

28 ΣΕΠΤΕΜΒΡΙΟΥ – 4 ΟΚΤΩΒΡΙΟΥ 2026

Define Resilience Brief

Το νέο τεύχος συγκεντρώνει τέσσερις εξελίξεις με άμεσο επιχειρησιακό αντίκτυπο: τη μετάβαση στο ISO 9001:2026, την προστασία APIs, την ασφάλεια των συστημάτων AI και τις νέες προθεσμίες για τα συστήματα καυσίμων.

01

QUALITY MANAGEMENT • ISO 9001:2026 • TRANSITION

Δημοσιεύθηκε το νέο ISO 9001:2026

Το ISO 9001:2026 δημοσιεύθηκε στις 16 Σεπτεμβρίου. Οι οργανισμοί με πιστοποίηση ISO 9001:2015 έχουν έως τις 30 Σεπτεμβρίου 2029 για να ολοκληρώσουν τη μετάβαση.

ΓΕΓΟΝΟΣ:

Στις 16 Σεπτεμβρίου 2026 δημοσιεύθηκε η νέα έκδοση του σημαντικότερου προτύπου ποιότητας, η οποία αντικαθιστά το ISO 9001:2015. Οι ήδη πιστοποιημένες επιχειρήσεις θα έχουν τρία χρόνια για τη μετάβαση. Οι βασικές αλλαγές αφορούν:

- ισχυρότερη σύνδεση του συστήματος ποιότητας με τη στρατηγική
- quality culture και ethical behaviour με μεγαλύτερη συμμετοχή και awareness των εργαζομένων
- σαφέστερο διαχωρισμό κινδύνων και ευκαιριών
- ενσωμάτωση θεμάτων digitalization, resilience και σύνθετων εφοδιαστικών αλυσίδων

ΣΗΜΑΣΙΑ:

Η μετάβαση απαιτεί οργανωμένη αξιολόγηση των διαφορών και προγραμματισμό των αλλαγών που αφορούν το σύστημα ποιότητας. Δεν προϋποθέτει αυτομάτως ανακατασκευή του συστήματος: η έκταση των ενεργειών θα εξαρτηθεί από το πώς εφαρμόζονται σήμερα οι απαιτήσεις στην επιχείρηση.

ΠΟΙΟΙ ΕΠΗΡΕΑΖΟΝΤΑΙ

Επιχειρήσεις πιστοποιημένες κατά ISO 9001:2015, οργανισμοί που σχεδιάζουν πιστοποίηση, υπεύθυνοι ποιότητας και φορείς πιστοποίησης.

ΠΗΓΗ: [ISO/TC 176 — ISO 9001:2026 και οδηγίες μετάβασης](#)

ACTION - ΤΙ ΝΑ ΕΛΕΓΞΕΤΕ ΓΙΑ ΤΗ ΜΕΤΑΒΑΣΗ:

- Έχει οριστεί υπεύθυνος και χρονοδιάγραμμα μετάβασης με ορόσημο την 30ή Σεπτεμβρίου 2029.
- Έχει γίνει αρχική σύγκριση των απαιτήσεων της έκδοσης 2026 με τις υφιστάμενες διαδικασίες και τεκμηρίωση.
- Έχουν αξιολογηθεί οι επιπτώσεις σε ηγεσία, κουλτούρα ποιότητας, λογοδοσία και διαχείριση κινδύνων και ευκαιριών.
- Έχει ενταχθεί η μετάβαση στον προγραμματισμό εσωτερικών ελέγχων και ανασκόπησης από τη Διοίκηση.

ΕΡΩΤΗΣΗ ΓΙΑ ΤΗ ΔΙΟΙΚΗΣΗ:

- Έχουμε σαφή εικόνα των αλλαγών που αφορούν τον οργανισμό μας και επαρκή χρόνο για να ολοκληρώσουμε τη μετάβαση έως τον Σεπτέμβριο 2029;

Τα APIs είναι η αθέατη περιοχή επίθεσης της επιχείρησης

Η Εθνική Αρχή Κυβερνοασφάλειας προκήρυξε υπηρεσίες προστασίας διαδικτυακών εφαρμογών και APIs από DDoS και επιθέσεις σε επίπεδο εφαρμογής.

ΓΕΓΟΝΟΣ:

Στις 30 Σεπτεμβρίου 2026, η Εθνική Αρχή Κυβερνοασφάλειας προκήρυξε διαγωνισμό για εξελιγμένες υπηρεσίες προστασίας διαδικτυακών εφαρμογών και APIs από DDoS και επιθέσεις επιπέδου εφαρμογής. Η προθεσμία υποβολής προσφορών είναι η 5η Νοεμβρίου 2026.

ΣΗΜΑΣΙΑ:

Ο διαγωνισμός δεν θεσπίζει νέα οριζόντια κανονιστική υποχρέωση για τις επιχειρήσεις. Αποτελεί, ωστόσο, ένδειξη ότι η προστασία εφαρμογών, των APIs και της διαθεσιμότητας υπηρεσιών βρίσκεται ψηλά στην ελληνική ατζέντα κυβερνοασφάλειας.

ΠΟΙΟΙ ΕΠΗΡΕΑΖΟΝΤΑΙ

Οντότητες NIS2, δημόσιοι φορείς, SaaS και fintech επιχειρήσεις, τηλεπικοινωνίες, e-commerce και οργανισμοί που παρέχουν κρίσιμες ψηφιακές υπηρεσίες.

ΠΗΓΗ: [Εθνική Αρχή Κυβερνοασφάλειας, 30.09.2026](#)

ACTION - ΤΙ ΝΑ ΕΛΕΓΞΕΤΕ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ ΤΩΝ APIs:

- Υπάρχει ενημερωμένος κατάλογος APIs, ιδιοκτητών, δεδομένων και εξωτερικών εκθέσεων.
- Οι έλεγχοι καλύπτουν authentication, authorization και κατάχρηση επιχειρησιακής λογικής, όχι μόνο υποδομές και endpoints.
- Έχουν οριστεί όρια κλήσεων (rate limiting), παρακολούθηση και ειδοποιήσεις για ασυνήθιστη κίνηση.
- Έχει δοκιμαστεί η ανθεκτικότητα εφαρμογών και APIs σε DDoS και επιθέσεις επιπέδου εφαρμογής.

ΕΡΩΤΗΣΗ ΓΙΑ ΤΗ ΔΙΟΙΚΗΣΗ:

- Μπορούμε να εντοπίσουμε ποια APIs είναι εκτεθειμένα, ποιος τα έχει υπό ευθύνη και τι θα συμβεί αν δεχθούν επίθεση;

Το ISO 27001 δεν αρκεί για την ασφάλεια του AI

Το ISO/IEC 27090 βρίσκεται στο στάδιο «under publication» και προσθέτει καθοδήγηση για απειλές που αφορούν ειδικά τα συστήματα AI.

ΓΕΓΟΝΟΣ:

Η πρώτη έκδοση του ISO/IEC 27090 (2026) καλύπτει την κατανόηση, ανίχνευση και αντιμετώπιση απειλών σε όλο τον κύκλο ζωής συστημάτων τεχνητής νοημοσύνης, όπως αλλοίωση δεδομένων εκπαίδευσης και κλοπή μοντέλων. Το πρότυπο συμπληρώνει τις πρακτικές των ISO/IEC 27001 και ISO/IEC 27002· δεν τις αντικαθιστά.

ΣΗΜΑΣΙΑ:

Η εφαρμογή του ISO 27001 από μόνη της δεν αποτυπώνει κατ' ανάγκη τους κινδύνους των δεδομένων, των μοντέλων και των ροών εργασίας AI. Χρειάζεται να συνδεθούν οι υφιστάμενοι έλεγχοι ασφάλειας με τον τρόπο ανάπτυξης, χρήσης και ενημέρωσης των μοντέλων.

ΠΟΙΟΙ ΕΠΗΡΕΑΖΟΝΤΑΙ

Developers και providers AI, επιχειρήσεις που ενσωματώνουν AI σε προϊόντα ή διαδικασίες, καθώς και οργανισμοί που διαχειρίζονται ευαίσθητα δεδομένα ή εφαρμόζουν ISO/IEC 42001.

ΠΗΓΗ: [ISO/IEC 27090](#)

ACTION - ΤΙ ΝΑ ΕΛΕΓΞΕΤΕ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ ΤΗΣ AI:

- Έχουν καταγραφεί τα συστήματα AI, τα μοντέλα, τα δεδομένα εκπαίδευσης και οι υπεύθυνοι λειτουργίας τους.
- Η αξιολόγηση απειλών καλύπτει ανάπτυξη, χρήση, ενημέρωση και επανεκπαίδευση μοντέλων.
- Έχουν οριστεί έλεγχοι πρόσβασης, logging και δοκιμές για μοντέλα και σχετικά δεδομένα.
- Υπάρχει διαδικασία αναφοράς και αντιμετώπισης περιστατικών που αφορούν συστήματα AI.

ΕΡΩΤΗΣΗ ΓΙΑ ΤΗ ΔΙΟΙΚΗΣΗ:

- Ξέρουμε ποια δεδομένα και μοντέλα AI είναι κρίσιμα για εμάς και πώς θα εντοπίσουμε αλλοίωση ή μη εξουσιοδοτημένη πρόσβαση;

Νέο χρονοδιάγραμμα συμμόρφωσης για πρατήρια και συστήματα καυσίμων

Οι νέες προθεσμίες για συστήματα εισροών-εκροών και Μητρώο Δεξαμενών φτάνουν έως το 2027, με διαφοροποίηση ανά περιοχή και τύπο εγκατάστασης.

ΓΕΓΟΝΟΣ:

Στις 2 Οκτωβρίου 2026 ανακοινώθηκε μετάθεση των προθεσμιών για την αναβάθμιση των συστημάτων εισροών-εκροών και την απογραφή ιδιωτικών πρατηρίων στο Μητρώο Δεξαμενών της ΑΑΔΕ:

- δημόσια πρατήρια Αττικής και Θεσσαλονίκης: **30 Ιουνίου 2027**
- δημόσια πρατήρια υπόλοιπης Ελλάδας: **31 Δεκεμβρίου 2027**
- ιδιωτικά πρατήρια και ηλεκτρονική απογραφή δεξαμενών: **31 Δεκεμβρίου 2027**

ΣΗΜΑΣΙΑ:

Η παράταση δίνει χρόνο για τεχνική προσαρμογή, όμως απαιτεί έγκαιρη επιβεβαίωση της κατηγορίας κάθε εγκατάστασης, των εφαρμοστέων απαιτήσεων και των απαιτούμενων αποδεικτικών.

ΠΟΙΟΙ ΕΠΗΡΕΑΖΟΝΤΑΙ

Δημόσια και ιδιωτικά πρατήρια, πωλητές πετρελαίου θέρμανσης, εγκαταστάτες, κατασκευαστές λογισμικού και διαπιστευμένοι φορείς ογκομέτρησης.

ΠΗΓΗ: [Υπουργείο Εθνικής Οικονομίας και Οικονομικών, 02.10.2026](#)

ACTION - ΤΙ ΝΑ ΕΛΕΓΞΕΤΕ ΓΙΑ ΤΙΣ ΝΕΕΣ ΠΡΟΘΕΣΜΙΕΣ:

- Έχει καταγραφεί ο τύπος, η χρήση και η περιοχή κάθε εγκατάστασης.
- Έχουν σημειωθεί χωριστά οι ημερομηνίες αναβάθμισης και απογραφής.
- Έχει συμφωνηθεί χρονοδιάγραμμα εργασιών με εγκαταστάτες και προμηθευτές.
- Τηρούνται στοιχεία δεξαμενών και αποδεικτικά ολοκλήρωσης.

ΕΡΩΤΗΣΗ ΓΙΑ ΤΗ ΔΙΟΙΚΗΣΗ:

- Γνωρίζουμε ποιες εγκαταστάσεις μας υπάγονται στις νέες προθεσμίες και έχουμε αναθέσει συγκεκριμένο υπεύθυνο και χρονοδιάγραμμα;

ΔΙΑΒΑΣΤΕ ΟΛΑ ΤΑ ΤΕΥΧΗ

Βοηθάμε οργανισμούς να διαχειρίζονται κανονιστικούς, ψηφιακούς και λειτουργικούς κινδύνους με εποπτεία.



Managing risk. Enabling growth.