SIGMA
PROFESSIONAL SERVICES ON RISK CHALLENGES ©

# Ψηφιακή Επιχειρησιακή Ανθεκτικότητα
# Ο Κανονισμός και ο δρόμος για την συμμόρφωση

DORA Regulation and the way to compliance

**Δρ. Σταμάτης Τουρνής** FBCI PMP CISA CRISC

ATHEX
Athens Stock Exchange

ATHEX Members Summit 2024

SIGMA BUSINESS NETWORK

VERSION 2.0

# Οι Κανονισμοί και ο DORA

SIGMA
PROFESSIONAL SERVICES ON RISK CHALLENGES ©

# Κανονισμός Ψηφιακής Λειτουργικής Ανθεκτικότητας (DORA)

**«Κανονισμός (ΕΕ) 2022/2554 σχετικά με την Ψηφιακή Επιχειρησιακή Ανθεκτικότητα του χρηματοπιστωτικού τομέα»**

DORA
DIGITAL OPERATIONAL RESILIENCE ACT

**Στόχος του Κανονισμού**

**Η διασφάλιση της ανθεκτικότητας της Αγοράς Χρηματοπιστωτικών Υπηρεσιών της ΕΕ** από τους **κινδύνους που σχετίζονται με τις Τεχνολογίες Πληροφορικής και Επικοινωνιών.**

Υλοποιείται μέσα από την **ενίσχυση της Ψηφιακής Ανθεκτικότητας των χρηματοπιστωτικών οντοτήτων, μεμονωμένα** και **σαν σύνολο**.

Από **17 Ιανουαρίου 2025** σε **όλη την Ευρωπαϊκή Ένωση**

# Ενιαίο Οικοσύστημα

**1. Τις Ευρωπαϊκές και Εθνικές Εποπτικές Αρχές**

**2. Το σύνολο των Χρηματοπιστωτικών Οντοτήτων**

- Πιστωτικά Ιδρύματα (Τράπεζες)
- Επενδυτικές Εταιρείες
- Ιδρύματα Πληρωμών
- Ιδρύματα Ηλεκτρονικού Χρήματος
- Ασφαλιστικές και Αντασφαλιστικές Εταιρείες
- Κεντρικοί Αντισυμβαλλόμενοι (CCPs)
- Χώροι Διαπραγμάτευσης (χρηματιστήρια)
- Πάροχοι Υπηρεσιών Κρυπτονομισμάτων
- Πάροχοι Υπηρεσιών Χρηματοδότησης Συγκέντρωσης Κεφαλαίων
- Εταιρείες Διαχείρισης Συλλογικών Επενδυτικών Σχημάτων
- Ταμεία Συντάξεων
- Πάροχοι Υπηρεσιών Αναφορών Δεδομένων
- Κεντρικά Αποθετήρια Τίτλων

**3. Τους παρόχους Υπηρεσιών Πληροφορικής και Επικοινωνιών (ICT) στις χρηματοπιστωτικές οντότητες**

# Οι απαιτήσεις του DORA σε 5 Πυλώνες

SIGMA
PROFESSIONAL SERVICES ON RISK CHALLENGES ©

# DORA – Οι κύριες απαιτήσεις

## 01
### Διαχείριση των Ψηφιακών Κινδύνων ΤΠΕ

- Πολιτικές & Πλαίσιο για τη διαχείριση κινδύνων ICT.
- Εναρμόνιση μεθόδων, εργαλείων διαδικασιών
- Διαχείριση Κινδύνων σε συνεχή βάση, παρακολούθηση και προσαρμογή
- Τεκμηρίωση

## 02
### Διαχείριση & Αναφορά Συμβάντων

- Διαχείριση συμβάντων
- Αναφορά μειζόνων συμβάντων και σημαντικών κυβερνοαπειλών
- Ταξινόμηση & κριτήρια
- Ανακοίνωση σε 4 – 24 ώρες, αναφορά σε 72 ώρες, αναφορά σε 1 μήνα

## 03
### Δοκιμές Ψηφιακής Επιχειρησιακής Ανθεκτικότητας

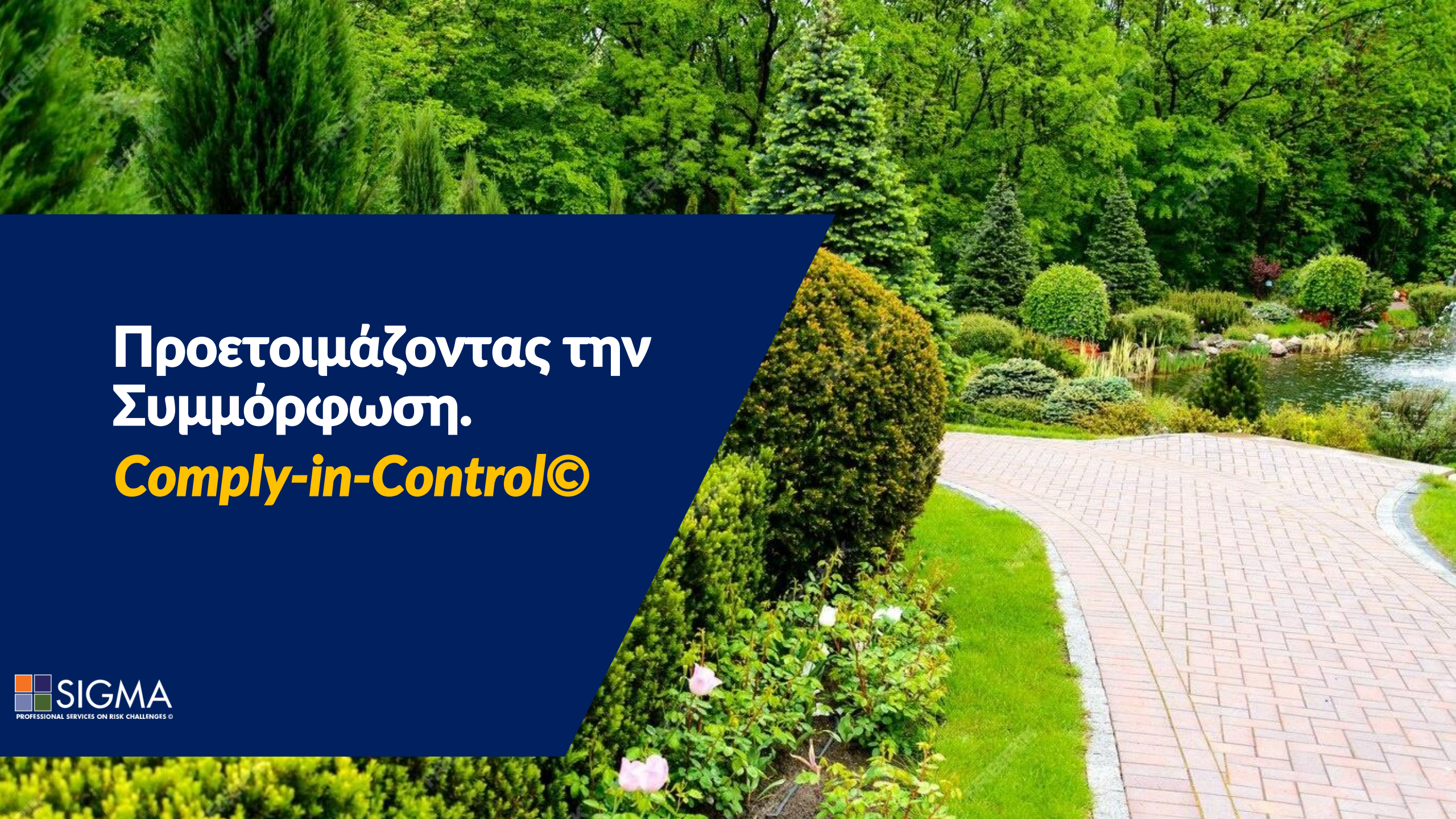
- Πολιτικές & Πλαίσιο για τη διαχείριση κινδύνων ICT.
- Δοκιμές εργαλείων και συστημάτων ΤΠΕ
- Προηγμένες δοκιμές διείσδυσης βάσει απειλών (TLPT, RTTP)
- Βελτιώσεις της ασφάλειας βάσει των αποτελεσμάτων

## 04
### Διαχείριση Κινδύνων Τρίτων Μερών

- Πολιτικές & Πλαίσιο
- Προκαταρκτική αξιολόγηση κινδύνων, συγκέντρωσης και υποαναθέσεων
- Κρίσιμοι πάροχοι
- Όροι συμβάσεων
- Μητρώο τρίτων μερών
- Περιοδική επαναξιολόγηση κινδύνων

## 05
### Επικοινωνία και Συνεργασία

- Συνεργασία και ανταλλαγή πληροφοριών πάνω σε κινδύνους και απειλές, τεχνικές κά
- Συμμετοχή σε ομάδες και forum
- Επικοινωνία με τις Εθνικές Αρχές



# Προετοιμάζοντας την Συμμόρφωση.

## *Comply-in-Control©*

SIGMA
PROFESSIONAL SERVICES ON RISK CHALLENGES ©

# Με την Μεθοδολογία μας ***Comply-in-Control© (*)*** σε 8 βήματα

**1 Ανάλυση Αποκλίσεων (Gap Analysis)**

- Εντοπισμός αποκλίσεων στις τρέχουσες πρακτικές διαχείρισης ICT κινδύνων.
- Χρονοδιάγραμμα & οδικός χάρτης Συμμόρφωσης

**2 Καθιέρωση / Βελτίωση Δομής Διακυβέρνησης**

- Οργανωτικό και διοικητικό πλαίσιο για τη διαχείριση της Ανθεκτικότητας και την συμμόρφωση.
- Ορισμός ρόλων και αρμοδιοτήτων

**3 Ανάπτυξη / Βελτίωση Πλαισίου Διαχείρισης Κινδύνων ICT**

- Βελτίωση /Δημιουργία και εφαρμογή πολιτικών & διαδικασιών για αναγνώριση, αξιολόγηση και μείωση των κινδύνων.
- Αρχιτεκτονική για την Ασφάλεια
- Συμμόρφωση / αναβάθμιση υποδομών ICT

**4 Οργάνωση Διαχείρισης Περιστατικών - Διαχείριση Αναφορών**

- Δημιουργία / Βελτίωση πολιτικών & διαδικασιών για την ανίχνευση, απόκριση και διαχείριση περιστατικών
- Ανάπτυξη διαδικασιών και προετοιμασία για την αναφορά περιστατικών στις ρυθμιστικές αρχές

**5 Σχεδιασμός Επιχειρησιακής Συνέχειας & Οργάνωση Δοκιμών**

- Ανάπτυξη / βελτίωση Σχεδίων Επιχειρησιακής Συνέχειας & υλοποίηση απαιτούμενων λύσεων
- Κατάρτιση σχεδίου δοκιμών & δοκιμών διείσδυσης αν χρειάζεται

**6 Πλαίσιο Διαχείρισης Κινδύνων από Τρίτους Παρόχους**

- Σχετικές Πολιτικές και διαδικασίες
- Αξιολόγηση τρίτων παρόχων
- Διαχείριση της συμμόρφωσης τους

**7 Τεκμηρίωση και Τήρηση Αρχείων & Εσωτερικών Αναφορών**

- Βελτίωση / Δημιουργία σχετικών πολιτικών & διαδικασιών

**8 Εκπαίδευση και Ευαισθητοποίηση Συνεχής Παρακολούθηση**

- Εκπαίδευση του προσωπικού
- Οργάνωση & λειτουργία δομών συνεχούς παρακολούθησης ICT περιβάλλοντος.
- Βελτίωση συστήματος βάσει αναφορών

SIGMA (*)
PROFESSIONAL SERVICES ON RISK CHALLENGES ©

# Προκλήσεις και σημεία προσοχής

SIGMA
PROFESSIONAL SERVICES ON RISK CHALLENGES ©

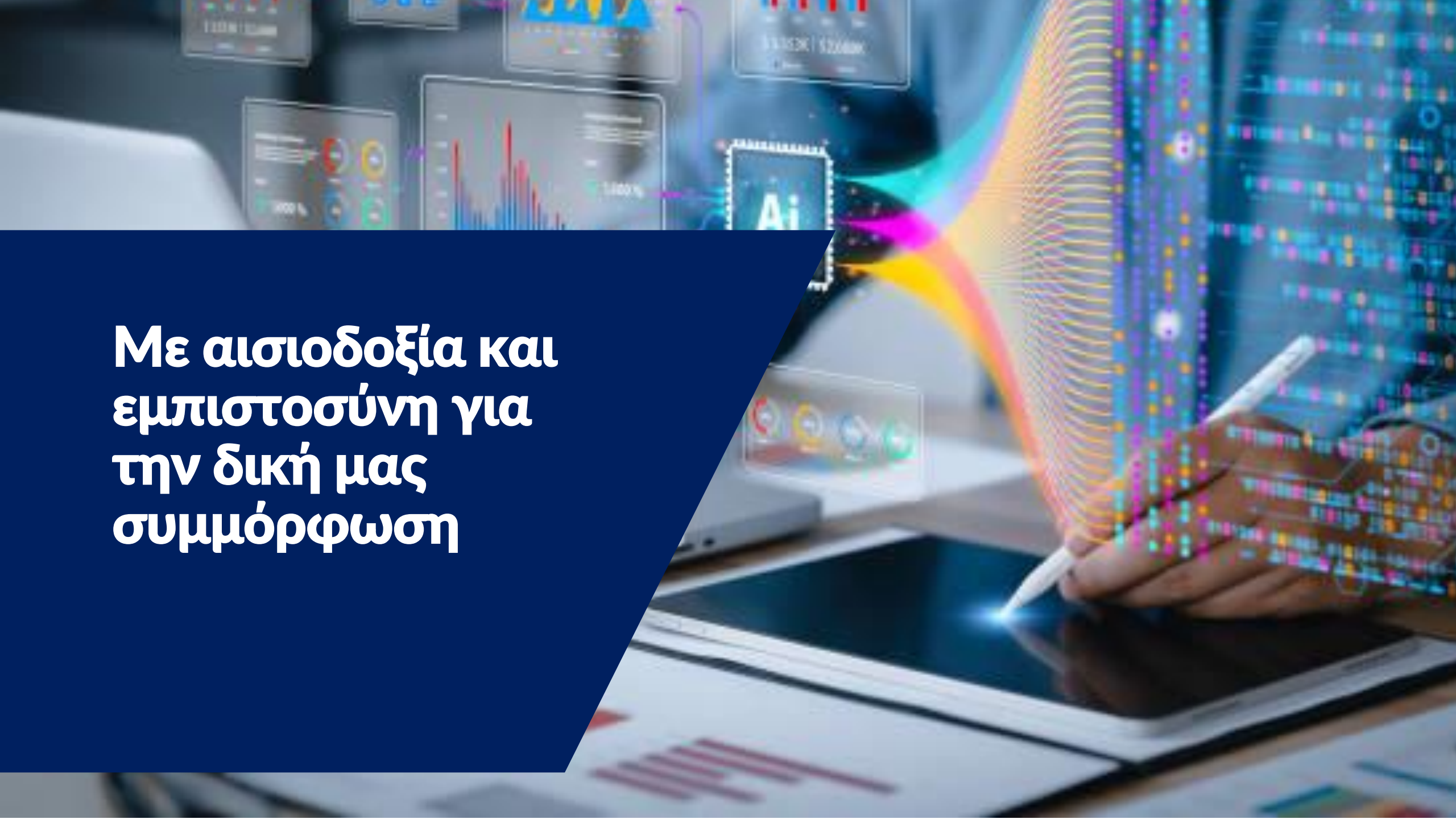
# Ενδεικτικές Προκλήσεις για την συμμόρφωση

1. Νέες επενδύσεις
2. Εκπαίδευση προσωπικού / Εξειδίκευση / Συμμετοχή
3. Παρακολούθηση εταιρικής λειτουργίας σε πραγματικό χρόνο
4. Ανάγκη για τακτικούς ελέγχους - Συνεχής αξιολόγηση της έκθεσης σε κίνδυνο & των μέτρων
5. Αυξημένες ανάγκες «διαχείρισης & τεκμηρίωσης του όλου συστήματος
6. Διαχείριση & «παρακολούθηση» των προμηθευτών ICT

Η Έμφαση είναι στην **ΔΕΣΜΕΥΣΗ** και στον **ΣΧΕΔΙΑΣΜΟ**

# «Ενημερώθηκα»

1. Κατανοώ ότι είμαι μέρος ενός Οικοσυστήματος που **ΔΕΝ με ξεχνά.**
2. Κατανοώ ότι το «Σύστημα συμμόρφωσης με τον Κανονισμό» που θα υλοποιηθεί,
   **είναι αναπόσπαστο μέρος της καθημερινής λειτουργίας** της εταιρείας
   θα είναι σε πλήρη **αρμονία με λοιπά συστήματα** διαχείρισης και συμμόρφωσης
3. Δεν υποτιμώ τους ICT κινδύνους
4. Συμβάντα: (α) Αξιολογώ και (β) **Αναφέρω** - **ΔΕΝ ΚΡΥΒΩ – Δεν Αμελώ να αναφέρω**
5. Κατανοώ ότι **μπορεί να επιβληθούν αυστηρές Ποινές** για την μη συμμόρφωση, την μη αναφορά συμβάντων κά



# Με αισιοδοξία και εμπιστοσύνη για την δική μας συμμόρφωση

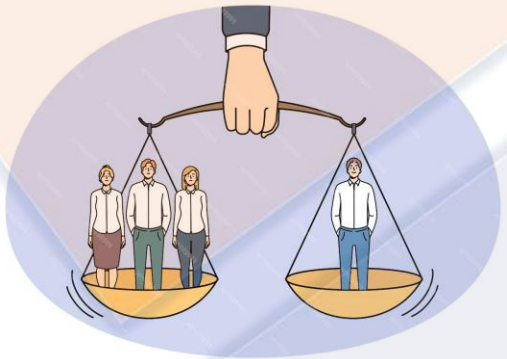
# 1. Δεν είμαστε όλοι το ίδιο

SIGMA
PROFESSIONAL SERVICES ON RISK CHALLENGES ©

# Αρχή της Αναλογικότητας

## Δεν είμαστε όλοι το ίδιο

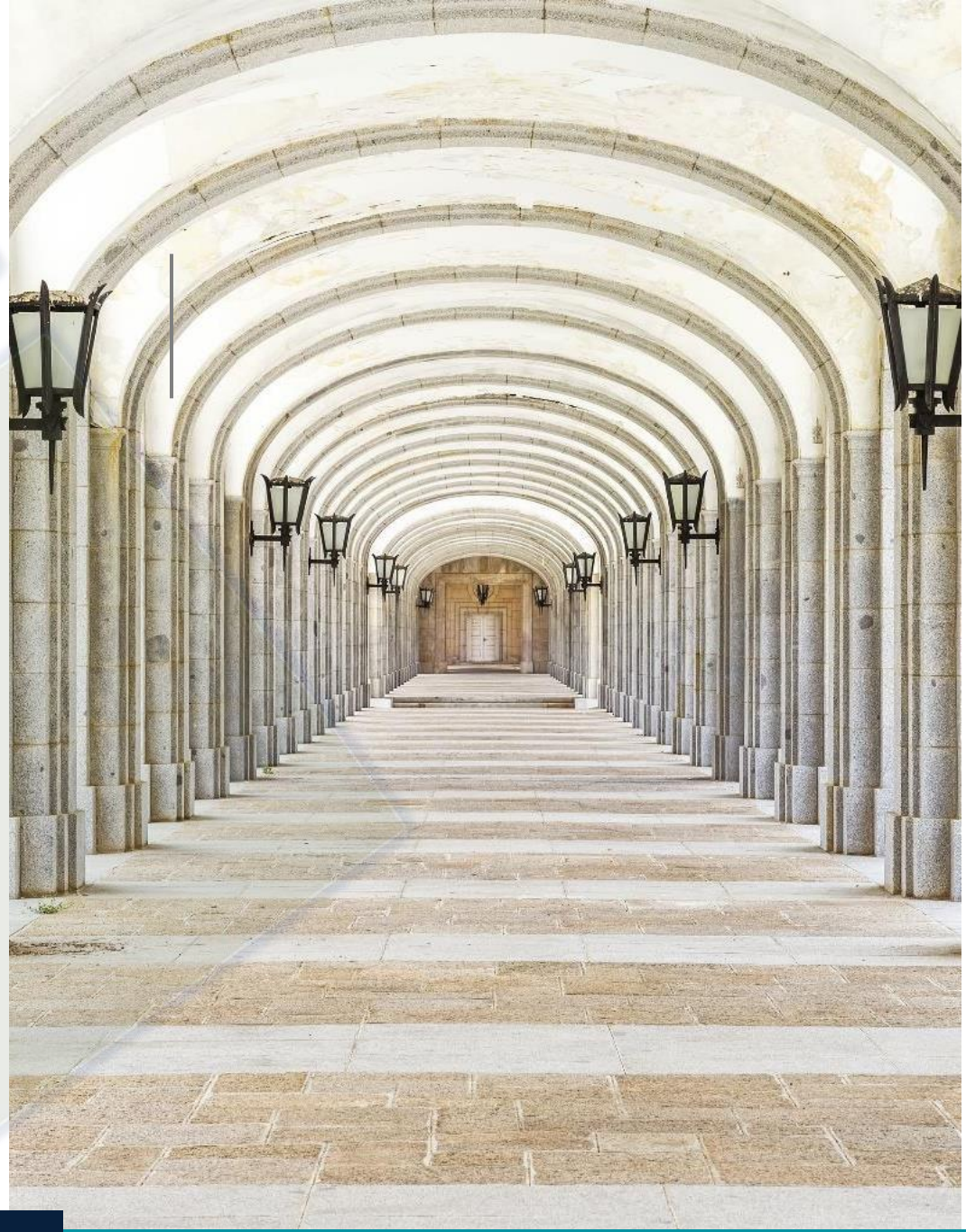
- Πιστωτικά Ιδρύματα (Τράπεζες)
- Επενδυτικές Εταιρείες
- Ιδρύματα Πληρωμών
- Ιδρύματα Ηλεκτρονικού Χρήματος
- Ασφαλιστικές και Αντασφαλιστικές Εταιρείες
- Κεντρικοί Αντισυμβαλλόμενοι (CCPs)
- Χώροι Διαπραγμάτευσης (χρηματιστήρια)
- Πάροχοι Υπηρεσιών Κρυπτονομισμάτων
- Πάροχοι Υπηρεσιών Χρηματοδότησης Συγκέντρωσης Κεφαλαίων
- Εταιρείες Διαχείρισης Συλλογικών Επενδυτικών Σχημάτων
- Ταμεία Συντάξεων
- Πάροχοι Υπηρεσιών Αναφορών Δεδομένων
- Κεντρικά Αποθετήρια Τίτλων



## Η έκταση και η ένταση της συμμόρφωσης λαμβάνει υπόψη

- το μέγεθος
- το συνολικό προφίλ κινδύνου
- την φύση
- την κλίμακα και την πολυπλοκότητα των υπηρεσιών, δραστηριοτήτων & λειτουργιών των οργανισμών

| | Κατηγορίες | | |
|---|---|---|---|
| Κριτήριο | Πολύ Μικρή | Μικρή | Μεσαία |
| Άτομα | < 10 | 10 - 50 | 250 < |
| Ετήσιος κύκλος εργασιών | < 2 M€ | 2 - 10 M€ | < 50 M€ |
| Ετήσιο σύνολο ισολογισμού | < 2 M€ | 2 – 10 M€ | < 43 M€ |

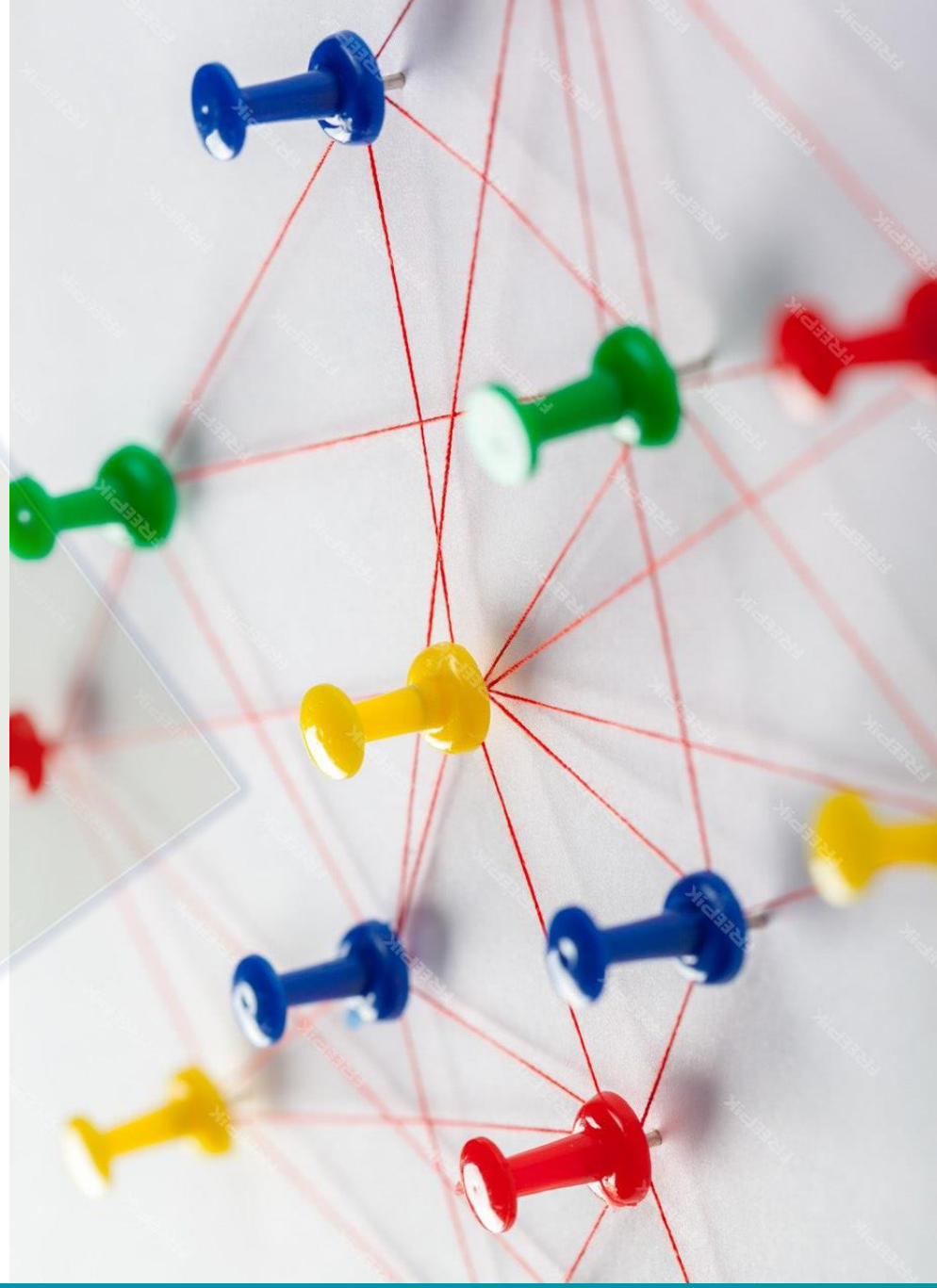


# 2. Με Κοινή λογική

SIGMA
PROFESSIONAL SERVICES ON RISK CHALLENGES ©

# Με κοινή λογική

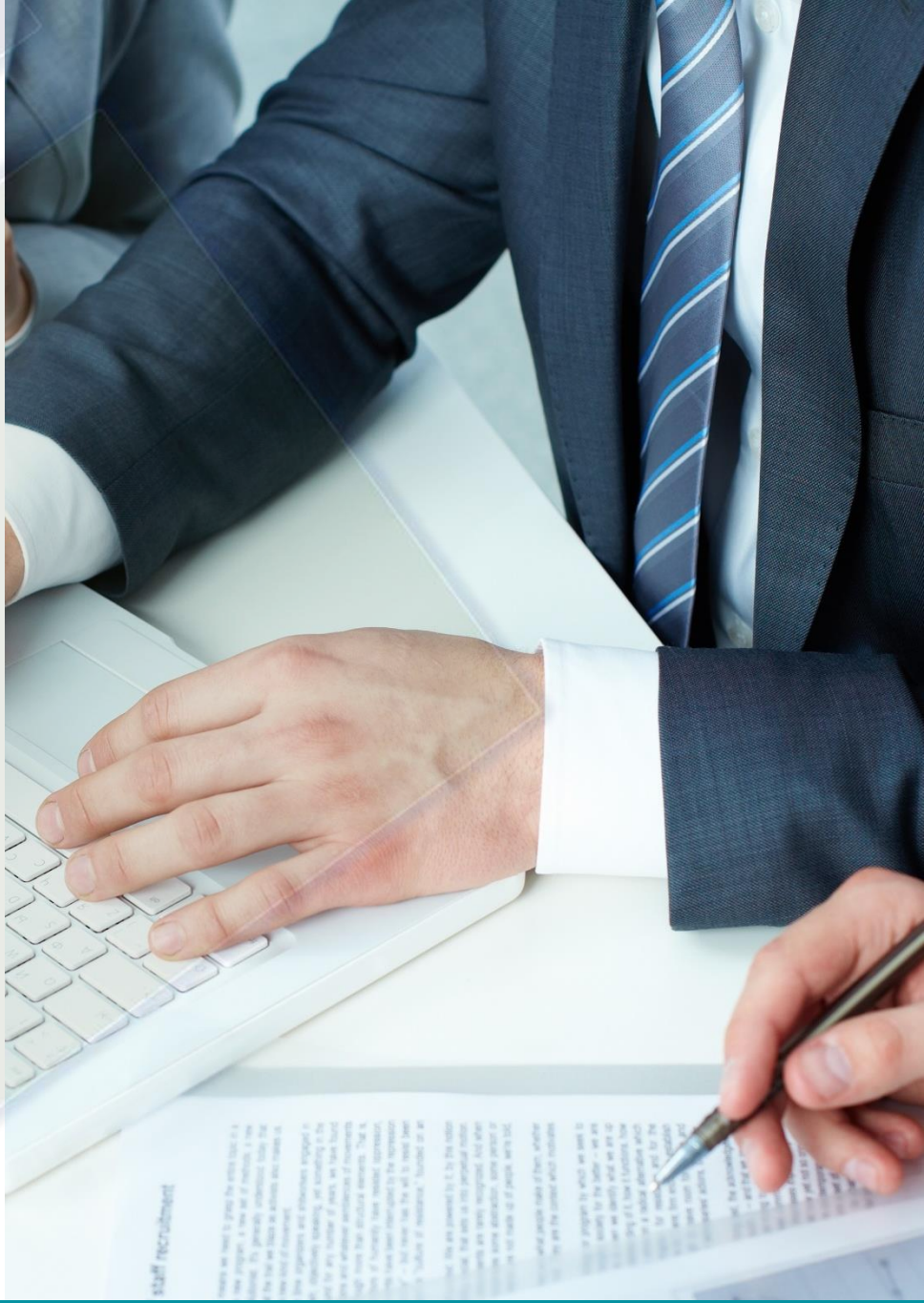
1. **Ξεκινήστε άμεσα**. Δεν υπάρχει χρόνος, ούτε πιθανότητες αναβολής. Ούτε πανικός όμως.
2. **Εκμεταλλευτείτε τις συνέργειες του οικοσυστήματός σας** για να λύσετε, άμεσα και με ασφάλεια, σύνθετες και σημαντικές απαιτήσεις (**ATHEX** !!!!)
3. Εκμεταλλευτείτε διεθνή πρότυπα και συγγενή συστήματα, «**έτοιμη» γνώση, μεθοδολογίες**, και δοκιμασμένη εμπειρία
4. **Για σύνθετα έργα** σαν αυτό, εστιαζόμαστε στην απάντηση σε γνωστό ερώτημα

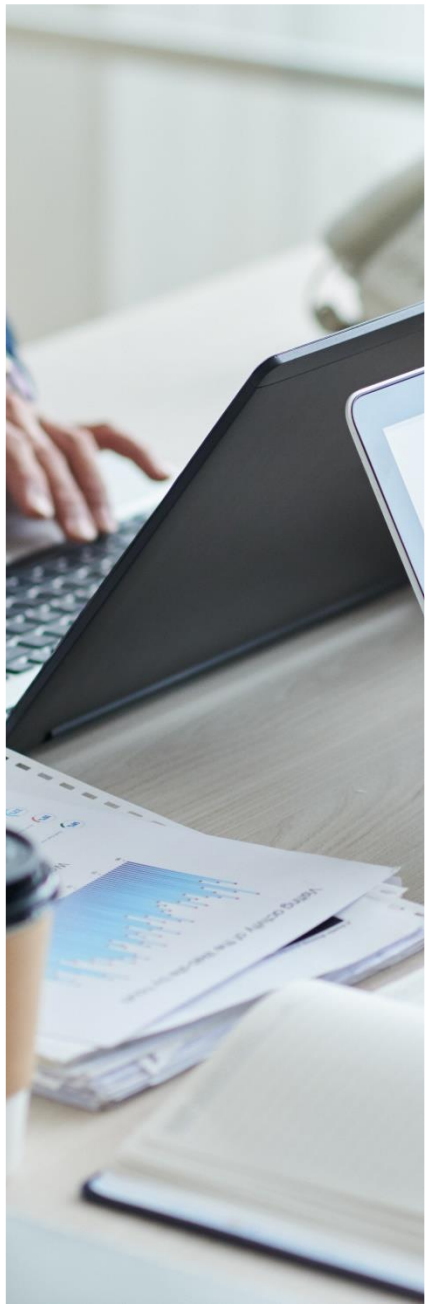


# Πως η SIGMA μπορεί να σας βοηθήσει

# Πως η SIGMA μπορεί να σας βοηθήσει

1. Εφαρμόζουμε **την Μεθοδολογία μας *Comply-in-Control©* για την υλοποίηση** του όλου έργου της Συμμόρφωσης με το DORA
2. Χρησιμοποιούμε **πιστοποιημένους ειδικούς** στην Ασφάλειας Πληροφοριών, την Επιχειρησιακή Ανθεκτικότητα, την εταιρική Διακυβέρνηση και Συμμόρφωση κά
3. **Βασιζόμαστε στην εμπειρία μας** σε μεγάλους και μικρούς πελάτες στους σχετικούς τομείς σε πολλές χώρες.
4. **Χρησιμοποιούμε τις δοκιμασμένες γνώσεις και μεθοδολογίες** της ομάδας μας από τα βραβευμένα Ευρωπαϊκά Ερευνητικά Έργα για SMEsστους τομείς Διακυβέρνησης, Διαχείρισης Κινδύνων, Ανθεκτικότητας και Κανονιστικής Συμμόρφωσης
5. **Υλοποιούμε** τις κορυφαίες παγκόσμια SaaS λύσεις και εργαλεία στα θέματα GRC για το συμφέρον των πελατών μας





SIGMA

## ΚΥΡΙΕΣ ΠΕΡΙΟΧΕΣ, ΥΠΗΡΕΣΙΕΣ ΚΑΙ ΛΥΣΕΙΣ

Η SIGMA είναι μια εξειδικευμένη Εταιρεία Συμβούλων που παρέχει Συμβουλευτικές Υπηρεσίες στη Διοίκηση σε κρίσιμους Επιχειρησιακούς και Λειτουργικούς τομείς των επιχειρήσεων όπως ενδεικτικά οι παρακάτω

- **Εταιρική Διακυβέρνηση, Διαχείριση Κινδύνων** και **Κανονιστική Συμμόρφωση**
- **Επιχειρησιακή & Λειτουργική Ανθεκτικότητα**
  - Στρατηγική
  - Επιχειρησιακή Συνέχεια
  - Διαχείριση Συμβάντων και Κρίσεων
  - Φυσική και Λογική Ασφάλεια
  - Ασφάλεια Πληροφοριών
  - Cyber Security
  - GDPR & Προσωπικά Δεδομένα
  - Διαχείριση Εκτάκτων Καταστάσεων
  - Ασκήσεις και Δοκιμές
- **Διαχείριση Λειτουργικών Κινδύνων**
- **Συστήματα Διαχείρισης**
  - Ποιότητας
  - Ασφάλειας Πληροφοριών
  - Επιχειρησιακής Συνέχειας
  - Ενέργειας & Περιβάλλοντος
  - Ασφάλειας Τροφίμων
  - Νοσοκομείων
  - Ασφάλειας & Υγείας

  κά
- **Εξειδικευμένες λύσεις (SaaS)**
- **Εκπαιδευτικές Υπηρεσίες**
- **Διαχείριση Έργων**
- **Συμμετοχή σε Ερευνητικά έργα**

## ΕΝΔΕΙΚΤΙΚΟΙ ΠΕΛΑΤΕΣ ΜΑΣ

SIGMA

PROFESSIONAL SERVICES ON RISK CHALLENGES ©

# Transforming Risk Into Value

REVENUE ~ MARKET SHARE AND SHAREHOLDER VALUE

## Ευχαριστούμε


+30 210 2526 321

info@thesigmanet.com

www.thesigmanet.com


SIGMA BUSINESS NETWORK