

Εφαρμογή του Γενικού Κανονισμού στον Ευρύτερο Δημόσιο Τομέα

Μύθοι και Πραγματικότητα

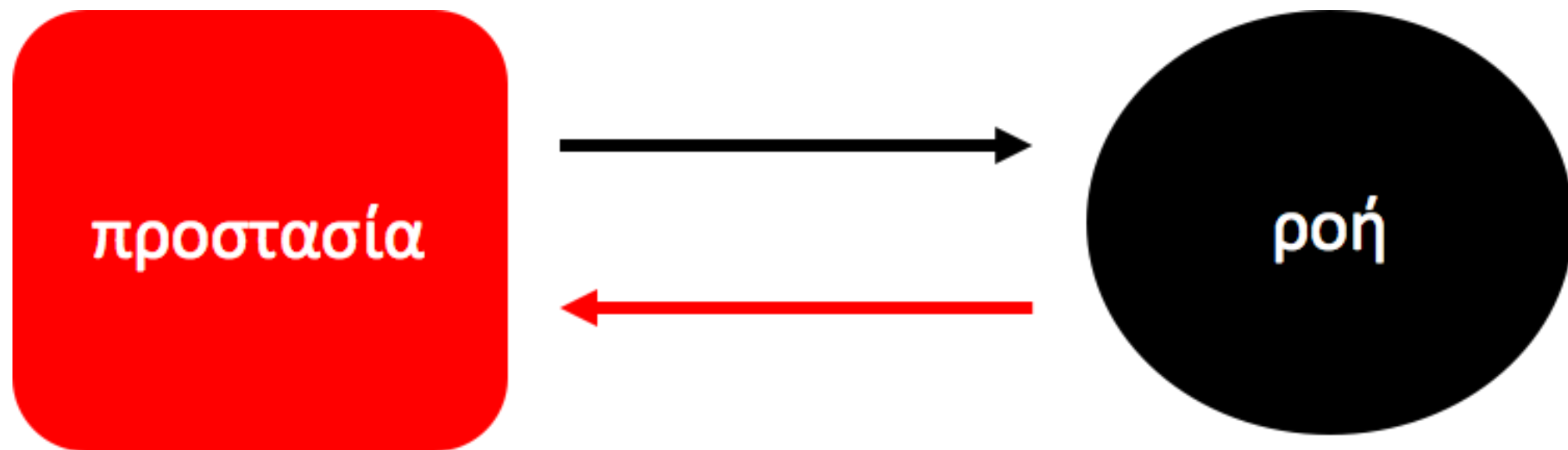
01

Προσφορά + Ροή

Προστασία + Ροή

- Τίτλος: «Γενικός Κανονισμός για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την **ελεύθερη κυκλοφορία των δεδομένων αυτών** και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων)»]

Προστασία + Ροή

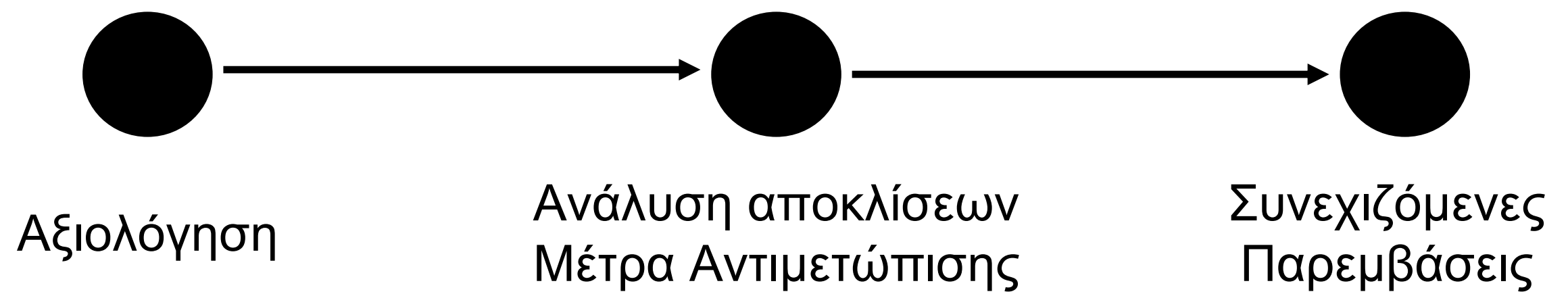


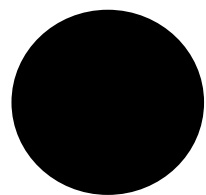
Προστασία + Ροή

- Η 5^η Ελευθερία:
- Ελεύθερη και απρόσκοπτη ροή της γνώσης/ πληροφορίας/ δεδομένων εντός της ΕΕ
- http://europa.eu/rapid/press-release_SPEECH-07-257_en.pdf
- Ο Γενικός Κανονισμός για την Προστασία των Δεδομένων ως μέρος της στρατηγικής για την Ενιαία Ψηφιακή Αγορά
- Μέρος ευρύτερων νομοθετικών παρεμβάσεων για την ελεύθερη ροή της πληροφορίας
- Οδηγία 2013/37 ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 26ης Ιουνίου 2013 για την τροποποίηση της οδηγίας 2003/98/ΕΚ σχετικά με την περαιτέρω χρήση πληροφοριών του δημόσιου τομέα
- Σχέδιο Κανονισμού για την ελεύθερη ροή των δεδομένων μη προσωπικού χαρακτήρα (COM(2017) 495 final)

02

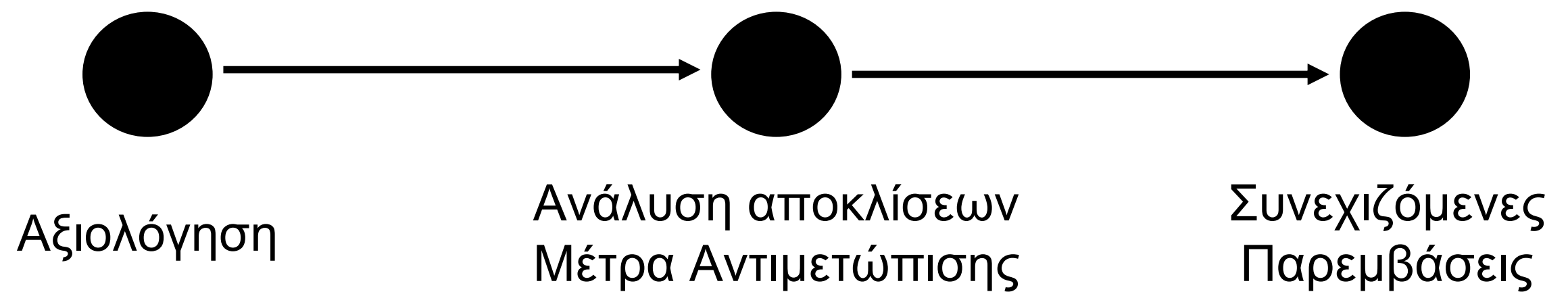
Βήματα

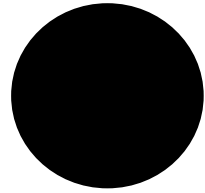




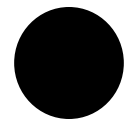
Αξιολόγηση

- Εντοπισμός πόρων/ δεδομένων
- Διαγράμματα ροής δεδομένων
- Έλεγχος 4 επιπέδων
(νομικός, τεχνικός, οργανωτικός, διαδικαστικός)
- Εντοπισμός Αποκλείσεων

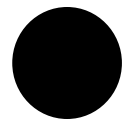




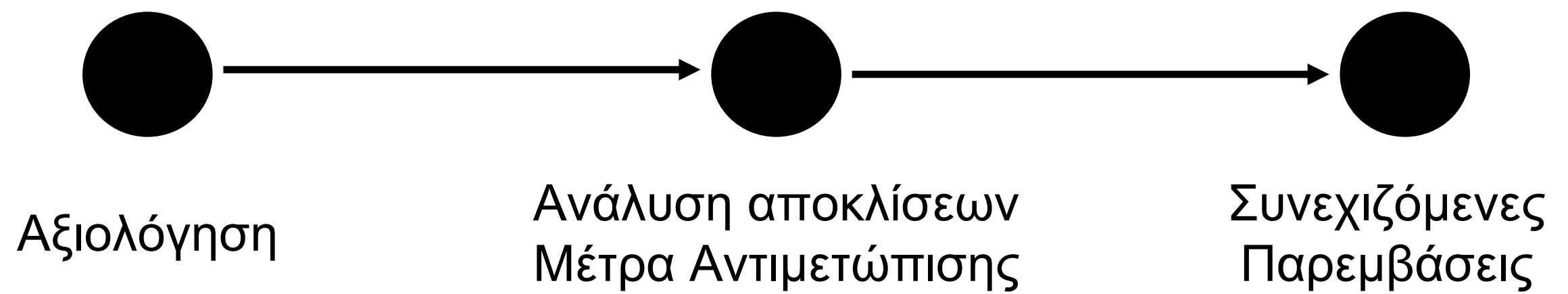
Ανάλυση αποκλίσεων
Μέτρα Αντιμετώπισης

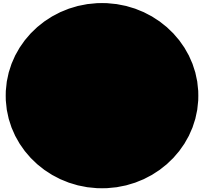


Ανάλυση Αποκλείσεων

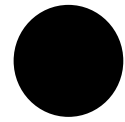


Πρόταση/ Επιλογή/ Υλοποίηση Μέτρων Αντιμετώπισης

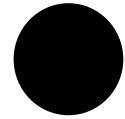




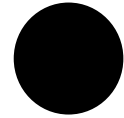
Συνεχιζόμενες
Παρεμβάσεις



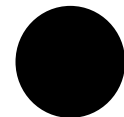
Κατάρτιση Συμβουλίου
Διακυβέρνησης Δεδομένων Προσωπικού Χαρακτήρα



Παρακολούθηση Εφαρμογής



Επικαιροποίηση Μέτρων



Εκπαίδευση

02.03.01

03

Οργάνωση

Οργάνωση

- * **Υπεύθυνος Προσωπικών Δεδομένων (data protection officer)**
 - * Κατανόηση του ρόλου (συντονισμός - όχι ευθύνη)
 - * Κατανόηση της σχέσης με υπάρχουσες οργανωτικές δομές και ρόλους (π.χ. Υπηρεσία Εσωτερικού Ελέγχου - Υπεύθυνοι διαδικασιών)
 - * ζητήματα σε σχέση με το πρόσωπο:
 - * Ανάγκη Εμπειρίας και κατανόησης του οργανισμού
 - * Πρόβλημα στη σύγκρουση συμφερόντων (να μην είναι “ιδιοκτήτης” διαδικασιών που σχετίζονται με την επεξεργασία δεδομένων προσωπικού χαρακτήρα)

Οργάνωση*

Ομάδα Διακυβέρνησης Δεδομένων Προσωπικού Χαρακτήρα:

- * Μορφή: Ομάδα Διοίκησης Έργου (;)
- * Αρμοδιότητες:
 - * Προκήρυξη διαγωνισμού για τη λήψη υπηρεσιών
 - * Εφαρμογή του Γενικού Κανονισμού
 - * Παρακολούθηση μέτρων και διαδικασιών
- * Σύνθεση:
 - * Αντιπροσωπευτική των κεντρικών υπηρεσιών που θα έχουν ιδιοκτησία επί των διαδικασιών
 - * Ανάγκη ευελιξίας
- * Σχέση με τον DPO
- * Σχέση με τη διοίκηση
 - * δυνατότητα ουσιαστικού μετασχηματισμού του οργανισμού

04

Καταγραφή + Αξιολόγηση

Καταγραφή Αξιολόγηση

Γενικές Βέλτιστες πρακτικές:

- * Ενημέρωση: πρέπει να προηγείται και να γίνεται οργανικά (όχι sales pitch)
- * Ερωτηματολόγια: πρέπει να εξηγούνται και να είναι στοχευμένα
- * Εντοπισμός των “ιδιοκτητών” των διαδικασιών
- * Εντοπισμός κρίσιμων ροών εργασίας
- * Αξιοποίηση DPO/ Συμβουλίου Διακυβέρνησης
- * Αξιοποίηση ISO - όπου υπάρχει
- * Αξιοποίηση καταγραφής ροών εργασιών για πληροφοριακά συστήματα/ παροχή υπηρεσιών

Καταγραφή Αξιολόγηση

Καταγραφή Πόρων & Ροών Δεδομένων (διαδικασιών)

- * Δεν μπορεί να γίνει μεμονωμένα το ένα από το άλλο
- * Καλό είναι να ξεκινάμε από περιπτώσεις εργασίας ή από (κρίσιμες) διαδικασίες
- * Διαιρούμε την επεξεργασία δεδομένων σε δύο διαστάσεις:
 - * Είσοδος/ Κυρίως Επεξεργασία/ Έξοδος
 - * Ανάγνωση/ Γραφή - Τροποποίηση/ Διαγραφή
- * Εντοπίζουμε τα πρόσωπα που έχουν επαφή με τα δεδομένα
- * Εντοπίζουμε τους τύπους, χρόνους και σκοπούς επεξεργασίας
- * Εντοπίζουμε νόμιμες βάσεις

Καταγραφή Αξιολόγηση

Νομικά Κείμενα

- * Νομοθετικό Πλαίσιο
- * Κανονιστικό Πλαίσιο (συγκεκριμένο)
- * Πολιτικές (εσωστρεφή κείμενα με εξωτερικό αντίκτυπο)
- * Συμβάσεις (ιδίως εργασίας και ΓΟΣ)
- * Σημειώματα

Καταγραφή Αξιολόγηση

Οργανωσιακή Δομή

- * Σε σχέση με το νομοθετικό και κανονιστικό πλαίσιο
- * Οργανόγραμμα και περιγράμματα
- * Έμφαση στο “μονοπάτι των δεδομένων”
- * Εντοπισμός σχέσεων με τρίτους (π.χ. τρέχουσες συμβάσεις/
πλαίσια συνεργασίας/ υποχρεώσεις ροών προς τρίτους)

Καταγραφή Αξιολόγηση

Τεχνολογική υποδομή

- * Πληροφοριακά Συστήματα
 - * Ιδίως Προσωπικού/ Λογιστηρίου - οικονομικών υπηρεσιών/
CRM/ Υπηρεσιών προς χρήστες
 - * Προσδιορισμός υπηρεσιών από τρίτους (νέφους -
λογιστηρίου/ μισθοδοσίας)
 - * Σχέση με διαδικασίες
 - * ΠΡΟΣΟΧΗ: δεν είναι πανάκεια
- * Φυσικά Συστήματα και κανονισμός ασφαλείας

05

Ανάλυση και Αντιμετώπιση

Ανάλυση Αντιμετώπιση

Στάδια:

- * Έμφαση στις διαδικασίες
 - * Εξορθολογισμός
- * Προσδιορισμός Κινδύνων:
 - * Πιθανότητα
 - * Αντίκτυπο
- * Προσδιορισμός κόστους:
 - * Περισσότερες από μία λύσεις
 - * Κόστος/ Κίνδυνος (πρόβλημα σε σχέση με την κουλτούρα ευθύνης)
- * Προσδιορισμός σημείων αποφάσεως:
 - * Ποιός και πότε παίρνει την ευθύνη;
 - * Ποια διαδικασία εφαρμόζεται ως προς αυτό;
 - * Πως διασφαλίζεται η παροχή της βέλτιστης υπηρεσίας για τον πελάτη

Ανάλυση Αντιμετώπιση

Σημεία προς προσοχή:

- * Αποφυγή μαξιμαλισμών: ο κανόνας pareto 80-20
- * Η πληροφορική δεν είναι η λύση για όλα
- * Διαδικασίες
- * Προσοχή στους χρόνους υλοποίησης
- * Τι κάνει ο σύμβουλος και τι κάνει ο οργανισμός

06

Συνεχιζόμενα μέτρα

Συνεχιζόμενα Μέτρα

Συμβούλιο Διακυβέρνησης

- * Δεν παραμένει στατικό
- * Από προμήθεια στην εφαρμογή
- * Ανάγκη επιλογής του σωστού επιπέδου συμμετεχόντων
 - * όχι πασαρέλα
 - * όχι ψυγείο
- * Διατήρηση της αίσθησης ότι ασκεί επιρροή στην αλλαγή των πραγμάτων
- * Το θέμα της ευθύνης

Συνεχιζόμενα Μέτρα

Παρακολούθηση Εφαρμογής

- * Οδικός Χάρτης
- * Σημεία προόδου
- * Μέτρα διαχείρισης κινδύνου στην υλοποίηση του έργου
- * Συμμετοχή της Διοίκησης

Συνεχιζόμενα Μέτρα

Επικαιροποίηση Μέτρων

- * Δυνατότητα επικαιροποίησης διαδικασιών
- * Παράθυρα ευκαιρίας για την επικαιροποίηση κανονιστικού πλαισίου
- * Κόστος πληροφοριακού συστήματος (SaaS λύσεις)
- * Προτυποποίηση νομικών κειμένων
- * Εσωτερικός Διαμοιρασμός Πληροφορίας

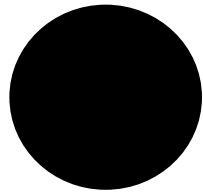
Συνεχιζόμενα Μέτρα

Εκπαίδευση

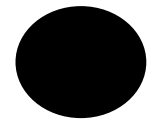
- * Γενική Ενημέρωση
- * Εκπαίδευση στελεχών που έχουν ιδιοκτησία σε διαδικασίες
- * Εκπαίδευση DPO
- * Έμφαση σε εργαστήρια
- * Πρόγραμμα εκπαιδεύσεων

07

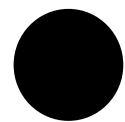
Συμπεράσματα



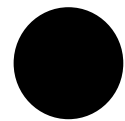
Συμπεράσματα



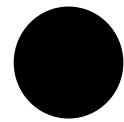
Διαύγεια/ Αρχεία/ Καταστροφή



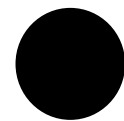
Η δουλειά γίνεται από τον οργανισμό όχι από τον DPO ή τους συμβούλους



Η έμφαση πρέπει να δίδεται στις διαδικασίες όχι στην τεχνολογία



Το συμβούλιο διακυβέρνησης είναι κρίσιμο για την επιτυχία του εγχειρήματος



Οι εκπαιδεύσεις μπορεί να μειώσουν σοβαρά το κόστος για τον οργανισμό

