Είστε έτοιμοι για τη DORA;

Νίκος Κοντιζάς και Γιάννης Κουτσουμπίνας

Τι είναι η DORA. Η «Πράξη για την Ψηφιακή Επιχειρησιακή Ανθεκτικότητα»[1] (Digital Operational Resilience Act – 'DORA') είναι Κανονισμός της ΕΕ και αποτελεί τη νέα, ολιστική κανονιστική προσέγγιση για την αντιμετώπιση των ψηφιακών κινδύνων και των κινδύνων στον κυβερνοχώρο σε ό,τι αφορά τον χρηματοπιστωτικό τομέα. Συνιστώντας ακρογωνιαίο λίθο της Δέσμης Μέτρων για τον Ψηφιακό Χρηματοοικονομικό Τομέα (Digital Finance Package), η DORA δημοσιεύθηκε στις 27 Δεκεμβρίου 2022 και τέθηκε σε ισχύ στις 16 Ιανουαρίου 2023. Η εφαρμογή της ξεκινά από τις 17 Ιανουαρίου 2025.

Στόχος και πεδίο εφαρμογής. Η DORA εστιάζει πρωτίστως στην εναρμόνιση των κανονιστικών απαιτήσεων για την διαχείριση ψηφιακών κινδύνων στον κλάδο των χρηματοοικονομικών υπηρεσιών. Θίγει την διάρθρωση των δομών διακυβέρνησης των υπόχρεων χρηματοοικονομικών οντοτήτων (financial entities—'FEs'), τις διαδικασίες αναφοράς στις αρμόδιες αρχές περιστατικών που σχετίζονται με τις τεχνολογίες πληροφοριών και επικοινωνιών (information and communication technology –'ICT'), τη διαχείριση κινδύνου σε σχέση με τρίτους παρόχους υπηρεσιών ICT και την ενισχυμένη εποπτεία των κρίσιμων παρόχων υπηρεσιών ICT.

Στο πεδίο εφαρμογής της DORA εμπίπτει μια ευρεία τυπολογία χρηματοοικονομικών οντοτήτων, που περιλαμβάνει, μεταξύ άλλων, πιστωτικά ιδρύματα, ιδρύματα πληρωμών, επιχειρήσεις επενδύσεων, οργανισμούς αξιολόγησης πιστοληπτικής ικανότητας και παρόχους υπηρεσιών κρυπτοστοιχείων.

Αναλογικότητα. Η DORA ενσωματώνει ρητά την αρχή της αναλογικότητας, σύμφωνα με την οποία η εφαρμογή της πρέπει να τελεί σε αναλογία με το μέγεθος, το συνολικό προφίλ κινδύνου κάθε χρηματοοικονομικής οντότητας και τη φύση, την κλίμακα και την πολυπλοκότητα των υπηρεσιών, των δραστηριοτήτων και των λειτουργιών της.

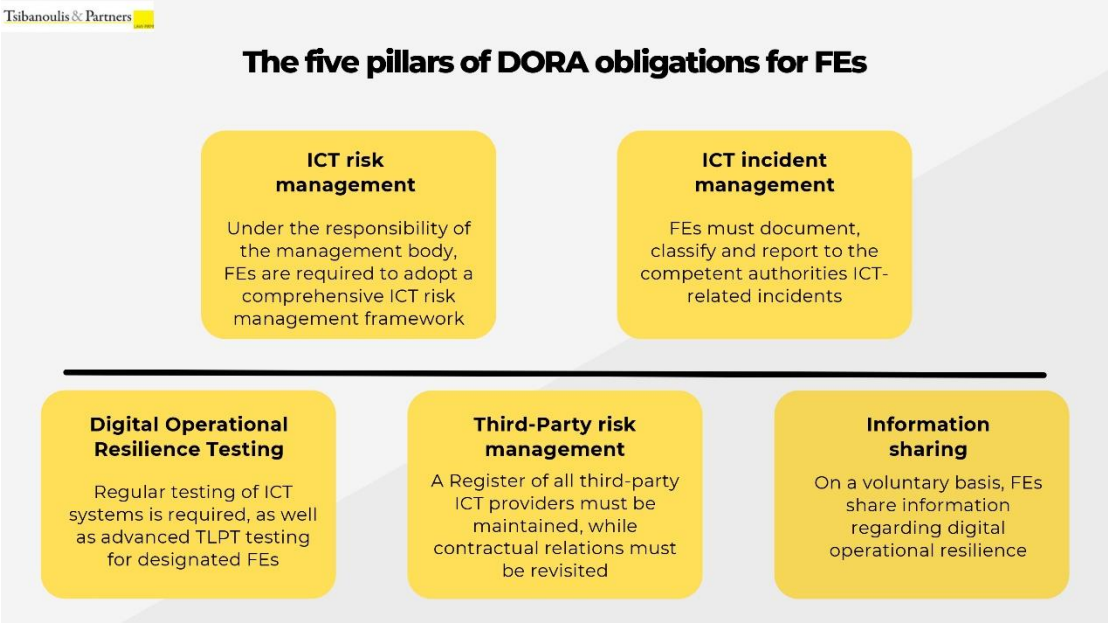
Εξωεδαφικότητα. Οι απαιτήσεις της DORA εφαρμόζονται σε όλες τις χρηματοοικονομικές οντότητες που αναπτύσσουν την δράση τους στον Ευρωπαϊκό Οικονομικό Χώρο (ΕΟΧ), ανεξαρτήτως του κράτους στο οποίο έχουν την έδρα τους ή έχουν συσταθεί. Παρομοίως,

[1] Κανονισμός (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 14ης Δεκεμβρίου 2022 σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014, (ΕΕ) αριθ. 909/2014 και (ΕΕ) 2016/1011.

τρίτοι πάροχοι υπηρεσιών ICT που βρίσκονται εκτός του ΕΟΧ καλύπτονται επίσης από τις απαιτήσεις εποπτείας της DORA.

Αλληλεπίδραση με την ισχύουσα νομοθεσία. Η DORA δεν είναι η πρώτη νομοθετική πράξη της ΕΕ που αφορά την ασφάλεια στον κυβερνοχώρο, αλλά αποτελεί προσθήκη στην υφιστάμενη νομοθεσία για την ασφάλεια δικτύων και πληροφοριών, η οποία τώρα διέπεται από την Οδηγία NIS 2[2]. Η DORA συνιστά *lex specialis* με αναφορά ειδικά στον χρηματοπιστωτικό τομέα, επομένως, σε κάθε πιθανή σύγκρουση μεταξύ των κανονιστικών πλαισίων, οι απαιτήσεις της DORA θα υπερισχύουν.

Πέντε Πυλώνες. Οι βασικοί πυλώνες της DORA μπορούν να διακριθούν σε πέντε αυτοτελείς κατηγορίες, όπως φαίνεται στο παρακάτω διάγραμμα.



Τεχνικά Πρότυπα. Δεδομένου του υψηλού βαθμού πολυπλοκότητας και του τεχνικού χαρακτήρα των απαιτήσεων που επιβάλλει η DORA στις χρηματοοικονομικές οντότητες, η Ευρωπαϊκή Επιτροπή εξουσιοδοτείται να εκδίδει ρυθμιστικά τεχνικά πρότυπα (Regulatory Technical Standards – 'RTS') και εκτελεστικά τεχνικά πρότυπα (Implementing Technical Standards – 'ITS') μέσω κατ' εξουσιοδότηση Κανονισμών, κατόπιν πρότασης από τις Ευρωπαϊκές Εποπτικές Αρχές (ΕΕΑ). Έως τον Σεπτέμβριο του 2024, η Ευρωπαϊκή Επιτροπή έχει εκδώσει τεχνικά πρότυπα για:

[2] Οδηγία (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 14ης Δεκεμβρίου 2022 σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, την τροποποίηση του κανονισμού (ΕΕ) αριθ. 910/2014 και της οδηγίας (ΕΕ) 2018/1972, και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148.

1. Τα κριτήρια για την ταξινόμηση των περιστατικών που σχετίζονται με ICT και τις απειλές στον κυβερνοχώρο, καθορίζοντας κατώτατα όρια σημαντικότητας και εξειδικεύοντας τις λεπτομέρειες των αναφορών μείζονων συμβάντων.
2. Το λεπτομερές περιεχόμενο της πολιτικής που αφορά τις συμβατικές ρυθμίσεις για την χρήση υπηρεσιών ICT, που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες και οι οποίες παρέχονται από τρίτους παρόχους υπηρεσιών ICT.
3. Τα εργαλεία διαχείρισης των κινδύνων ICT και τις συναφείς μεθόδους, διαδικασίες και πολιτικές και το απλουστευμένο πλαίσιο διαχείρισης κινδύνων ICT.

Οι ΕΕΑ έχουν επίσης υποβάλει τελικά σχέδια RTS και ITS με αντικείμενο, μεταξύ άλλων, τις απαιτήσεις για τις δοκιμές παρείσδυσης βάσει απειλών (threat-led penetration testing – "TLPT") και το Μητρώο Πληροφοριών τρίτων παρόχων ICT, τα οποία αναμένεται να εκδοθούν από την Επιτροπή. Συνολικά, οι ΕΕΑ έχουν δημοσιεύσει 8 RTS και 2 ITS.

Τι πρέπει να γίνει πριν τον Ιανουάριο. Από τις 17 Ιανουαρίου 2025, όλες οι χρηματοοικονομικές οντότητες που βρίσκονται εντός του πεδίου εφαρμογής πρέπει να συμμορφώνονται πλήρως με την DORA. Πρακτικά, αυτό σημαίνει ότι οι χρηματοοικονομικές οντότητες πρέπει να προβούν το συντομότερο δυνατό στα εξής βήματα:

- Να δημιουργήσουν ένα διεξοδικό πλαίσιο διαχείρισης κινδύνων ICT, το οποίο να περιέχει τον προσδιορισμό, την αξιολόγηση και τα μέτρα ελαχιστοποίησης των κινδύνων ICT και των ευπαθειών του συστήματος. Το πλαίσιο θα ορίζει τις σχετικές πολιτικές, τις δομές διακυβέρνησης, τα σχέδια απόκρισης σε περιστατικά, καθώς και τα μέτρα για την επιχειρησιακή συνέχεια.
- Να προετοιμαστούν για την αναφορά περιστατικών σχετιζόμενων με ICT στις αρμόδιες αρχές.
- Να προσαρμοστούν και να προετοιμαστούν για την εφαρμογή ενός προγράμματος δοκιμών (testing), αποτελούμενου τόσο από τακτικές μεθόδους δοκιμών, όπως είναι οι αξιολογήσεις ευπαθειών και οι αναλύσεις ελλείψεων, όσο και από προηγμένες δοκιμές που βασίζονται σε TLPT, κατά περίπτωση. Πρακτικά αυτό μπορεί να απαιτήσει τη συνεργασία με εταιρείες πληροφορικής, οι οποίες διαθέτουν την αναγκαία κατάρτιση και τα σχετικά λογισμικά για να πραγματοποιήσουν τους απαραίτητους ελέγχους.
- Να συστήσουν και να διατηρούν ενημερωμένο ένα Μητρώο Πληροφοριών αναφορικά με τρίτους παρόχους ICT, και να επανεξετάσουν και αναθεωρήσουν συμβατικές ρυθμίσεις με τους εν λόγω παρόχους.

Η ενεργός συμμετοχή του διοικητικού οργάνου, του τμήματος συμμόρφωσης (compliance unit) και του τμήματος IT των χρηματοοικονομικών οντοτήτων είναι απαραίτητη ώστε να

διασφαλιστεί η ομαλή μετάβαση στο νέο κανονιστικό περιβάλλον, ενώ θα πρέπει να διαμορφωθεί και μια νέα κουλτούρα επιχειρησιακής ανθεκτικότητας.

Συμπερασματικές παρατηρήσεις. Η DORA σηματοδοτεί μια καίρια ρυθμιστική καμπή με στόχο την ενδυνάμωση της ψηφιακής ανθεκτικότητας των χρηματοοικονομικών οντοτήτων. Καθώς η προθεσμία του Ιανουαρίου 2025 πλησιάζει, οι υπόχρεες εταιρείες θα πρέπει να λάβουν άμεση δράση για να ευθυγραμμίσουν την διαχείριση κινδύνων ICT, την εποπτεία των τρίτων παρόχων και το πλαίσια αναφοράς περιστατικών με τις απαιτήσεις της DORA. Η μη συμμόρφωση μπορεί να οδηγήσει σε σημαντική διακινδύνευση για τις υπόχρεες εταιρείες, τόσο από οικονομική άποψη, όσο και από άποψη φήμης.

Η DORA θα επιφέρει σημαντικές οικονομικές και οργανωτικές επιβαρύνσεις στις χρηματοοικονομικές οντότητες, λαμβάνοντας υπόψη και το ότι οι hackers είναι συχνά ένα βήμα πιο μπροστά από τα ρυθμιστικά πλαίσια και τις βέλτιστες πρακτικές. Οι υποχρεώσεις διαρκούς παρακολούθησης, δοκιμών και υποβολής αναφορών θα επηρεάσουν το προσωπικό και τους χρηματικούς πόρους των υπόχρεων χρηματοοικονομικών οντοτήτων, ιδίως των μικρότερων, καθώς θα αγωνίζονται να συμβαδίσουν με το εξελισσόμενο τοπίο απειλών και την αυξανόμενη πολυπλοκότητα των κανονιστικών απαιτήσεων.