encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

Το Πρότυπο PCI DSS και το Έργο Συμμόρφωσης Εμπορικών Επιχειρήσεων

Κωνσταντίνος Παπαδάτος
Εμπορικός Διευθυντής ENCODE

15 Σεπτεμβρίου 2009

Ατζέντα

- Το Προφίλ της ENCODE
- Το Πρότυπο PCI DSS
- Μεθοδολογία / Φάσεις Έργου
- Συμμετοχή Εμπορικών Επιχειρήσεων
- Οφέλη Συμμόρφωσης

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

ENCODE

Η ENCODE, αποτελεί τη μεγαλύτερη & πλέον εξειδικευμένη στην Ελλάδα εταιρεία, με **αποκλειστικό αντικείμενο** την παροχή υπηρεσιών ασφαλείας και διαχείρισης κινδύνου πληροφοριών.

- **Ίδρυση**: Απρίλιος 2001
- **Έδρα** : Αθήνα
- **Θυγατρικές**: ENCODE Middle East: Dubai, Ηνωμένα Αραβικά Εμιράτα
- **Παραρτήματα**: ENCODE UK: Λονδίνο, Αγγλία
- **Περιοχές παροχής υπηρεσιών**: Δυτική & ΝΑ Ευρώπη, Μέση Ανατολή, Βαλκάνια και ΗΠΑ
- **Στελέχωση**: Περισσότερους από 30 ειδικούς στην Ασφάλεια Πληροφοριών

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

Πιστοποιητικά

- ISO 9001:2000
- ISO 27001/BS7799
- PCI QSA & ASV
- CISSP/CISM/CISA…

encode
Information Risk Management

Οι Πελάτες μας

- **Περισσότερες από 25 μεγάλες Τράπεζες**
  - 6 μεγαλύτερες τράπεζες στην Ελλάδα,
  - 8 από τις μεγαλύτερες τράπεζες της Μέσης Ανατολής
- **10 μεγάλοι τηλεπικοινωνιακοί οργανισμοί**
  - 4 μεγάλοι τηλεπικοινωνιακοί οργανισμοί στην Ελλάδα
  - 5 από τους μεγαλύτερους τηλεπικοινωνιακούς οργανισμούς της Μέσης Ανατολής
- **Πάνω από 80 μεγάλοι πελάτες ανά τον κόσμο**
  - Η μεγαλύτερη πετρελαϊκή εταιρία της Μέσης Ανατολής
  - Η μεγαλύτερη μη-πετρελαϊκή κατασκευαστική εταιρία της Μέσης Ανατολής
  - Η δεύτερη παγκοσμίως μεγαλύτερη εταιρεία ολοκληρωμένων συστημάτων τυχερών παιχνιδιών & διαχείρισης συναλλαγών
  - Μεγάλοι Δημόσιοι Οργανισμοί & Υπηρεσίες στην Ελλάδα και τη Μέση Ανατολή

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

Ατζέντα

- Το Προφίλ της ENCODE
- Το Πρότυπο PCI DSS
- Μεθοδολογία / Φάσεις Έργου
- Συμμετοχή Εμπορικών Επιχειρήσεων
- Οφέλη Συμμόρφωσης

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

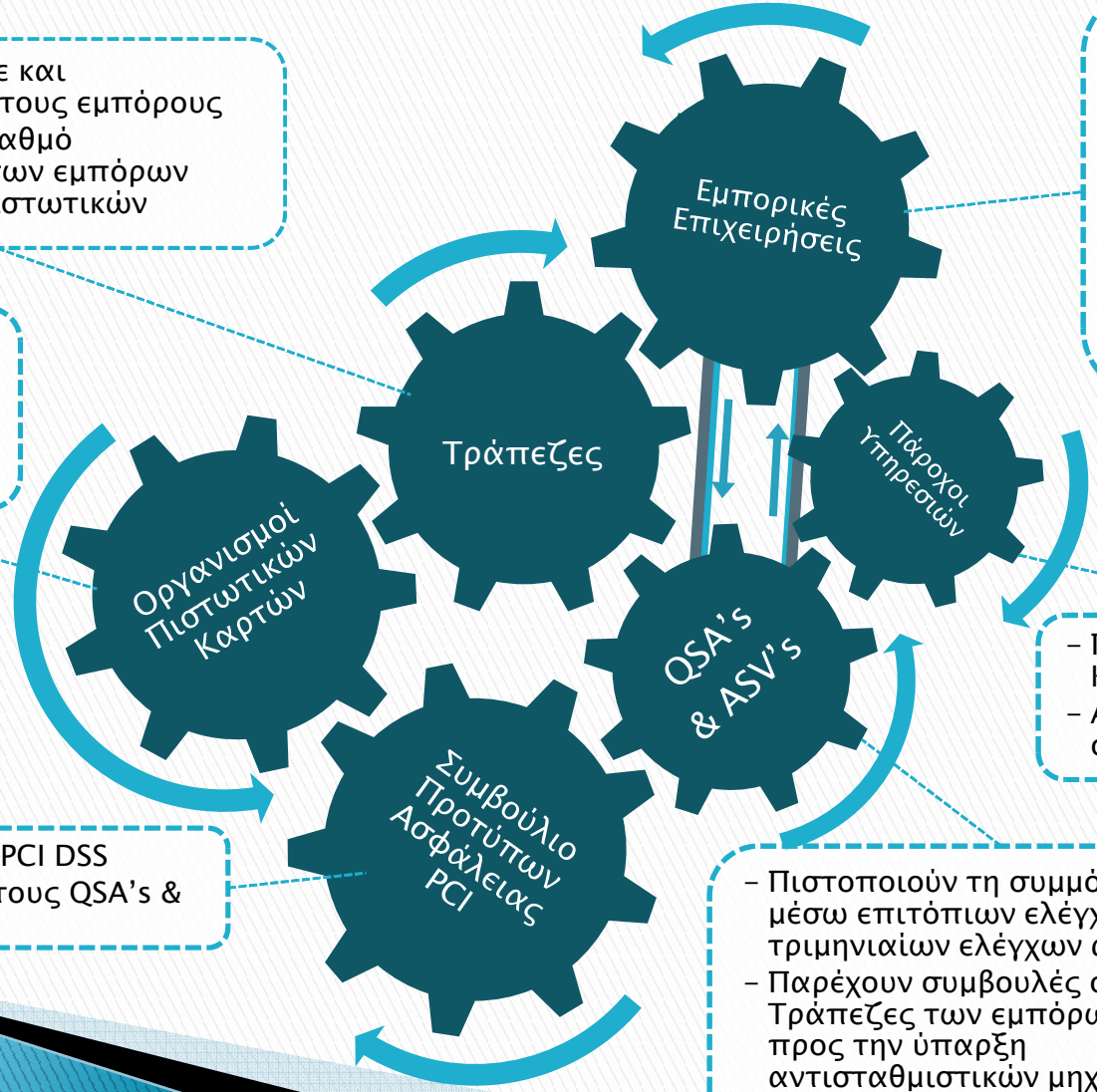
Κανονιστική Απαίτηση ή Πρότυπο;

- Το PCI DSS αποτελεί συμβατική υποχρέωση μεταξύ και των εμπορικών επιχειρήσεων και των Τραπεζών
- Αφορά σε όλες τις οντότητες που αποθηκεύουν, επεξεργάζονται ή μεταδίδουν δεδομένα κατόχων καρτών πληρωμής καθώς και σε όλα τα κανάλια πληρωμών (ταχυδρομείο, τηλέφωνο, e-commerce / Internet)
- Καλύπτει τεχνικά και λειτουργικά τμήματα των συστημάτων που περιλαμβάνονται ή συνδέονται με τα δεδομένα των καρτούχων
- Μια εμπορική επιχείρηση που δέχεται ή επεξεργάζεται κάρτες πληρωμών, πρέπει να συμμορφωθεί με τις απαιτήσεις του Προτύπου Ασφάλειας Δεδομένων PCI
- Μη συμμόρφωση μπορεί να οδηγήσει σε πρόστιμα και ενδεχομένως στην απώλεια του δικαιώματος αποδοχής συναλλαγών με κάρτες πληρωμών

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

Εμπλεκόμενα Μέρη



- Επικοινωνούν με και συμμορφώνουν τους εμπόρους
- Αναφέρουν το βαθμό συμμόρφωσης των εμπόρων στις εταιρίες πιστωτικών καρτών

- Επιβάλλουν το PCI DSS
- Προωθούν την υιοθέτησή του (π.χ. μέσω προστίμων)

- Απαιτείται να συμμορφώνονται με το PCI
- Προστατεύουν τα δεδομένα καρτούχων
- Χρησιμοποιούν συμμορφωμένους με το PCI παρόχους υπηρεσιών

- Προστατεύουν τα Δεδομένα Καρτούχων
- Απαιτείται να συμμορφώνονται με το PCI

- Συντηρεί το PCI DSS
- Πιστοποιεί τους QSA's & ASV's

- Πιστοποιούν τη συμμόρφωση μέσω επιτόπιων ελέγχων & τριμηνιαίων ελέγχων αδυναμιών
- Παρέχουν συμβουλές στις Τράπεζες των εμπόρων ως προς την ύπαρξη αντισταθμιστικών μηχανισμών ασφάλειας

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

Σύνοψη Προτύπου PCI DSS

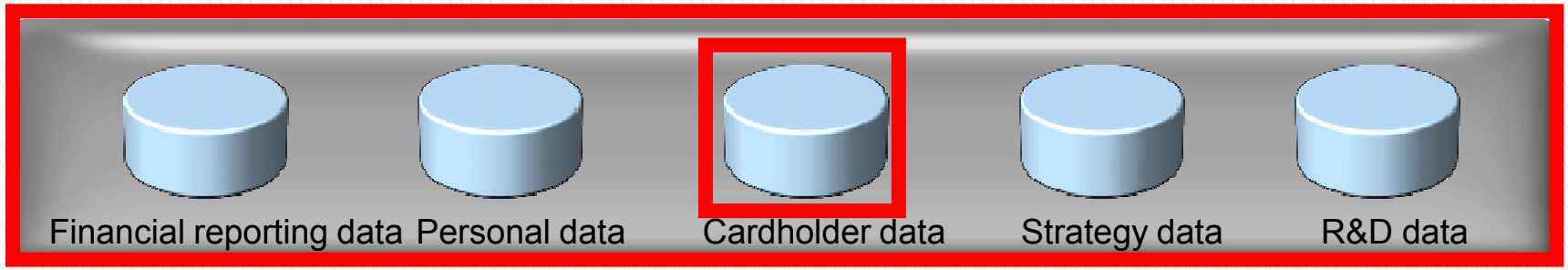
- Εγκατάσταση και Συντήρηση Ασφαλούς Δικτύου
- Προστασία Δεδομένων Καρτούχων
- Συντήρηση Προγράμματος Διαχείρισης Αδυναμιών Ασφάλειας
- Υλοποίηση Ισχυρών Μέτρων Ελέγχου Πρόσβασης
- Περιοδική Παρακολούθηση και Έλεγχος Δικτύων
- Τήρηση Πολιτικής Ασφάλειας Πληροφοριών

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

Απαιτήσεις Μηχανισμών Ασφάλειας

- Το πρότυπο καλύπτει ευρύ φάσμα μηχανισμών ασφάλειας:
  - Διοικητικούς Μηχανισμούς (πολιτικές και διαδικασίες),
  - Τεχνολογικούς Μηχανισμούς (passwords, κρυπτογράφηση δεδομένων),
  - Μηχανισμούς Φυσικής Ασφάλειας

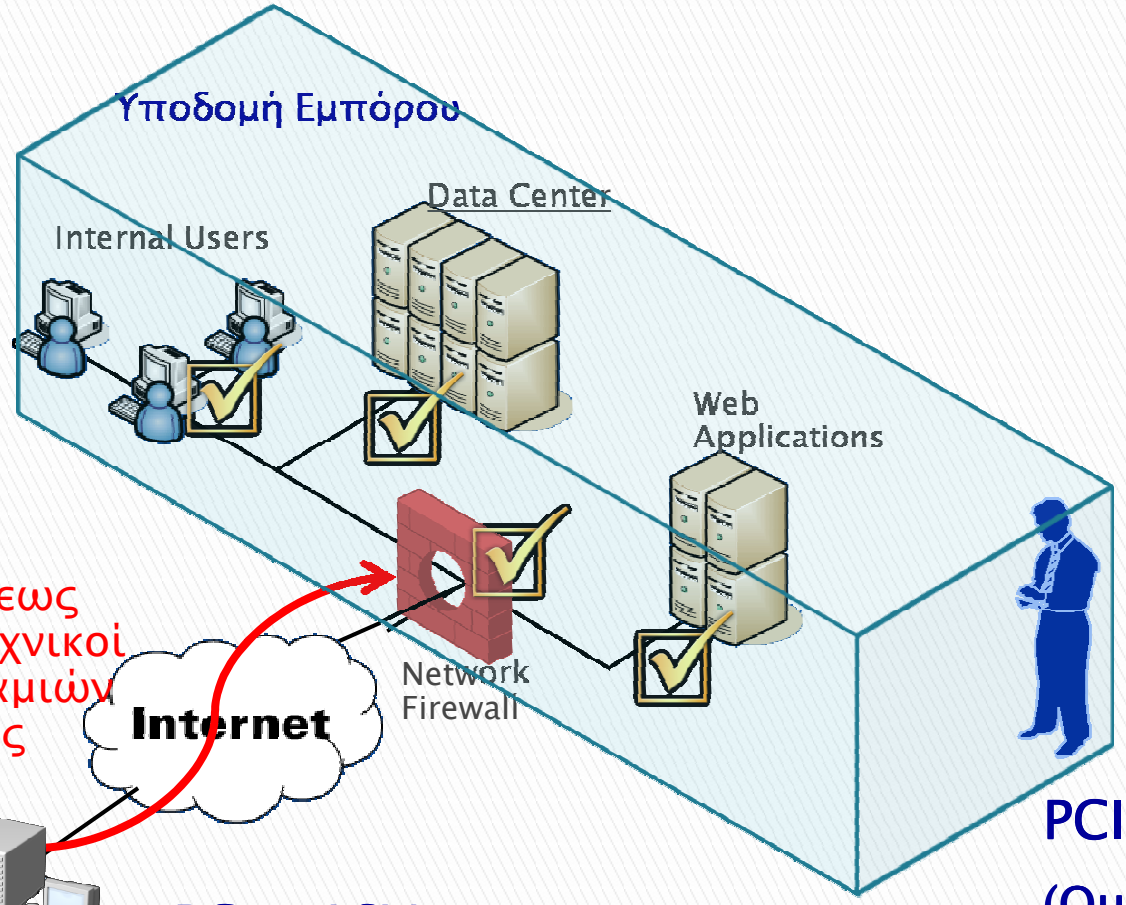


Παρότι το πρότυπο εστιάζει σε δεδομένα πιστωτικών καρτών, η υλοποίηση των εν λόγω μηχανισμών προστασίας μπορεί να αυξήσει σημαντικά **το συνολικό επίπεδο ασφάλειας μιας επιχείρησης!**

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

Αποδεκτές Μέθοδοι Επικύρωσης Συμμόρφωσης από PCI



1

Εξ Αποστάσεως Τριμηνιαίοι Τεχνικοί Έλεγχοι Αδυναμιών Ασφάλειας

PCI – ASV

(Approved Scanning Vendor)

2

Ετήσιος Επιτόπιος Έλεγχος Συμμόρφωσης

(ή Αυτό-αξιολόγηση)

PCI – QSA

(Qualified Security Assessor)

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

Επίπεδα Εμπορικών Επιχειρήσεων & Επικύρωση Συμμόρφωσης

Επίπεδο	Περιγραφή	Επικύρωση Συμμόρφωσης
1	▪ Επιχειρήσεις, ανεξαρτήτως καναλιού πληρωμών, με περισσότερες από **6.000.000 VISA/MasterCard ή 2.500.000 AMEX** συναλλαγές το χρόνο. ▪ **Επιχειρήσεις οι οποίες έχουν υποστεί διαρροή δεδομένων** καρτών. ▪ Εμπορικές επιχειρήσεις οι οποίες κατηγοριοποιούνται κατά την κρίση οποιασδήποτε εταιρίας πιστωτικών καρτών ως Επιπέδου 1.	▪ Ετήσιος Επιτόπιος Έλεγχος Συμμόρφωσης από Πιστοποιημένο Αξιολογητή Ασφάλειας [**Qualified Security Assessor (QSA) Audit**] ▪ Τριμηνιαίοι Τεχνικοί Έλεγχοι Αδυναμιών Ασφάλειας από Πιστοποιημένο **ASV (Approved Scanning Vendor)**
2	▪ Επιχειρήσεις, ανεξαρτήτως καναλιού πληρωμών, με **1.000.000 έως 6.000.000 VISA/MasterCard ή 50.000 έως 2.500.000 AMEX** συναλλαγές το χρόνο.	▪ Συμπλήρωση Ερωτηματολογίου Αυτό-Αξιολόγησης PCI DSS Ετησίως ▪ Τριμηνιαίοι Τεχνικοί Έλεγχοι Αδυναμιών Ασφάλειας από Πιστοποιημένο ASV
3	▪ Επιχειρήσεις με **20.000 έως 1.000.000 VISA/MasterCard** συναλλαγές μέσω καναλιών **ηλεκτρονικού εμπορίου** το χρόνο. ▪ Επιχειρήσεις, ανεξαρτήτως καναλιού πληρωμών, με **λιγότερες από 50.000 AMEX** συναλλαγές το χρόνο.	▪ Συμπλήρωση Ερωτηματολογίου Αυτό-Αξιολόγησης PCI DSS Ετησίως ▪ Τριμηνιαίοι Τεχνικοί Έλεγχοι Αδυναμιών Ασφάλειας από Πιστοποιημένο ASV
4	▪ Επιχειρήσεις με **λιγότερες από 20.000 VISA/MasterCard** συναλλαγές μέσω καναλιών **ηλεκτρονικού εμπορίου** το χρόνο. ▪ Επιχειρήσεις, ανεξαρτήτως καναλιού πληρωμών, με **λιγότερες από 1.000.000 VISA/MasterCard** συναλλαγές το χρόνο.	▪ Συμπλήρωση Ερωτηματολογίου Αυτό-Αξιολόγησης PCI DSS Ετησίως ▪ Τριμηνιαίοι Τεχνικοί Έλεγχοι Αδυναμιών Ασφάλειας από Πιστοποιημένο ASV (προτεινόμενο)

Ατζέντα

- Το Προφίλ της ENCODE
- Το Πρότυπο PCI DSS
- Μεθοδολογία / Φάσεις Έργου
- Συμμετοχή Εμπορικών Επιχειρήσεων
- Οφέλη Συμμόρφωσης

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

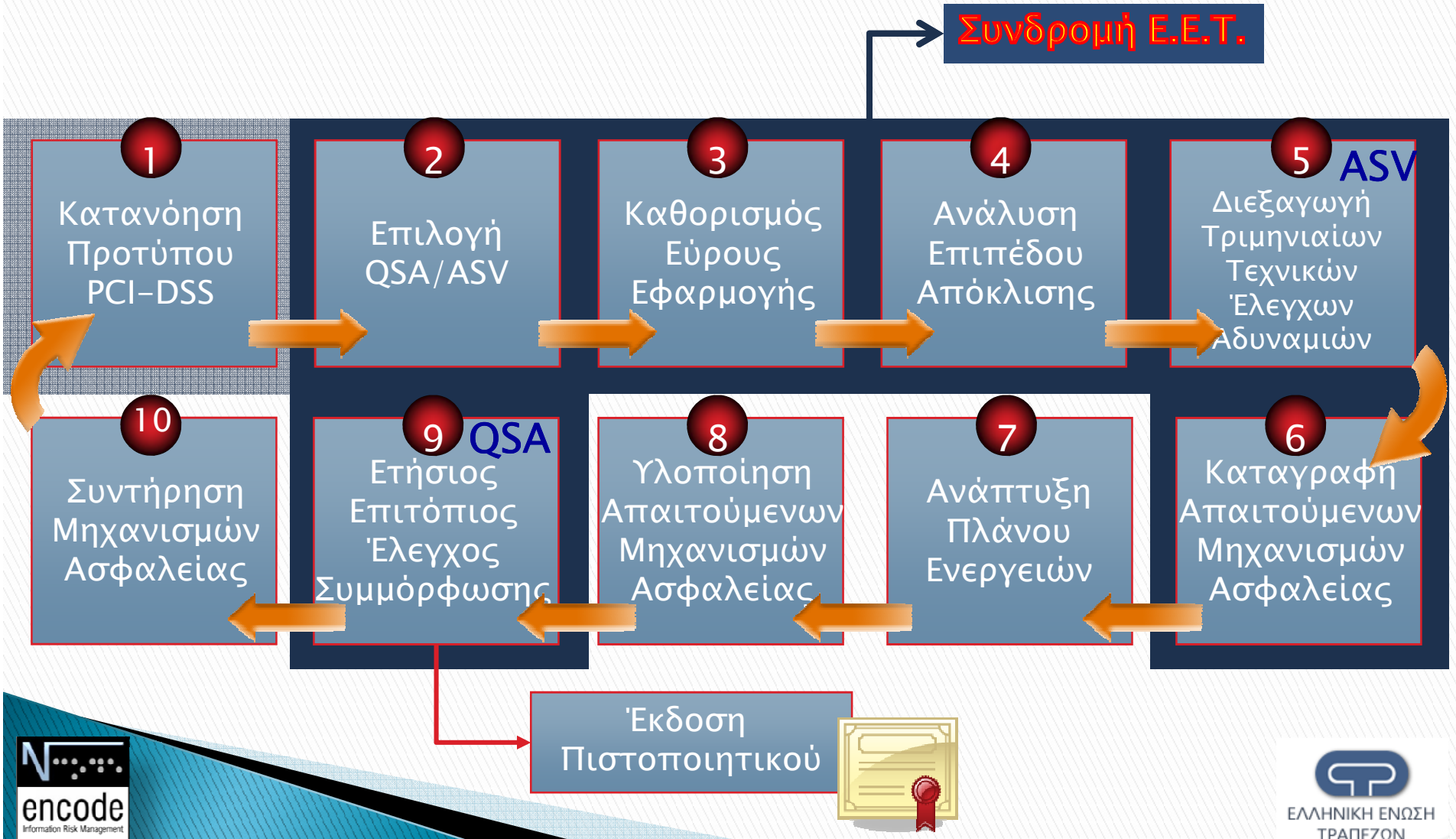
Βασικοί Στόχοι Έργου

- Προκειμένου να επιτευχθεί η προστασία και εύρυθμη λειτουργία των εμπορικών επιχειρήσεων, οι βασικοί στόχοι του έργου είναι :
  - η ουσιαστική ενημέρωση των εμπορικών επιχειρήσεων,
  - η πιστοποίηση συμμόρφωσης των εμπορικών επιχειρήσεων με το πρότυπο ασφαλείας PCI DSS, και
  - η διατήρηση πιστοποίησης της συμμόρφωσής τους για τρία τουλάχιστον έτη.

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

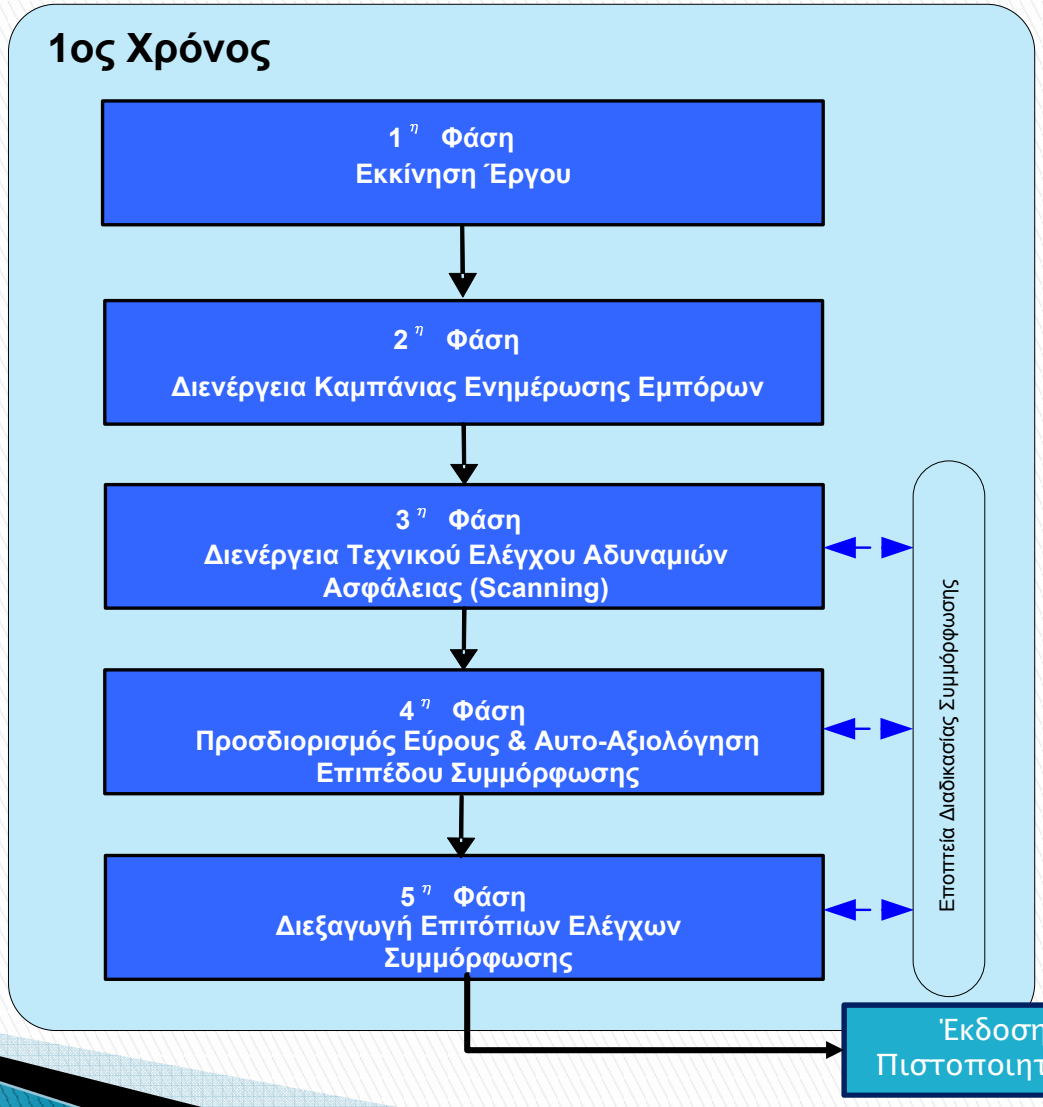
Γενικό Πλάνο Συμμόρφωσης με το Πρότυπο PCI – DSS



encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

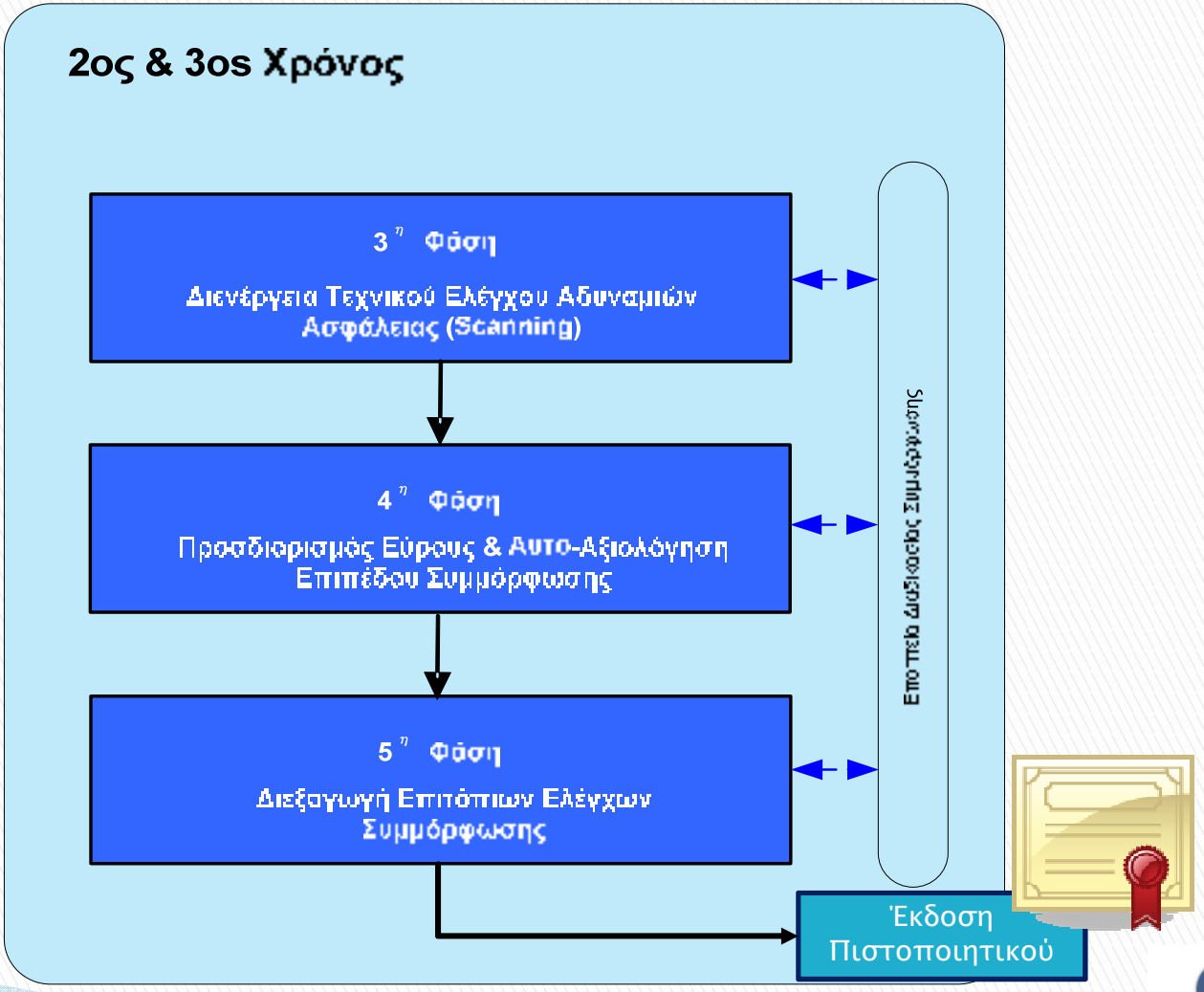
Μεθοδολογία Έργου…



encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

...Μεθοδολογία Έργου



encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

Ατζέντα

- Το Προφίλ της ENCODE
- Το Πρότυπο PCI DSS
- Μεθοδολογία / Φάσεις Έργου
- Συμμετοχή Εμπορικών Επιχειρήσεων
- Οφέλη Συμμόρφωσης

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

Βασικές Απαιτήσεις

- Διοικητική δέσμευση προς το έργο:
  - Διάχυση της δέσμευσης της Διοίκησης στους εμπλεκόμενους
  - Επένδυση στους απαιτούμενους Μηχανισμούς Ασφαλείας
- Καλή συνεργασία μεταξύ Επιχειρήσεων, Συνεργαζομένων Τραπεζών και ENCODE
- Στο πλαίσιο συνεργασίας με την ENCODE:
  - **Καθορισμός Τεχνικού Υπευθύνου (από κάθε επιχείρηση)**
  - Αποδοχή πλαισίου συνεργασίας (Συμφωνητικό Συνεργασίας)
  - Διαθεσιμότητα προσωπικού
  - Διαθεσιμότητα πληροφοριών

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

Επόμενα Άμεσα Βήματα…

- **Καθορισμός Τεχνικού Υπευθύνου** (σχετική φόρμα υπάρχει στο ενημερωτικό υλικό)

- **Συμμετοχή των Τεχνικών Υπευθύνων κάθε επιχείρησης στην αντίστοιχη Ημερίδα** που θα ακολουθήσει:
  - 23 Σεπτεμβρίου 2009
  - Ξενοδοχείο «Αμαλία»

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

Ατζέντα

- Το Προφίλ της ENCODE
- Το Πρότυπο PCI DSS
- Μεθοδολογία / Φάσεις Έργου
- Συμμετοχή Εμπορικών Επιχειρήσεων
- Οφέλη Συμμόρφωσης

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

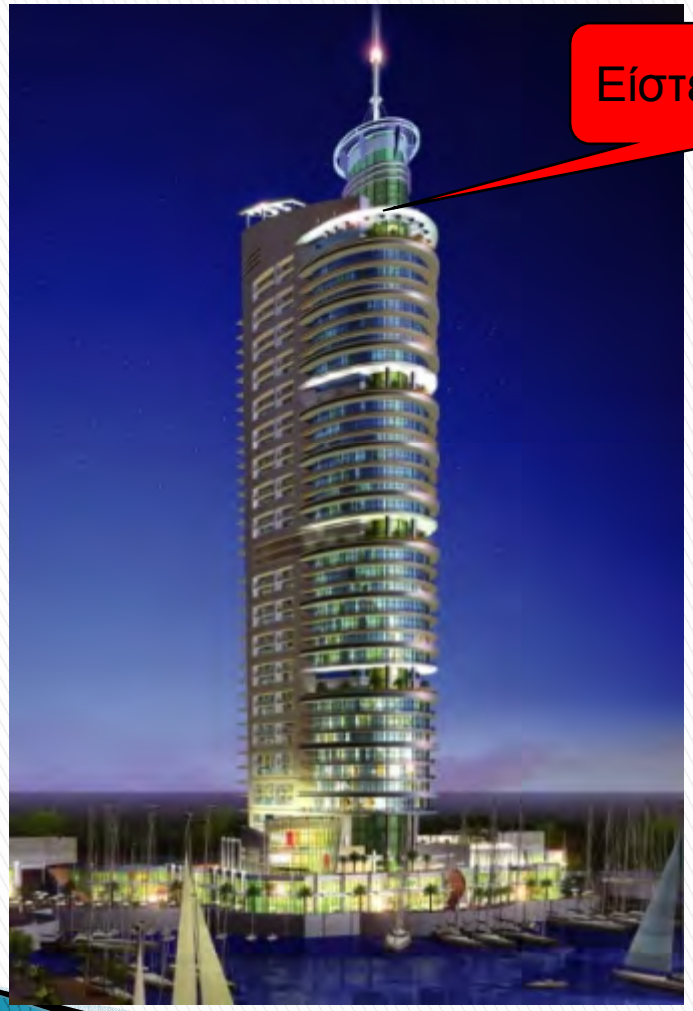
Οφέλη Συμμόρφωσης

- Διασφάλιση δημόσιας εικόνας της επιχείρησης:
  - Διασφάλιση των μετόχων της επιχείρησης
  - Εμπιστοσύνη πελατών
  - Αποφυγή αρνητικής δημοσιότητας
- Βελτίωση συνολικού επιπέδου ασφάλειας / Μείωση κινδύνων:
  - Βελτιστοποίηση εσωτερικών διαδικασιών
  - Βελτιστοποίηση τεχνολογιών ασφαλείας
- Αποφυγή οικονομικών επιβαρύνσεων / κυρώσεων & διατήρηση δυνατότητας εκτέλεσης συναλλαγών με πιστωτικές κάρτες
- Αποφυγή δαπανών έρευνας ηλεκτρονικού εγκλήματος & νομικών εξόδων (σε περίπτωση περιστατικού διακύβευσης)
- Κάλυψη συναφών απαιτήσεων συμμόρφωσης διαφορετικών προτύπων / κανονιστικών απαιτήσεων (π.χ. SoX, ΑΔΑΕ, ISO27001)

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

Πως πρέπει να βλέπουμε την Ασφάλεια Πληροφοριών…

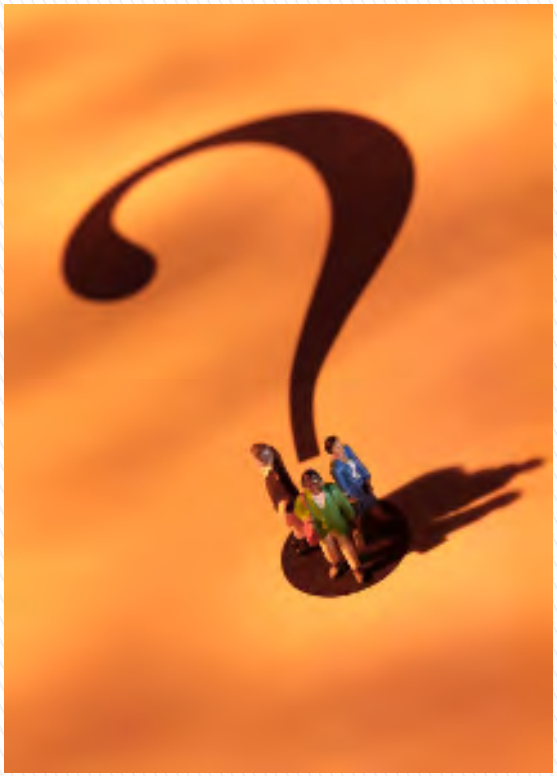


Είστε ΕΔΩ!!

Ασφάλεια Πληροφοριών

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ



Ευχαριστούμε για το χρόνο σας

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ
ΤΡΑΠΕΖΩΝ

securing the future of e-business

www.encodegroup.com_