

ΟΔΗΓΟΣ ΒΑΘΜΟΛΟΓΗΣΗΣ ΤΕΧΝΟΛΟΓΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΩΣ ΠΡΟΣ ΤΗΝ ΑΣΦΑΛΕΙΑ

Έκδοση 1.0
Οκτώβριος 2026

Πίνακας Περιεχομένων

1. Σκοπός και κανονιστική θέση του Οδηγού....4
2. Βασικές αρχές βαθμολόγησης....4
2.1. Ουσιώδες εφαρμοστέο στοιχείο....5
2.2. Κατανομή ευθυνών και εξωτερικά μέτρα ασφάλειας....5
3. Διαδικασία εφαρμογής της βαθμολόγησης....5
4. Αποδεικτική αξία τεκμηρίων....6
4.2. Κριτήρια αξιοπιστίας τεκμηρίου....6
5. Ενιαία λογική των βαθμών 0–10....7
5.1. Κανόνες «κόφτη»....7
6. Κριτήριο 1: Αρχιτεκτονική Ασφάλειας και Μοντέλο Απειλών....8
Ειδικά σημεία αναφοράς βαθμολόγησης....8
Ενδείξεις που κατά κανόνα δεν επιτρέπουν 6/10 ή μεγαλύτερο....8
7. Κριτήριο 2: Ταυτοποίηση, Αυθεντικοποίηση και Έλεγχος Πρόσβασης....8
Ειδικά σημεία αναφοράς βαθμολόγησης....9
Ενδείξεις που κατά κανόνα δεν επιτρέπουν 6/10 ή μεγαλύτερο....9
8. Κριτήριο 3: Προστασία Δεδομένων και Κρυπτογραφία....9
Ειδικά σημεία αναφοράς βαθμολόγησης....10
Ενδείξεις που κατά κανόνα δεν επιτρέπουν 6/10 ή μεγαλύτερο....10
9. Κριτήριο 4: Ασφάλεια Επικοινωνιών, Δικτύων και Διεπαφών....10
Ειδικά σημεία αναφοράς βαθμολόγησης....10
Ενδείξεις που κατά κανόνα δεν επιτρέπουν 6/10 ή μεγαλύτερο....11
10. Κριτήριο 5: Ακεραιότητα Συστήματος, Εκτέλεσης και Λειτουργιών....11
Ειδικά σημεία αναφοράς βαθμολόγησης....11
Ενδείξεις που κατά κανόνα δεν επιτρέπουν 6/10 ή μεγαλύτερο....12
11. Κριτήριο 6: Καταγραφή, Ιχνηλασιμότητα και Παρακολούθηση....12
Ειδικά σημεία αναφοράς βαθμολόγησης....12
Ενδείξεις που κατά κανόνα δεν επιτρέπουν 6/10 ή μεγαλύτερο....12
12. Κριτήριο 7: Διαχείριση Ευπαθειών, Διαμόρφωσης και Ενημερώσεων....13
Ειδικά σημεία αναφοράς βαθμολόγησης....13
Ενδείξεις που κατά κανόνα δεν επιτρέπουν 6/10 ή μεγαλύτερο....13
13. Κριτήριο 8: Διαθεσιμότητα, Ανθεκτικότητα και Ανάκτηση....14
Ειδικά σημεία αναφοράς βαθμολόγησης....14
Ενδείξεις που κατά κανόνα δεν επιτρέπουν 6/10 ή μεγαλύτερο....14
14. Κριτήριο 9: Εξαρτήσεις, Τρίτα Συστατικά και Αλυσίδα Εφοδιασμού....14
Ειδικά σημεία αναφοράς βαθμολόγησης....15
Ενδείξεις που κατά κανόνα δεν επιτρέπουν 6/10 ή μεγαλύτερο....15

15. Κριτήριο 10: Ασφαλής Ανάπτυξη, Μεταβολές και Διάθεση Εκδόσεων 15
Ειδικά σημεία αναφοράς βαθμολόγησης 16
Ενδείξεις που κατά κανόνα δεν επιτρέπουν 6/10 ή μεγαλύτερο 16
16. Κρίσιμες Αδυναμίες 16
16.2. Παράγοντες που συνεκτιμώνται 16
16.3. Ενδεικτικές περιπτώσεις 17
17. Εφαρμογή σε Κατάσταση «Υπό ανάπτυξη» και «Υλοποιημένο» 17
18. Συνέπεια μεταξύ αξιολογητών και ανεξάρτητη επανεξέταση 18
Παράρτημα Α. Κατανομή χαρακτηριστικών μεταξύ κριτηρίων 18
Παράρτημα Β. Ελάχιστα ενδεικτικά τεκμήρια για βαθμό 6/10 19
Παράρτημα Γ. Φύλλο Βαθμολόγησης 20
Παράρτημα Δ. Τεχνικές πηγές αναφοράς 20
Παράρτημα Ε. Ενιαία εφαρμογή των κριτηρίων ανά τύπο συστήματος 21
19. Έναρξη εφαρμογής και αναθεώρηση του Οδηγού 23

1. Σκοπός και κανονιστική θέση του Οδηγού

1.1. Ο παρών Οδηγός εξειδικεύει την εφαρμογή των άρθρων 10 έως 22 της Διαδικασίας Πιστοποίησης Τεχνολογικών Συστημάτων ως προς την Ασφάλεια του ΚΕΜΕΑ και χρησιμοποιείται από τους αξιολογητές, τους επανεξεταστές και τα αρμόδια όργανα λήψης απόφασης.

1.2. Ο Οδηγός δεν τροποποιεί τη Διαδικασία και δεν εισάγει πρόσθετα κριτήρια πιστοποίησης. Σε περίπτωση αμφιβολίας ή σύγκρουσης υπερισχύει η Διαδικασία.

1.3. Οι διεθνείς και ευρωπαϊκές πηγές τεχνικής αναφοράς που αναφέρονται στον παρόντα χρησιμοποιούνται αποκλειστικά ως πηγές καλών πρακτικών, τεχνικής ορολογίας και μεθοδολογικής υποστήριξης. Η εφαρμογή τους δεν σημαίνει πιστοποίηση ή δήλωση συμμόρφωσης προς συγκεκριμένο πρότυπο.

1.4. Κάθε έκδοση του Οδηγού φέρει μοναδικό αριθμό έκδοσης. Σε κάθε αίτηση εφαρμόζεται η έκδοση του Οδηγού που ισχύει κατά την υποβολή της αίτησης και παραμένει εφαρμοστέα έως την ολοκλήρωση της διαδικασίας, σύμφωνα με τη Διαδικασία. Μεταγενέστερη έκδοση δεν εφαρμόζεται σε εκκρεμή αίτηση.

1.5. Ο παρών Οδηγός αφορά αποκλειστικά την αξιολόγηση και βαθμολόγηση Τεχνολογικών Συστημάτων στο πλαίσιο της αντίστοιχης Διαδικασίας του ΚΕΜΕΑ. Δεν εφαρμόζεται σε διαδικασίες, μελέτες, σχέδια ή άλλα αντικείμενα πιστοποίησης, για τα οποία εφαρμόζονται ή θα θεσπιστούν αυτοτελή πλαίσια.

2. Βασικές αρχές βαθμολόγησης

- Κάθε ένα από τα δέκα Κριτήρια Ασφάλειας βαθμολογείται απευθείας με ακέραιο βαθμό από 0 έως 10.
- Δεν χρησιμοποιούνται υποβαθμολογίες που αθροίζονται ή αναγωγές που μεταβάλλουν τη βαθμολογία του κριτηρίου. Τα επιμέρους στοιχεία λειτουργούν ως σημεία ελέγχου για την τεκμηριωμένη συνολική κρίση του αξιολογητή.
- Η συνολική βαθμολογία προκύπτει αποκλειστικά από το άθροισμα των δέκα βαθμών.
- Η αξιολόγηση κάθε κριτηρίου λαμβάνει ταυτόχρονα υπόψη: (α) τη λειτουργική και τεχνική επάρκεια των μέτρων ασφάλειας και (β) τον βαθμό εμπιστοσύνης που παρέχουν τα υποβαλλόμενα τεκμήρια. Δεν αποδίδονται δύο χωριστές βαθμολογίες.
- Η απουσία συγκεκριμένης λειτουργίας ή επιφάνειας επίθεσης δεν αποτελεί αυτομάτως έλλειψη. Εφόσον τεκμηριώνεται ότι ο σχετικός κίνδυνος δεν υφίσταται λόγω της αρχιτεκτονικής, το στοιχείο δεν λαμβάνεται υπόψη κατά τη βαθμολόγηση και η μη εφαρμογή του αιτιολογείται. Η μη εφαρμογή στοιχείου δεν δημιουργεί αυτοτελώς θετική βαθμολογική προσαύξηση.
- Κανένα από τα δέκα κριτήρια δεν χαρακτηρίζεται κατά κανόνα στο σύνολό του ως «μη εφαρμοστέο». Κατ' εξαίρεση, εφόσον μετά από ειδικά αιτιολογημένη εξέταση εφαρμοσιμότητας διαπιστώνεται ότι κανένα επιμέρους στοιχείο συγκεκριμένου Κριτηρίου Ασφάλειας δεν είναι εφαρμοστέο στο Αντικείμενο Αξιολόγησης λόγω της φύσης και της τεκμηριωμένης αρχιτεκτονικής του, το κριτήριο βαθμολογείται με έξι (6) μονάδες αποκλειστικά για τη διατήρηση της ενιαίας κλίμακας βαθμολόγησης. Η βαθμολογία αυτή δεν συνιστά θετική αξιολόγηση μέτρων ασφάλειας ούτε επιβράβευση της μη εφαρμογής. Η πλήρης μη εφαρμογή αιτιολογείται ειδικά στην Έκθεση Αξιολόγησης και επιβεβαιώνεται κατά την ανεξάρτητη επανεξέταση.
- Το ίδιο τεχνικό χαρακτηριστικό βαθμολογείται μία μόνο φορά. Άλλο κριτήριο μπορεί να αναφερθεί στο ίδιο χαρακτηριστικό μόνο ως εξάρτηση ή προϋπόθεση, χωρίς δεύτερη βαθμολογική προσμέτρηση.
- Βαθμολογία 6/10 ή μεγαλύτερη προϋποθέτει κατάλληλο υποστηρικτικό τεχνικό τεκμήριο. Απλή δήλωση ή αφηγηματική περιγραφή του αιτούντος δεν επαρκεί.

- Η ύπαρξη Κρίσιμης Αδυναμίας αποτελεί ανεξάρτητο λόγο μη χορήγησης πιστοποιητικού και δεν μετατρέπεται σε πρόσθετη αριθμητική ποινή.
- Η βαθμολογία αφορά αποκλειστικά το Αντικείμενο Αξιολόγησης, την έκδοση, τη διαμόρφωση, την αρχιτεκτονική, την Κατάσταση Συστήματος και τις παραδοχές περιβάλλοντος λειτουργίας που έχουν τεθεί υπόψη του ΚΕΜΕΑ.

Μεθοδολογική βάση: η διάκριση μεταξύ λειτουργικότητας των μέτρων και διασφάλισης (assurance) ή εμπιστοσύνης στην εφαρμογή τους ακολουθεί τη διεθνή πρακτική που αποτυπώνεται, μεταξύ άλλων, στο NIST SP 800-53 Rev. 5. Ο παρών Οδηγός συνδυάζει τις δύο διαστάσεις σε μία ενιαία βαθμολογία ανά κριτήριο, ώστε να παραμένει απλός και εφαρμόσιμος.

2.1. Ουσιώδες εφαρμοστέο στοιχείο

Ως «ουσιώδες εφαρμοστέο στοιχείο» νοείται στοιχείο του οποίου η απουσία ή ουσιωδώς ανεπαρκής εφαρμογή μπορεί, λαμβανομένων υπόψη της αρχιτεκτονικής, των απειλών και του περιβάλλοντος λειτουργίας, να μειώσει ουσιωδώς την προστασία κρίσιμων δεδομένων ή λειτουργιών ή την αποτελεσματικότητα άλλου μέτρου ασφάλειας.

Σε περίπτωση αμφιβολίας μεταξύ βαθμού 5 και 6, βαθμός 6 αποδίδεται μόνο εφόσον τεκμηριώνεται θετικά ότι όλα τα ουσιώδη εφαρμοστέα στοιχεία του κριτηρίου καλύπτονται σε ικανοποιητικό επίπεδο και δεν υφίσταται σοβαρή αδυναμία.

2.2. Κατανομή ευθυνών και εξωτερικά μέτρα ασφάλειας

Όταν μέτρο ασφάλειας υλοποιείται ή λειτουργεί από τον χρήστη, πάροχο υποδομής ή άλλο εξωτερικό μέρος, δεν θεωρείται αυτομάτως απόν ούτε αποδίδεται αυτομάτως ως ιδιότητα του Αντικειμένου Αξιολόγησης. Αξιολογούνται η σαφής και τεκμηριωμένη κατανομή της ευθύνης, οι τεχνικές προϋποθέσεις και διεπαφές του Αντικειμένου Αξιολόγησης, οι απαιτήσεις ασφαλούς εγκατάστασης ή ενσωμάτωσης, οι οδηγίες προς το υπεύθυνο μέρος και η εύλογη δυνατότητα εφαρμογής του μέτρου.

Η απλή μετακύλιση ευθύνης σε τρίτο, χωρίς επαρκή τεχνική ή άλλη τεκμηρίωση των σχετικών προϋποθέσεων, δεν θεωρείται επαρκής κάλυψη. Η αποτελεσματικότητα μέτρου που ελέγχεται αποκλειστικά από τρίτο δεν προσμετράται δεύτερη φορά ως ιδιότητα του Αντικειμένου Αξιολόγησης.

3. Διαδικασία εφαρμογής της βαθμολόγησης

Βήμα	Ενέργεια	Απαίτηση
1	Οριοθέτηση	Επιβεβαιώνονται το Αντικείμενο Αξιολόγησης, η έκδοση ή διαμόρφωση, η Κατάσταση Συστήματος, τα εξαιρούμενα στοιχεία και οι παραδοχές του περιβάλλοντος λειτουργίας.
2	Ευρετήριο τεκμηρίων	Κάθε τεκμήριο λαμβάνει αναγνωριστικό και αντιστοιχίζεται στα κριτήρια στα οποία είναι σχετικό.
3	Έλεγχος εφαρμοσιμότητας	Για κάθε κριτήριο προσδιορίζονται τα επιμέρους στοιχεία που είναι εφαρμοστέα. Κάθε μη εφαρμοστέο στοιχείο αιτιολογείται.
4	Προκαταρκτικός έλεγχος Κρίσιμων Αδυναμιών	Εντοπίζονται ευρήματα που ενδέχεται να εμπίπτουν στο άρθρο 3 παρ. 7 και στο άρθρο 22 της Διαδικασίας.
5	Αξιολόγηση ανά κριτήριο	Ο αξιολογητής εξετάζει την τεχνική κάλυψη και την αποδεικτική επάρκεια και επιλέγει τον βαθμό που αντιστοιχεί καλύτερα στα ειδικά σημεία αναφοράς (anchors) του παρόντος Οδηγού.
6	Αιτιολόγηση	Για κάθε κριτήριο καταγράφονται ο βαθμός, τα βασικά τεκμήρια, οι μη εφαρμοστέες υποπεριοχές, οι αδυναμίες και ο λόγος επιλογής του συγκεκριμένου βαθμού.
7	Τελικός έλεγχος Κρίσιμων Αδυναμιών	Κάθε πιθανή Κρίσιμη Αδυναμία επανεξετάζεται με βάση το σύνολο των τεκμηρίων, τις αντισταθμιστικές δικλείδες και τη σοβαρότητα του αποτελέσματος.

Βήμα	Ενέργεια	Απαίτηση
8	Συνολική βαθμολογία	Αθροίζονται οι δέκα βαθμοί. Η αριθμητική βαθμολογία δεν υπερισχύει των προϋποθέσεων του άρθρου 26 της Διαδικασίας.
9	Ανεξάρτητη επανεξέταση	Ο επανεξεταστής ελέγχει ιδίως τη συνέπεια της εφαρμογής των σημείων αναφοράς, τη μη διπλή βαθμολόγηση και την επάρκεια των τεκμηρίων.

4. Αποδεικτική αξία τεκμηρίων

4.1. Η αποδεικτική αξία δεν προσδιορίζεται από τον τίτλο του εγγράφου αλλά από τον βαθμό στον οποίο το τεκμήριο είναι συγκεκριμένο, τεχνικό, επίκαιρο, ιχνηλάσιμο προς το Αντικείμενο Αξιολόγησης και εσωτερικά συνεπές.

Κατηγορία	Ενδεικτικά τεκμήρια	Αξιολογική χρήση
Α. Τεχνικά τεκμήρια συγκεκριμένης έκδοσης ή διαμόρφωσης	Διαγράμματα αρχιτεκτονικής και ροών, εξαγωγές διαμόρφωσης (configuration exports), προδιαγραφές API, κατάλογοι κρυπτογραφικών αλγορίθμων και πρωτοκόλλων (cipher/protocol inventories), πίνακες ρόλων και δικαιωμάτων IAM, SBOM/BOM, δηλωτικά δόμησης και διάθεσης εκδόσεων (build/release manifests), δηλωτικά υλικολογισμικού (firmware manifests), σχήματα καταγραφής συμβάντων (logging schemas), σχεδιασμός αντιγράφων ασφαλείας και ανάκτησης (backup/recovery), προδιαγραφές μηχανισμού ενημερώσεων.	Υψηλή αποδεικτική αξία όταν είναι ιχνηλάσιμα προς τη συγκεκριμένη έκδοση και συνεπή μεταξύ τους.
Β. Ελεγχόμενα τεκμήρια σχεδιασμού και διαδικασιών	Εγκεκριμένες προδιαγραφές ασφάλειας, μοντέλο απειλών (threat model), αρχεία ασφαλούς σχεδιασμού (secure design records), διαδικασία διαχείρισης αλλαγών (change management), διαδικασίες SDLC, διαδικασία διαχείρισης ευπαθειών (vulnerability management), πολιτική υποστήριξης και λήξης κύκλου ζωής (support/EOL policy).	Υψηλή αξία ιδίως για Κατάσταση «Υπό ανάπτυξη». Για «Υλοποιημένο» πρέπει να συνδέονται με στοιχεία της υλοποιημένης έκδοσης.
Γ. Εκθέσεις και πιστοποιήσεις τρίτων	Εκθέσεις δοκιμών διείσδυσης (penetration tests), εκθέσεις αξιολόγησης ευπαθειών (vulnerability assessment), εκθέσεις ανάλυσης κώδικα (code analysis), εργαστηριακές εκθέσεις, εξωτερικοί έλεγχοι, άλλες πιστοποιήσεις.	Ισχυρά υποστηρικτικά τεκμήρια όταν καλύπτουν την ίδια έκδοση και το ίδιο πεδίο εφαρμογής (scope). Δεν υποκαθιστούν την αξιολόγηση του ΚΕΜΕΑ και δεν αποδεικνύουν από μόνα τους όλα τα κριτήρια.
Δ. Τεχνική τεκμηρίωση προμηθευτή	Τεχνικά κείμενα ασφάλειας (security white papers), οδηγοί θωράκισης (hardening guides), εγχειρίδια διαχείρισης, ενημερωτικά δελτία ασφάλειας του προμηθευτή (vendor advisories), σημειώσεις έκδοσης (release notes).	Μέση έως υψηλή αξία ανάλογα με τη συγκεκριμενοποίηση, την έκδοση και τη δυνατότητα αντιστοίχισης με το Αντικείμενο Αξιολόγησης.
Ε. Γενικές δηλώσεις ή περιγραφές	Απαντήσεις ερωτηματολογίου, εμπορικές περιγραφές, μη τεχνικές δηλώσεις χωρίς υποστηρικτικό στοιχείο.	Περιορισμένη αξία. Μόνες τους δεν επιτρέπουν βαθμολογία 6/10 ή μεγαλύτερη.

4.2. Κριτήρια αξιοπιστίας τεκμηρίου

- Ειδικότητα: αφορά το συγκεκριμένο Σύστημα και όχι γενικά την εταιρεία ή την οικογένεια προϊόντων.
- Ιχνηλασιμότητα: συνδέεται με συγκεκριμένη έκδοση, δόμηση (build), διαμόρφωση (configuration) ή αρχιτεκτονική.
- Επικαιρότητα: αντανακλά την τρέχουσα κατάσταση του Αντικειμένου Αξιολόγησης.
- Τεχνικό βάθος: επιτρέπει ουσιαστική κρίση και όχι απλή αποδοχή ισχυρισμού.

- Συνέπεια: δεν αντιφάσκει με άλλα τεκμήρια του φακέλου.
- Ανεξαρτησία: όταν προέρχεται από τρίτο, εξετάζεται η επάρκεια, η μεθοδολογία και το πεδίο εφαρμογής (scope) του τρίτου χωρίς αυτόματη αποδοχή του συμπεράσματός του.

Ανεπίλυτη ουσιώδης αντίφαση μεταξύ τεκμηρίων εμποδίζει βαθμολογία 6/10 ή μεγαλύτερη στο επηρεαζόμενο κριτήριο, εκτός αν ο αξιολογητής τεκμηριώσει ότι η αντίφαση δεν επηρεάζει την ουσιαστική ασφάλεια.

5. Ενιαία λογική των βαθμών 0–10

Βαθμός	Ερμηνεία
0	Δεν υπάρχει κάλυψη, η κατάσταση είναι προφανώς μη ασφαλής ή δεν υπάρχει επαρκές υλικό για αξιολόγηση.
1	Μεταξύ 0 και 2. Υπάρχει ελάχιστη ένδειξη μέτρου χωρίς ουσιαστική κάλυψη.
2	Υπάρχει στοιχειώδης κάλυψη, αλλά σοβαρές ελλείψεις αφήνουν σημαντικό μέρος του κινδύνου ανεξέλεγκτο.
3	Μεταξύ 2 και 4. Υπάρχουν περισσότερα μέτρα, αλλά παραμένουν σημαντικές λειτουργικές ή τεκμηριωτικές αδυναμίες.
4	Υπάρχει ουσιαστική αλλά μερική κάλυψη. Ένα ή περισσότερα σημαντικά στοιχεία λείπουν ή είναι ανεπαρκή.
5	Μεταξύ 4 και 6. Η κάλυψη πλησιάζει το ικανοποιητικό επίπεδο, αλλά υπάρχει τουλάχιστον μία ουσιώδης έλλειψη ή ανεπαρκής τεκμηρίωση που δεν επιτρέπει 6.
6	Ικανοποιητικό επίπεδο. Όλα τα ουσιώδη εφαρμοστέα στοιχεία καλύπτονται χωρίς σοβαρή αδυναμία και υπάρχουν κατάλληλα υποστηρικτικά τεκμήρια. Εξαίρεση αποτελεί μόνο η ουδέτερη βαθμολογία του πλήρως μη εφαρμοστέου κριτηρίου κατά την ενότητα 2, η οποία δεν δηλώνει ύπαρξη ή ποιότητα μέτρων ασφάλειας.
7	Μεταξύ 6 και 8. Η κάλυψη είναι σαφώς ανώτερη του ελάχιστα ικανοποιητικού επιπέδου, με περιορισμένα περιθώρια βελτίωσης.
8	Υψηλό επίπεδο. Η κάλυψη είναι συνεκτική, σύγχρονη, ολοκληρωμένη στα περισσότερα εφαρμοστέα στοιχεία και τεκμηριώνεται ισχυρά.
9	Μεταξύ 8 και 10. Υπάρχουν μόνο πολύ περιορισμένες μη ουσιώδεις αποκλίσεις.
10	Πολύ υψηλό επίπεδο. Δεν εντοπίζεται ουσιώδες κενό στα εφαρμοστέα στοιχεία, η αρχιτεκτονική ή διαδικασία είναι ισχυρή και η τεκμηρίωση παρέχει πολύ υψηλή εμπιστοσύνη.

5.1. Κανόνες «κόφτη»

- Απλή δήλωση ή αφηγηματική περιγραφή χωρίς υποστηρικτικό τεχνικό τεκμήριο: μέγιστος βαθμός 5/10.
- Απουσία ουσιώδους εφαρμοστέου στοιχείου ή ανεπίλυτη ουσιώδης αντίφαση τεκμηρίων: κατά κανόνα μέγιστος βαθμός 5/10.
- Σοβαρή αδυναμία που μειώνει ουσιωδώς την αποτελεσματικότητα του κριτηρίου: ο βαθμός δεν μπορεί να είναι 6/10 ή μεγαλύτερος.
- Βαθμός 8/10 ή μεγαλύτερος απαιτεί ισχυρή τεκμηρίωση και απουσία ουσιωδών κενών.
- Βαθμός 10/10 δεν αποδίδεται επειδή απλώς δεν εντοπίστηκε πρόβλημα. Απαιτεί θετική, σαφή και εκτενή τεκμηρίωση πολύ υψηλού επιπέδου.
- Η αδυναμία που χαρακτηρίζεται ως Κρίσιμη Αδυναμία λαμβάνεται κανονικά υπόψη κατά τη βαθμολόγηση του κριτηρίου στο οποίο υπάγεται. Ο χαρακτηρισμός της ως Κρίσιμης Αδυναμίας δεν συνεπάγεται δεύτερη ή πρόσθετη αριθμητική αφαίρεση. Η τεχνική αδυναμία που χαρακτηρίζεται ως Κρίσιμη Αδυναμία συνιστά κατά κανόνα και σοβαρή αδυναμία κατά την τρίτη περίπτωση της παρούσας ενότητας.

6. Κριτήριο 1: Αρχιτεκτονική Ασφάλειας και Μοντέλο Απειλών

Σκοπός. Αξιολογείται αν η ασφάλεια έχει ενσωματωθεί στη συνολική αρχιτεκτονική και αν οι κίνδυνοι, τα όρια εμπιστοσύνης, οι ροές και οι παραδοχές έχουν αναγνωριστεί με τρόπο που επιτρέπει συνεπή σχεδιασμό μέτρων.

Όρια με άλλα κριτήρια. Εδώ αξιολογείται η ποιότητα της ανάλυσης και της αρχιτεκτονικής λογικής. Δεν επαναβαθμολογείται η ισχύς της αυθεντικοποίησης, της κρυπτογραφίας, της καταγραφής συμβάντων (logging) ή άλλων συγκεκριμένων ελέγχων.

Ενδεικτικά τεκμήρια. Διάγραμμα αρχιτεκτονικής, διαγράμματα ροής δεδομένων (data-flow diagrams), όρια εμπιστοσύνης (trust boundaries), κατάλογος περιουσιακών στοιχείων (asset inventory), μοντέλο απειλών (threat model), ανάλυση επιφάνειας επίθεσης (attack surface), σενάρια κακής χρήσης και κατάχρησης (misuse/abuse scenarios), παραδοχές ασφάλειας (security assumptions), μοντέλο εγκατάστασης (deployment model), διάγραμμα εξωτερικών εξαρτήσεων.

Ειδικά σημεία αναφοράς βαθμολόγησης

Βαθμός	Ειδική ερμηνεία
0	Δεν υπάρχει αξιόπιστη αρχιτεκτονική αποτύπωση ή τα υποβαλλόμενα στοιχεία είναι αντιφατικά σε βαθμό που δεν επιτρέπει κατανόηση του Συστήματος.
2	Υπάρχει μόνο υψηλού επιπέδου περιγραφή. Λείπουν ουσιωδώς ροές, όρια εμπιστοσύνης (trust boundaries), επιφάνειες επίθεσης (attack surfaces) ή βασικές απειλές.
4	Η αρχιτεκτονική αποτυπώνεται μερικώς και έχουν αναγνωριστεί ορισμένες απειλές, αλλά σημαντικά τμήματα, παραδοχές ή διασυνδέσεις παραμένουν ασαφή.
6	Υπάρχει επαρκής και συνεπής αποτύπωση συστατικών, βασικών ροών, ορίων εμπιστοσύνης, επιφανειών επίθεσης, παραδοχών και βασικών απειλών. Η ανάλυση υποστηρίζει ουσιαστικά την αξιολόγηση των μέτρων.
8	Η ανάλυση είναι συστηματική και ιχνηλάσιμη προς τη συγκεκριμένη έκδοση, καλύπτει σενάρια κατάχρησης/παραβίασης, εξαρτήσεις και διαφορετικά περιβάλλοντα λειτουργίας και συνδέει καθαρά απειλές με σχεδιαστικές αποφάσεις.
10	Η αρχιτεκτονική και το μοντέλο απειλών (threat model) είναι εξαιρετικά πλήρη, επικαιροποιημένα και ελεγχόμενα ως προς εκδόσεις, καλύπτουν μεταβολές, καταστάσεις αστοχίας (failure states), περιπτώσεις κατάχρησης (abuse cases) και σύνθετες αλληλεπιδράσεις και δεν εμφανίζουν ουσιώδες κενό.

Ενδείξεις που κατά κανόνα δεν επιτρέπουν 6/10 ή μεγαλύτερο

- Δεν υπάρχει σαφής οριοθέτηση του Αντικειμένου Αξιολόγησης.
- Δεν αποτυπώνονται όρια εμπιστοσύνης ή κρίσιμες ροές για σύστημα με εξωτερικές διασυνδέσεις.
- Δεν υπάρχει ουσιαστική ανάλυση απειλών ή αυτή περιορίζεται σε γενικές δηλώσεις.

7. Κριτήριο 2: Ταυτοποίηση, Αυθεντικοποίηση και Έλεγχος Πρόσβασης

Σκοπός. Αξιολογείται αν μόνο κατάλληλα ταυτοποιημένες και εξουσιοδοτημένες οντότητες μπορούν να εκτελούν τις αντίστοιχες λειτουργίες ή να προσπελαύνουν δεδομένα.

Όρια με άλλα κριτήρια. Η κρυπτογραφική προστασία συνθηματικών (passwords), διακριτικών (tokens) και διαπιστευτηρίων (credentials) βαθμολογείται στο Κ3. Η ακεραιότητα της κατάστασης εφαρμογής (application state), η προστασία από επανάληψη (anti-replay) ή η αλλοίωση συνεδρίας (session tampering) βαθμολογείται στο Κ5. Εδώ βαθμολογούνται η ταυτότητα, η αυθεντικοποίηση, η εξουσιοδότηση και ο κύκλος ζωής της συνεδρίας.

Ενδεικτικά τεκμήρια. Αρχιτεκτονική αυθεντικοποίησης, πίνακας ρόλων και δικαιωμάτων (role/permission matrix), σχεδιασμός προνομιακής πρόσβασης (privileged access), σχεδιασμός MFA, κύκλος ζωής λογαριασμών (account lifecycle), μοντέλο ταυτοτήτων υπηρεσιών και συσκευών (service/device identities), κανόνες λήξης και ανάκλησης συνεδριών (session timeout/revocation), διαχωρισμός διαχειριστικών ρόλων (admin separation), προδιαγραφές ενοποίησης SSO/IdP.

Ειδικά σημεία αναφοράς βαθμολόγησης

Βαθμός	Ειδική ερμηνεία
0	Κρίσιμες λειτουργίες είναι προσβάσιμες χωρίς κατάλληλη ταυτοποίηση/εξουσιοδότηση ή δεν υπάρχει επαρκής τεκμηρίωση των μηχανισμών.
2	Υπάρχει βασική αυθεντικοποίηση αλλά με σοβαρές ελλείψεις, όπως κοινόχρηστοι λογαριασμοί, υπερβολικά δικαιώματα ή ανεπαρκής έλεγχος προνομιακών λειτουργιών.
4	Υπάρχουν μοναδικές ταυτότητες και βασικοί ρόλοι, αλλά η κάλυψη της προνομιακής πρόσβασης (privileged access), των ταυτοτήτων υπηρεσιών (service identities), της MFA, του κύκλου ζωής (lifecycle) ή της διαχείρισης συνεδριών (session management) είναι μερική.
6	Οι ταυτότητες, η αυθεντικοποίηση, οι ρόλοι, η αρχή των ελάχιστων δικαιωμάτων (least privilege), οι προνομιακοί λογαριασμοί, ο κύκλος ζωής και η λήξη/ανάκληση συνεδριών καλύπτονται επαρκώς ανάλογα με τον κίνδυνο.
8	Υπάρχει ισχυρή, λεπτομερής και συνεκτική πολιτική πρόσβασης, σαφής διαχωρισμός προνομίων, κατάλληλη MFA, ελεγχόμενες ταυτότητες υπηρεσιών και συσκευών (service/device identities) και αυστηρή διαχείριση του κύκλου ζωής.
10	Το μοντέλο ταυτότητας και πρόσβασης (identity and access) είναι πλήρες και ιδιαίτερα ισχυρό, με συνεπή επιβολή (enforcement) σε όλα τα όρια εμπιστοσύνης (trust boundaries), αυστηρή προνομιακή πρόσβαση, ισχυρή MFA όπου απαιτείται και πλήρη ιχνηλασιμότητα κύκλου ζωής.

Ενδείξεις που κατά κανόνα δεν επιτρέπουν 6/10 ή μεγαλύτερο

- Κοινά ή μη μεταβαλλόμενα προνομιακά διαπιστευτήρια χωρίς αποτελεσματικό αντισταθμιστικό μέτρο.
- Ανεξέλεγκτη πρόσβαση σε κρίσιμη διαχειριστική λειτουργία.
- Εξουσιοδότηση που βασίζεται μόνο στη διεπαφή χρήστη ή στην πλευρά του πελάτη (UI/client) χωρίς επιβολή στην πλευρά του διακομιστή (server-side) ή ισοδύναμη επιβολή όπου αυτή απαιτείται.

8. Κριτήριο 3: Προστασία Δεδομένων και Κρυπτογραφία

Σκοπός. Αξιολογείται αν δεδομένα, διαπιστευτήρια, κλειδιά και λοιπά μυστικά προστατεύονται με κατάλληλους σύγχρονους μηχανισμούς σε όλο τον κύκλο ζωής τους. Στα δεδομένα περιλαμβάνονται και τα δεδομένα προσωπικού χαρακτήρα. Δεν αξιολογείται η νομιμότητα της επεξεργασίας τους.

Όρια με άλλα κριτήρια. Η δικτυακή έκθεση βαθμολογείται στο Κ4. Η ίδια η ύπαρξη TPM ή ασφαλούς στοιχείου (secure element) ως μηχανισμού απομόνωσης σε επίπεδο υλικού (hardware isolation) βαθμολογείται στο Κ5, ενώ εδώ αξιολογείται το αποτέλεσμα για την προστασία και τον κύκλο ζωής των κλειδιών.

Ενδεικτικά τεκμήρια. Πίνακας προστασίας δεδομένων (data protection matrix), κατάλογος πρωτοκόλλων και κρυπτογραφικών αλγορίθμων (protocol/cipher inventory), προδιαγραφές διαμόρφωσης TLS/VPN, σχεδιασμός διαχείρισης κλειδιών (key management), κύκλος ζωής ψηφιακών πιστοποιητικών (certificate lifecycle), σχεδιασμός αποθήκευσης μυστικών (secret storage), χρήση HSM ή χώρου αποθήκευσης κλειδιών (keystore), προδιαγραφή κατακερματισμού συνθηματικών (password hashing), κύκλος ζωής κλειδιών υπογραφής (signing keys), σχέδιο κρυπτογραφικής ευελιξίας (crypto agility).

Ειδικά σημεία αναφοράς βαθμολόγησης

Βαθμός	Ειδική ερμηνεία
0	Κρίσιμα δεδομένα ή μυστικά εκτίθενται χωρίς κατάλληλη προστασία, χρησιμοποιούνται αποδεδειγμένα μη ασφαλείς μηχανισμοί ή η κρυπτογραφική αρχιτεκτονική δεν μπορεί να αξιολογηθεί.
2	Υπάρχει αποσπασματική κρυπτογράφηση, αλλά σημαντικά κανάλια, αποθηκευμένα δεδομένα ή μυστικά παραμένουν ανεπαρκώς προστατευμένα και η διαχείριση κλειδιών (key management) είναι ελλιπής.
4	Χρησιμοποιούνται γενικά κατάλληλοι μηχανισμοί αλλά υπάρχουν σημαντικά κενά σε αλγορίθμους και εκδόσεις πρωτοκόλλων, στον κύκλο ζωής των κλειδιών, στον χειρισμό μυστικών (secret handling) ή στην κρυπτογραφική ευελιξία (crypto agility).
6	Τα εφαρμοστέα δεδομένα προστατεύονται επαρκώς σε μεταφορά και αποθήκευση, οι μηχανισμοί είναι σύγχρονοι και υπάρχει τεκμηριωμένη διαχείριση κλειδιών, ψηφιακών πιστοποιητικών (certificates) και μυστικών.
8	Η κρυπτογραφική αρχιτεκτονική είναι ολοκληρωμένη, με ισχυρό κύκλο ζωής (lifecycle), διαχωρισμό κλειδιών, ασφαλή αποθήκευση, εναλλαγή και ανάκληση (rotation/revocation), ευελιξία αλγορίθμων (algorithm agility) και ειδική προστασία των κρίσιμων κλειδιών υπογραφής (signing keys).
10	Υπάρχει πολύ υψηλού επιπέδου, συνεπής και πλήρως τεκμηριωμένη κρυπτογραφική αρχιτεκτονική, χωρίς ουσιώδη κενά, με ισχυρή απομόνωση μυστικών, σαφή κρυπτογραφική ευελιξία και πλήρη διακυβέρνηση του κύκλου ζωής (lifecycle governance).

Ενδείξεις που κατά κανόνα δεν επιτρέπουν 6/10 ή μεγαλύτερο

- Δεν προσδιορίζονται αλγόριθμοι, εκδόσεις πρωτοκόλλων ή παράμετροι κλειδιών για κρίσιμες λειτουργίες.
- Δεν υπάρχει τεκμηριωμένος κύκλος ζωής κλειδιών/πιστοποιητικών όπου αυτά χρησιμοποιούνται.
- Μυστικά (secrets) ή προνομιακά διαπιστευτήρια (privileged credentials) αποθηκεύονται ή μεταδίδονται σε μη προστατευμένη μορφή.

9. Κριτήριο 4: Ασφάλεια Επικοινωνιών, Δικτύων και Διεπαφών

Σκοπός. Αξιολογείται αν η επιφάνεια επικοινωνιακής έκθεσης είναι γνωστή, ελαχιστοποιημένη, διαχωρισμένη και ελεγχόμενη.

Όρια με άλλα κριτήρια. Η κρυπτογραφική ισχύς των επικοινωνιών βαθμολογείται στο Κ3. Η αυθεντικοποίηση/εξουσιοδότηση API στο Κ2. Η επικύρωση εισόδων (input validation) και η επιχειρησιακή λογική API στο Κ5. Η προστασία από DoS στο Κ8.

Ενδεικτικά τεκμήρια. Κατάλογος θυρών και υπηρεσιών, διαγράμματα δικτύου, σχεδιασμός ζωνών και τμημάτων δικτύου (zones/segments), κανόνες ή προδιαγραφές τείχους προστασίας και ACL (firewall rulesets), κατάλογος API, σχεδιασμός επιπέδου διαχείρισης (management plane), αρχιτεκτονική απομακρυσμένης πρόσβασης (remote access), κατάλογος ασύρματων διεπαφών, οδηγίες θωράκισης διεπαφών (hardening).

Ειδικά σημεία αναφοράς βαθμολόγησης

Βαθμός	Ειδική ερμηνεία
0	Υπάρχουν ανεξέλεγκτες ή άγνωστες εξωτερικές διεπαφές/υπηρεσίες ή κρίσιμη διαχείριση είναι αδικαιολόγητα εκτεθειμένη.
2	Η έκθεση είναι μόνο εν μέρει γνωστή και υπάρχουν σοβαρά κενά στον περιορισμό υπηρεσιών, στην κατάτμηση δικτύου (segmentation) ή στις διαχειριστικές διεπαφές (management interfaces).
4	Υπάρχει βασική καταγραφή και ορισμένοι περιορισμοί, αλλά σημαντικές διεπαφές, ζώνες ή απομακρυσμένη πρόσβαση δεν ελέγχονται επαρκώς.
6	Οι εφαρμοστέες διεπαφές, υπηρεσίες και θύρες είναι καταγεγραμμένες, η έκθεση είναι αναγκαία και ελεγχόμενη, οι ζώνες εμπιστοσύνης (trust zones) διαχωρίζονται επαρκώς και οι διαχειριστικές διεπαφές προστατεύονται.

Βαθμός	Ειδική ερμηνεία
8	Υπάρχει ισχυρή ελαχιστοποίηση επιφάνειας, λεπτομερής κατάτμηση δικτύου, αυστηρός έλεγχος του επιπέδου διαχείρισης (management plane), των εξωτερικών API, της απομακρυσμένης πρόσβασης (remote access) και των ασύρματων διεπαφών.
10	Η επικοινωνιακή αρχιτεκτονική επιτυγχάνει πολύ υψηλό βαθμό ελαχιστοποίησης και απομόνωσης, με σαφή επιβολή (enforcement) μεταξύ ζωνών, αυστηρή διαχείριση όλων των διεπαφών και χωρίς ουσιώδη μη αναγκαία έκθεση (exposure).

Ενδείξεις που κατά κανόνα δεν επιτρέπουν 6/10 ή μεγαλύτερο

- Δεν υπάρχει αξιόπιστος κατάλογος (inventory) των ενεργών διεπαφών, υπηρεσιών και θυρών.
- Διαχειριστική διεπαφή (management interface) είναι άμεσα εκτεθειμένη σε μη έμπιστο δίκτυο χωρίς κατάλληλους περιορισμούς.
- Υφίστανται διαφορετικές ζώνες εμπιστοσύνης χωρίς επαρκή τεχνικό διαχωρισμό όπου αυτό απαιτείται.

10. Κριτήριο 5: Ακεραιότητα Συστήματος, Εκτέλεσης και Λειτουργιών

Σκοπός. Αξιολογείται αν το Σύστημα αποτρέπει μη εξουσιοδοτημένη μεταβολή της προβλεπόμενης εκτέλεσης, της κατάστασης, του υλικολογισμικού (firmware) και των κρίσιμων λειτουργιών του.

Όρια με άλλα κριτήρια. Η επαλήθευση των πακέτων ενημέρωσης (update packages) πριν από την εγκατάσταση βαθμολογείται στο Κ7. Η ακεραιότητα της δόμησης και της διάθεσης εκδόσεων (build/release) κατά την παραγωγή στο Κ10. Η κρυπτογραφική ισχύς (cryptographic strength) που χρησιμοποιείται στους μηχανισμούς στο Κ3.

Ενδεικτικά τεκμήρια. Σχεδιασμός επικύρωσης εισόδων (input validation), μέτρα προστασίας της επιχειρησιακής λογικής (business logic), ακεραιότητα της κατάστασης συνεδρίας (session state), απομόνωση μισθωτών και διεργασιών (tenant/process isolation), σχεδιασμός ασφαλούς εκκίνησης (secure boot), αλυσίδα ακεραιότητας υλικολογισμικού, αρχιτεκτονική TPM, ασφαλούς στοιχείου (secure element) ή TEE, έλεγχοι διεπαφών αποσφαλμάτωσης (debug interfaces), σχεδιασμός προστασίας από φυσική παραβίαση (tamper protection).

Ειδικά σημεία αναφοράς βαθμολόγησης

Βαθμός	Ειδική ερμηνεία
0	Η προβλεπόμενη εκτέλεση ή κρίσιμη κατάσταση μπορεί να μεταβληθεί χωρίς ουσιαστικό έλεγχο ή απουσιάζουν θεμελιώδεις μηχανισμοί ακεραιότητας που απαιτούνται από τη φύση του Συστήματος.
2	Υπάρχουν μεμονωμένοι μηχανισμοί ακεραιότητας αλλά σημαντικές επιφάνειες παραμένουν χωρίς προστασία.
4	Υπάρχει ουσιαστική προστασία σε ορισμένα επίπεδα, αλλά παραμένουν σημαντικά κενά στον χειρισμό εισόδων (input handling), στην απομόνωση (isolation), στην επιχειρησιακή λογική (business logic), στην εκκίνηση και στο υλικολογισμικό (firmware) ή στη φυσική προστασία και στην προστασία διεπαφών αποσφαλμάτωσης (debug), ανάλογα με τον τύπο.
6	Οι ουσιώδεις εφαρμοστέοι μηχανισμοί ακεραιότητας καλύπτονται επαρκώς: ασφαλής επεξεργασία εισόδων/ροών για λογισμικό ή ασφαλής εκκίνηση, υλικολογισμικό, διεπαφές αποσφαλμάτωσης και φυσική προστασία για υλικό (hardware), με κατάλληλη απομόνωση όπου απαιτείται.
8	Υπάρχει πολυεπίπεδη προστασία ακεραιότητας, ισχυρή απομόνωση, συνεκτική αλυσίδα εμπιστοσύνης (chain of trust) ή αντίστοιχη αρχιτεκτονική ακεραιότητας λογισμικού και ουσιαστική προστασία από παραποίηση, επανάληψη και χειραγώγηση κατάστασης (tampering/replay/state manipulation).
10	Η ακεραιότητα εκτέλεσης και λειτουργιών προστατεύεται σε βάθος σε όλα τα εφαρμοστέα επίπεδα, με ισχυρή αλυσίδα εμπιστοσύνης και απομόνωση, πλήρη κάλυψη των κρίσιμων ροών και ιδιαίτερα ισχυρή τεκμηρίωση.

Ενδείξεις που κατά κανόνα δεν επιτρέπουν 6/10 ή μεγαλύτερο

- Για λογισμικό, μη έμπιστες είσοδοι ή κρίσιμες επιχειρησιακές ροές δεν προστατεύονται επαρκώς.
- Για υλικό και υλικολογισμικό (hardware/firmware), κρίσιμη εκκίνηση ή υλικολογισμικό μπορεί να τροποποιηθεί χωρίς αποτελεσματικό μηχανισμό ακεραιότητας, όπου τέτοιος μηχανισμός είναι αναγκαίος.
- Κρίσιμες διεπαφές αποσφαλμάτωσης ή συντήρησης (debug/service) παραμένουν μη ελεγχόμενες ή η απομόνωση μισθωτών και διεργασιών είναι ουσιωδώς ανεπαρκής.

11. Κριτήριο 6: Καταγραφή, Ιχνηλασιμότητα και Παρακολούθηση

Σκοπός. Αξιολογείται αν κρίσιμα γεγονότα και ενέργειες μπορούν να καταγραφούν, να αποδοθούν σε οντότητα, να προστατευθούν και να αξιοποιηθούν για εντοπισμό και διερεύνηση περιστατικών.

Όρια με άλλα κριτήρια. Η αυθεντικοποίηση της ταυτότητας που παράγει το συμβάν (event) ανήκει στο K2. Η κρυπτογραφική προστασία της μεταφοράς των αρχείων καταγραφής (logs) στο K3. Εδώ αξιολογούνται η πληρότητα, η ακεραιότητα, η ιχνηλασιμότητα και η επιχειρησιακή αξιοποίηση των καταγραφών.

Ενδεικτικά τεκμήρια. Πίνακας συμβάντων και καταγραφής, δείγματα σχημάτων αρχείων καταγραφής (log schemas), διαμόρφωση αρχείου ελέγχου (audit log), πολιτική διατήρησης (retention), σχεδιασμός συγχρονισμού χρόνου, διαμόρφωση SIEM και εξαγωγής, κανόνες ειδοποιήσεων (alerts), κατάλογος διαχειριστικών συμβάντων και συμβάντων ελέγχου, σχεδιασμός προστασίας αρχείων καταγραφής, ροή εργασιών διερεύνησης περιστατικών.

Ειδικά σημεία αναφοράς βαθμολόγησης

Βαθμός	Ειδική ερμηνεία
0	Κρίσιμες ενέργειες δεν καταγράφονται ή οι καταγραφές δεν είναι αξιόπιστες για βασική ιχνηλασιμότητα.
2	Υπάρχουν περιορισμένες καταγραφές αλλά λείπουν κρίσιμα συμβάντα ασφάλειας και διαχείρισης, η απόδοση ενεργειών σε πρόσωπα (attribution) ή η προστασία.
4	Η καταγραφή καλύπτει αρκετά γεγονότα αλλά υπάρχουν σημαντικά κενά σε ακεραιότητα, χρονική συνέπεια, διατήρηση (retention), ειδοποιήσεις (alerting) ή εξαγωγή (export).
6	Καταγράφονται επαρκώς κρίσιμες και προνομιακές ενέργειες, υπάρχει απόδοση ενεργειών σε πρόσωπα, χρονική συνέπεια, κατάλληλη προστασία και διατήρηση και δυνατότητα παρακολούθησης ή εξαγωγής όπου απαιτείται.
8	Η καταγραφή είναι ολοκληρωμένη και επιχειρησιακά αξιοποιήσιμη, με ισχυρή προστασία, κεντρική συσχέτιση ή εξαγωγή, κατάλληλες ειδοποιήσεις (alerts) και επαρκή υποστήριξη ψηφιακής εγκληματολογικής διερεύνησης (forensic investigation).
10	Υπάρχει πολύ υψηλού επιπέδου, πλήρως τεκμηριωμένος σχεδιασμός παρακολούθησης και ελέγχου (monitoring/audit), με σαφή ταξινόμηση συμβάντων (event taxonomy), αξιόπιστη συσχέτιση, ανθεκτική προστασία των αρχείων καταγραφής (logs) και ισχυρή ικανότητα ανίχνευσης και διερεύνησης.

Ενδείξεις που κατά κανόνα δεν επιτρέπουν 6/10 ή μεγαλύτερο

- Δεν καταγράφονται προνομιακές ή κρίσιμες ενέργειες όπου αυτό είναι τεχνικά εφικτό και αναγκαίο.
- Δεν είναι δυνατό να αποδοθούν κρίσιμα συμβάντα σε χρήστη/υπηρεσία/συσκευή όπου απαιτείται.
- Οι καταγραφές μπορούν να αλλοιωθούν ή διαγραφούν χωρίς κατάλληλο έλεγχο και χωρίς εναλλακτική αξιόπιστη καταγραφή.

12. Κριτήριο 7: Διαχείριση Ευπαθειών, Διαμόρφωσης και Ενημερώσεων

Σκοπός. Αξιολογείται αν το Σύστημα μπορεί να διατηρεί αποδεκτό επίπεδο ασφάλειας μετά τη διάθεσή του μέσω ασφαλούς διαμόρφωσης (configuration), χειρισμού ευπαθειών (vulnerability handling), ενημερώσεων (updates), υποστήριξης (support) και διαχείρισης της λήξης του κύκλου ζωής (end-of-life management).

Όρια με άλλα κριτήρια. Ο κατάλογος (inventory) και η προέλευση των συστατικών τρίτων βαθμολογούνται στο Κ9. Η ανάπτυξη και η δόμηση (build) νέας έκδοσης στο Κ10. Τα προεπιλεγμένα ή κοινόχρηστα διαπιστευτήρια, καθώς και η απαίτηση αλλαγής τους, βαθμολογούνται αποκλειστικά στο Κ2. Η έκθεση που προκύπτει από ενεργοποιημένες μη αναγκαίες δικτυακές υπηρεσίες βαθμολογείται στο Κ4. Στο Κ7 αξιολογούνται η συνολική διαδικασία ασφαλούς βασικής διαμόρφωσης και θωράκισης των προεπιλογών (secure baseline/default hardening), ο χειρισμός ευπαθειών και η ασφαλής διάθεση και εγκατάσταση ενημερώσεων, χωρίς επαναβαθμολόγηση των ίδιων επιμέρους ρυθμίσεων.

Ενδεικτικά τεκμήρια. Βασική διαμόρφωση θωράκισης (hardening baseline), προεπιλεγμένη διαμόρφωση (default configuration), διαδικασία διαχείρισης ευπαθειών (vulnerability management), PSIRT/VDP, διαδικασία έκδοσης ενημερωτικών δελτίων ασφάλειας (advisories), SLA εφαρμογής διορθώσεων (patches), αρχιτεκτονική ενημερώσεων, σχεδιασμός υπογραφής, επαλήθευσης και προστασίας από επαναφορά παλαιότερης έκδοσης (anti-rollback), περίοδος υποστήριξης, πολιτική EOL, παραδείγματα εκδόσεων και ενημερωτικών δελτίων.

Ειδικά σημεία αναφοράς βαθμολόγησης

Βαθμός	Ειδική ερμηνεία
0	Δεν υπάρχει ουσιαστικός μηχανισμός αντιμετώπισης γνωστών ευπαθειών ή το Σύστημα βρίσκεται σε κρίσιμο βαθμό εκτός υποστήριξης (unsupported) χωρίς επαρκή αντισταθμιστικά μέτρα.
2	Η αντιμετώπιση είναι κυρίως περιστασιακή, χωρίς σαφή βασική διαμόρφωση (baseline), διαδικασία ενημερώσεων ή δεσμεύσεις υποστήριξης.
4	Υπάρχουν διαδικασίες διαχείρισης ευπαθειών και διορθώσεων (vulnerability/patch management) και δυνατότητα ενημέρωσης, αλλά σημαντικά κενά παραμένουν στην ασφαλή εγκατάσταση, στα SLA, στη γνωστοποίηση ευπαθειών (disclosure), στη θωράκιση των προεπιλογών (default hardening) ή στη λήξη του κύκλου ζωής (EOL).
6	Υπάρχει τεκμηριωμένη ασφαλής βασική διαμόρφωση, παρακολούθηση και αντιμετώπιση ευπαθειών, ασφαλής ενημέρωση, σαφής περίοδος υποστήριξης και προβλέψεις EOL.
8	Η διαδικασία είναι ώριμη, με συντονισμένη γνωστοποίηση (coordinated disclosure), καθορισμένα επίπεδα σοβαρότητας και χρονικά πλαίσια, αυθεντικοποιημένες ενημερώσεις, κατάλληλη επαναφορά (rollback) και προστασία από επαναφορά παλαιότερης έκδοσης (anti-rollback), σαφή ενημερωτικά δελτία ασφάλειας (advisories) και γρήγορη αντιμετώπιση σοβαρών ευπαθειών.
10	Ο κύκλος ζωής ευπαθειών και ενημερώσεων είναι εξαιρετικά ώριμος και πλήρης, με ισχυρή τεχνική επιβολή (enforcement), σαφείς δεσμεύσεις κύκλου ζωής, έκτακτη απόκριση (emergency response), τεκμηριωμένη αποτελεσματικότητα και χωρίς ουσιώδες κενό.

Ενδείξεις που κατά κανόνα δεν επιτρέπουν 6/10 ή μεγαλύτερο

- Δεν υπάρχει αξιόπιστος τρόπος διάθεσης και εφαρμογής διορθώσεων ασφάλειας (security fixes) σε σύστημα που απαιτεί ενημερώσεις.
- Δεν δηλώνεται περίοδος υποστήριξης ασφάλειας (security support) ή χειρισμός της λήξης του κύκλου ζωής (EOL).
- Δεν υπάρχει διαδικασία λήψης, αξιολόγησης και αντιμετώπισης αναφορών ευπαθειών.
- Η προεπιλεγμένη διαμόρφωση αφήνει ενεργά ουσιώδη μη αναγκαία επικίνδυνα χαρακτηριστικά.

13. Κριτήριο 8: Διαθεσιμότητα, Ανθεκτικότητα και Ανάκτηση

Σκοπός. Αξιολογείται αν το Σύστημα μπορεί να διατηρήσει ή να αποκαταστήσει τις απαιτούμενες λειτουργίες του και να αποφεύγει μη ασφαλείς καταστάσεις σε αστοχία, επίθεση ή απώλεια εξαρτήσεων.

Όρια με άλλα κριτήρια. Η ασφάλεια και η προέλευση εξωτερικού παρόχου βαθμολογείται στο Κ9. Εδώ αξιολογείται η επίπτωση της μη διαθεσιμότητάς του. Η ενημέρωση μετά από αστοχία (failure) ανήκει στο Κ7, ενώ η ασφαλής συμπεριφορά κατά την αστοχία στο Κ8.

Ενδεικτικά τεκμήρια. Αρχιτεκτονική υψηλής διαθεσιμότητας και ανθεκτικότητας (HA/resilience), σχεδιασμός πλεονασμού (redundancy), πολιτική και αρχιτεκτονική αντιγράφων ασφαλείας (backup), διαδικασίες και αποτελέσματα αποκατάστασης που προσκομίζει ο αιτών, RTO/RPO όπου αρμόζει, σχεδιασμός ασφαλούς αστοχίας (fail-safe/fail-secure), έλεγχοι εξάντλησης πόρων (resource exhaustion), σενάρια αστοχίας εξαρτήσεων, σχεδιασμός ανάκαμψης από καταστροφή (disaster recovery).

Ειδικά σημεία αναφοράς βαθμολόγησης

Βαθμός	Ειδική ερμηνεία
0	Μία προβλέψιμη αστοχία ή απώλεια κρίσιμου στοιχείου μπορεί να προκαλέσει μη αποδεκτή απώλεια λειτουργίας ή μη ασφαλή κατάσταση χωρίς προβλεπόμενη ανάκτηση.
2	Υπάρχουν βασικές δυνατότητες επανεκκίνησης και αντιγράφων ασφαλείας (backup) αλλά σοβαρά κενά στην ανάκτηση (recovery), στον πλεονασμό (redundancy), στη συμπεριφορά σε αστοχία (failure) ή στην προστασία από DoS και εξάντληση πόρων.
4	Υπάρχει ουσιαστική ανθεκτικότητα σε ορισμένα σενάρια, αλλά σημαντικοί τρόποι αστοχίας (failure modes) ή εξαρτήσεις ανάκτησης (recovery dependencies) παραμένουν ανεπαρκώς καλυμμένοι.
6	Οι κρίσιμες λειτουργίες έχουν κατάλληλη ανθεκτικότητα, αντίγραφα ασφαλείας και ανάκτηση (backup/recovery) όπου απαιτείται, προβλεπόμενη ασφαλή συμπεριφορά σε αστοχία και βασική προστασία από εξάντληση πόρων (resource exhaustion) και DoS.
8	Υπάρχει ισχυρή και πολυεπίπεδη αρχιτεκτονική ανθεκτικότητας (resilience), προστατευμένα αντίγραφα ασφαλείας (backups), τεκμηριωμένη αποκατάσταση, πλεονασμός και σαφής ασφαλής υποβάθμιση ή απομόνωση σε αστοχία.
10	Η ανθεκτικότητα είναι εξαιρετικά ολοκληρωμένη, με πλήρη κάλυψη των κρίσιμων σεναρίων αστοχίας (failure scenarios), υψηλή ανεξαρτησία των μηχανισμών ανάκτησης (recovery mechanisms), σαφείς στόχους ανάκτησης (recovery objectives) όπου αρμόζουν και πολύ ισχυρή τεκμηρίωση.

Ενδείξεις που κατά κανόνα δεν επιτρέπουν 6/10 ή μεγαλύτερο

- Απαιτούνται αντίγραφα ασφαλείας και ανάκτηση (backups/recovery) αλλά δεν υπάρχουν ή δεν είναι τεκμηριωμένα.
- Υφίσταται κρίσιμο μοναδικό σημείο αστοχίας (single point of failure) χωρίς τεχνική ή οργανωτική αντιστάθμιση ανάλογη του κινδύνου.
- Η αστοχία κρίσιμου υποσυστήματος οδηγεί σε μη ασφαλή κατάσταση χωρίς προβλεπόμενο περιορισμό (containment) ή ασφαλή συμπεριφορά αστοχίας (fail-secure/fail-safe).

14. Κριτήριο 9: Εξαρτήσεις, Τρίτα Συστατικά και Αλυσίδα Εφοδιασμού

Σκοπός. Αξιολογείται ο βαθμός στον οποίο τα συστατικά τρίτων (third-party components), το υλικολογισμικό (firmware), οι βιβλιοθήκες (libraries), οι υπηρεσίες και οι προμηθευτές είναι γνωστά, ιχνηλάσιμα, υποστηριζόμενα και ελεγχόμενα ως προς τον κίνδυνο που εισάγουν.

Όρια με άλλα κριτήρια. Οι ιδιότητες ασφάλειας που παρέχει συστατικό τρίτου (component) βαθμολογούνται στο αντίστοιχο λειτουργικό κριτήριο. Η διαχείριση των ευπαθειών του βαθμολογείται

στο Κ7. Εδώ βαθμολογούνται ο κατάλογος (inventory), η προέλευση (provenance), η εξάρτηση από προμηθευτές (supplier dependency) και η διασφάλιση της αλυσίδας εφοδιασμού (supply-chain assurance).

Ενδεικτικά τεκμήρια. SBOM/HBOM/BOM, κατάλογος εξαρτήσεων (dependency inventory), κατάλογοι εκδόσεων, προέλευση και βεβαιώσεις (provenance/attestation), κατάλογος προμηθευτών, χάρτης εξαρτήσεων από υπηρεσίες νέφους (cloud), κατάσταση υποστήριξης συστατικών, έλεγχοι ακεραιότητας και γνησιότητας εισερχόμενων στοιχείων (artifacts), στρατηγική αντικατάστασης και μετριασμού.

Ειδικά σημεία αναφοράς βαθμολόγησης

Βαθμός	Ειδική ερμηνεία
0	Κρίσιμες εξαρτήσεις είναι άγνωστες ή μη ιχνηλάσιμες και δεν είναι δυνατό να αξιολογηθεί ουσιαστικά η αλυσίδα εφοδιασμού.
2	Υπάρχει αποσπασματική γνώση των εξαρτήσεων (dependencies) αλλά σημαντικά συστατικά (components), εκδόσεις, η προέλευση (provenance) ή η κατάσταση υποστήριξης (support status) παραμένουν άγνωστα.
4	Υπάρχει ουσιαστικός κατάλογος (inventory) αλλά σημαντικά κενά στην προέλευση, στον κίνδυνο προμηθευτή (supplier risk), στην κατάσταση υποστήριξης, στους ελέγχους ακεραιότητας ή στη δυνατότητα αντιμετώπισης προβληματικού συστατικού (component).
6	Υπάρχει επαρκής καταγραφή των κρίσιμων συστατικών και υπηρεσιών τρίτων, των εκδόσεων και της κατάστασης υποστήριξης, έλεγχος προέλευσης και ακεραιότητας (provenance/integrity) όπου αρμόζει και διαχείριση των κρίσιμων εξαρτήσεων από προμηθευτές (supplier dependencies).
8	Η αλυσίδα εφοδιασμού είναι πολύ καλά ελεγχόμενη, με πλήρες SBOM/BOM όπου εφαρμόζεται, ισχυρή τεκμηρίωση προέλευσης, αξιολόγηση προμηθευτών, παρακολούθηση (monitoring) και σαφές σχέδιο αντικατάστασης και μετριασμού.
10	Υπάρχει εξαιρετικά ώριμη, ιχνηλάσιμη και τεκμηριωμένη διασφάλιση της αλυσίδας εφοδιασμού (supply-chain assurance) σε όλο το κρίσιμο σύνολο εξαρτήσεων (dependency set), με υψηλή διαφάνεια, επαλήθευση ακεραιότητας (integrity verification) και πολύ ισχυρή δυνατότητα απόκρισης (response) σε παραβίαση προμηθευτή ή συστατικού.

Ενδείξεις που κατά κανόνα δεν επιτρέπουν 6/10 ή μεγαλύτερο

- Δεν υπάρχει επαρκής κατάλογος των κρίσιμων συστατικών και υπηρεσιών τρίτων (third-party components/services).
- Κρίσιμη εξάρτηση (dependency) είναι εκτός υποστήριξης χωρίς τεκμηριωμένο αντισταθμιστικό μέτρο ή σχέδιο αντικατάστασης.
- Η προέλευση ή η γνησιότητα των κρίσιμων εισερχόμενων στοιχείων και συστατικών (components) δεν μπορεί να τεκμηριωθεί όπου απαιτείται.

15. Κριτήριο 10: Ασφαλής Ανάπτυξη, Μεταβολές και Διάθεση Εκδόσεων

Σκοπός. Αξιολογείται αν η ασφάλεια είναι ενσωματωμένη στον κύκλο ζωής ανάπτυξης, αλλαγών, δόμησης (build) και παραγωγής, καθώς και διάθεσης εκδόσεων (release) του ίδιου του Συστήματος.

Όρια με άλλα κριτήρια. Οι ευπάθειες (vulnerabilities) που προκύπτουν μετά τη διάθεση και η διαχείριση διορθώσεων (patch management) βαθμολογούνται στο Κ7. Ο κατάλογος (inventory) των συστατικών τρίτων στο Κ9. Το περιεχόμενο του μοντέλου απειλών (threat model) στο Κ1. Εδώ αξιολογείται η διαδικασία παραγωγής ασφαλών εκδόσεων.

Ενδεικτικά τεκμήρια. Ασφαλής SDLC, απαιτήσεις ασφάλειας, πρότυπα κώδικα και σχεδιασμού (coding/design standards), αξιολόγηση από ομοτίμους (peer review) και έλεγχος αλλαγών (change control), έλεγχοι κλάδων και αποθετηρίων κώδικα (branch/repository controls), ασφάλεια CI/CD,

απομόνωση του περιβάλλοντος δόμησης (build isolation), έγκριση διάθεσης εκδόσεων (release approval), διαδικασία υπογραφής, ιχνηλασιμότητα εκδόσεων, εκθέσεις SAST/DAST, δοκιμών με τυχαία δεδομένα (fuzzing) και δοκιμών διείσδυσης (pentest) που παράγονται κατά την ανάπτυξη, παρακολούθηση της αποκατάστασης ευρημάτων (remediation tracking). Όταν ο αιτών δεν είναι ο κατασκευαστής ή ο υπεύθυνος ανάπτυξης, το κριτήριο εξακολουθεί να εφαρμόζεται βάσει τεκμηρίων του κατασκευαστή ή παρόχου. Η απουσία επαρκούς τεκμηρίωσης δεν επιτρέπει βαθμολογία 6/10 ή μεγαλύτερη.

Ειδικά σημεία αναφοράς βαθμολόγησης

Βαθμός	Ειδική ερμηνεία
0	Δεν υπάρχει ελεγχόμενη διαδικασία ανάπτυξης/μεταβολών ή δεν είναι δυνατό να τεκμηριωθεί πώς παράγονται και εγκρίνονται οι εκδόσεις.
2	Η ανάπτυξη είναι κυρίως περιστασιακή, με ελάχιστο έλεγχο αλλαγών (change control) και χωρίς σταθερή ενσωμάτωση απαιτήσεων ή ελέγχων ασφάλειας.
4	Υπάρχει βασικός SDLC και βασική διαχείριση αλλαγών (change management) και ορισμένοι έλεγχοι, αλλά σημαντικά κενά στην επισκόπηση (review), στον διαχωρισμό περιβαλλόντων, στην προστασία της δόμησης (build), στις δοκιμές ασφάλειας ή στην ακεραιότητα των εκδόσεων (release integrity).
6	Υπάρχει τεκμηριωμένος κύκλος ζωής ασφαλούς ανάπτυξης, αλλαγών και διάθεσης εκδόσεων (secure development/change/release lifecycle), με απαιτήσεις ασφάλειας, ελεγχόμενες αλλαγές, διαχωρισμό περιβαλλόντων, προστασία της δόμησης και της διάθεσης εκδόσεων (build/release), ιχνηλασιμότητα και κατάλληλες δοκιμές ασφάλειας με διαχείριση ευρημάτων.
8	Η ασφάλεια είναι ώριμα ενσωματωμένη στον SDLC, με ισχυρή επισκόπηση κώδικα και σχεδιασμού (code/design review), προστατευμένο CI/CD ή προστατευμένη διαδικασία παραγωγής, αυτοματοποιημένους ελέγχους, σαφή σημεία ελέγχου πριν από τη διάθεση (release gates) και πλήρη ιχνηλασιμότητα (traceability).
10	Ο κύκλος ζωής ασφαλούς ανάπτυξης (secure development lifecycle) είναι εξαιρετικά ώριμος και μετρήσιμος, με ισχυρή διασφάλιση (assurance) της αλυσίδας δόμησης και διάθεσης εκδόσεων, συστηματική επαλήθευση, αξιοποίηση διδαγμάτων και βελτίωση μέσω ανάλυσης γενεσιουργών αιτίων (lessons learned/root cause) και χωρίς ουσιώδες διαδικαστικό κενό.

Ενδείξεις που κατά κανόνα δεν επιτρέπουν 6/10 ή μεγαλύτερο

- Δεν υπάρχει ελεγχόμενη διαχείριση αλλαγών (change management) για τον κώδικα, το υλικολογισμικό (firmware) και τον σχεδιασμό.
- Δεν πραγματοποιούνται καθόλου κατάλληλοι έλεγχοι ασφάλειας κατά την ανάπτυξη ή δεν υπάρχει διαχείριση των ευρημάτων.
- Δεν υπάρχει ιχνηλασιμότητα μεταξύ πηγαίου κώδικα και σχεδιασμού, δόμησης και διάθεσης εκδόσεων ή η διαδικασία δόμησης και διάθεσης μπορεί να μεταβληθεί ανεξέλεγκτα.

16. Κρίσιμες Αδυναμίες

16.1. Η Κρίσιμη Αδυναμία είναι ποιοτική κρίση σοβαρότητας και όχι πρόσθετη βαθμολογική κατηγορία. Χαρακτηρίζεται σύμφωνα με το άρθρο 3 παρ. 7 και το άρθρο 22 της Διαδικασίας και πρέπει να αιτιολογείται ειδικά.

16.1.1. Η υποκείμενη τεχνική αδυναμία αποτυπώνεται στη βαθμολογία του αντίστοιχου κριτηρίου σύμφωνα με τα σημεία αναφοράς (anchors) του παρόντος. Η ιδιότητα «Κρίσιμη Αδυναμία» λειτουργεί επιπλέον ως αυτοτελής λόγος μη χορήγησης πιστοποιητικού και όχι ως δεύτερη αριθμητική ποινή.

16.2. Παράγοντες που συνεκτιμώνται

- η κρισιμότητα των επηρεαζόμενων δεδομένων ή λειτουργιών,
- η δυνατότητα πραγματικής εκμετάλλευσης ή κατάχρησης με βάση το αρχιτεκτονικό περιβάλλον,

- η απαιτούμενη πρόσβαση ή προϋπόθεση για την εκμετάλλευση,
- η έκταση και το βάθος της πιθανής επίπτωσης,
- η ύπαρξη και αποτελεσματικότητα αντισταθμιστικών δικλείδων,
- η συστημικότητα της αδυναμίας, δηλαδή αν αφορά μεμονωμένη λειτουργία ή θεμελιώδες όριο εμπιστοσύνης (trust boundary),
- η ύπαρξη γνωστής ενεργής εκμετάλλευσης ή αξιόπιστης δημόσιας τεκμηρίωσης,
- η κατάσταση υποστήριξης του επηρεαζόμενου κρίσιμου στοιχείου.

16.3. Ενδεικτικές περιπτώσεις

Περιοχή	Παράδειγμα
K2	Μη αυθεντικοποιημένη ή ανεπαρκώς εξουσιοδοτημένη πρόσβαση σε κρίσιμη/προνομιακή λειτουργία. Κοινά και μη μεταβαλλόμενα προνομιακά διαπιστευτήρια (privileged credentials).
K3	Μετάδοση κρίσιμων διαπιστευτηρίων (credentials) ή ιδιαίτερα ευαίσθητων δεδομένων χωρίς κατάλληλη προστασία σε μη έμπιστο δίκτυο. Αποδεδειγμένα μη ασφαλής κρυπτογραφικός μηχανισμός σε κρίσιμη λειτουργία.
K4	Άμεσα προσβάσιμη κρίσιμη διαχειριστική διεπαφή (management interface) από μη έμπιστο δίκτυο χωρίς ουσιαστικό περιορισμό, όταν αυτό δημιουργεί άμεσο σοβαρό κίνδυνο.
K5	Δυνατότητα μη εξουσιοδοτημένης εγκατάστασης/εκτέλεσης κώδικα ή υλικολογισμικού (firmware) σε κρίσιμο στοιχείο. Ανεπαρκής απομόνωση μισθωτών (tenant isolation) που επιτρέπει πρόσβαση σε δεδομένα άλλου μισθωτή.
K7	Γνωστή και μη αντιμετωπισμένη ευπάθεια σε κρίσιμο στοιχείο με ενδείξεις ενεργής εκμετάλλευσης. Κρίσιμο στοιχείο εκτός υποστήριξης ασφάλειας (security support) χωρίς επαρκή αντιστάθμιση.
K9	Παραβιασμένη ή μη αξιόπιστη κρίσιμη εξάρτηση της αλυσίδας εφοδιασμού (supply-chain dependency) χωρίς δυνατότητα περιορισμού (containment) ή αντικατάστασης, εφόσον δημιουργεί άμεσο ιδιαίτερα σοβαρό κίνδυνο.
Οποιοδήποτε	Ανοικτό εύρημα κρίσιμης σοβαρότητας από έκθεση τρίτου που αφορά το ίδιο Αντικείμενο Αξιολόγησης, εκτός αν τεκμηριωθεί η αντιμετώπισή του.

Υψηλή βαθμολογία CVSS, η ύπαρξη CVE ή η απουσία ενός επιμέρους τεκμηρίου δεν αρκούν από μόνα τους για χαρακτηρισμό Κρίσιμης Αδυναμίας. Πρέπει να επιβεβαιώνεται η εφαρμοσιμότητα στο συγκεκριμένο Αντικείμενο Αξιολόγησης και η σοβαρότητα στο συγκεκριμένο περιβάλλον.

Δημόσια διαθέσιμες πληροφορίες χρησιμοποιούνται σύμφωνα με τη Διαδικασία για τη διαπίστωση πιθανής Κρίσιμης Αδυναμίας. Δεν χρησιμοποιούνται για να αυξήσουν αριθμητικά τη βαθμολογία. Όταν δημόσια πληροφορία ενδέχεται να οδηγήσει σε Κρίσιμη Αδυναμία, ο αιτών καλείται, όπου είναι εφικτό, να τεκμηριώσει την εφαρμοσιμότητα, την αντιμετώπιση ή τα αντισταθμιστικά μέτρα.

17. Εφαρμογή σε Κατάσταση «Υπό ανάπτυξη» και «Υλοποιημένο»

17.1. Η ίδια κλίμακα και τα ίδια σημεία αναφοράς (anchors) εφαρμόζονται και στις δύο Καταστάσεις Συστήματος. Η διαφορά αφορά το είδος των τεκμηρίων που είναι λογικά διαθέσιμα.

Κατάσταση	Κανόνας
Υπό ανάπτυξη	Μπορεί να λάβει έως 10/10 σε κριτήριο όταν η τεκμηριωμένη αρχιτεκτονική, οι εγκεκριμένες προδιαγραφές, τα μοντέλα απειλών (threat models), οι διαδικασίες και ο σχεδιασμός παρέχουν πολύ υψηλή εμπιστοσύνη ως προς το προβλεπόμενο μέτρο. Ο βαθμός αφορά τον σχεδιασμό και όχι ανεξάρτητα επαληθευμένη υλοποίηση.
Υλοποιημένο	Σύστημα του οποίου η υλοποίηση έχει ήδη ολοκληρωθεί μπορεί να αξιολογηθεί απευθείας ως «Υλοποιημένο» κατά την αρχική αίτηση. Για βαθμό 6/10 ή μεγαλύτερο απαιτούνται τεκμήρια που συνδέουν τα δηλωμένα μέτρα με τη συγκεκριμένη υλοποιημένη έκδοση, όπως αρχεία εκδόσεων και διαμόρφωσης (version/configuration records), δηλωτικά εκδόσεων (release manifests), SBOM/BOM, αποσπάσματα διαμόρφωσης (configuration extracts), τεκμηρίωση επιχειρησιακής ασφάλειας (operational security documentation), αρχεία καταγραφής (logs) ή άλλα κατάλληλα στοιχεία.

Κατάσταση	Κανόνας
Μετάβαση σε Υλοποιημένο	Η συμπληρωματική αξιολόγηση συγκρίνει την υλοποιημένη έκδοση με την πιστοποιημένη αρχιτεκτονική και επαναβαθμολογεί μόνο τα κριτήρια που επηρεάζονται από αποκλίσεις, νέες εξαρτήσεις, αλλαγές διεπαφών ή άλλα ουσιώδη στοιχεία. Οι βαθμολογίες των μη επηρεαζόμενων κριτηρίων διατηρούνται, η συνολική Βαθμολογία Ασφάλειας επαναϋπολογίζεται και εφαρμόζονται εκ νέου οι προϋποθέσεις πιστοποίησης της Διαδικασίας. Δεν διενεργούνται από το ΚΕΜΕΑ εργαστηριακές δοκιμές ή δοκιμές διείσδυσης (penetration tests).

18. Συνέπεια μεταξύ αξιολογητών και ανεξάρτητη επανεξέταση

- Για βαθμούς 5/6, 7/8 και 9/10 ο αξιολογητής αναφέρει ρητά ποιο συγκεκριμένο στοιχείο τον τοποθετεί κάτω ή πάνω από το αντίστοιχο όριο.
- Ο επανεξεταστής ελέγχει όχι μόνο την αριθμητική τιμή αλλά και αν τα ίδια πραγματικά δεδομένα θα οδηγούσαν σε αντίστοιχο βαθμό σε άλλο παρόμοιο σύστημα.
- Δεν αποδίδεται πρόσθετη βαθμολογία λόγω φήμης κατασκευαστή, μεγέθους επιχείρησης, εμπορικής διείσδυσης ή κατοχής άσχετης πιστοποίησης.
- Υφιστάμενη πιστοποίηση ή έκθεση τρίτου λαμβάνεται υπόψη μόνο στο μέτρο που καλύπτει το ίδιο πεδίο εφαρμογής (scope), την ίδια έκδοση και το ίδιο τεχνικό χαρακτηριστικό.
- Το ΚΕΜΕΑ μπορεί να τηρεί εσωτερικό, ανωνυμοποιημένο σύνολο παραδειγμάτων βαθμολόγησης για τη βαθμονόμηση (calibration) των αξιολογητών. Τα παραδείγματα δεν δημιουργούν δεδικασμένο και δεν υποκαθιστούν την κρίση επί του συγκεκριμένου φακέλου.

Παράρτημα Α. Κατανομή χαρακτηριστικών μεταξύ κριτηρίων

Χαρακτηριστικό	Κριτήριο	Όριο / Παρατήρηση
Μοντέλο απειλών (threat model), επιφάνεια επίθεσης (attack surface), όρια εμπιστοσύνης (trust boundaries)	K1	Δεν βαθμολογείται εδώ η ισχύς των επιμέρους μέτρων ελέγχου (controls).
Ταυτότητα, αυθεντικοποίηση, MFA, ρόλοι, εξουσιοδότηση	K2	Κρυπτογραφική προστασία διαπιστευτηρίων (credentials) → K3.
Δημιουργία συνεδρίας, λήξη λόγω αδράνειας (timeout), αποσύνδεση (logout), ανάκληση	K2	Ανθεκτικότητα σε παραποίηση συνεδρίας ή κατάστασης (tampering) ή σε επανάληψη (replay) → K5.
Συνθηματικά (passwords), διακριτικά (tokens), μυστικά (secrets), ψηφιακά πιστοποιητικά (certificates), κύκλος ζωής κλειδιών	K3	Σημασιολογία ταυτότητας και εξουσιοδότησης → K2.
Ισχύς TLS/VPN και κρυπτογραφικών αλγορίθμων	K3	Δικτυακή έκθεση (network exposure) και κατάτμηση δικτύου (segmentation) → K4.
Θύρες, υπηρεσίες, κατάτμηση δικτύου, επίπεδο διαχείρισης (management plane)	K4	Ανθεκτικότητα σε DoS και εξάντληση πόρων → K8.
Έκθεση και κατάλογος (inventory) API	K4	Εξουσιοδότηση API → K2. Επικύρωση εισόδων (input validation) και επιχειρησιακή λογική (business logic) → K5.
Επικύρωση εισόδων, ανθεκτικότητα σε επιθέσεις έγχυσης (injection), ακεραιότητα επιχειρησιακής λογικής	K5	Διαδικασία δοκιμών κατά την ανάπτυξη → K10.
Ασφαλής εκκίνηση (secure boot),	K5	Επαλήθευση πακέτων ενημέρωσης πριν από την

Χαρακτηριστικό	Κριτήριο	Όριο / Παρατήρηση
ακεραιότητα εκτέλεσης (runtime) και υλικολογισμικού (firmware), TPM/TEE/ασφαλές στοιχείο (secure element)		εγκατάσταση → K7.
Θύρες JTAG/UART και θύρες συντήρησης, φυσική παραβίαση (physical tamper)	K5	Θύρες διαχείρισης δικτύου → K4.
Καταγραφή συμβάντων ασφάλειας και διαχείρισης και ίχνος ελέγχου (audit trail)	K6	Κρυπτογράφηση της μεταφοράς αρχείων καταγραφής (logs) → K3.
Ασφαλής βασική διαμόρφωση (secure baseline) και θωράκιση προεπιλογών (default hardening)	K7	Οι επιμέρους ρυθμίσεις δικτυακής έκθεσης μπορεί να ανήκουν στο K4. Αποφεύγεται η διπλή προσμέτρηση.
Παραλαβή αναφορών ευπαθειών (vulnerability intake), αποκατάσταση, κύκλος ζωής διορθώσεων και ενημερώσεων (patch/update lifecycle)	K7	Κατάλογος και προέλευση (provenance) συστατικών τρίτων → K9.
Αυθεντικοποίηση ενημερώσεων, επαλήθευση ακεραιότητας, προστασία από επαναφορά παλαιότερης έκδοσης (anti-rollback)	K7	Κύκλος ζωής κλειδιών υπογραφής → K3. Διαδικασία υπογραφής εκδόσεων → K10.
Αντίγραφα ασφαλείας (backup), ανάκτηση (recovery), πλεονασμός (redundancy), ασφαλής αστοχία (fail-safe/fail-secure), ανθεκτικότητα σε DoS	K8	Εμπιστοσύνη σε προμηθευτές και υπηρεσίες → K9.
Επίπτωση στη διαθεσιμότητα από διακοπή εξωτερικής υπηρεσίας νέφους (cloud) ή παρόχου	K8	Ασφάλεια και προέλευση του παρόχου → K9.
SBOM/BOM, προέλευση συστατικών, εξαρτήσεις από προμηθευτές	K9	Χειρισμός ευπαθειών των συστατικών αυτών → K7.
Ασφαλής SDLC, έλεγχος αλλαγών (change control), CI/CD, ακεραιότητα δόμησης (build) και διάθεσης εκδόσεων (release)	K10	Εφαρμογή διορθώσεων (patching) κατά τη λειτουργία, μετά τη διάθεση → K7.
Δοκιμές ασφάλειας κατά την ανάπτυξη και διαχείριση ευρημάτων	K10	Πραγματική τεχνική αδυναμία που αναδεικνύεται από δοκιμή → σχετικό λειτουργικό κριτήριο ή/και Κρίσιμη Αδυναμία.
Προεπιλεγμένα, προρυθμισμένα ή κοινόχρηστα διαπιστευτήρια	K2	Αποκλειστικά στο K2. Η γενική διαδικασία ασφαλούς βασικής διαμόρφωσης και θωράκισης προεπιλογών αξιολογείται στο K7, χωρίς επαναβαθμολόγηση των ίδιων διαπιστευτηρίων.
Προεπιλεγμένη διαμόρφωση (default configuration) που ενεργοποιεί μη αναγκαία δικτυακή υπηρεσία	K4 / K7	Η συγκεκριμένη δικτυακή έκθεση βαθμολογείται στο K4. Η διαδικασία και η πολιτική ασφαλούς βασικής διαμόρφωσης και θωράκισης (hardening) βαθμολογείται στο K7. Δεν επιτρέπεται διπλή ποινή για το ίδιο πραγματικό εύρημα.

Παράρτημα Β. Ελάχιστα ενδεικτικά τεκμήρια για βαθμό 6/10

Κριτήριο	Ελάχιστη ενδεικτική βάση τεκμηρίωσης
K1	Αρχιτεκτονική/συστατικά, βασικές ροές, όρια εμπιστοσύνης (trust boundaries), μοντέλο απειλών

Κριτήριο	Ελάχιστη ενδεικτική βάση τεκμηρίωσης
	(threat model) ή ισοδύναμη ανάλυση, παραδοχές περιβάλλοντος.
K2	Σχεδιασμός αυθεντικοποίησης και εξουσιοδότησης, ρόλοι/δικαιώματα, προνομιακή πρόσβαση (privileged access), κύκλος ζωής ταυτοτήτων, κύκλος ζωής συνεδριών όπου εφαρμόζεται.
K3	Αντιστοίχιση της προστασίας δεδομένων και μυστικών (data/secret protection mapping), αλγόριθμοι, πρωτόκολλα και εκδόσεις, κύκλος ζωής κλειδιών, ψηφιακών πιστοποιητικών (certificates) και μυστικών.
K4	Κατάλογος (inventory) διεπαφών, θυρών και υπηρεσιών, αρχιτεκτονική δικτύου και ζωνών, έλεγχοι διαχειριστικής και απομακρυσμένης πρόσβασης (management/remote access).
K5	Τεκμήρια των εφαρμοστέων μέτρων ακεραιότητας (integrity controls): για λογισμικό, εισόδων, κατάστασης και απομόνωσης ή, για υλικό, εκκίνησης, υλικολογισμικού (firmware), διεπαφών αποσφαλμάτωσης (debug) και προστασίας από φυσική παραβίαση (tamper).
K6	Προδιαγραφή καταγραφής και συμβάντων (logging/event specification), κρίσιμα και διαχειριστικά συμβάντα, απόδοση ενεργειών σε πρόσωπα (attribution), προστασία και διατήρηση (retention), παρακολούθηση και εξαγωγή όπου εφαρμόζεται.
K7	Ασφαλής βασική διαμόρφωση (secure baseline), διαδικασία διαχείρισης ευπαθειών (vulnerability management), μηχανισμός ενημερώσεων και διορθώσεων (update/patch), περίοδος υποστήριξης και χειρισμός της λήξης του κύκλου ζωής (EOL).
K8	Σχεδιασμός ανθεκτικότητας και συμπεριφοράς σε αστοχία (resilience/failure design), αντίγραφα ασφαλείας και ανάκτηση (backup/recovery) όπου απαιτείται, ασφαλής συμπεριφορά σε αστοχία (safe failure behavior), κρίσιμες εξαρτήσεις διαθεσιμότητας.
K9	Κατάλογος κρίσιμων συστατικών και υπηρεσιών τρίτων (third-party components/services), εκδόσεις, υποστήριξη και προέλευση (provenance), καθώς και χειρισμός προμηθευτών και εξαρτήσεων.
K10	Διαδικασία ασφαλούς ανάπτυξης, αλλαγών και διάθεσης εκδόσεων, ιχνηλασιμότητα δόμησης (build) και διάθεσης εκδόσεων (release), διαδικασία δοκιμών ασφάλειας και διαχείριση ευρημάτων.

Παράρτημα Γ. Φύλλο Βαθμολόγησης

Η βαθμολογία ανά κριτήριο, η συνολική Βαθμολογία Ασφάλειας, τυχόν Κρίσιμες Αδυναμίες και το τελικό αποτέλεσμα κατά το άρθρο 26 της Διαδικασίας καταγράφονται στο Ενιαίο Φύλλο Αξιολόγησης Τεχνολογικού Συστήματος, που εγκρίνεται κατά το άρθρο 5 παρ. 3 της Διαδικασίας.

Παράρτημα Δ. Τεχνικές πηγές αναφοράς

Πηγή	Χρήση στον Οδηγό
NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations, με τις ισχύουσες ενημερώσεις Release 5.2.0 (2025).	Χρησιμοποιείται ως γενικό πλαίσιο οικογενειών μέτρων ελέγχου (control families), λειτουργικότητας (functionality) και διασφάλισης (assurance).
NIST SP 800-53A Rev. 5, Assessing Security and Privacy Controls in Information Systems and Organizations, με Release 5.2.0.	Χρησιμοποιείται ως μεθοδολογικό υπόβαθρο για την αξιολόγηση βάσει τεκμηρίων (evidence-based assessment) και την προσαρμογή (tailoring) των διαδικασιών αξιολόγησης (assessment procedures).
NIST SP 800-218, Secure Software Development Framework (SSDF) Version 1.1, Final.	Χρησιμοποιείται κυρίως για το K10 και συναφή στοιχεία πρόληψης ευπαθειών και ασφαλούς ανάπτυξης (vulnerability prevention/secure development).
OWASP Application Security Verification Standard (ASVS) 5.0.0, Stable Release, 30 May 2025.	Χρησιμοποιείται ως τεχνική πηγή για την ασφάλεια εφαρμογών (application security), την αυθεντικοποίηση, τις συνεδρίες, τον έλεγχο πρόσβασης (access control), την επικύρωση δεδομένων (validation), την κρυπτογραφία και την καταγραφή συμβάντων (logging).

Πηγή	Χρήση στον Οδηγό
IEC 62443-4-1:2018, Secure product development lifecycle requirements.	Χρησιμοποιείται κυρίως για τον κύκλο ζωής ασφαλούς ανάπτυξης (secure development lifecycle), τη διαχείριση ελαττωμάτων και διορθώσεων (defect/patch management), την επαλήθευση και επικύρωση (verification/validation) και τη λήξη του κύκλου ζωής του προϊόντος (product end-of-life) σε υλικό, λογισμικό και υλικολογισμικό.
NIST IR 8259 Rev. 1, Foundational Cybersecurity Activities for IoT Product Manufacturers, Final, April 2026, και NISTIR 8259A, IoT Device Cybersecurity Capability Core Baseline.	Χρησιμοποιούνται για δυνατότητες υλικού και IoT, διαμόρφωση συσκευών (device configuration), προστασία δεδομένων, λογική πρόσβαση σε διεπαφές (logical access to interfaces), ενημέρωση λογισμικού (software update) και επίγνωση της κατάστασης κυβερνοασφάλειας (cybersecurity state awareness).

Οι ανωτέρω πηγές δεν αποτελούν κανονιστικές απαιτήσεις του παρόντος Οδηγού και δεν χρησιμοποιούνται ως βάση δήλωσης συμμόρφωσης προς τα αντίστοιχα πρότυπα ή πλαίσια.

Παράρτημα Ε. Ενιαία εφαρμογή των κριτηρίων ανά τύπο συστήματος

Ο ακόλουθος πίνακας συγκεντρώνει, για λόγους ευχρηστίας, την κύρια τεχνική εστίαση κάθε κριτηρίου σε συστήματα λογισμικού/SaaS, υλικού/IoT και μικτά/OT. Ο πίνακας δεν εισάγει διαφορετικά κριτήρια, βάρη ή απαιτήσεις ανά τύπο συστήματος και δεν υποκαθιστά την εξέταση εφαρμοσιμότητας των επιμέρους στοιχείων.

Κριτήριο	Λογισμικό / SaaS	Υλικό / IoT	Μικτό / OT
K1	Συστατικά (components), υπηρεσίες, API, χώροι αποθήκευσης δεδομένων (data stores), μισθωτές (tenants), πάροχοι ταυτότητας (identity providers), εξωτερικές διασυνδέσεις, ροές δεδομένων.	Δομικά στοιχεία υλικού (hardware blocks), υλικολογισμικό (firmware), αλυσίδα εκκίνησης (boot chain), φυσικές διεπαφές και διεπαφές αποσφαλμάτωσης (debug), επικοινωνίες, ταυτότητα συσκευής, διαδρομή ενημέρωσης.	Όρια μεταξύ υλικού, υλικολογισμικού, λογισμικού, νέφους/συστημάτων υποστήριξης (cloud/backend), σταθμών χειριστών (operator stations), ζωνών και αγωγών επικοινωνίας (zones/conduits) και αλληλεξαρτήσεις.
K2	RBAC/ABAC, εξουσιοδότηση μισθωτών, διαχειριστικοί ρόλοι, κύκλος ζωής συνεδριών, SSO/MFA, λογαριασμοί υπηρεσιών (service accounts).	Ταυτότητα συσκευής και χρήστη, τοπικός διαχειριστής, πρόσβαση συντήρησης, ταυτότητες σύζευξης και εγγραφής (pairing/enrolment), διαπιστευτήρια υπηρεσιών.	Ρόλοι χειριστών και μηχανικών (operator/engineering roles), ταυτότητες μηχανών, απομακρυσμένη συντήρηση, προνομιακές λειτουργίες μεταξύ συστατικών.
K3	TLS, κρυπτογράφηση βάσεων δεδομένων και αποθήκευσης, διαχειριστές μυστικών (secret managers), κατακερματισμός συνθηματικών (password hashing), κύκλος ζωής διακριτικών (tokens), πιστοποιητικών και κλειδιών.	Κλειδιά συσκευών, κλειδιά υπογραφής υλικολογισμικού, ασφαλής αποθήκευση μυστικών, προστατευμένες επικοινωνίες, παροχή διαπιστευτηρίων (credential provisioning).	Διαπιστευτήρια αμοιβαίας αυθεντικοποίησης (mutual authentication), κλειδιά μεταξύ συστατικών, μακράς διάρκειας πιστοποιητικά συσκευών, ασφαλής εναλλαγή κλειδιών (key rotation).

Κριτήριο	Λογισμικό / SaaS	Υλικό / IoT	Μικτό / OT
K4	Δημόσια και ιδιωτικά API, επίπεδο διαχείρισης (admin plane), ομάδες ασφάλειας νέφους (cloud security groups), εισερχόμενη και εξερχόμενη κίνηση (ingress/egress), έκθεση μεταξύ υπηρεσιών (service-to-service).	Δίκτυο, ραδιοσυχνότητες, Bluetooth/Wi-Fi/κινητή τηλεφωνία, διεπαφές συντήρησης, τοπικές δικτυακές υπηρεσίες.	Ζώνες και αγωγοί επικοινωνίας, διεπαφές μηχανικών (engineering interfaces), απομακρυσμένη πρόσβαση προμηθευτών, βιομηχανικά πρωτόκολλα και δίαυλοι πεδίου (fieldbus), πύλες (gateways).
K5	Επικύρωση εισόδων (input validation), προστασία από έγχυση (injection), ακεραιότητα επιχειρησιακής λογικής, ακεραιότητα συνεδρίας και κατάστασης, απομόνωση μισθωτών και διεργασιών (tenant/process isolation).	Ασφαλής εκκίνηση (secure boot), ακεραιότητα υλικολογισμικού, ρίζα εμπιστοσύνης (root of trust), θύρες αποσφαλμάτωσης (debug ports), αντίσταση σε φυσική παραβίαση και ανίχνευσή της (tamper resistance/detection), προστατευμένη εκτέλεση.	Αλυσίδα εμπιστοσύνης από άκρο σε άκρο (end-to-end chain of trust) μεταξύ υλικού, υλικολογισμικού και λογισμικού και προστασία εντολών και κατάστασης μεταξύ επιπέδων.
K6	Συμβάντα αυθεντικοποίησης και διαχείρισης, πρόσβαση σε δεδομένα, προνομιακές λειτουργίες, συμβάντα ασφάλειας API, ενοποίηση με SIEM.	Συμβάντα συσκευής, αλλαγές διαμόρφωσης, απόπειρες ενημέρωσης, κατάσταση φυσικής παραβίασης και ασφάλειας (tamper/security state), απομακρυσμένη διαχείριση.	Συμβάντα χειριστών και μηχανικών, συμβάντα συσκευών, αρχεία καταγραφής πυλών (gateway logs), συγχρονισμένες χρονοσημάνσεις, κεντρική παρακολούθηση.
K7	Διαδικασία διορθώσεων και διάθεσης εκδόσεων (patch/release), ασφαλείς προεπιλογές (secure defaults), παραλαβή αναφορών ευπαθειών (vulnerability intake), ενημερωτικά δελτία ασφάλειας (advisories), διακυβέρνηση ενημερώσεων υπηρεσίας.	Υπογεγραμμένες και επαληθευμένες ενημερώσεις υλικολογισμικού, προστασία από επαναφορά παλαιότερης έκδοσης (anti-rollback) όπου χρειάζεται, περίοδος υποστήριξης, ασφαλείς προεπιλογές, ενημέρωση ανάκτησης (recovery update).	Συντονισμένη εφαρμογή διορθώσεων (patching) σε εξαρτώμενα συστατικά, παράθυρα συντήρησης (maintenance windows), αντισταθμιστικά μέτρα για καθυστερημένη εφαρμογή διορθώσεων.
K8	Υψηλή διαθεσιμότητα (HA), αντίγραφα ασφαλείας (backups), ανάκτηση δεδομένων, εξαρτήσεις από περιοχές και υπηρεσίες νέφους (cloud region/service), περιορισμός ρυθμού αιτημάτων (rate limiting) και προστασία πόρων.	Ασφαλείς τρόποι αστοχίας (safe failure modes), μηχανισμοί επιτήρησης και ανάκτησης (watchdog/recovery), τοπική λειτουργία σε απώλεια συνδεσιμότητας, συμπεριφορά κατά την επαναφορά (restore/reset).	Πλεονασμός (redundancy), λειτουργία σε υποβαθμισμένη κατάσταση (degraded modes), ασφαλής συμπεριφορά αστοχίας (fail-safe/fail-secure), απώλεια εξαρτήσεων από νέφος, πύλες ή ελεγκτές (cloud/gateway/controller).
K9	Βιβλιοθήκες (libraries), πλαίσια λογισμικού (frameworks), περιέκτες (containers), εξαρτήσεις SaaS/PaaS, IdP, εξωτερικά API, SBOM.	Ολοκληρωμένα κυκλώματα και αρθρώματα (chipsets/modules), φορτωτές εκκίνησης (bootloaders), υλικολογισμικό τρίτων, βιβλιοθήκες, εξαρτήσεις κατασκευής και εφοδιασμού, HBOM/BOM.	Ελεγκτές (controllers), πύλες, υπηρεσίες νέφους, πρωτόκολλα και στοίβες λογισμικού τρίτων (third-party protocols/stacks), απομακρυσμένες υπηρεσίες προμηθευτών, αλυσίδες εξαρτήσεων κύκλου ζωής.

Κριτήριο	Λογισμικό / SaaS	Υλικό / IoT	Μικτό / OT
K10	Ασφαλής SDLC, επισκόπηση κώδικα (code review), CI/CD, SAST/DAST/δοκιμές με τυχαία δεδομένα (fuzzing), σημεία ελέγχου πριν από τη διάθεση (release gates), διαχωρισμός παραγωγικού περιβάλλοντος (production).	Ασφαλής ανάπτυξη υλικού και υλικολογισμικού, ελεγχόμενες εισροές κατασκευής, δόμηση και υπογραφή υλικολογισμικού (firmware build/signing), επικύρωση, έλεγχος διάθεσης εκδόσεων (release control).	Συντονισμένος κύκλος ζωής για υλικό, υλικολογισμικό, λογισμικό και συστήματα υποστήριξης (backend), συμβατότητα και επίπτωση στην ασφάλεια των συντονισμένων εκδόσεων.

19. Έναρξη εφαρμογής και αναθεώρηση του Οδηγού

19.1. Ο Οδηγός εφαρμόζεται από την ημερομηνία έναρξης ισχύος της Διαδικασίας, όπως ορίζεται στην απόφαση έγκρισης.

19.2. Αναθεωρείται όταν μεταβάλλονται ουσιωδώς η Διαδικασία, η τεχνολογική κατάσταση της τέχνης ή οι βασικές διεθνείς πρακτικές στις οποίες στηρίζεται.

19.3. Κάθε αναθεώρηση φέρει νέο αριθμό έκδοσης και εφαρμόζεται σύμφωνα με το άρθρο 10 παρ. 10 της Διαδικασίας.