσεις και οι ευθύνες του εργαζομένου όσον αφορά την ασφάλεια πληροφοριών.
3	3	Η πολιτική αποδεκτή χρήσης κοινοποιείται σε όλο το προσωπικό και γίνεται αποδεκτή μέσω των συμφωνιών εργοδότησης.
3	4	Το προσωπικό του οργανισμού έχει λάβει σχετική εκπαίδευση για την πολιτική αποδεκτής χρήσης.
3	5	Η πολιτική αποδεκτής χρήσης καθορίζει ότι: (α) Τα στοιχεία του οργανισμού χρησιμοποιούνται μόνο από εξουσιοδοτημένα άτομα
3	6	(β) Οι κωδικοί ή άλλα μέσα αυθεντικοποίησης της πρόσβασης δεν διαμοιράζονται με οποιονδήποτε άλλο
3	7	(γ) Το προσωπικό να οφείλει να εφαρμόζει μέτρα ανάλογα με την κρισιμότητα της πληροφορίας σύμφωνα με τις προδιαγραφές του [DS2].
3	8	(δ) Γίνεται χρήση μόνο αδειοδοτημένου λογισμικού
3	9	(ε) Σε περίπτωση περιστατικού ασφαλείας χρειάζεται ενημέρωση, μαζί με τα στοιχεία ενημέρωσης
3	10	(ζ) Υπάρχει αποδεκτή χρήση για μεταφερόμενα μέσα (περιλαμβανομένης της αποθήκευσης on transit, της μετακίνησης κ.α.), η οποία περιγράφεται.
3	11	Γενικά η πολιτική περιέχει αναμενόμενες και μη αποδεκτές συμπεριφορές και χειρισμό εντός του οργανισμού και σε σχέση με τον χειρισμό των πληροφοριών και πόρων του οργανισμού. Επιπλέον στην πολιτική αναφέρονται και οι τρόποι παρακολούθησης (monitoring & logging) που έχει υλοποιήσει ο οργανισμός.
4	1	Η επίγνωση σχετικά με την πολιτική αποδεκτής χρήσης, ελέγχεται μέσω ερωτηματολογίων που συμπληρώνονται από το προσωπικό σε ετήσια βάση.
4	2	Οι συγκεκριμένοι κανόνες και πολιτικές αφορούν τόσο προσωπικό που εργοδοτείται από τον οργανισμό και αυτούς που παρέχουν υπηρεσία στον οργανισμό μέσω τρίτων μερών ή μπορεί να επηρεάσουν την ασφάλεια του οργανισμού.
4	3	Οι πολιτικές που έχουν δημιουργηθεί καλύπτουν: (α) Την πρόσβαση στο διαδίκτυο και το σχετικό φιλτράρισμα που γίνεται από τον οργανισμό (Web Access and filtering Policy)
4	4	(β) Την χρήση μεταφερόμενων συσκευών (Mobile computing policy)
4	5	(γ) Την χρήση μεταφερόμενων μέσων (Media policy)
4	6	(δ) Την εργασία από απόσταση (Teleworking policy)

4	7	(ε) Την πολιτική ελέγχου πρόσβασης με έμφαση στο κάθε επίπεδο διαβάθμισης όπως αναφέρονται στο [AM1] και στο [DS2].
4	8	(ζ) Οδηγίες σε σχέση με την συντήρηση και την αποθήκευση των πόρων από το προσωπικό βάσει του ρόλου τους
4	9	(η) Πολιτική για την ασφαλή διαγραφή και απόσυρση πληροφοριών και πόρων (Secure erasure & disposal policy).
4	10	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Υλοποιούνται τεχνικά μέτρα ώστε να ενημερώνεται το προσωπικό κάθε φορά που πρόκειται να αποκτήσει πρόσβαση στα συστήματα του οργανισμού για τις οδηγίες αποδεκτής χρήσης.
5	2	Για κάθε περίπτωση πρόσβασης, ζητείται ενεργητική κίνηση από το σχετικό προσωπικό για την ανάγνωση των οδηγιών και τηρούνται τα σχετικά στοιχεία (χρόνος και τοποθεσία) της κίνησης.
5	3	Οι συγκεκριμένες ενέργειες και οδηγίες γίνονται σε συμφωνία με την κείμενη νομοθεσία ειδικά για θέματα προσωπικών δεδομένων.
5	4	Σε περίπτωση χρήσης cloud services, οι σχετικές οδηγίες και πολιτικές εφαρμόζονται και για τους συγκεκριμένους πόρους τόσο από το προσωπικό του οργανισμού όσο και από τον cloud provider (το τελευταίο εξασφαλίζεται μέσα από τις σχετικές συμβάσεις / συμφωνίες).
5	5	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	6	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

Κατηγορία		ΦΥΣΙΚΗ ΑΣΦΑΛΕΙΑ
PS1		**Μέτρο:** Περιβαλλοντικά μέτρα **Στόχος Μέτρου:** Να εξασφαλιστούν επαρκή μέτρα για την προστασία του οργανισμού από τις επιπτώσεις φυσικών καταστροφών, όπως οι πλημμύρες, οι σεισμοί και οι πυρκαγιές. **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση κατάλληλων μέτρων για την προστασία του οργανισμού από τις επιπτώσεις φυσικών καταστροφών, όπως οι πλημμύρες, οι σεισμοί και οι πυρκαγιές. Ο οργανισμός πρέπει να λαμβάνει υπόψη τη γεωγραφική θέση κατά τη δημιουργία της υποδομής δικτύου και να εξασφαλίζει ότι τα κρίσιμα στοιχεία υποδομής και συστήματα είναι γεωγραφικά διάσπαρτα. **Πηγή:** ENISA
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**
0	1	Ο οργανισμός δεν λαμβάνει μέτρα για την προστασία του οργανισμού από τις επιπτώσεις φυσικών καταστροφών.
1	1	Έχουν ληφθεί κάποια βασικά μέτρα σχετικά με την προστασία του οργανισμού από τις επιπτώσεις φυσικών καταστροφών, όπως οι πλημμύρες, σεισμοί και πυρκαγιές.
1	2	Το(α) κτήριο(α) που στεγάζει, λειτουργεί, εξυπηρετεί μέρος ή ολόκληρες τις κρίσιμες λειτουργίες και προσωπικό του οργανισμού έχει σχεδιαστεί και δομηθεί σύμφωνα με τα πρότυπα, τους κώδικες πρακτικής και τον αντισεισμικό κώδικα όπως ίσχυε στην ημερομηνία ανέγερσής του.
1	3	Το(α) κτήριο(α) έχουν σχετική έγκυρη άδεια σύμφωνα με την χρήση τους.
1	4	Δεν έχουν ληφθεί συγκεκριμένα μέτρα κατά άλλων κινδύνων.
1	5	Έχει συνταχθεί και υλοποιειθεί ο κατάλληλος σχεδιασμός για την πυροπροστασία του κτηρίου όπως προβλέπουν οι κανονισμοί πυροπροστασίας σύμφωνα με την κατηγορία κινδύνου πυρκαγιά, τον ρυθμό ανάπτυξης πυρκαγιάς και τον τύπο χρήσης οικοδομής.
2	1	Διενεργούνται δοκιμές εκκένωσης σε τακτική βάση για σενάρια κινδύνων που ανήκουν στην συγκεκριμένη κατηγορία.
2	2	Τα στοιχεία από τις δοκιμές λαμβάνονται υπόψη στον σχεδιασμό των σχεδίων επιχειρησιακής συνέχειας και ανάκαμψης από καταστροφή.
3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται κατάλληλα μέτρα για την προστασία του οργανισμού από τις επιπτώσεις φυσικών καταστροφών, όπως οι πλημμύρες, οι σεισμοί και οι πυρκαγιές.
3	2	Λαμβάνεται υπόψη η γεωγραφική θέση κατά τη δημιουργία της υποδομής δικτύου και εξασφαλίζεται ότι τα κρίσιμα στοιχεία υποδομής και συστήματα είναι γεωγραφικά διάσπαρτα.
3	3	Εξασφαλίζεται ότι οι βασικές παροχές (π.χ. ρεύμα, δίκτυο) και οι κρίσιμες διασυνδέσεις με τρίτα μέρη, όπου απαιτούνται, έχουν τουλάχιστον 2 διαφορετικές οδεύσεις και αν είναι δυνατό, διαφορετικούς παρόχους.
3	4	Έχουν καταγραφεί και επικαιροποιηθεί, όπως απαιτείται, σχετικά σχέδια που αποτυπώνουν τις σχετικές οδεύσεις.
4	1	Έχει διενεργηθεί αξιολόγηση κινδύνου σε σχέση με τους περιβαλλοντικούς κινδύνους (π.χ. σεισμός, πλημμύρα, πυρκαγιά).
4	2	Για τους κινδύνους αυτούς έχει γίνει ανάλυση και σχεδιασμός βασικών προληπτικών μέτρων τόσο στο εξωτερικό του κτηρίου όσο και στο εσωτερικό όπως αναφέρεται στο [PS5], λαμβάνοντας υπόψη ιστορικά στοιχεία και διαθέσιμες μελέτες ανά περιοχή. (Ειδικά μέτρα θα πρέπει να ληφθούν αν το(α) κτήριο(α) βρίσκονται σε περιοχές που έχουν αναγνωριστεί ως Περιοχές Δυνητικού Σημαντικού Κινδύνου Πλημμύρας σύμφωνα με την Οδηγία 2007/60/ΕΚ.
4	3	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται πολιτική για μέτρα φυσικής ασφάλειας και περιβαλλοντικούς ελέγχους.
4	4	Στο χώρο του computer room έχει τοποθετηθεί σύστημα το οποίο ενημερώνει σε περίπτωση πλημμύρας.

4	5	Στο χώρο του computer room έχει τοποθετηθεί αυτόματο σύστημα πυρανίχνευσης και πυρόσβεσης.
4	6	Έχει δημιουργηθεί σχετικό σχέδιο για την αντιμετώπισης των αντίστοιχων κινδύνων.
4	7	Έχει πραγματοποιηθεί μελέτη για τα περιβαλλοντικά μέτρα που υλοποιήθηκαν σύμφωνα και με την κείμενη νομοθεσία.
4	8	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Διενεργείται τακτική επιθεώρηση κτηρίων όσο αφορά τη δομοστατική τους επάρκεια από κατάλληλα εξουσιοδοτημένο και έμπειρο προσωπικό. Σε περίπτωση που προκύπτουν αποκλίσεις, υλοποιούνται τα κατάλληλα διορθωτικά μέτρα.
5	2	Τηρούνται κατάλληλες διασυνδέσεις και επαφές με αξιόπιστες πηγές (π.χ. εθνικές αρχές, ομάδες ενδιαφέροντος, παρατηρητήρια κ.α.) για την λήψη έγκυρης και έγκαιρης ενημέρωσης σχετικά με περιβαλλοντικούς κινδύνους.
5	3	Η σχετική πληροφορία που λαμβάνεται, αξιολογείται ώστε να εξασφαλίζεται η υψηλότερη ετοιμότητα του οργανισμού έναντι των συγκεκριμένων κινδύνων. Ο οργανισμός τηρεί δομημένα σχέδια ανταπόκρισης σε καταστάσεις κρίσεων σύμφωνα με τα [BCR1-4].
5	4	Τα σχέδια δοκιμάζονται τακτικά με την συμμετοχή των κατάλληλων αρχών και εθνικών ομάδων αντιμετώπισης.
5	5	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	6	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
PS2		**Μέτρο:** Έλεγχος περιμετρικής πρόσβασης **Στόχος Μέτρου:** Να διασφαλιστεί η φυσική περίμετρος του οργανισμού, με την εξασφάλιση και αποτροπή της μη εξουσιοδοτημένης πρόσβασης. **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση φυσικής περιμέτρου ασφάλειας με σκοπό την προστασία των εγκαταστάσεων επεξεργασίας πληροφοριών. Ο οργανισμός πρέπει να καθιερώσει κατάλληλα μέτρα ελέγχου της περιμετρικής πρόσβασης με την εφαρμογή φυσικών συνόρων, όπως φράχτες, πόρτες και τοίχοι. Ο οργανισμός απαιτεί επίσης από τους υπαλλήλους και τους επισκέπτες να αποδεικνύουν την ταυτότητά τους στους φρουρούς ασφαλείας προκειμένου να εισέλθουν (σε κάποιο μέρος) του οργανισμού. Ο οργανισμός θα πρέπει να εξετάσει την εγκατάσταση καμερών κλειστού κυκλώματος με σκοπό τον εντοπισμό εισβολέων στα όρια του οργανισμού. **Πηγή:** NIST
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**
0	1	Ο οργανισμός δεν λαμβάνει μέτρα για την ασφάλεια της φυσικής περιμέτρου του οργανισμού.
1	1	Τηρούνται κάποια βασικά μέτρα σχετικά με την περιμετρική ασφάλεια του οργανισμού, όπως το κλείδωμα όλων των κεντρικών εισόδων και ο έλεγχος στην είσοδο των ατόμων που εισέρχονται στο οργανισμό, χωρίς όμως να γίνεται καταγραφή.
2	1	Διατηρείται λίστα στην είσοδο των εγκαταστάσεων με τα άτομα που έχουν μπει στον οργανισμό.
2	2	Έχει τοποθετηθεί κάμερα μόνο στην κεντρική είσοδο του οργανισμού στην οποία όμως δεν γίνεται καταγραφή.
3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται μέτρα για την ασφάλεια της περιμέτρου του οργανισμού με σκοπό την προστασία των εγκαταστάσεων επεξεργασίας πληροφοριών.
3	2	Έχουν καθιερωθεί κατάλληλα μέτρα ελέγχου της περιμετρικής πρόσβασης με την εφαρμογή φυσικών συνόρων, όπως φράχτες, πόρτες και τοίχους.
3	3	Έχει εγκατασταθεί σύστημα συναγερμού στις εγκαταστάσεις του.

3	4	Έχει εγκατασταθεί σύστημα access control για την είσοδο του προσωπικού στις εγκαταστάσεις του οργανισμού.
3	5	Οι επισκέπτες του οργανισμού συνοδεύονται καθ' όλη τη διάρκεια της παρουσίας τους στις εγκαταστάσεις του οργανισμού.
4	1	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται διαδικασία και πολιτική σχετικά με την ασφάλεια της περιμέτρου του οργανισμού και την είσοδο στις εγκαταστάσεις.
4	2	Έχει εγκατασταθεί σύστημα καμερών κλειστού κυκλώματος με σκοπό τον εντοπισμό εισβολέων στα όρια του οργανισμού.
4	3	Διατηρούνται logs σχετικά με την καταγραφή των καμερών σύμφωνα με τη σχετική νομοθεσία για τα προσωπικά δεδομένα.
4	4	Διατηρούνται Logs από το σύστημα access control και ενημερώνεται μέσω ειδοποιήσεων για τυχόν παραβιάσεις.
4	5	Παρακολουθείται το σύστημα συναγερμού και το σύστημα καμερών κλειστού κυκλώματος και λαμβάνονται σχετικές ενημερώσεις σε περίπτωση που παρουσιαστεί οποιαδήποτε κίνηση.
4	6	Εκτελούνται έλεγχοι ασφαλείας στο φυσικό όριο της εγκατάστασης του οργανισμού για τη μη εξουσιοδοτημένη πρόσβαση και εξαγωγή πληροφοριών.
4	7	Ανασκοπούνται τουλάχιστον σε ετήσια βάση τα δικαιώματα και τις προσβάσεις του προσωπικού όσον αφορά το συναγερμό και το access control.
4	8	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Υπάρχει σύμβαση με εταιρεία που έχει αναλάβει τη φύλαξη των εγκαταστάσεων του οργανισμού και την παρακολούθηση του κλειστού κυκλώματος καμερών σε 24ώρη βάση.
5	2	Πραγματοποιούνται σε ετήσια βάση, δοκιμές παρείσδυσης που περιλαμβάνουν απροειδοποίητες προσπάθειες παράκαμψης ή παράκαμψης ελέγχων ασφαλείας που σχετίζονται με τα φυσικά σημεία πρόσβασης στην εγκατάσταση.
5	3	Έχουν υλοποιηθεί για την είσοδο στις εγκαταστάσεις του οργανισμού 2 επίπεδα ελέγχου, ο πρώτος έλεγχος πραγματοποιείται στην περίμετρο των εγκαταστάσεων και ο δεύτερος στην είσοδο του κτιρίου.
5	4	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	5	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
PS3		**Μέτρο:** Έλεγχος εσωτερικής πρόσβασης **Στόχος Μέτρου:** Να εξασφαλιστεί ο έλεγχος της πρόσβασης σε εσωτερικούς χώρους εργασίας και τις εγκαταστάσεις, ώστε να διασφαλίζεται ότι η φυσική πρόσβαση περιορίζεται κατόπιν ανάγκης. **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση εσωτερικών μέτρων πρόσβασης, ευθυγραμμισμένων με τους ρόλους που περιγράφονται στο [IAM1], προκειμένου να διασφαλιστεί ότι μόνο τα στελέχη με έννομο συμφέρον έχουν πρόσβαση σε (συγκεκριμένα μέρη) του οργανισμού, π.χ. με τη δημιουργία ειδικών σαρωτών ταυτότητας για την πρόσβαση σε ένα μέρος του οργανισμού. **Πηγή:** 27002, NIST
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**
0	1	Ο οργανισμός δεν λαμβάνει μέτρα για την εσωτερική πρόσβαση.
1	1	Τα άτομα που εισέρχονται και εξέρχονται από τις εγκαταστάσεις του οργανισμού ελέγχονται, χωρίς να πραγματοποιείται επιπλέον καταγραφή.
2	1	Διατηρείται λίστα στην είσοδο των εγκαταστάσεων με τα άτομα που έχουν μπει στον οργανισμό.

3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται εσωτερικά μέτρα πρόσβασης, τα οποία είναι ευθυγραμμισμένα με τους ρόλους που περιγράφονται στο [IAM1], προκειμένου να διασφαλιστεί ότι μόνο τα στελέχη με έννομο συμφέρον έχουν πρόσβαση σε (συγκεκριμένα μέρη) του οργανισμού.
3	2	Έχει εγκατασταθεί σύστημα access control για την είσοδο του προσωπικού στις εγκαταστάσεις του οργανισμού.
3	3	Οι επιμέρους προσβάσεις σε χώρους ορίζονται σύμφωνα με τον ρόλο του εκάστοτε υπαλλήλου.
3	4	Για τους επισκέπτες δίδονται κάρτες που έχουν πρόσβαση μόνο στην κεντρική είσοδο. Κατά τη διάρκεια παραμονής τους στις εγκαταστάσεις συνοδεύονται υποχρεωτικά.
4	1	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται διαδικασία και πολιτική σχετικά με τον έλεγχο της εσωτερικής πρόσβασης σε χώρους εργασίας.
4	2	Εκτελούνται έλεγχοι ασφαλείας στις εγκαταστάσεις του οργανισμού για μη εξουσιοδοτημένη πρόσβαση.
4	3	Οι προσβάσεις και τα δικαιώματα που δίδονται στο προσωπικό σε σχέση με το access control ανασκοπούνται τουλάχιστον μία φορά το χρόνο.
4	4	Διατηρούνται Logs από το σύστημα access control και ενημερώνεται μέσω ειδοποιήσεων για τυχόν παραβιάσεις.
4	5	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Για την είσοδο στις εγκαταστάσεις του οργανισμού, υλοποιούνται 2 επίπεδα ελέγχου, ο πρώτος έλεγχος πραγματοποιείται στην περίμετρο των εγκαταστάσεων και ο δεύτερος στην είσοδο του κτιρίου.
5	2	Πραγματοποιείούνται σε ετήσια βάση, δοκιμές παρείσδυσης που περιλαμβάνουν απροειδοποίητες προσπάθειες παράκαμψης ή παράκαμψης ελέγχων ασφαλείας που σχετίζονται με τα φυσικά σημεία πρόσβασης στην εγκατάσταση.
5	3	Χρησιμοποιούνται αυτοματοποιημένοι μηχανισμοί για να διευκολύνει τον έλεγχο των αρχείων πρόσβασης επισκεπτών και προσωπικού.
5	4	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	5	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
PS4		**Μέτρο:** Ασφάλεια καλωδίωσης, εξοπλισμού και εγκαταστάσεων **Στόχος Μέτρου:** Να εξασφαλιστεί ότι για την καλωδίωση και τον εξοπλισμό που υποστηρίζουν την επεξεργασία των πληροφοριών, εξασφαλίζεται η φυσική προστασία από παρεμβολές, υποκλοπή ή ζημιά **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση κατάλληλων μέτρων προκειμένου να προστατεύει την καλωδίωση και τον λοιπό εξοπλισμό από παρεμβολές, υποκλοπή ή ζημιά, οι οποίες θα προκαλούσαν διακοπή στις υπηρεσίες του οργανισμού. Ο οργανισμός πρέπει να εξασφαλίζει ότι τα καλώδια που παρέχουν ηλεκτρική ενέργεια σε κρίσιμες υποδομές προστατεύονται δεόντως και να εκπαιδεύει τους υπαλλήλους σύμφωνα με το μέτρο [TA2], ώστε να γνωρίζουν τη σημασία του εξοπλισμού που υποστηρίζει τις δραστηριότητες επεξεργασίας πληροφοριών. Η φυσική πρόσβαση στα λογικά δίκτυα θα πρέπει επίσης να προστατεύεται με κατάλληλα μέτρα ώστε να αποτρέπεται η μη εξουσιοδοτημένη φυσική πρόσβαση στο λογικό εξοπλισμό και το δίκτυο του οργανισμού. Ο φορέας εξετάζει κατάλληλα μέτρα πρόσβασης στο δίκτυο, όπως ορίζονται στο [NS5]. Ο οργανισμός διασφαλίζει τη φυσική ακεραιότητα και την τακτική συντήρηση των εγκαταστάσεων στις οποίες είναι εγκατεστημένος ο εξοπλισμός δικτύου, καθώς και την ορθή λειτουργία των μέτρων ασφάλειας. **Πηγή:** 27002, NIST
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**

0	1	Ο οργανισμός δεν εφαρμόζει κάποια μέτρα σχετικά με ασφάλεια της καλωδίωσης και τη φυσική πρόσβαση στα λογικά δίκτυα.
1	1	Υπάρχει προστασία στα καλώδια τροφοδοσίας και τηλεπικοινωνιών που μεταφέρουν δεδομένα ή υπηρεσίες υποστήριξης πληροφοριών από υποκλοπές, παρεμβολές ή ζημιές.
1	2	Ο εξοπλισμός συντηρείται σύμφωνα με τα προτεινόμενα διαστήματα συντήρησης και τις προδιαγραφές του προμηθευτή.
2	1	Οι γραμμές ηλεκτρικού ρεύματος και τηλεπικοινωνιών στις εγκαταστάσεις επεξεργασίας πληροφοριών είναι υπόγειες, όπου είναι δυνατόν.
2	2	Χρησιμοποιείται μόνο εξουσιοδοτημένο προσωπικό συντήρησης για τις επισκευές και τον πιθανό εξοπλισμό συντήρησης.
3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται κατάλληλα μέτρα προκειμένου να προστατεύεται η καλωδίωση και ο λοιπός εξοπλισμός από παρεμβολές, υποκλοπή ή ζημιά, οι οποίες θα προκαλούσαν διακοπή στις υπηρεσίες του οργανισμού.
3	2	Εξασφαλίζεται ότι τα καλώδια που παρέχουν ηλεκτρική ενέργεια σε κρίσιμες υποδομές προστατεύονται δεόντως και οι υπαλληλοι εκπαιδεύονται σύμφωνα με το μέτρο [TA2], ώστε να γνωρίζουν τη σημασία του εξοπλισμού που υποστηρίζει τις δραστηριότητες επεξεργασίας πληροφοριών.
3	3	Τα καλώδια τροφοδοσίας διαχωρίζονται από τα καλώδια επικοινωνίας για την αποφυγή παρεμβολών.
3	4	Η φυσική πρόσβαση στα λογικά δίκτυα προστατεύεται με κατάλληλα μέτρα ώστε να αποτρέπεται η μη εξουσιοδοτημένη φυσική πρόσβαση στο λογικό εξοπλισμό και το δίκτυο του οργανισμού.
3	5	Ασφαλίζονται (π.χ racks που κλειδώνουν) οι χώροι όπου υπάρχει πιθανότητα πρόσβασης στα patch panels ή σε οποιοδήποτε δικτυακό εξοπλισμό.
3	6	Ο φορέας εξετάζει κατάλληλα μέτρα πρόσβασης στο δίκτυο, όπως ορίζονται στο [NS5].
3	7	Διασφαλίζεται η φυσική ακεραιότητα και η τακτική συντήρηση των εγκαταστάσεων στις οποίες είναι εγκατεστημένος ο εξοπλισμός δικτύου, καθώς και η ορθή λειτουργία των μέτρων ασφάλειας.
3	8	Τηρούνται αρχεία για όλες τις βλάβες και για κάθε προληπτική και διορθωτική συντήρηση.
3	9	Η απομακρυσμένη συντήρηση των περιουσιακών στοιχείων του οργανισμού εγκρίνεται, καταγράφεται και εκτελείται με τρόπο που αποτρέπει τη μη εξουσιοδοτημένη πρόσβαση.
3	10	Εφαρμόζονται έλεγχοι όταν ο εξοπλισμός προγραμματίζεται για συντήρηση, λαμβάνοντας υπόψη εάν αυτή η συντήρηση εκτελείται από προσωπικό στο χώρο του οργανισμού ή εκτός αυτού. Όπου είναι απαραίτητο, οι εμπιστευτικές πληροφορίες διαγράφονται από τον εξοπλισμό.
4	1	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται διαδικασία και πολιτική σχετικά με την ασφάλεια καλωδίωσης, εξοπλισμού και εγκαταστάσεων.
4	2	Έχει εγκατασταθεί για την προστασία των καλωδίων επικοινωνίας θωρακισμένος αγωγός καλωδίωσης.
4	3	Πραγματοποιούνται τεχνικές σαρώσεις και φυσικές επιθεωρήσεις για μη εξουσιοδοτημένες συσκευές που συνδέονται στα καλώδια.
4	4	Ο εξοπλισμός ελέγχεται πριν τεθεί ξανά σε λειτουργία ότι δεν έχει παραβιαστεί και ότι δεν παρουσιάζει δυσλειτουργία.
4	5	Τηρούνται από τους προμηθευτές όλες οι απαιτήσεις που επιβάλλονται από τα ασφαλιστήρια συμβόλαια.
4	6	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Γίνεται χρήση ηλεκτρομαγνητικής θωράκισης για την προστασία των καλωδίων.
5	2	Χρησιμοποιούνται μηχανισμοί ελέγχου ακεραιότητας για την επαλήθευση της ακεραιότητας του υλικού.

5	3	Κατά τη διάρκεια των εργασιών συντήρησης οι μηχανικοί υποχρεούνται να χρησιμοποιούν ιμάντα καρπού ηλεκτροστατικής εκκένωσης (ESD) ώστε να αποφευχθεί η συσσώρευση στατικού ηλεκτρισμού κοντά σε ευαίσθητα ηλεκτρονικά.
5	4	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	5	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
PS5		**Μέτρο:** Εσωτερικά περιβαλλοντικά μέτρα **Στόχος Μέτρου:** Να εξασφαλιστεί ότι οι εσωτερικοί χώροι και οι εγκαταστάσεις του οργανισμού προστατεύονται από φυσικές ζημιές **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση μέτρων φυσικής ασφάλειας και προστασίας, ώστε να αποφεύγεται η φυσική ζημία στους εσωτερικούς χώρους και τις εγκαταστάσεις του οργανισμού. Κατά την εφαρμογή εσωτερικών περιβαλλοντικών μέτρων, ο οργανισμός θα πρέπει να εξετάζει τους κινδύνους που σχετίζονται με τη φωτιά και τη θερμοκρασία, την υγρασία, την ηλεκτρική ενέργεια, τη χρήση του νερού και άλλα στοιχεία που θα μπορούσαν να επηρεάσουν αρνητικά τη φυσική ασφάλεια των στοιχείων ενεργητικού. Ο οργανισμός πρέπει να εξετάζει την πυρόσβεση, τον έλεγχο της υγρασίας και άλλα μέτρα ανάλογα με τα χαρακτηριστικά των εσωτερικών φυσικών χώρων, όπως είναι τα κέντρα δεδομένων ή άλλους χώρους όπου βρίσκεται εξοπλισμός επεξεργασίας πληροφοριών. **Πηγή:**
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**
0	1	Ο οργανισμός δεν έχει λάβει κανένα μέτρο για την προστασία των εσωτερικών χώρων και των εγκαταστάσεων του οργανισμού από φυσικές ζημιές.
1	1	Τα κρίσιμα στοιχεία του οργανισμού, όπως έχουν αναγνωριστεί στο [DS2] και στο [AM2], φιλοξενούνται σε διακριτούς χώρους που εφαρμόζεται έλεγχος πρόσβασης (χωρίς να γίνεται σχετική καταγραφή).
1	2	Έχουν ληφθεί κάποια βασικά μέτρα σχετικά με την προστασία του χώρου, του εξοπλισμού και των πληροφοριών που στεγάζονται εκεί από τις επιπτώσεις φυσικών καταστροφών, όπως οι πλημμύρες, οι σεισμοί και οι πυρκαγιές. (Π.χ. υπάρχει τουλάχιστον ένας πυροσβεστήρας έξω από τον χώρο, ο εξοπλισμός είναι τοποθετημένος σε σημείο που δεν μπορεί να μετακινηθεί εύκολα σε περίπτωση σεισμού κλπ).
2	1	Παρακολουθούνται (έστω και χειροκίνητα) οι συνθήκες θερμοκρασίας και υγρασίας στους χώρους που φιλοξενούν τα κρίσιμα στοιχεία του οργανισμού.
2	2	Έχει οριστεί τουλάχιστον ένα άτομο εντός του οργανισμού που είναι υπεύθυνο για την παρακολούθηση των σχετικών στοιχείων και την ενημέρωση αρμόδιου προσωπικού σε περίπτωση που βρεθούν εκτός των προδιαγεγραμμένων αποδεκτών ορίων.
2	3	Υλοποιούνται κατάλληλα μέτρα (τουλάχιστον μια μονάδα κλιματισμού) προκειμένου να διασφαλίζεται ένα σταθερό επίπεδο θερμοκρασίας στους συγκεκριμένους χώρους.
3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται μέτρα φυσικής ασφάλειας και προστασίας, ώστε να αποφεύγεται η φυσική ζημία στους εσωτερικούς χώρους και τις εγκαταστάσεις του οργανισμού.
3	2	Κατά την εφαρμογή εσωτερικών περιβαλλοντικών μέτρων, ο οργανισμός έχει εξετάσει τους κινδύνους που σχετίζονται με τη φωτιά και τη θερμοκρασία, την υγρασία, την ηλεκτρική ενέργεια, τη χρήση του νερού και άλλα στοιχεία που μπορούν να επηρεάσουν αρνητικά τη φυσική ασφάλεια των στοιχείων ενεργητικού.
3	3	Εξετάζεται η πυρόσβεση, ο έλεγχος της υγρασίας και άλλα μέτρα ανάλογα με τα χαρακτηριστικά των εσωτερικών φυσικών χώρων, όπως είναι τα κέντρα δεδομένων ή άλλους χώρους όπου βρίσκεται εξοπλισμός επεξεργασίας πληροφοριών.
3	4	Παρακολουθούνται με αυτόματα μέσα οι συνθήκες θερμοκρασίας και υγρασίας στους χώρους που φιλοξενούνται τα κρίσιμα στοιχεία του οργανισμού.

3	5	Έχουν οριστεί σχετικοί κανόνες για την ενημέρωση του κατάλληλου προσωπικού σε περίπτωση που οι τιμές βρεθούν εκτός των προδιαγεγραμμένων αποδεκτών ορίων.
3	6	Τα ελάχιστα μέτρα περιλαμβάνουν: (α)Αυτόματο σύστημα πυρανίχνευσης
3	7	(β) Το σύνολο του εξοπλισμού βρίσκεται τοποθετημένο εντός rack τα οποία έχουν ελεγχόμενη πρόσβαση
3	8	(γ) Αποτυπωμένο σχέδιο του χώρου με αναγνώριση των σημείων που βρίσκεται ο εξοπλισμός
3	9	(δ) Σήμανση, μεγάφωνο και κουμπί εκκένωσης καθώς και κατάλληλο φωτισμό ασφαλείας
3	10	(ε) Υπερυψωμένο πάτωμα
3	11	(ζ) Στους χώρους απαγορεύεται η φορτοεκφόρτωση και η είσοδος μη εξουσιοδοτημένου προσωπικού.
3	12	(η) Για τους χώρους της γεννήτριας και του σημείου αποθήκευσης καυσίμου υπάρχουν κατάλληλα μέτρα πυρανίχνευσης και πυρόσβεσης σύμφωνα με την κείμενη νομοθεσία.
4	1	Έχει δημιουργηθεί ένα πλάνο και μια διαδικασία για τον διαχωρισμό και διαβάθμιση των χώρων επεξεργασίας πληροφοριών.
4	2	Η διαβάθμιση των χώρων λαμβάνει υπόψη την κρισιμότητα των διεργασιών που εκτελούνται εντός τους σύμφωνα με τα στοιχεία που έχουν εξαχθεί από το Business Impact Analysis [BCR1], την κρισιμότητα και ευαισθησία των πληροφοριών που επεξεργάζονται όπως περιγράφεται στο [DS2] και τα αποτελέσματα της διαδικασίας διαχείρισης διακινδύνευσης.
4	3	Έχουν καταγραφεί τα μέτρα που εφαρμόζονται για την κάθε κατηγορία χώρου.
4	4	Ειδικά για τους χώρους που ανήκουν στην υψηλότερη κατηγορία κατ' ελάχιστο εφαρμόζονται τα ακόλουθα μέτρα: (α) Αυτόματο σύστημα πυρόσβεσης με κατάλληλο μέσο ώστε να εξασφαλίζεται η μικρότερη επίπτωση επί των ανθρώπων, του εξοπλισμού ή των πληροφοριών.
4	5	(β) Διπλά (εφεδρικά) συστήματα για την διατήρηση της σταθερής θερμοκρασίας εντός των χώρων
4	6	(γ) Εφεδρικές διασυνδέσεις σε επίπεδο ενέργειες και δικτύου
4	7	(δ) Ύπαρξη τουλάχιστον 3 ειδών παροχής ενέργειας (δίκτυο, UPS, γεννήτρια)
4	8	(ε) Κατάλληλα μέτρα προστασίας για φυσική προστασία των καλωδίων από τρωκτικά και άλλους παράγοντες
4	9	(ζ) Ειδικά power strips για κάθε rack το οποίο φιλοξενεί εξοπλισμό τα οποία συνδέονται με τουλάχιστον 2 διακριτές πηγές ενέργειας.
4	10	(η) Προσωπικό που είναι εξουσιοδοτημένο για την παρακολούθηση, συντήρηση, ορθή λειτουργία και άμεση ανταπόκριση σε σχέση με τα φυσικά μέσα προστασίας.
4	11	(θ) Σύστημα αναγνώρισης και σήμανσης σχετικών καλωδίων
4	12	(ι) Υπάρχει μελέτη και σχεδιασμός του χώρου και του πατώματος σχετικά με το μέγιστο βάρος που μπορεί να αντέξει και την σχετική κατανομή του.
4	13	(κ) Σε περίπτωση ενεργοποίησης της γεννήτριας, εξασφαλίζεται παροχή ρεύματος και στα συστήματα ελέγχου θερμοκρασίας, στα συστήματα φωτισμού και ελέγχου πρόσβασης καθώς και σε όλα τα σημεία δικτύου που απαιτούνται για την λειτουργική διασύνδεση και παροχή των κρίσιμων υπηρεσιών.
4	14	(λ) Τηρείται διαδικασία για την συντήρηση, τον έλεγχο και την δοκιμή των στοιχείων που παρέχουν ενέργεια σε τακτική βάση.
4	15	(μ) Έχει μετρηθεί ο χρόνος και ο τρόπος με τον οποίο εκκινείται η γεννήτρια και έχει ενσωματωθεί στον σχετικό σχεδιασμό για την ικανότητα του UPS και για την αυτοματοποίηση των ενεργειών.
4	16	(ν) Υπάρχει αυτοματοποιημένο σύστημα by-pass για την απομόνωση στοιχείων ενέργειας σε περίπτωση που γίνεται συντήρηση, αντικατάσταση στοιχείων ή μπαταριών ή υπάρχει κάποια αστοχία.
4	17	(ξ) Τηρείται διαδικασία για την συντήρηση, τον έλεγχο και την δοκιμή των στοιχείων πυροπροστασίας και διατήρησης θερμοκρασίας σε τακτική βάση.
4	18	(ο) Υπάρχει κατάλληλη σήμανση και ανιχνευτές που υποδεικνύουν ότι στο χώρο έχει απελευθερωθεί αέριο που δεν είναι κατάλληλο για ανθρώπους.

4	19	(π) Επαρκή μέτρα έχουν ληφθεί για την γείωση του συνόλου της εγκατάστασης ή του εξοπλισμού.
4	20	Όλα τα παραπάνω μέτρα τηρούνται και στις περιπτώσεις που ο οργανισμός χρησιμοποιεί χώρους και εγκαταστάσεις τρίτων για την φιλοξενία του σχετικού εξοπλισμού.
4	21	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Οι σχετικές εγκαταστάσεις αποθήκευσης και λειτουργίας ακολουθούν διεθνείς βέλτιστες πρακτικές για την ανθεκτικότητα – π.χ. επιπέδου τουλάχιστον Tier III Uptime institute.
5	2	Διενεργούνται δοκιμές για την αξιολόγηση της ύπαρξης και δυνατότητας ορθής και αποτελεσματικής λειτουργίας του εν λόγω εξοπλισμού. Σε περίπτωση αναγνώρισης προβλημάτων, αυτά διορθώνονται άμεσα και τηρούνται καταγραφές σύμφωνα με την διαδικασία διαχείρισης αλλαγών [CM1].
5	3	Έχει καταγραφεί τα μέτρα που εφαρμόζονται για την κάθε κατηγορία χώρου. Ειδικά για τους χώρους που ανήκουν στην υψηλότερη κατηγορία κατ' ελάχιστο εφαρμόζονται τα ακόλουθα μέτρα: (α) Ειδικό σχεδιασμό για την εξασφάλιση της μέγιστης απόδοσης σε επίπεδο θερμότητας και διατήρησης θερμοκρασίας (θερμοί και ψυχροί διάδρομοι κ.α.)
5	4	(β) Διασυνδέσεις δικτύου για το core δίκτυο και για τα κρίσιμα συστήματα με οπτική ίνα
5	5	(γ) Σε περίπτωση που κάποια από τα racks δεν χρησιμοποιούνται τοποθετούνται σχετικά στοιχεία ώστε να επιτυγχάνεται ο έλεγχος πρόσβασης αλλά ταυτόχρονα να μην επηρεάζεται η λειτουργία και αποτελεσματικότητα των ψυχρών και θερμών διαδρόμων
5	6	(δ) Αυτόματο σύστημα παρακολούθησης των περιεχομένων των rack, της κατανάλωσης ενέργειας και της κατάστασης
5	7	(ε) Τα μηχανήματα είναι παραμετροποιημένα ώστε να ενεργοποιείται graceful shutdown σε περίπτωση επικείμενης ολικής απώλειας ενέργειας. Σε αυτές τις περιπτώσεις τα UPS αντέχουν το συνολικό φορτίο για τουλάχιστον 30 λεπτά.
5	8	(ζ) Έχει υλοποιήθεί ένα battery monitoring σύστημα για τα UPS στα οποία παρακολουθείται, καταγράφεται και αναλύεται η επίδοση και οι τάσεις λειτουργίας των μπαταριών.
5	9	(η) Υπάρχει κατάλληλος εξοπλισμός εκτός των συγκεκριμένων χώρων για εξοπλισμό για το προσωπικό όπως μάσκες / αναπνευστήρες / φακοί / κουβέρτες φωτιάς κ.α.
5	10	(θ) Για το χώρο που είναι αποθηκευμένα τα UPS και οι σχετικές μπαταρίες θα πρέπει να υπάρχουν μέτρα προστασίας – πρόσβασης, υγρασίας και θερμοκρασίας.
5	11	(ι) Υπάρχει σύστημα για την αντικεραυνική προστασία
5	12	(κ) Έχει εφαρμοσθεί ένα BMS για την συνολική παρακολούθηση και λειτουργία των μηχανολογικών, ηλεκτρικών μέτρων καθώς και των μέτρων πυρασφάλειας.
5	13	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	14	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

Κατηγορία		ΔΙΑΧΕΙΡΙΣΗ ΣΥΜΒΑΝΤΩΝ ΚΑΙ ΠΕΡΙΣΤΑΤΙΚΩΝ
EIM1		**Μέτρο:** Ετοιμότητα και εντοπισμός συμβάντων και περιστατικών **Στόχος Μέτρου:** Να διασφαλίζει ότι ο οργανισμός είναι σε θέση να εντοπίζει συμβάντα και περιστατικά που ενδέχεται να συνιστούν απειλή για τους στόχους της ασφάλειας πληροφοριών του οργανισμού και να ενεργοποιεί τις αντίστοιχες διαδικασίες αντιμετώπισης περιστατικών. **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση σχεδίου διαχείρισης και αντιμετώπισης συμβάντων και περιστατικών προκειμένου να διασφαλιστεί ότι ο οργανισμός είναι έτοιμος να αντιδράσει σε περίπτωση σοβαρού συμβάντος ή περιστατικού που αφορά την ασφάλεια πληροφοριών. Ο οργανισμός εξετάζει το ενδεχόμενο ευθυγράμμισης των διαδικασιών του για την αντιμετώπιση συμβάντων και περιστατικών με γενικές δυνατότητες παρακολούθησης και ειδικές λειτουργίες παρακολούθησης της ασφάλειας, όπως τις υπηρεσίες ανίχνευσης και πρόληψης εισβολών που περιγράφονται στο μέτρο [NS7]. **Πηγή:** NIST
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**
0	1	Ο οργανισμός δεν έχει θεσπίσει σχέδιο διαχείρισης και αντιμετώπισης συμβάντων και περιστατικών προκειμένου να διασφαλιστεί ότι ο οργανισμός είναι έτοιμος να αντιδράσει σε περίπτωση σοβαρού συμβάντος ή περιστατικού που αφορά την ασφάλεια πληροφοριών.
1	1	Η διαχείριση για τα περιστατικά και τα συμβάντα είναι ad hoc χωρίς να έχει θεσπιστεί σχέδιο διαχείρισης και αντιμετώπισης συμβάντων και περιστατικών
2	1	Έχει θεσπιστεί και εφαρμόζεται ένα βασικό σχέδιο διαχείρισης και αντιμετώπισης συμβάντων και περιστατικών.
3	1	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται σχέδιο διαχείρισης και αντιμετώπισης συμβάντων και περιστατικών προκειμένου να διασφαλιστεί ότι ο οργανισμός είναι έτοιμος να αντιδράσει σε περίπτωση σοβαρού συμβάντος ή περιστατικού που αφορά την ασφάλεια πληροφοριών.
3	2	Το σχέδιο αντιμετώπισης συμβάντων και περιστατικών: (α) Παρέχει στον οργανισμό έναν οδικό χάρτη για την εφαρμογή της ικανότητας απόκρισης συμβάντων
3	3	(β) Περιγράφει τη δομή και την οργάνωση της ικανότητας απόκρισης σε περιστατικό.
3	4	(γ) Παρέχει μία high level προσέγγιση για τον τρόπο με τον οποίο η ικανότητα απόκρισης περιστατικού ταιριάζει στο σύνολο του οργανισμού.
3	5	(δ) Πληροί τις μοναδικές απαιτήσεις του οργανισμού, οι οποίες σχετίζονται με την αποστολή, το μέγεθος, τη δομή και τις λειτουργίες.
3	6	(ε) Καθορίζει τα περιστατικά ασφάλειας για τα οποία θα πρέπει να συμπληρώνονται σχετικές αναφορές.
3	7	(ζ) Παρέχει KPI's για τη μέτρηση της ικανότητας απόκρισης περιστατικού εντός του οργανισμού.
3	8	(θ) Καθορίζει τους πόρους και τη διοικητική υποστήριξη που απαιτούνται για την αποτελεσματική διατήρηση και ωρίμανση της ικανότητας απόκρισης σε περιστατικά.
3	9	Εξετάζεται το ενδεχόμενο ευθυγράμμισης των διαδικασιών του για την αντιμετώπιση συμβάντων και περιστατικών με γενικές δυνατότητες παρακολούθησης και ειδικές λειτουργίες παρακολούθησης της ασφάλειας, όπως τις υπηρεσίες ανίχνευσης και πρόληψης εισβολών που περιγράφονται στο μέτρο [NS7].
3	10	Ο οργανισμός διανέμει αντίγραφα του σχεδίου αντιμετώπισης συμβάντων και περιστατικών σε όλους τους εμπλεκόμενους (εσωτερικούς ή/και εξωτερικούς) και διατηρεί σχετική λίστα.
3	11	Το σχέδιο αντιμετώπισης συμβάντων και περιστατικών εγκρίνεται από τη διοίκηση του οργανισμού.
4	1	Οι διαδικασίες του για την αντιμετώπιση συμβάντων και περιστατικών είναι ευθυγραμμισμένες με γενικές δυνατότητες παρακολούθησης και ειδικές λειτουργίες παρακολούθησης της ασφάλειας, όπως τις υπηρεσίες ανίχνευσης και πρόληψης εισβολών που περιγράφονται στο μέτρο [NS7].

4	2	Οι αλλαγές του σχεδίου αντιμετώπισης συμβάντων και περιστατικών επικοινωνούνται σε όλους τους εμπλεκόμενους (εσωτερικούς ή/και εξωτερικούς).
4	3	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Το σχέδιο αντιμετώπισης συμβάντων και περιστατικών προστατεύεται από μη εξουσιοδοτημένη αποκάλυψη και μη εξουσιοδοτημένη/ελεγχόμενη τροποποίηση.
5	2	Έγκυρες πληροφορίες Cyber threat intelligence λαμβάνονται έγκαιρα και μεταξύ άλλων χρησιμοποιούνται για την επικαιροποίηση του καταλόγου απειλών, ευπαθειών και κινδύνων στους οποίους είναι εκτεθειμένος ο οργανισμός.
5	3	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	4	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
EIM2		**Μέτρο:** Ανάλυση και αξιολόγηση συμβάντων και περιστατικών **Στόχος Μέτρου:** Να διασφαλιστεί ότι ο οργανισμός είναι σε θέση να αναλύει και να αξιολογεί συμβάντα και περιστατικά που αφορούν την ασφάλεια πληροφοριών, ούτως ώστε να ενεργοποιεί κατάλληλες διαδικασίες περιορισμού και ανάκτησης. **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση διαδικασιών που επιτρέπουν την ανάλυση και την αξιολόγηση συμβάντων και περιστατικών, ώστε να είναι σε θέση ο οργανισμός να λαμβάνει αιτιολογημένες αποφάσεις σχετικά με τις δράσεις και τα μέτρα που πρέπει να ληφθούν για την αντιμετώπιση ή την αποκατάσταση από συμβάντα και περιστατικά που αφορούν την ασφάλεια. Ο οργανισμός εξετάζει τον αντίκτυπο στα υποκείμενα δεδομένων, στις επιχειρηματικές δραστηριότητες, στα εξωτερικά μέρη και στο οικοσύστημα των φορέων. Ο οργανισμός διασφαλίζει ότι η ανάλυση και αξιολόγηση συμβάντων και περιστατικών διεκπεραιώνεται σε συνεννόηση με την ανώτατη διοίκηση για τη σύνδεση συμβάντων και περιστατικών με σενάρια υψηλού κινδύνου. **Πηγή:** 27035-2, 27002, NIST
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**
0	1	Ο οργανισμός δεν αναλύει και δεν αξιολογεί συμβάντα και περιστατικά που αφορούν την ασφάλεια πληροφοριών. Δεν έχει θεσπίσει διαδικασίες για την ανάλυση και την αξιολόγηση συμβάντων και περιστατικών.
1	1	Τα συμβάντα και περιστατικά αξιολογούνται και αναλύονται ad hoc, χωρίς να έχει δημιουργήσει κάποια σχετική διαδικασία.
2	1	Έχει θεσπίστεί μία διαδικασία η οποία αφορά τον τρόπο που πραγματοποιείται η ανάλυση και η αξιολόγηση συμβάντων και περιστατικών.
3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται διαδικασίες που επιτρέπουν την ανάλυση και την αξιολόγηση συμβάντων και περιστατικών, ώστε ο οργανισμός να λαμβάνει αιτιολογημένες αποφάσεις σχετικά με τις δράσεις και τα μέτρα για την αντιμετώπιση ή την αποκατάσταση από συμβάντα και περιστατικά που αφορούν την ασφάλεια.
3	2	Εξετάζεται ο αντίκτυπος στα υποκείμενα δεδομένων, στις επιχειρηματικές δραστηριότητες, στα εξωτερικά μέρη και στο οικοσύστημα των φορέων.
3	3	Διασφαλίζεται ότι η ανάλυση και αξιολόγηση συμβάντων και περιστατικών διεκπεραιώνεται σε συνεννόηση με την ανώτατη διοίκηση για τη σύνδεση συμβάντων και περιστατικών με σενάρια υψηλού κινδύνου.
3	4	Γίνεται καταγραφή των αποτελεσμάτων της ανάλυσης και της αξιολόγησης των εκάστοτε συμβάντων ή περιστατικών που έχουν εντοπιστεί από τον οργανισμό.

3	5	Τα περιστατικά ασφάλειας πληροφοριών ταξινομούνται κατά σοβαρότητα χρησιμοποιώντας την κλίμακα: (α) Πληροφορίες: κανένα αντίκτυπο, αλλά η ανάλυση θα μπορούσε να χρησιμοποιηθεί για τη βελτίωση των πολιτικών, διαδικασιών ή ελέγχων ασφάλειας πληροφοριών, (β) Προειδοποίηση: χαμηλό αντίκτυπο, (γ) Κρίσιμο: μέτριο αντίκτυπο, και (δ) Έκτακτη ανάγκη: σοβαρό αντίκτυπο, ή αντίστοιχο 'πολυεπιπεδές σχήμα ταξινόμησης'.
3	6	Σύμφωνα με τους παραπάνω παράγοντες ταξινόμησης, αυτή η προσέγγιση ταξινομεί τα συμβάντα ασφάλειας πληροφοριών σε τέσσερις κατηγορίες: (α) Πολύ σοβαρά, (β) Σοβαρά, (γ) Λιγότερο σοβαρά, και (δ) Μικρά ή αντίστοιχο' πολυεπιπεδές σχήμα ταξινόμησης. (α) Πολύ σοβαρά περιστατικά είναι αυτά που ενεργούν σε κρίσιμα συστήματα πληροφοριών και οδηγούν σε ιδιαίτερα σοβαρή επιχειρησιακή απώλεια, ή οδηγούν σε ιδιαίτερα σημαντικό κοινωνικό αντίκτυπο. (β) Σοβαρά περιστατικά είναι αυτά που ενεργούν σε κρίσιμα συστήματα πληροφοριών ή σημαντικά συστήματα πληροφοριών και οδηγούν σε σοβαρή επιχειρησιακή απώλεια ή οδηγούν σε σημαντικό κοινωνικό αντίκτυπο. (γ) Λιγότερο σοβαρά περιστατικά είναι αυτά που ενεργούν σε σημαντικά συστήματα πληροφοριών ή συστήματα πληροφοριών που δεν έχουν μεγάλο αντίκτυπο για τον οργανισμό και οδηγούν σε σημαντική επιχειρησιακή απώλεια, ή οδηγούν σε σημαντικό κοινωνικό αντίκτυπο. (δ) Μικρά περιστατικά είναι αυτά που ενεργούν σε συστήματα πληροφοριών που δεν έχουν μεγάλο αντίκτυπο για τον οργανισμό και οδηγούν σε μικρή επιχειρησιακή απώλεια ή καμία επιχειρησιακή απώλεια, ή οδηγούν σε μικρό κοινωνικό αντίκτυπο ή χωρίς κοινωνικό αντίκτυπο
3	7	Έχει ορισθεί σημείο επαφής (εσωτερικά του οργανισμού) το οποίο αξιολογεί κάθε συμβάν ασφάλειας πληροφοριών χρησιμοποιώντας τη συμφωνημένη κλίμακα ταξινόμησης περιστατικών και αποφασίζει εάν το συμβάν πρέπει να ταξινομηθεί ως περιστατικό ασφάλειας πληροφοριών.
4	1	Υπάρχει ομάδα αντιμετώπισης περιστατικών ασφάλειας πληροφοριών (ISIRT).
4	2	Διαβιβάζεται η αξιολόγηση και η απόφαση ενός περιστατικού ή/και συμβάντος για επιβεβαίωση ή επανεκτίμηση ανάλογα με τη σοβαρότητα.
4	3	Η ομάδα αντιμετώπισης περιστατικών ασφάλειας πληροφοριών αναλύει τα περιστατικά που έχουν εντοπιστεί με σκοπό την κατανόηση των μεθόδων και των στόχων της επίθεσης.
4	4	Υπάρχει συνεργασία με πάροχο υπηρεσιών για τη διαχείριση περιστατικών.
4	5	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Υπάρχει σύμβαση με τρίτο μέρος το οποίο εκτελεί ψηφιακή εγκληματολογία για τον οργανισμό σε περίπτωση σχετικού περιστατικού ασφαλείας ή συμβάντος.
5	2	Υπάρχει συμμετοχή σε εσωτερικές ή και εξωτερικές ασκήσεις για την αξιολόγηση της αποτελεσματικότητας και επίγνωσης του προσωπικού σχετικά με την ανάλυση και αξιολόγηση περιστατικών.
5	3	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	4	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

EIM3	**Μέτρο:** Περιορισμός και ανάκτηση από συμβάντα και περιστατικά **Στόχος Μέτρου:** Να εξασφαλιστεί επαρκής περιορισμός και αποκατάσταση από συμβάντα και περιστατικά ασφάλειας που επηρεάζουν αρνητικά τους στόχους ασφάλειας πληροφοριών του οργανισμού. **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση διαδικασιών για τον περιορισμό και την ανάκτηση από συμβάντα και περιστατικά, ώστε να περιορίζονται στο ελάχιστο οι επιπτώσεις στα συστήματα, τις εφαρμογές, τα δίκτυα και τα δεδομένα, καθώς και να διασφαλίζονται, στο μέτρο του δυνατού, οι κρίσιμες λειτουργίες του οργανισμού. Ο οργανισμός εξετάζει τους στόχους αποκατάστασης από συμβάντα και περιστατικά, λαμβάνοντας υπόψη τον στόχο του σημείου ανάκτησης (RPO) και τον χρόνο αποκατάστασης (RTO), προκειμένου να προσδιορίσει τη στοχοθετημένη διάρκεια και το επίπεδο των υπηρεσιών εντός των οποίων πρέπει να αποκατασταθεί μια επιχειρηματική διαδικασία μετά από κάποιο περιστατικό. **Πηγή:**

Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν έχει θεσπίσει και δεν εφαρμόζει διαδικασίες για τον περιορισμό και την αποκατάσταση από συμβάντα και περιστατικά.
1	1	Η αντίδραση στα περιστατικά ασφαλείας δεν γίνεται με κάποιο καθορισμένο τρόπο.
2	1	Έχουν αναγνωρισθεί κάποιοι ρόλοι σε σχέση με την ανταπόκριση σε περιστατικά ασφαλείας και έχει ενημερωθεί το λοιπό προσωπικό και τα συγκεκριμένα άτομα σχετικά με τις υποχρεώσεις τους σε σχέση με πιθανά περιστατικά ασφαλείας.
3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται διαδικασίες για τον περιορισμό και την αποκατάσταση (ανάκαμψη) από συμβάντα και περιστατικά, ώστε να περιορίζονται στο ελάχιστο οι επιπτώσεις στα συστήματα, τις εφαρμογές, τα δίκτυα και τα δεδομένα, καθώς και να διασφαλίζονται, στο μέτρο του δυνατού, οι κρίσιμες λειτουργίες του οργανισμού.
3	2	Οι στόχοι αποκατάστασης από συμβάντα και περιστατικά εξετάζονται, λαμβάνοντας υπόψη τον στόχο του σημείου ανάκτησης (RPO) και τον χρόνο αποκατάστασης (RTO), προκειμένου να προσδιορισθεί η στοχοθετημένη διάρκεια και το επίπεδο των υπηρεσιών εντός των οποίων πρέπει να αποκατασταθεί μια επιχειρηματική διαδικασία μετά από κάποιο περιστατικό.
3	3	Ακολουθείται η κατηγοριοποίηση περιστατικών που αναλύεται στο [EIM2].
4	1	Έχουν δημιουργηθεί συγκεκριμένα σχέδια στα οποία περιγράφονται τρόποι λειτουργίας, μέτρα και βήματα σε περίπτωση συγκεκριμένων τύπων περιστατικών.
4	2	Τα δεδομένα των σχεδίων έχουν προκύψει από την σχετική αξιολόγηση κινδύνων και να καλύπτουν τα κυριότερα είδη απειλών / επιθέσεων σύμφωνα με διεθνείς αναφορές και στοιχεία.
4	3	Κατ΄ ελάχιστο τέτοια σχέδια περιλαμβάνουν περιπτώσεις όπως: (α) Ransomware
4	4	b) Malware
4	5	c) Social engineering attack
4	6	d) Denial of Service
4	7	e) Supply chain availability attack
4	8	f) Physical security attack
4	9	g) Theft of media / device / information
4	10	Λαμβάνεται υπόψη ο στόχος του σημείου ανάκτησης (RPO) και του χρόνο αποκατάστασης (RTO), προκειμένου να προσδιορίσει η στοχοθετημένη διάρκεια και το επίπεδο των υπηρεσιών εντός των οποίων πρέπει να αποκατασταθεί μια επιχειρηματική διαδικασία μετά από κάποιο περιστατικό.
4	11	Οι ενέργειες που προβλέπονται για τον περιορισμό των επιπτώσεων του οργανισμού είναι κατάλληλες ανάλογα με την κρισιμότητα του περιστατικού και τις πληροφορίες ή λειτουργίες που επηρεάζονται ή δύναται να επηρεαστούν. Ο οργανισμός στα πλαίσια του περιορισμού και της ανταπόκρισης μπορεί να ζητήσει την συνδρομή από τις σχετικές αρχές.

4	12	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Έχουν προδιαγραφεί συγκεκριμένες διαδικασίες σχετικά με τον χειρισμό και την διατήρηση δεδομένων σε περίπτωση περιστατικού ασφαλείας.
5	2	Υλοποιούνται κατάλληλες ενέργειες ώστε κατάλληλα εξουσιοδοτημένοι ρόλοι να αναλάβουν την ασφαλή λήψη (με διατήρηση του chain of custody) στοιχείων ώστε να μπορούν να χρησιμοποιηθούν στην συνέχεια από τις αρμόδιες αρχές ή άλλα ειδικά εξουσιοδοτημένα μέρη.
5	3	Διενεργούνται τακτικές ασκήσεις και δοκιμές για να εξασφαλισθεί ότι το προσωπικό έχει επίγνωση των σχετικών σχεδίων, ότι οι προβλέψεις τους είναι ορθές και αποτελεσματικές και έχουν την δυνατότητα να επιτύχουν το επίπεδο ασφάλειας και λειτουργίας που επιθυμεί ο οργανισμός ακόμα και σε περίπτωση περιστατικού.
5	4	Υπάρχει απίτηση από τους συνεργάτες και υπεργολάβους του (που απαρτίζουν το supply chain των κρίσιμων λειτουργιών) να έχουν αντίστοιχες καταγεγραμμένες και ελεγμένες διαδικασίες ανταπόκρισης στα περιστατικά ασφαλείας και να δεσμεύονται για την άμεση συνδρομή τους σε περίπτωση που απαιτείται από τον οργανισμό.
5	5	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	6	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
EIM4		**Μέτρο:** Δραστηριότητες μετά το συμβάν και το περιστατικό. **Στόχος Μέτρου:** Να διασφαλιστεί ότι ο οργανισμός μαθαίνει από συμβάντα και περιστατικά ασφάλειας, προκειμένου να αποτρέπονται παρόμοια συμβάντα και περιστατικά στο μέλλον. **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση διαδικασιών μετά την εκδήλωση συμβάντων και περιστατικών, προκειμένου να αποτυπωθούν τα διδάγματα που έχουν αντληθεί από τα συμβάντα και περιστατικά ασφάλειας πληροφοριών και να προσδιορίζουν κατά πόσον πρέπει να θεσπιστούν πρόσθετα μέτρα ασφάλειας για την πρόληψη παρόμοιων συμβάντων και περιστατικών. Ο οργανισμός εξετάζει το ενδεχόμενο θέσπισης εκ των υστέρων διαδικασίας, η οποία περιλαμβάνει συνάντηση για την αξιολόγηση του συμβάντος ή περιστατικού με τους επηρεαζόμενους ιδιοκτήτες του συστήματος, τους διαχειριστές δεδομένων και άλλα ενδιαφερόμενα μέρη που συμμετείχαν στην αντιμετώπιση του περιστατικού, με σκοπό την ανταλλαγή διδαγμάτων και τον προσδιορισμό προληπτικών μέτρων. **Πηγή:** 27002, 27035
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**
0	1	Ο οργανισμός δεν έχει θεσπίσει διαδικασίες ώστε μετά την εκδήλωση συμβάντων και περιστατικών να αποτυπωθούν τα διδάγματα από τα συμβάντα και περιστατικά ασφάλειας πληροφοριών και να προσδιορίζουν κατά πόσον πρέπει να θεσπιστούν πρόσθετα μέτρα ασφάλειας για την πρόληψη παρόμοιων συμβάντων και περιστατικών.
1	1	Μετά από συμβάν ή περιστατικό ασφαλείας οι διαθέσιμες πληροφορίες συλλέγονται με ad hoc τρόπο ώστε να κατανοηθεί το περιστατικό ή το συμβάν.
2	1	Έχει θεσπιστεί διαδικασία σχετικά με τα βήματα που πρέπει να ακολουθούνται μετά από ένα περιστατικό ώστε ο οργανισμός να αξιολογεί το επίπεδο ασφάλειάς του και να αποτρέπονται παρόμοια συμβάντα και περιστατικά στο μέλλον.
3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται διαδικασίες μετά την εκδήλωση συμβάντων και περιστατικών, προκειμένου να αποτυπωθούν τα διδάγματα που έχουν αντληθεί από τα συμβάντα και περιστατικά ασφάλειας πληροφοριών και να προσδιορίζουν κατά πόσον πρέπει να θεσπιστούν πρόσθετα μέτρα ασφάλειας για την πρόληψη παρόμοιων συμβάντων και περιστατικών.

3	2	Για τη φάση των διδαγμάτων, εκτελούνται οι ακόλουθες δραστηριότητες οι οποίες αποτυπώνονται και στη διαδικασία: (α) Ο οργανισμός εντοπίζει τα διδάγματα που αντλήθηκαν από συμβάντα και τρωτά σημεία ασφάλειας πληροφοριών.
3	3	(β) Αναγνώριση, επανεξέταση και πραγματοποίηση βελτιώσεων στην εφαρμογή μέτρων ασφάλειας πληροφοριών.
3	4	(γ) Επανεξέταση και βελτίωση στην αξιολόγηση κινδύνου για την ασφάλεια των πληροφοριών.
3	5	(δ) Εξέταση της αποτελεσματικότητας των διαδικασιών, των πολιτικών, των εμπλεκόμενων με το περιστατικό (π.χ. Ομάδα ανταπόκρισης), την ανάλυση και την ανάκτηση από περιστατικό και την αντιμετώπιση τρωτών σημείων σε σχέση με την ασφάλεια πληροφοριών. Με βάση τα διδάγματα που αντλήθηκαν, εντοπίζονται και πραγματοποιούνται βελτιώσεις στο σχέδιο διαχείρισης συμβάντων ασφάλειας πληροφοριών.
3	6	Χρησιμοποιούνται οι πληροφορίες που λαμβάνονται από την αξιολόγηση των συμβάντων ή περιστατικών ασφάλειας πληροφοριών για τον επαναλαμβανόμενων ή υψηλού αντίκτυπου συμβάντων.
3	7	Εξετάζεται το ενδεχόμενο θέσπισης εκ των υστέρων διαδικασίας, η οποία περιλαμβάνει συνάντηση για την αξιολόγηση του συμβάντος ή περιστατικού με τους επηρεαζόμενους ιδιοκτήτες του συστήματος, τους διαχειριστές δεδομένων και άλλα ενδιαφερόμενα μέρη που συμμετείχαν στην αντιμετώπιση του περιστατικού, με σκοπό την ανταλλαγή διδαγμάτων και τον προσδιορισμό προληπτικών μέτρων.
4	1	Έχει θεσπιστεί και εφαρμόζεται διαδικασία η οποία περιλαμβάνει συνάντηση για την αξιολόγηση του συμβάντος ή περιστατικού με τους επηρεαζόμενους ιδιοκτήτες του συστήματος, τους διαχειριστές δεδομένων και άλλα ενδιαφερόμενα μέρη που συμμετείχαν στην αντιμετώπιση του περιστατικού, με σκοπό την ανταλλαγή διδαγμάτων και τον προσδιορισμό προληπτικών μέτρων.
4	2	Μετά από ένα περιστατικό ή ένα συμβάν αξιολογείται η αποτελεσματικότητα και η σωστή ανταπόκριση της ομάδας αντιμετώπισης περιστατικών ασφάλειας πληροφοριών.
4	3	Χρησιμοποιούνται στοιχεία από πραγματικά περιστατικά ασφαλείας πληροφοριών που μπορούν να συμπεριληφθούν στην εκπαίδευση του προσωπικού ως παραδείγματα για το τι θα μπορούσε να συμβεί, πώς να αντιδράσετε σε τέτοια περιστατικά και πώς να τα αποφύγετε στο μέλλον.
4	4	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Ελέγχεται εάν οι πληροφορίες του περιστατικού, οι σχετικοί φορείς επίθεσης και τα τρωτά σημεία μπορούν να κοινοποιηθούν με συνεργαζόμενους οργανισμούς για να βοηθήσουν στην αποτροπή εμφάνισης ίδιων περιστατικών στο περιβάλλον τους.
5	2	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	3	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

EIM5	**Μέτρο:** Ρυθμιστικές υποχρεώσεις κοινοποίησης συμβάντος και συνεργασίας. **Στόχος Μέτρου:** Να διασφαλίσει ότι ο οργανισμός ενημερώνει τα σχετικά ενδιαφερόμενα μέρη στην περίπτωση συμβάντων ή περιστατικών ασφάλειας, όπως περιγράφεται σε νομικές και ρυθμιστικές υποχρεώσεις. **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση διαδικασιών για τη διασφάλιση της συμμόρφωσης με ρυθμιστικές και νομοθετικές απαιτήσεις όσον αφορά την κοινοποίηση περιστατικών. Ο οργανισμός διασφαλίζει ότι υπάρχουν επαρκείς διαδικασίες κοινοποίησης και υποβολής εκθέσεων για συμβάντα και περιστατικά ασφάλειας πληροφοριών σε αρμόδιες ρυθμιστικές αρχές, όπως την ΑΨΑ. Στο πλαίσιο των δεδομένων προσωπικού χαρακτήρα, ο οργανισμός διασφαλίζει τη συμμόρφωση με τις σχετικές νομοθετικές και ρυθμιστικές διατάξεις που αφορούν την προστασία των δεδομένων προσωπικού χαρακτήρα και επικοινωνεί, όπου είναι απαραίτητο, με την αρμόδια αρχή προστασίας δεδομένων. **Πηγή:**

Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν έχει θεσπίσει διαδικασία για τη διασφάλιση της συμμόρφωσης με ρυθμιστικές και νομοθετικές απαιτήσεις όσον αφορά την κοινοποίηση περιστατικών.
1	1	Τα σχετικά ενδιαφερόμενα μέρη στην περίπτωση συμβάντων ή περιστατικών ασφάλειας ενημερώνονται με τρόπο ad hoc.
2	1	Έχουν καταγραφεί σε λίστα τα σχετικά στοιχεία επικοινωνίας και τα ενδιαφερόμενα μέρη τα οποία πρέπει να ενημερωθούν στην περίπτωση συμβάντων ή περιστατικών ασφάλειας.
2	2	Στην λίστα έχει καταγραφεί επίσης, το χρονικό διάστημα στο οποίο πρέπει να γίνει η ενημέρωση, το είδος του περιστατικού που αφορά η ενημέρωση και το υπεύθυνο άτομο από την μεριά του οργανισμού.
3	1	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται διαδικασία για τη διασφάλιση της συμμόρφωσης με ρυθμιστικές και νομοθετικές απαιτήσεις όσον αφορά την κοινοποίηση περιστατικών.
3	2	Διασφαλίζεται ότι υπάρχουν επαρκείς διαδικασίες κοινοποίησης και υποβολής εκθέσεων για συμβάντα και περιστατικά ασφάλειας πληροφοριών σε αρμόδιες ρυθμιστικές αρχές, όπως την ΑΨΑ.
3	3	Στο πλαίσιο των δεδομένων προσωπικού χαρακτήρα,διασφαλίζεται η συμμόρφωση με τις σχετικές νομοθετικές και ρυθμιστικές διατάξεις που αφορούν την προστασία των δεδομένων προσωπικού χαρακτήρα και επικοινωνεί, όπου είναι απαραίτητο, με την αρμόδια αρχή προστασίας δεδομένων.
3	4	Έχουν ορισθεί συγκεκριμένες αρμοδιότητες και υπευθυνότητες σε σχέση με την γνωστοποίηση των περιστατικών στις ρυθμιστικές αρχές και έχουν ανατεθεί εγγράφως στα αντίστοιχα άτομα ή ρόλους. Σε αυτά περιλαμβάνονται και οι αρμοδιότητες του Υπεύθυνου ασφάλειας δικτύων και πληροφοριών όπως αναφέρεται στο [GOV1].
4	1	Έχουν σχεδιασθεί και διενεργούνται σε προκαθορισμένους χρόνους ασκήσεις προσομοίωσης περιστατικών ασφαλείας, με σκοπό την αποτύπωση και τον έλεγχο του χρόνου κοινοποίησης και υποβολής εκθέσεων για συμβάντα και περιστατικά ασφάλειας πληροφοριών σε αρμόδιες ρυθμιστικές αρχές ώστε να υπάρχει συμμόρφωση με τις ρυθμιστικές και νομοθετικές απαιτήσεις όσον αφορά την κοινοποίηση περιστατικών.
4	2	Έχουν δημιουργηθεί σχετικές πρότυπες φόρμες συμπληρώνονται από το αρμόδιο προσωπικό σε περίπτωση περιστατικού ανά είδος και ανά σχετική αρχή.
4	3	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.

5	1	Έχει δημιουργηθεί μια σειρά από αναλυτικές οδηγίες / οδηγούς που περιέχουν τα βήματα που πρέπει να ακολουθηθούν σε διακριτές χρονικές στιγμές από το αρμόδιο προσωπικό για την ορθή, έγκαιρη και αποτελεσματική πληροφόρηση των ανά περίπτωση εμπλεκόμενων αρχών. (Οι οδηγοί περιέχουν χρονικά διαστήματα, ρόλους, πρακτικά, οδηγίες για ψηφιακά πειστήρια, οδηγούς για τον προσδιορισμό ποιοι πρέπει να είναι οι αποδέκτες της ενημέρωσης – π.χ. σε περίπτωση περιστατικού που αφορά δεδομένα προσωπικού χαρακτήρα αν απαιτείται να ενημερωθούν και τα υποκείμενα -, πρότυπα κείμενα ενημέρωσης κ.α.)
5	2	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	3	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
ΕΙΜ6		**Μέτρο:** Επικοινωνία με ενδιαφερόμενους φορείς για συμβάντα και περιστατικά. **Στόχος Μέτρου:** Να εξασφαλίζει ότι ο οργανισμός κοινοποιεί πληροφορίες σχετικά με συμβάντα και περιστατικά ασφάλειας δικτύων και πληροφοριών σε εσωτερικούς και εξωτερικούς ενδιαφερόμενους φορείς. **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση διαδικασιών για τη διασφάλιση σχετικής επικοινωνίας όσον αφορά συμβάντα και περιστατικά ασφάλειας πληροφοριών προς εξωτερικούς και εσωτερικούς αποδέκτες, προκειμένου να εξασφαλίζεται η επίγνωση του συμβάντος ή περιστατικού και να παρέχεται στους εξωτερικούς και εσωτερικούς ενδιαφερόμενους φορείς η δυνατότητα να καθορίζουν κατάλληλα μέτρα αντίδρασης, εάν αυτό είναι απαραίτητο. Ο οργανισμός πρέπει να εξετάζει το ενδεχόμενο συνεργασίας με εξωτερικούς και εσωτερικούς ενδιαφερόμενους φορείς όσον αφορά τον περιορισμό συμβάντων και περιστατικών, προκειμένου να ελαχιστοποιούνται οι σχετικές επιπτώσεις και οι εκ των υστέρων δραστηριότητες προκειμένου να καθορίζονται προληπτικά μέτρα, όπως με την ΑΨΑ και τις υπηρεσίες έκτακτης ανάγκης. **Πηγή:**
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**
0	1	Ο οργανισμός δεν πραγματοποιεί επικοινωνία με ενδιαφερόμενους φορείς για συμβάντα και περιστατικά.
1	1	Πραγματοποιείται ad hoc και όχι συστηματικά επικοινωνία με ενδιαφερόμενους φορείς για συμβάντα και περιστατικά ασφαλείας.
2	1	Διατηρείται λίστα με ενδιαφερόμενους φορείς με τους οποίους επικοινωνεί συστηματικά προκειμένου να εξασφαλίζεται η επίγνωση του συμβάντος.
3	1	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται διαδικασία για τη διασφάλιση σχετικής επικοινωνίας όσον αφορά συμβάντα και περιστατικά ασφάλειας πληροφοριών προς εξωτερικούς και εσωτερικούς αποδέκτες, προκειμένου να εξασφαλίζεται η επίγνωση του συμβάντος ή περιστατικού και να παρέχεται στους εξωτερικούς και εσωτερικούς ενδιαφερόμενους φορείς η δυνατότητα να καθορίζουν κατάλληλα μέτρα αντίδρασης, εάν αυτό είναι απαραίτητο.
3	2	Εξετάζεται το ενδεχόμενο συνεργασίας με εξωτερικούς και εσωτερικούς ενδιαφερόμενους φορείς όσον αφορά τον περιορισμό συμβάντων και περιστατικών, προκειμένου να ελαχιστοποιούνται οι σχετικές επιπτώσεις και οι εκ των υστέρων δραστηριότητες προκειμένου να καθορίζονται προληπτικά μέτρα, όπως με την ΑΨΑ και τις υπηρεσίες έκτακτης ανάγκης.
4	1	Υπάρχει συνεργασία με εξωτερικούς και εσωτερικούς ενδιαφερόμενους φορείς όσον αφορά τον περιορισμό συμβάντων και περιστατικών, προκειμένου να ελαχιστοποιούνται οι σχετικές επιπτώσεις και οι εκ των υστέρων δραστηριότητες προκειμένου να καθορίζονται προληπτικά μέτρα, όπως με την ΑΨΑ και τις υπηρεσίες έκτακτης ανάγκης.
4	2	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.

5	1	Χρησιμοποιούνται αυτοματοποιημένοι μηχανισμοί για να αυξηθεί η διαθεσιμότητα πληροφοριών και υποστήριξης που σχετίζονται με την αντιμετώπιση περιστατικών. (π.χ. Να υπάρχει η δυνατότητα να λαμβάνει ο οργανισμός αυτοματοποιημένες πληροφορίες μέσω μηνυμάτων ή emails ως μέρος της αυξανόμενης κατανόησης των τρεχουσών δυνατοτήτων απόκρισης και υποστήριξης.)
5	2	Λαμβάνονται αλλά και διαμοιράζονται έγκυρες πληροφορίες Cyber threat intelligence μέσω σχετικών επαφών με σχετικούς οργανισμούς (όπως είναι sector specific ISAC's, CSIRTs, coallitions κλπ).
5	3	Υπάρχουν διαδικασίες που αποτυπώνουν τα μέτρα και βήματα που διενεργεί ο οργανισμός σε περίπτωση που ανταλλάσσει σχετικές πληροφορίες ώστε να μπορούν να μεταφερθούν αποτελεσματικά, να μπορούν να αναγνωστούν αποτελεσματικά και να μην εκθέσουν εσωτερικές εμπιστευτικές πληροφορίες του οργανισμού σε άλλα μη εξουσιοδοτημένα μέρη. Στα πλαίσια των διαδικασιών αυτών θα προσδιορίζει και πρωτόκολλα, εργαλεία και δομή της πληροφορίας.
5	4	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	5	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

Κατηγορία		ΕΠΙΧΕΙΡΙΣΙΑΚΗ ΣΥΝΕΧΕΙΑ ΚΑΙ ΑΝΘΕΚΤΙΚΟΤΗΤΑ
BCR1		**Μέτρο:** Ανάλυση επιχειρησιακών επιπτώσεων **Στόχος Μέτρου:** Να εξασφαλιστεί ότι ο οργανισμός έχει αναλύσει και αξιολογήσει τις κρίσιμες επιχειρηματικές διαδικασίες που πρέπει να ληφθεί υπόψη στο σχέδιο επιχειρησιακής συνέχειας, ώστε να μπορέσει ο οργανισμός να αποκαταστήσει τις επιχειρηματικές διαδικασίες σε αποδεκτό επίπεδο, το συντομότερο δυνατόν, σε περίπτωση συμβάντος ή περιστατικού. **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση διαδικασίας ανάλυσης επιχειρησιακών επιπτώσεων προκειμένου να προσδιορίσει όλα τα κρίσιμα περιουσιακά στοιχεία εντός του οργανισμού. Η ανάλυση των επιχειρησιακών επιπτώσεων θα επιτρέψει στον οργανισμό να ιεραρχήσει τις λειτουργίες και τα συστήματα με βάση την αναγκαιότητα παροχής επιχειρησιακών υπηρεσιών. Η ανάλυση των επιχειρησιακών επιπτώσεων διενεργείται βάσει συστήματος ταξινόμησης που λαμβάνει υπόψη καθορισμένα επίπεδα κρισιμότητας και εξετάζει εάν κρίσιμες λειτουργίες ή συστήματα λειτουργούν αυτόνομα ή συνδέονται με άλλη λειτουργία ή σύστημα του οργανισμού. **Πηγή:** 22313
Επίπεδο Ωριμότητας	**Επιμέρους**	**Περιγραφή Ελέγχου**
0	1	Ο οργανισμός δεν έχει διενεργήσει ανάλυση επιχειρησιακών επιπτώσεων.
1	1	Έχει γίνει μια ανάλυση των βασικών υπηρεσιών που παρέχει και έχει αναγνωρίσει και κάποιες από τις επιχειρησιακές του δραστηριότητες αλλά χωρίς ο τρόπος αναγνώρισης να είναι συστηματικός.
2	1	Έχει δημιουργηθεί μια απλή διαδικασία για την αναγνώριση των κρίσιμων επιχειρησιακών δραστηριοτήτων.
2	2	Τα αποτελέσματα της διενέργειας της συγκεκριμένης διαδικασίας καταγράφονται στα πλαίσια του ενιαίου κατάλογο στοιχείων ενεργητικού, συστημάτων και διαδικασιών εντός του οργανισμού όπως αναφέρεται στο [RM2].
2	3	Έχουν ανατεθεί ρόλοι και αρμοδιότητες σε σχέση με την συγκεκριμένη διαδικασία σε κατάλληλο προσωπικό.
2	4	Η διαδικασία διενεργείται τουλάχιστον μια φορά το χρόνο.
3	1	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται διαδικασία ανάλυσης επιχειρησιακών επιπτώσεων προκειμένου να προσδιορίσει όλα τα κρίσιμα περιουσιακά στοιχεία εντός του οργανισμού.
3	2	Η ανάλυση των επιχειρησιακών επιπτώσεων επιτρέπει στον οργανισμό να ιεραρχήσει τις λειτουργίες και τα συστήματα με βάση την αναγκαιότητα παροχής επιχειρησιακών υπηρεσιών.
3	3	Η ανάλυση των επιχειρησιακών επιπτώσεων διενεργείται βάσει συστήματος ταξινόμησης που λαμβάνει υπόψη καθορισμένα επίπεδα κρισιμότητας και εξετάζει εάν κρίσιμες λειτουργίες ή συστήματα λειτουργούν αυτόνομα ή συνδέονται με άλλη λειτουργία ή σύστημα του οργανισμού.
3	4	Η διαδικασία περιλαμβάνει: (α) τον καθορισμό κριτηρίων αξιολόγησης σχετικά με το πλαίσιο του οργανισμού, συμπεριλαμβανομένου των τύπων επιπτώσεων και χρονικά πλαίσια
3	4	(β) τον εντοπισμό δραστηριοτήτων που υποστηρίζουν την παράδοση των προϊόντων και των υπηρεσιών του οργανισμού
3	5	(γ) χρήση των κριτηρίων αξιολόγησης για την αξιολόγηση των αναμενόμενων επιπτώσεων με την πάροδο του χρόνου που προκύπτουν από τη διακοπή αυτών των δραστηριοτήτων
3	6	(δ) εκτίμηση του χρόνου εντός του οποίου οι επιπτώσεις από τη μη επανέναρξη των δραστηριοτήτων θα γίνουν μη αποδεκτές
3	7	(ε) καθορισμό χρονικών πλαισίων εντός του χρόνου που προσδιορίζεται παραπάνω για την επανέναρξη των δραστηριοτήτων σε καθορισμένες ελάχιστες αποδεκτές λειτουργικότητες
3	8	(ζ) τον προσδιορισμό των δραστηριοτήτων με προτεραιότητα

3	9	(η) εντοπισμό των εξαρτήσεων των δραστηριοτήτων με προτεραιότητα, συμπεριλαμβανομένων των ανθρώπων, των πληροφοριών και των δεδομένων, των κτιρίων, των χώρων εργασίας και των σχετικών υπηρεσιών κοινής ωφέλειας, του εξοπλισμού και των αναλώσιμων, των συστημάτων ICT, μεταφορές και logistics, χρηματοδότηση και συνεργάτες και εφοδιαστική αλυσίδα
3	10	Υλοποιείται σχετική διαδικασία και εξάγονται αποτελέσματα σε σχετική αναφορά η οποία παρουσιάζεται στην διοίκηση από την οποία και εγκρίνεται.
3	11	Η αναφορά περιέχει κατ' ελάχιστον τα στοιχεία για τα RTO, MAO/MTPD, RPO και MBCO που έχει αναγνωρίσει ο οργανισμός ανά διεργασία ή και δραστηριότητα.
4	1	Διενεργούνταιο workshops και συναντήσεις με αντιπροσωπευτικό μέρος του προσωπικού ανά εμπλεκόμενο τμήμα ή διεργασία για την λήψη των στοιχείων για την ανάλυση επιχειρησιακών επιπτώσεων.
4	2	Στα πλαίσια της ανάλυσης, το προσωπικό αναγνωρίζει, αναλύει και αξιολογεί κινδύνους που μπορεί να οδηγήσουν στην διακύβευσης της δυνατότητας του οργανισμού να συνεχίσει την λειτουργία του συγκεκριμένου τμήματος / διεργασίας / υπηρεσίας.
4	3	Οι κλίμακες που χρησιμοποιούνται για την αξιολόγηση των αναμενόμενων επιπτώσεων αλλά και για την ανάλυση και αξιολόγηση κινδύνων είναι εγκεκριμένα από την διοίκηση και εκφρασμένα με τέτοιο τρόπο ώστε να είναι κατανοητά από το σύνολο του εμπλεκόμενου προσωπικού (ακόμα και από αυτό που δεν έχει κάποια ειδική γνώση σε σχέση με την πληροφορική ή την επιχειρησιακή συνέχεια).
4	4	Τα κριτήρια σε κάθε περίπτωση λαμβάνουν υπόψη και είναι ευθυγραμμισμένα με τις προδιαγραφές της σχετικής εφαρμόσιμης νομοθεσίας.
4	5	Η αξιολόγηση της επίπτωσης γίνεται τουλάχιστον σε επίπεδο: επίπτωσης στην συμμόρφωση του οργανισμού, επίπτωση στην επίτευξη των στόχων του οργανισμού, οικονομική επίπτωση, επίπτωση στην φήμη, επίπτωση στην υγεία, ασφάλεια και ευμάρεια του προσωπικού και επίπτωση στην υγεία, ασφάλεια και ευμάρεια των χρηστών των υπηρεσιών.
4	6	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Χρησιμοποιείται αυτοματοποιημένο εργαλείο για την υποστήριξη της υλοποίησης της διαδικασίας ανάλυσης των επιχειρησιακών επιπτώσεων. Μέσα από το εργαλείο, ο οργανισμός έχει την δυνατότητα να αποτυπώνει τις εξαρτήσεις ανάμεσα στους πόρους (άτομα, εξοπλισμό, IT διεργασίες, αρχεία κ.α.) αλλά και μεταξύ των διαφόρων διεργασιών. Ο οργανισμός διενεργεί επικαιροποίηση των στοιχείων της ανάλυσης επιχειρησιακών επιπτώσεων μια φορά το χρόνο (κατ΄ελάχιστο) και σε περίπτωση σημαντικών αλλαγών.
5	2	Διενεργούνται σχετικές δοκιμές, αναλύσεις και ασκήσεις για έλεγχο της εγκυρότητας των στοιχείων της ανάλυσης επιχειρησιακών επιπτώσεων. Σε περίπτωση αναγνωρισμένης απόκλισης, διενεργεί άμεσα κατάλληλες ενέργειες για την αντιμετώπιση της αιτίας της απόκλισης και την διόρθωση του προβλήματος.
5	3	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	4	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

BCR2	**Μέτρο:** Σχέδιο επιχειρησιακής συνέχειας **Στόχος Μέτρου:** Να εξασφαλιστεί ότι ο οργανισμός διαθέτει σχέδιο για τη διατήρηση της συνέχειας των κρίσιμων επιχειρηματικών διαδικασιών και την αποκατάσταση κατά τη διάρκεια συμβάντος ή περιστατικού και μετά από αυτό. **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση σχεδίου επιχειρησιακής συνέχειας προκειμένου να διασφαλιστεί ότι ο οργανισμός μπορεί να ανταποκρίνεται σε καταστάσεις έκτακτης ανάγκης με άμεσο και κατάλληλο τρόπο, και είναι σε θέση να διατηρεί επιχειρηματικές λειτουργίες ελαχιστοποιώντας τις συνέπειες και τις ζημίες που προκύπτουν από ένα περιστατικό. Το σχέδιο επιχειρησιακής συνέχειας περιλαμβάνει το σχέδιο αποκατάστασης από καταστροφή, όπως περιγράφεται στο μέτρο [BCR4] και λαμβάνει υπόψη την ανάλυση των επιχειρησιακών επιπτώσεων. **Πηγή:**

Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν έχει καταρτίσει σχέδιο επιχειρησιακής συνέχειας.
1	1	Έχουν προσδιορισθεί κάποια work arounds σε περίπτωση περιστατικού διαταραχής (disruptive) τα οποία όμως είναι περιστασιακά, δεν στηρίζονται στην ανάλυση επιχειρησιακών επιπτώσεων και δεν είναι πλήρως καταγεγραμμένα.
2	1	Έχουν δομηθεί σχέδια επιχειρησιακής συνέχειας για τις κρίσιμες δραστηριότητες.
2	2	Τα συγκεκριμένα σχέδια είναι καταγεγραμμένα αλλά δεν στηρίζονται σε δομημένα στοιχεία Business Impact Analysis.
2	3	Στα σχέδια περιέχονται στοιχεία σε σχέση με τον επιθυμητό χρόνο ανάκαμψης ανά δραστηριότητα καθώς και ενέργειες που πρέπει να υλοποιηθούν σε περίπτωση διαταραχής.
3	1	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται σχέδιο επιχειρησιακής συνέχειας προκειμένου να διασφαλιστεί ότι ο οργανισμός μπορεί να ανταποκρίνεται σε καταστάσεις έκτακτης ανάγκης με άμεσο και κατάλληλο τρόπο, και είναι σε θέση να διατηρεί επιχειρηματικές λειτουργίες ελαχιστοποιώντας τις συνέπειες και τις ζημίες που προκύπτουν από ένα περιστατικό.
3	2	Το σχέδιο επιχειρησιακής συνέχειας περιλαμβάνει το σχέδιο αποκατάστασης από καταστροφή, όπως περιγράφεται στο μέτρο [BCR4] και λαμβάνει υπόψη την ανάλυση των επιχειρησιακών επιπτώσεων [BCR1].
3	3	Έχει δημιουργηθεί ένα (ή πολλαπλά) σχέδια επιχειρησιακής συνέχειας με έμφαση στις επιπτώσεις που μπορεί να αντιμετωπίσει ένας οργανισμός ως αποτέλεσμα μιας διαταραχής και όχι τον/ τους λόγο/λόγους που μπορεί να οδηγήσουν στις επιπτώσεις αυτές.
3	4	Το/ τα σχέδιο/α περιλαμβάνουν: (α) το σκοπό, το πεδίο εφαρμογής και τους στόχους του κάθε σχεδίου.
3	5	(β) τις παραδοχές και τις εξαιρέσεις του σχεδίου
3	6	(γ) τους ρόλους και τις ευθύνες της ομάδας που θα εφαρμόσει το σχέδιο.
3	7	(δ) τα βήματα και τις λεπτομέρειες τους που θα κάνουν οι ομάδες προκειμένου να (Α) συνεχίζουν ή ανακτήσουν τις επιχειρησιακές δραστηριότητες σε προκαθορισμένο επίπεδο και εντός προσυμφωνημένου και (Β) αποδεκτού χρονικού διαστήματος και να παρακολουθήσουν τις επιπτώσεις του περιστατικού και ανταποκριθούν σε αυτές ώστε να μειώσουν την έκτασή του στους ανθρώπους και στον οργανισμό όσο γίνεται περισσότερο, λαμβάνοντας υπόψη την υγεία και ασφάλεια των ατόμων, τον περιορισμό της επέκτασης της επίπτωσης της διαταραχής και την μείωση των σχετικών επιπτώσεων, την επίπτωση στο περιβάλλον και στην κοινωνία.
3	8	(ε) Τα RTO/ RPO / MAO-MTPD ανά διεργασία / υπηρεσία και αν είναι εφικτό δραστηριότητα
3	9	(ζ) Την διαδικασία και τις αρμοδιότητες σε σχέση με την ενημέρωση, διάγνωση, απόφαση για ενεργοποίηση και υλοποίηση του σχεδίου
3	10	(η) τις εσωτερικές και εξωτερικές αλληλεξαρτήσεις και τις προβλέψεις που έχουν γίνει για την συνέχειά τους
3	11	(θ) τις απαιτήσεις πόρων
3	12	(ι) τους τρόπους και τα στοιχεία επικοινωνίας μεταξύ των ενδιαφερόμενων μερών

3	13	(κ) την ανάλυση των απαιτούμενων ανθρώπινων πόρων συναρτήσει του χρόνου
3	14	(λ) την σχετική τεκμηρίωση που θα τηρείται σε περίπτωση ενεργοποίησης και
3	15	(μ) την διαδικασία υπαναχώρησης (standing down)
3	16	Κάθε σχέδιο επιχειρησιακής συνέχειας είναι γνωστό στο εμπλεκόμενο προσωπικό και είναι διαθέσιμο όταν το χρειάζονται.
4	1	Αναλύονται οι δυνατές στρατηγικές επιχειρησιακής συνέχειας και ανάκαμψης από καταστροφή και ξεχωρίζουν και καταγράφονται εκείνες που ανά διεργασία / ανά είδος επίπτωσης / ανά RTO /MAO έχουν την δυνατότητα να επιτρέψουν στον οργανισμό να ανακάμψει τις επιχειρησιακές του δραστηριότητες σε προδιαγεγραμμένο αποδεκτό χρόνο και σε προκαθορισμένο επίπεδο.
4	2	Οι επιλογές των στρατηγικών καταγράφονται και παρουσιάζονται στην διοίκηση του οργανισμού, συνοδευόμενες και από στοιχεία κόστους οφέλους (Cost Benefit analysis).
4	3	Ο διοίκηση του οργανισμού εγκρίνει τις αποδεκτές στρατηγικές.
4	4	Καταρτίζονται σχέδια επιχειρησιακής συνέχειας και ανάκαμψης από καταστροφή σύμφωνα με τις αποδεκτές και εγκεκριμένες από τη διοίκηση στρατηγικές.
4	5	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Κάθε σχέδιο επιχειρησιακής συνέχειας έχει έναν ιδιοκτήτη, ο οποίος είναι υπεύθυνος για την παρακολούθησή του καθ' όλο τον κύκλο ζωής του.
5	2	Ο Υπεύθυνος δημιουργεί πλάνο ενεργειών για την υλοποίηση των προβλέψεων του κάθε σχεδίου επιχειρησιακής συνέχειας.
5	3	Το πλάνο ενεργειών περιλαμβάνει ενέργειες όπως: συντονισμός και διαθεσιμότητα των σχετικών πόρων, εκπαίδευση προσωπικού, δημιουργία σχετικών οδηγιών, δημιουργία πλάνου δοκιμών για τον έλεγχο της αποτελεσματικότητας του σχεδίου, ενέργειες για την ασφαλή αποθήκευση του σχεδίου όπου χρειάζεται και την κατάλληλη διαθεσιμότητά του όταν χρειαστεί, τον συντονισμό για την καταγραφή και την επικαιροποίηση των call trees όπου απαιτείται, αναγνώριση ρόλων για την ανταπόκριση, την λειτουργία, την ενεργοποίηση και τον έλεγχο του σχεδίου κ.α.
5	4	Ο υπεύθυνος παρακολουθεί τις ενέργειες για την ετοιμότητα του οργανισμού ανά πλάνο επιχειρησιακής συνέχειας και αναφέρει στην διοίκηση το βαθμό ετοιμότητας και την επίδοσή του.
5	5	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	6	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

BCR3	**Μέτρο:** Ασκήσεις και προσομοιώσεις επιχειρησιακής συνέχειας **Στόχος Μέτρου:** Να διασφαλιστεί ότι ο οργανισμός και τα στελέχη του γνωρίζουν τις ευθύνες τους κατά τη διάρκεια ενός συμβάντος ή περιστατικού που ενεργοποιεί το σχέδιο επιχειρησιακής συνέχειας. **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση μέτρων για τον έλεγχο, την αναθεώρηση και τη βελτίωση του σχεδίου επιχειρησιακής συνέχειας μέσω ασκήσεων όπου προσομοιώνονται συμβάντα και περιστατικά στον οργανισμό, με σκοπό τον έλεγχο της ανταπόκρισης του οργανισμού σε παρόμοια συμβάντα και περιστατικά, και τη βελτίωση των διαδικασιών επιχειρησιακής συνέχειας. Οι ασκήσεις και οι προσομοιώσεις επιχειρησιακής συνέχειας θα πρέπει να παρέχουν στον οργανισμό τη δυνατότητα να εντοπίζει ευκαιρίες βελτίωσης και να επιτυγχάνει καλύτερα αποτελέσματα με την πάροδο του χρόνου. Ο οργανισμός θα πρέπει να εξετάσει το ενδεχόμενο να συνδέσει το σχέδιο επιχειρησιακής συνέχειας με τις διαδικασίες διαχείρισης αλλαγών, όπως περιγράφονται στο [CM1], προκειμένου να λαμβάνονται υπόψη στο σχέδιο επιχειρησιακής συνέχειας οι συνέπειες από όποιες αλλαγές εντός του οργανισμού. Ο οργανισμός θα πρέπει να διενεργεί ασκήσεις και προσομοιώσεις επιχειρησιακής συνέχειας σε τακτά χρονικά διαστήματα, προκειμένου οι εργαζόμενοι να είσαι σε επαγρύπνηση για συμβάντα και περιστατικά που θα μπορούσαν να βλάψουν τον οργανισμό. Κατά την κατάρτιση του σχεδίου επιχειρησιακής συνέχειας, ο οργανισμός εξετάζει και την αποκατάσταση από καταστροφή, όπως ορίζεται στο μέτρο [BCR4]. **Πηγή:**

Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν έχει καταρτίσει σχέδιο επιχειρησιακής συνέχειας.
1	1	Έχουν προσδιορισθεί κάποια work arounds σε περίπτωση περιστατικού διαταραχής (disruptive) τα οποία όμως είναι περιστασιακά, δεν στηρίζονται στην ανάλυση επιχειρησιακών επιπτώσεων και δεν είναι πλήρως καταγεγραμμένα και δεν εξασκούνται με συστηματικό τρόπο.
2	1	Έχουν δομηθεί σχέδια επιχειρησιακής συνέχειας για τις κρίσιμες δραστηριότητες.
2	2	Τα συγκεκριμένα σχέδια είναι καταγεγραμμένα αλλά δεν στηρίζονται σε δομημένα στοιχεία Business Impact Analysis.
2	3	Στα σχέδια περιέχονται στοιχεία σε σχέση με τον επιθυμητό χρόνο ανάκαμψης ανά δραστηριότητα καθώς και ενέργειες που πρέπει να υλοποιηθούν για την επίτευξή τους σε περίπτωση διαταραχής.
2	4	Έχει γίνει τουλάχιστον μια δοκιμή των σχεδίων επιχειρησιακής συνέχειας κατά τη διάρκεια των δυο τελευταίων ετών.
3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται μέτρα για τον έλεγχο, την αναθεώρηση και τη βελτίωση του σχεδίου επιχειρησιακής συνέχειας μέσω ασκήσεων όπου προσομοιώνονται συμβάντα και περιστατικά στον οργανισμό, με σκοπό τον έλεγχο της ανταπόκρισης του οργανισμού σε παρόμοια συμβάντα και περιστατικά, και τη βελτίωση των διαδικασιών επιχειρησιακής συνέχειας.
3	2	Οι ασκήσεις και οι προσομοιώσεις επιχειρησιακής συνέχειας παρέχουν στον οργανισμό τη δυνατότητα να εντοπίζει ευκαιρίες βελτίωσης και να επιτυγχάνει καλύτερα αποτελέσματα με την πάροδο του χρόνου.
3	3	Διενεργούνται ασκήσεις και προσομοιώσεις επιχειρησιακής συνέχειας σε τακτά χρονικά διαστήματα, προκειμένου οι εργαζόμενοι να είσαι σε επαγρύπνηση για συμβάντα και περιστατικά που θα μπορούσαν να βλάψουν τον οργανισμό. Κατά την κατάρτιση του σχεδίου επιχειρησιακής συνέχειας, ο οργανισμός εξετάζει και την αποκατάσταση από καταστροφή, όπως ορίζεται στο μέτρο [BCR4].
3	4	Οι δοκιμές και οι ασκήσεις γίνονται τουλάχιστον μια φορά το χρόνο και καλύπτουν το σύνολο των προβλέψεων επιχειρησιακής συνέχειας τουλάχιστον μια φορά και με έναν τουλάχιστον τρόπο (ακόμα και αν είναι table top).
4	1	Έχει δημιουργηθεί σχέδιο / πρόγραμμα ασκήσεων και δοκιμών.

4	2	Το πρόγραμμα εξασφαλίζει ότι διενεργούνται ασκήσεις και δοκιμές που είναι συμβατές με τους στόχους του οργανισμού για επιχειρησιακή συνέχεια, στηρίζονται σε κατάλληλα σενάρια (τα οποία είναι ξεκάθαρα και καταγεγραμμένα, κάθε ένα εκ των οποίων χει συγκεκριμένο στόχο), στοχεύουν σε συγκεκριμένες πτυχές των σχεδίων (π.χ. επικοινωνία, τεχνολογική ετοιμότητα, συνεργατικότητα, αποτελεσματικότητα κ.α.) και ότι όταν συνδυάζονται όλες οι ασκήσεις και δοκιμές στο διάστημα ενός ολόκληρου έτους, καταφέρουν να δοκιμάσουν το σύνολο των προβλέψεων επιχειρησιακής συνέχειας του οργανισμού με μια ποικιλία μεθόδων.
4	3	Για τις ασκήσεις και τις δοκιμές τηρούνται καταγεγραμμένα πρακτικά τα οποία αναφέρουν το ιστορικό της δοκιμής, τους χρόνους ανά βήμα σύμφωνα με το εφαρμόσιμο σχέδιο ή μέρος του σχεδίου, και πιθανές παρατηρήσεις.
4	4	Έχει συνδεθεί το σχέδιο επιχειρησιακής συνέχειας με τις διαδικασίες διαχείρισης αλλαγών, όπως περιγράφονται στο [CM1], προκειμένου να λαμβάνονται υπόψη στο σχέδιο επιχειρησιακής συνέχειας οι συνέπειες από όποιες αλλαγές εντός του οργανισμού.
4	5	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Έχει δημιουργηθεί σχέδιο / πρόγραμμα ασκήσεων και δοκιμών.
5	2	Το πρόγραμμα εξασφαλίζει ότι διενεργούνται ασκήσεις και δοκιμές που είναι συμβατές με τους στόχους του οργανισμού για επιχειρησιακή συνέχεια και στο σύνολό τους στο διάστημα ενός ολόκληρου έτους, καταφέρουν να δοκιμάσουν το σύνολο των προβλέψεων επιχειρησιακής συνέχειας του οργανισμού με μια ποικιλία μεθόδων.
5	3	Στα πλαίσια του πλάνου προβλέπεται και υλοποιείται τουλάχιστον σε ετήσια βάση μια πλήρης δοκιμή του/των σχεδίων επιχειρησιακής συνέχειας και του σχεδίου αποκατάστασης από καταστροφή. Σε περίπτωση λόγω της ιδιομορφίας του περιβάλλοντος του οργανισμού δεν είναι δυνατή η πλήρης δοκιμή, γίνεται καταγραφή της σχετικής αιτιολόγησης και δημιουργούνται τόσες ασκήσεις προσομοίωσης ή μικρότερες δοκιμές ώστε να είναι δυνατός ο έλεγχος του συνόλου τον προβλέψεων.
5	4	Στο βαθμό που είναι δυνατό, ζητείται η συμμετοχή σχετικών αρχών στην υλοποίηση των σχετικών δοκιμών. Σε περίπτωση που αυτό είναι εφικτό, ο οργανισμός διενεργεί προσομοιώσεις περιστατικών σε περιβάλλοντα digital tweens.
5	5	Διενεργείται σχετική ανάλυση και αξιολόγηση κινδύνου για τον προσδιορισμό του βαθμού ενημέρωσης που θα έχει το προσωπικό σχετικά με την υλοποίηση των δοκιμών, λαμβάνοντας και ως γνώμονα την υγεία και ασφάλεια του προσωπικού.
5	6	Διενεργούνται συζητήσεις και συναντήσεις μετά τις δοκιμές για την αξιολόγηση της επίδοσης των επιμέρους μερών των σχεδίων, την ανάδειξη προβλημάτων και την αναγνώριση σημείων βελτίωσης.
5	7	Οι δοκιμές και οι συζητήσεις συντονίζονται και παρακολουθούνται από ανεξάρτητο παρατηρητή (μπορεί να είναι εσωτερικό άτομο του οργανισμού αλλά πρέπει να μην συμμετέχει στην διαδικασία της ανάκαμψης, αντιμετώπισης και λειτουργίας).
5	8	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	9	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

BCR4	**Μέτρο:** Σχέδιο αποκατάστασης από καταστροφή **Στόχος Μέτρου:** Να εξασφαλιστεί ότι ο οργανισμός διαθέτει σχέδιο για την αποκατάσταση των συστημάτων κρίσιμων πληροφοριών σε αποδεκτό επίπεδο κατά τη διάρκεια ή μετά από περιστατικό. **Περιγραφή Μέτρου:** Θέσπιση, εφαρμογή και διατήρηση σχεδίου αποκατάστασης από καταστροφή, προκειμένου να διασφαλίζεται η αποκατάσταση και η ανάκτηση όλων των κρίσιμων διαδικασιών των συστημάτων πληροφορικής και των υποστηρικτικών στοιχείων ενεργητικού, όπως η παροχή ηλεκτρικής ενέργειας, μετά την ύπαρξη ενός περιστατικού. Το σχέδιο αποκατάστασης από καταστροφή θα πρέπει να περιλαμβάνει σαφείς οδηγίες για το προσωπικό πληροφορικής, ώστε να εξασφαλίζεται έγκαιρη και αποτελεσματική αντίδραση σε όλα τα περιστατικά που επηρεάζουν το περιβάλλον πληροφορικής του οργανισμού. Στο σχέδιο αποκατάστασης από καταστροφή θα πρέπει να καθορίζεται ο στόχος του σημείου ανάκτησης (RPO) και ο στόχος για τον χρόνο αποκατάστασης (RTO), ώστε να αποφεύγονται μη αποδεκτές συνέπειες για τον οργανισμό. **Πηγή:**

Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν έχει καταρτίσει σχέδιο αποκατάστασης από καταστροφή
1	1	Έχουν προσδιορισθεί κάποια βήματα εκτελούνται σε περίπτωση καταστροφής τα οποία όμως είναι περιστασιακά, δεν στηρίζονται στην ανάλυση επιχειρησιακών επιπτώσεων και δεν είναι πλήρως καταγεγραμμένα.
2	1	Έχει δομηθεί σχέδιο αποκατάστασης από καταστροφή για τις κρίσιμες δραστηριότητες.
2	2	Το συγκεκριμένο σχέδιο είναι καταγεγραμμένο αλλά δεν στηρίζεται σε δομημένα στοιχεία Business Impact Analysis.
2	3	Το σχέδιο στηρίζεται στην ύπαρξη εφεδρικών αντιγράφων ασφαλείας και στην χρήση τους για την ανάκαμψη στον ίδιο ή σε διαφορετικό χώρο σε περίπτωση καταστροφής.
3	1	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται σχέδιο αποκατάστασης από καταστροφή, προκειμένου να διασφαλίζεται η αποκατάσταση και η ανάκτηση όλων των κρίσιμων διαδικασιών των συστημάτων πληροφορικής και των υποστηρικτικών στοιχείων ενεργητικού, όπως η παροχή ηλεκτρικής ενέργειας, μετά την ύπαρξη ενός περιστατικού.
3	2	Το σχέδιο αποκατάστασης από καταστροφή περιλαμβάνει σαφείς οδηγίες για το προσωπικό πληροφορικής, ώστε να εξασφαλίζεται έγκαιρη και αποτελεσματική αντίδραση σε όλα τα περιστατικά που επηρεάζουν το περιβάλλον πληροφορικής του οργανισμού.
3	3	Στο σχέδιο αποκατάστασης από καταστροφή καθορίζεται ο στόχος του σημείου ανάκτησης (RPO) και ο στόχος για τον χρόνο αποκατάστασης (RTO), ώστε να αποφεύγονται μη αποδεκτές συνέπειες για τον οργανισμό.
3	4	Το σχέδιο αποκατάστασης από καταστροφή περιλαμβάνει όλους τους πόρους που χρειάζονται και έχουν αναγνωριστεί κατά την ανάλυση επιχειρησιακών επιπτώσεων ότι απαιτούνται για την ορθή λειτουργία των κρίσιμων διεργασιών εντός προκαθορισμένου χρονικού διαστήματος.
3	5	Το προσωπικό που εμπλέκεται στην λειτουργία του σχεδίου αποκατάστασης από καταστροφή είναι πλήρως ενημερωμένο σχετικά με τις αρμοδιότητες και τις υπευθυνότητές του.
3	6	Γίνεται δοκιμή του σχεδίου σύμφωνα με το [BCR3].
3	7	Διενεργούνται ενημερώσεις και αλλαγές σύμφωνα με την διαδικασία διαχείρισης αλλαγών [CM1].
4	1	Το σχέδιο αποκατάστασης από καταστροφή προβλέπει την ύπαρξη κατάλληλου αδειοδοτημένου λογισμικού για την ανάκτηση των στοιχείων από τα σχετικά αντίγραφα ασφαλείας.
4	2	Τα αρχεία εφεδρικών αντιγράφων κρυπτογραφούνται με την χρήση αλγορίθμων όπως προβλέπεται από το [AM1].

4	3	Έχει γίνει πρόβλεψη ώστε να υπάρχει δυνατότητα πρόσβασης και ανάκτησης των δεδομένων όπως απαιτείται από τα εφεδρικά αντίγραφα (π.χ. υπάρχει δυνατότητα λήψης, εγκατάστασης ή χρήσης του λογισμικού αντιγράφων ασφαλείας και υπάρχει διαθεσιμότητα των σχετικών κλειδιών).
4	4	Τα σχέδια αποκατάστασης από καταστροφή αποθηκεύονται σε ασφαλή τοποθεσία, προστατεύονται με τα κατάλληλα μέτρα ώς πληροφορία του υψηλότερου επιπέδου διαβάθμισης και εξασφαλίζεται ότι είναι διαθέσιμα σε περίπτωση καταστροφής της κύριας εγκατάστασης.
4	5	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Έχουν εφαρμοσθεί λύσεις συγχρονισμού (replication) σε εναλλακτικό χώρο για τα κρίσιμα συστήματα όπως αυτά έχουν αναγνωριστεί σύμφωνα με την ανάλυση επιχειρησιακών επιπτώσεων και τις σχετικές στρατηγικές.
5	2	Τα σχέδια εξασκούνται τουλάχιστον ετησίως και αξιολογείται η δυνατότητα ορθής και αποτελεσματικής εφαρμογής τους.
5	3	Διενεργούνται συζητήσεις και συναντήσεις μετά τις δοκιμές για την αξιολόγηση της επίδοσης των επιμέρους μερών των σχεδίων, την ανάδειξη προβλημάτων και την αναγνώριση σημείων βελτίωσης.
5	4	Οι δοκιμές και οι συζητήσεις συντονίζονται και παρακολουθούνται από ανεξάρτητο παρατηρητή (μπορεί να είναι εσωτερικό άτομο του οργανισμού αλλά πρέπει να μην συμμετέχει στην διαδικασία της ανάκαμψης, αντιμετώπισης και λειτουργίας).
5	5	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	6	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.