# Ασφάλεια Πληροφοριακών Συστημάτων

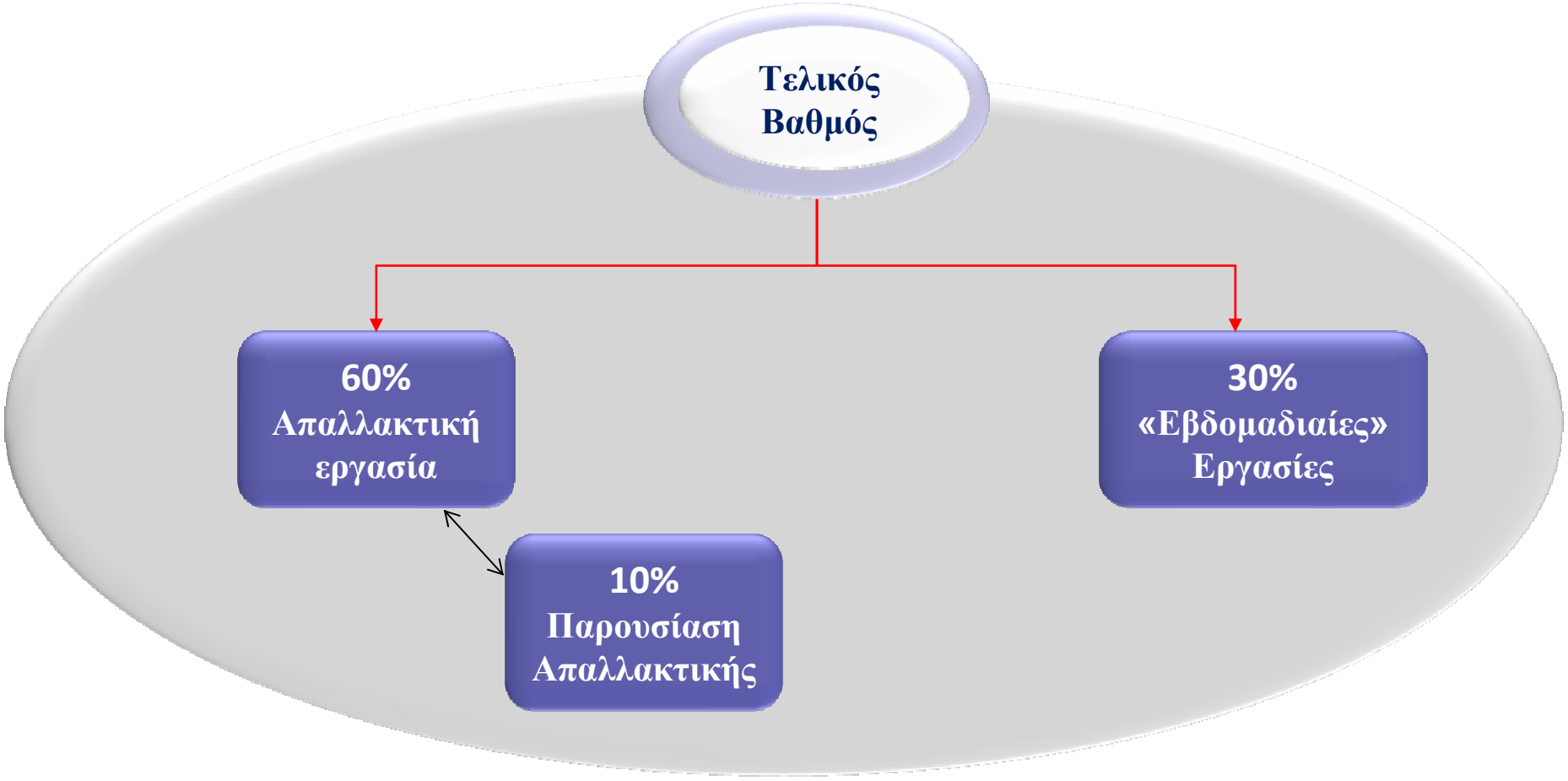
## «Διαχείριση Ασφάλειας και Ιδιωτικότητας

Τμήμα Πληροφορικής
ΠΜΣ «ΠΛΗΡΟΦΟΡΙΚΗ»

Επ. Καθ. Δ. Πολέμη
Λέκτορας Π.Κοτζανικολάου
Δρ. Θ. Καραντζιάς
dpolemi@unipi.gr, pkotzani@unipi.gr

# Τρόπος Διεξαγωγής Μαθήματος

# *Μέθοδος αξιολόγησης μαθήματος*



# *Διδακτικές μέθοδοι*

- Διαλέξεις
- Εργαστηριακά μαθήματα
  - *Χρήση laptop*(;)
- Συμμετοχή φοιτητών μέσω ενδιάμεσων εργασιών
  - Εργασίες μικρής κλίμακας
- Συχνή ενημέρωση σελίδας μαθήματος
  - http://athina.cs.unipi.gr/site-ergastirio/asfaleia/index.php
  - http://gunet2.cs.unipi.gr/eclass/courses/TME135/

# Κύρια Ύλη Μαθήματος (1)

- Διαχείριση Ασφάλειας και Ιδιωτικότητας
  - Ανάλυση Επικινδυνότητας
  - Μεθοδολογίες και Πρότυπα για την Ανάλυση Επικινδυνότητας
  - Πολιτική Ασφάλειας και Πρότυπα
  - Σχέδιο Επιχειρησιακής Συνέχειας και Πρότυπα
  - Σχέδιο Ανάκαμψης Καταστροφών και Πρότυπα
  - Εργαλεία Διαχείρισης Ασφάλειας
- Κρυπτογραφικά συστήματα
  - Κρυπτο-συστήματα μοναδιαίας κλείδας (Συμμετρική Κρυπτογράφηση)
  - Κρυπτο-συστήματα δημόσιας κλείδας (Ασύμμετρη Κρυπτογράφηση)
  - Υβριδική κρυπτογραφία και εφαρμογές σε πρωτόκολλα ασφάλειας

# Κύρια Ύλη Μαθήματος (2)

- Υποδομή Δημόσιας Κλείδας (ΥΔΚ)
  - Οργανωτικές δομές
  - Υπηρεσίες ΥΔΚ / Συναρτήσεις ΥΔΚ
  - Πρότυπα / Νομικό Πλαίσιο
- Ασφάλεια στις Τεχνολογίες
  - Java / .Net Microsoft
  - XML
  - Υπηρεσίες Ιστού
  - Έξυπνες κάρτες
- Χρήση ΥΔΚ σε Ηλεκτρονικές & Ασύρματες εφαρμογές
  - η/α-διακυβέρνηση (e/m-Government)
  - η/α-εμπόριο (e/m-Commerce)

# 1. Διαχείριση Ασφάλειας και Ιδιωτικότητας

1. **Βασικές έννοιες διαχείρισης ασφάλειας Π.Σ.**
2. Ο κύκλος ζωής της Ασφάλειας – Συστήματα διαχείρισης ασφάλειας
3. Ανάλυση Επικινδυνότητας – Μεθοδολογίες και Πρότυπα
4. Πολιτική Ασφάλειας και Πρότυπα
5. Σχέδιο Επιχειρησιακής Συνέχειας / Σχέδιο Ανάκαμψης Καταστροφών και Πρότυπα
6. Εργαλεία Διαχείρισης Ασφάλειας

# Τι είναι ασφάλεια;

Security
Safety
Insurance
Assurance
Police
Fuse

$\overset{?}{=}$ Ασφάλεια

# Ορισμοί της Ασφάλειας

- Security:
  - **Freedom from danger or anxiety**
  - Safety from criminal activity such as terrorism
  - A thing deposited or pledged as a guarantee of the fulfillment of an undertaking or the repayment of a loan, to be forfeited in case of default
  - A certificate attesting credit, the ownership of stocks or bonds, or the right to ownership connected with tradable derivatives

- Ασφάλεια:
  - **Η κατάσταση στην οποία δεν υπάρχουν κίνδυνοι, όπου αισθάνεται κανείς ότι δεν απειλείται.**
  - **Η αποτροπή κινδύνου ή απειλής, η εξασφάλιση σιγουριάς και βεβαιότητας**
  - Υπηρεσία της Αστυνομίας
  - Ηλεκτρική διάταξη που αποτρέπει πιθανά ατυχήματα
  - Μηχανισμός στην πόρτα αυτοκινήτου
  - Συμφωνία μεταξύ ασφαλιστικής εταιρείας και πελάτη
  - Ιατροφαρμακευτική περίθαλψη

# Η έννοια της ασφάλειας πληροφοριακού συστήματος

- **Σύστημα:** ένα σύνολο από *κατάλληλα οργανωμένα* αλληλοεξαρτώμενα ή/και αλληλεπιδρώντα στοιχεία, τα οποία αποτελούν μία ενιαία οντότητα η οποία δρα για την εκπλήρωση συγκεκριμένων σκοπών

- **Πληροφοριακό σύστημα:** ένα οργανωμένο σύνολο το οποίο απαρτίζεται από:
  - Ανθρώπους
  - Δεδομένα
  - Υλικό (h/w)
  - Λογισμικό (s/w)
  - Διαδικασίες

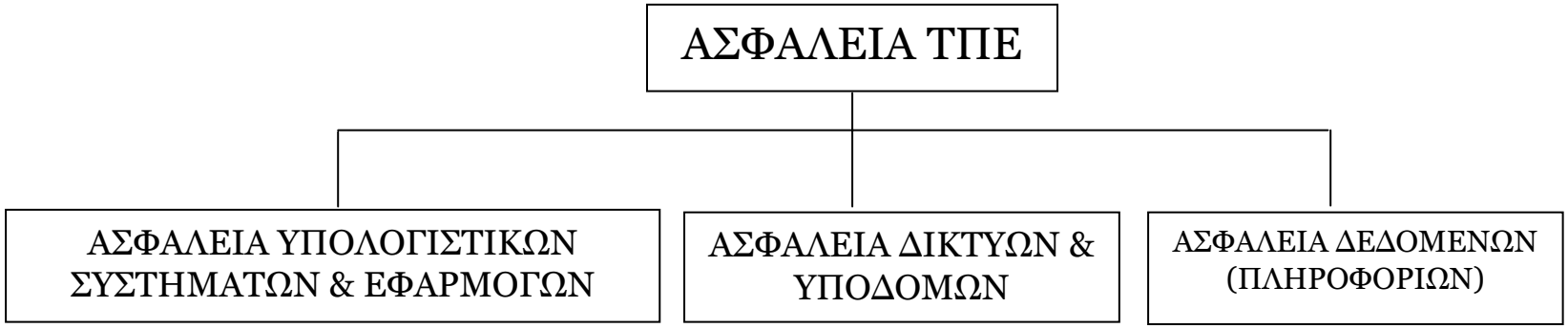
  με σκοπό την υποστήριξη των επιχειρησιακών δραστηριοτήτων, μέσω της επεξεργασίας, ανταλλαγής και διαχείρισης πληροφορίας.

# Τεχνική vs Ολιστική προσέγγιση ασφάλειας

- **Ασφάλεια Τεχνολογιών Πληροφορίας & Επικοινωνιών (ΤΠΕ)** (Information & Communication Technology (ICT) Security)
  - Ασφάλεια υπολογιστικών συστημάτων & εφαρμογών
  - Ασφάλεια δικτύων & υποδομών
  - Ασφάλεια δεδομένων

- **Ολιστική προσέγγιση ασφάλειας Π.Σ.**
  - Ασφάλεια υπολογιστικών συστημάτων & εφαρμογών
  - Ασφάλεια δικτύων & υποδομών
  - Ασφάλεια δεδομένων + **πληροφορίας**
  - **Ασφάλεια χρηστών (προσωπικού)**
  - **Λειτουργική ασφάλεια (διαδικασίες λειτουργίας)**

# Τεχνική Προσέγγιση: Ασφάλεια ΤΠΕ



# Ασφάλεια Υπολογιστικών Συστημάτων & Εφαρμογών

- Η διασφάλιση της ορθής λειτουργίας του υπολογιστικού συστήματος/εφαρμογής (hardware/software)
- Η προστασία από μη εξουσιοδοτημένη λογική πρόσβαση στο σύστημα/εφαρμογή
- Προστασία από μη εξουσιοδοτημένη τροποποίηση της διάρθρωσης του συστήματος
- Η προστασία από κακόβουλη χρήση (π.χ. εκτέλεση κακόβουλου λογισμικού)
- Η προστασία από λανθασμένες ενέργειες
- Η προστασία της διαθεσιμότητας των συστημάτων/ εφαρμογών
- Η φυσική προστασία των συστημάτων

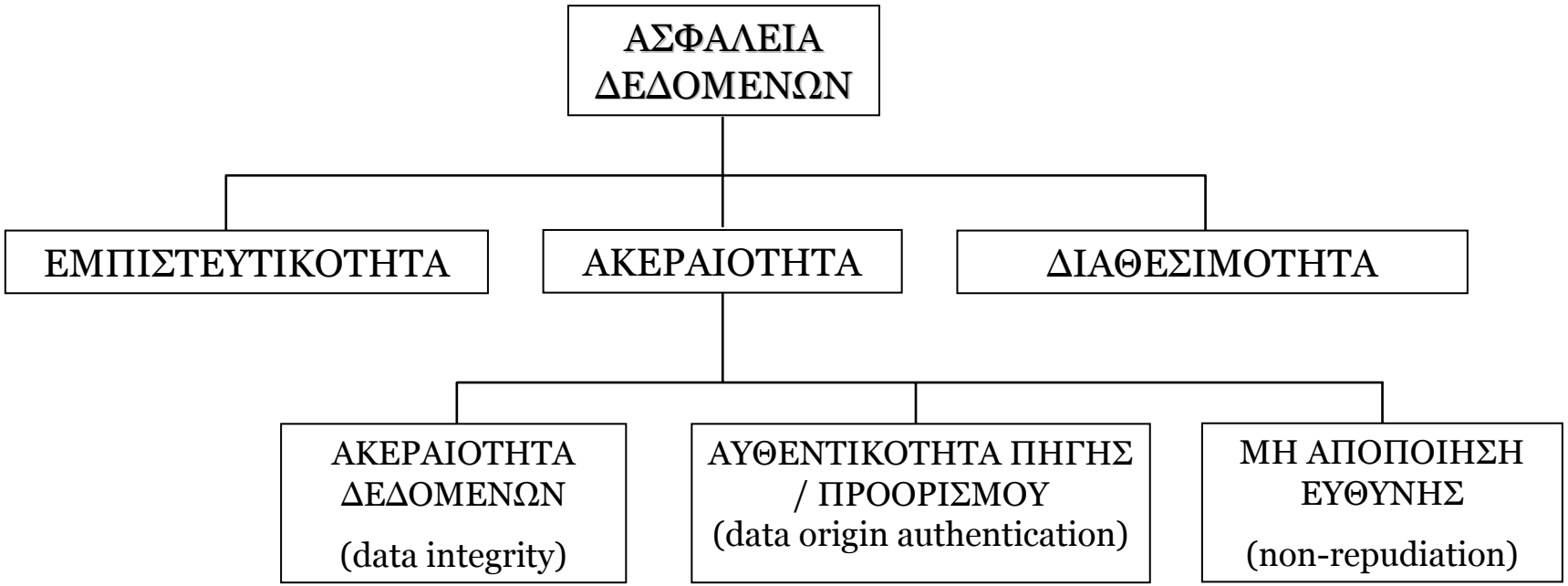
# Ασφάλεια Δικτύων & Υποδομών

- Η προστασία από μη εξουσιοδοτημένη λογική πρόσβαση σε ένα δίκτυο
- Η προστασία από την παρακολούθηση του μέσου επικοινωνίας (υποκλοπή)
- Η προστασία από παράκαμψη ή τροποποίηση των κανόνων δρομολόγησης στο δίκτυο
- Η διασφάλιση της δικτυακής διασύνδεσης και η προστασία από τη διακοπή της επικοινωνίας
- Η φυσική προστασία των υποδομών επικοινωνίας (routers, gateways, κτλ)

# Ασφάλεια Δεδομένων (Πληροφοριών)

- Προστασία των δεδομένων κατά την επεξεργασία, αποθήκευση ή μετάδοσή τους, ως προς την:
  - Εμπιστευτικότητα (Confidentiality)
    - Η αποφυγή μη εξουσιοδοτημένης αποκάλυψης της πληροφορίας
  - Ακεραιότητα (Integrity)
    - Η αποφυγή μη εξουσιοδοτημένης τροποποίησης μιας πληροφορίας
  - Διαθεσιμότητα (Availability)
    - Η αποφυγή μη εξουσιοδοτημένης προσωρινής ή μόνιμης παρακράτησης μιας πληροφορίας

# Άλλες ιδιότητες ασφάλειας



# Ολιστική προσέγγιση ασφάλειας Π.Σ.

- Η τεχνική πλευρά της ασφάλειας ΤΠΕ (ασφάλεια δεδομένων, H/W, S/W) +

  Ανθρώπινος παράγοντας +

  Διαδικασίες Λειτουργίας +

  Περιβάλλον λειτουργίας

- Άρα:
  - Κανόνες χρήσης /λειτουργίας και διαδικασίες ασφάλειας (operational view)
  - Νομοθετικό / ρυθμιστικό πλαίσιο λειτουργίας (legal/regulatory view)

# Πρακτική προσέγγιση ασφάλειας

- Κάθε Π.Σ. υποστηρίζει ορισμένες επιχειρησιακές δραστηριότητες (business processes). Άρα πρακτικός στόχος της ασφάλειας Π.Σ.
  - Η προστασία των επιχειρησιακών δραστηριοτήτων που υποστηρίζονται από του Π.Σ.
  - Η ορθή λειτουργία του Π.Σ.

- Η απόλυτη ασφάλεια είναι ΑΔΥΝΑΤΗ. Συνεπώς ακολουθείται η προσέγγιση μείωσης των κινδύνων (risk-based approach)
  - Εντοπισμός κινδύνων
  - Λήψη κατάλληλων μέτρων προστασίας για την αντιμετώπισή τους
    - Πρόληψης (prevention)
    - Ανίχνευσης (detection)
    - Αποκατάστασης (recovery)

# Βασικοί όροι ασφάλειας

- **Αγαθό** (Asset)
  - Κάθε αντικείμενο ή πόρος το οποίο αξίζει να προστατευθεί.
    - Φυσικά Αγαθά (Physical Assets):
      - **Χρήστες**
      - Υπολογιστικά συστήματα
      - Δικτυακή υποδομή
      - Λοιπός εξοπλισμός
    - Αγαθά Δεδομένων (Data Assets):
      - Αρχεία (ηλεκτρονικά, έντυπα)
      - Λοιπά έγγραφα *(διαδικασίες)*
    - Αγαθά Λογισμικού (Software Assets):
      - Εφαρμογές
      - Λειτουργικά Συστήματα

# Βασικοί όροι ασφάλειας

- **Ιδιοκτήτης αγαθού** (asset owner)
  - ονομάζεται το φυσικό ή νομικό πρόσωπο που έχει την ευθύνη και αρμοδιότητα για τη σωστή χρήση του αγαθού.
    - Π.χ. ο Διευθυντής Πληροφορικής είναι ο Ιδιοκτήτης των δεδομένων που διαχειρίζεται η Διεύθυνση Πληροφορικής
- **Χρήστης Αγαθού** (asset user)
  - Το φυσικό πρόσωπο που επεξεργάζεται ένα αγαθό, με την καθοδήγηση και εξουσιοδότηση του Ιδιοκτήτη του αγαθού

# Βασικοί όροι ασφάλειας

- **Συνέπεια** (Impact)
  - Η απώλεια που θα προκληθεί από την προσβολή ενός αγαθού
    - Άμεσες Συνέπειες – π.χ.
      - κόστος επαναγοράς
      - κόστος διαμόρφωσης, εισαγωγής δεδομένων
    - Έμμεσες Συνέπειες – π.χ.
      - Κοινωνικές συνέπειες
      - Δυσφήμηση
      - Νομικές συνέπειες
      - Απώλειες από διακοπή ή παρεμπόδιση λειτουργιών

# Βασικοί όροι ασφάλειας

- **Απειλή** (Threat)
  - Οποιοδήποτε γεγονός η εκδήλωση του οποίου προκαλεί αρνητικές συνέπειες (impact) σε κάποιο αγαθό
    - Φυσικές Απειλές:
      - Φωτιά, Σεισμός, Πλημμύρα,...
    - Ανθρώπινες Εσκεμμένες:
      - Κλοπή, Βανδαλισμός, Αλλοίωση, Αποκάλυψη πληροφορίας, hacking, cracking, Denial of Service, miss-routing, ...)
    - Ανθρώπινες Τυχαίες:
      - Κακή χρήση πόρου, πρόκληση ζημιάς, τυχαία αποκάλυψη πληροφορίας κτλ

# Βασικοί όροι ασφάλειας

- **Αδυναμία** (Vulnerability)
  - Οποιοδήποτε χαρακτηριστικό κάνει ευάλωτο ένα αγαθό σε μία ή περισσότερες απειλές, δηλαδή αυξάνει την πιθανότητα εκδήλωσης της απειλής
    - Π.χ: εάν η πρόσβαση σε ένα απόρρητο αρχείο δεν προστατεύεται, το αρχείο έχει μεγάλη αδυναμία στην απειλή της κλοπής
  - Οτιδήποτε μεγιστοποιεί τις συνέπειες από την εκδήλωση μίας απειλής
    - Π.χ: εάν δεν υπάρχει σύστημα αυτόματης πυρόσβεσης σε ένα χώρο, η συνέπειες από μία πιθανή πυρκαγιά θα είναι πολύ μεγάλες

# Βασικοί όροι ασφάλειας

- **Κίνδυνος ή επικινδυνότητα ασφάλειας** (security risk)
  - Επικινδυνότητα = Συνέπεια ◇ Απειλή ◇ Αδυναμία
  - Security Risk = Impact ◇ Threat ◇ Vulnerability
- Οι κίνδυνοι ασφάλειας υπολογίζονται για όλα τα αγαθά ενός Π.Σ.
- Η διαδικασία υπολογισμού κινδύνων υποστηρίζεται από μεθοδολογίες και εργαλεία ανάλυσης επικινδυνότητας (risk analysis)

# Βασικοί όροι ασφάλειας

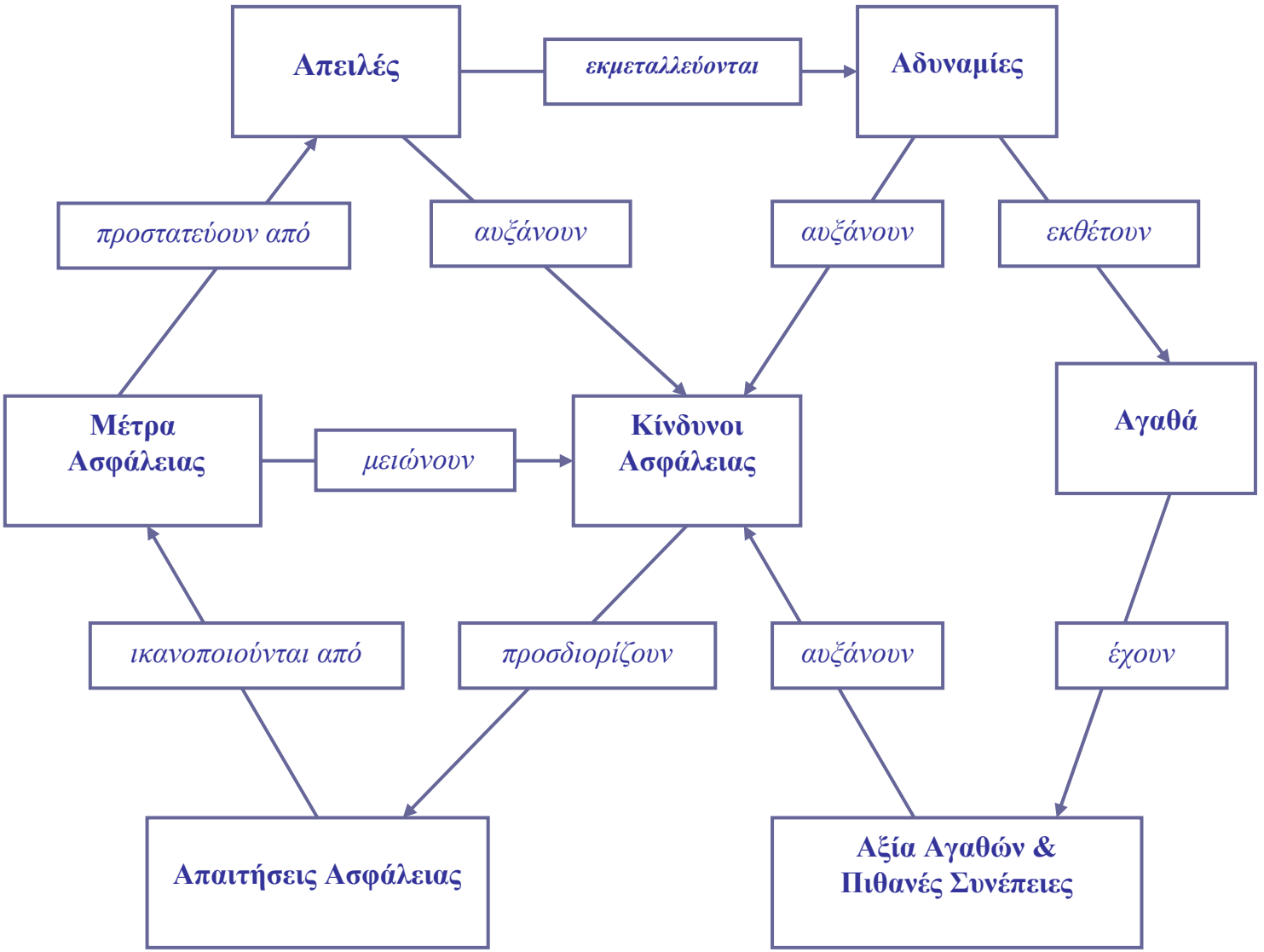
- **Μέτρο ασφάλειας (ή έλεγχος ασφάλειας)** (safeguard, security control, countermeasure):
  - Οτιδήποτε περιορίζει τον κίνδυνο για ένα ή περισσότερα αγαθά
    - **Προληπτικά μέτρα (preventive):**
      - στοχεύουν στο να αποτρέψουν κινδύνους
      - π.χ, η χρήση ενός συστήματος Firewall σε ένα δίκτυο αποτρέπει τη μη εξουσιοδοτημένη είσοδο πακέτων σε ένα δίκτυο.
    - **Μέτρα Ανίχνευσης (detective):**
      - αποσκοπούν στο να εντοπίσουν την πηγή της προσβολής σε ένα αγαθό, εφόσον το αγαθό αυτό έχει προσβληθεί από κάποιο κίνδυνο.
      - π.χ., η χρήση ενός Συστήματος Ανίχνευσης Εισβολών (Intrusion Detection System – IDS) σε ένα δίκτυο
    - **Μέτρα Αποκατάστασης (recovery):**
      - στοχεύουν στο να μειώσουν τον απαιτούμενο χρόνο για την ανάκαμψη μετά από την εκδήλωση μίας προσβολής σε ένα αγαθό.
      - π.χ., η λήψη εφεδρικών αρχείων σε ένα υπολογιστικό σύστημα ελαχιστοποιεί τον χρόνο ανάκαμψης ενός συστήματος από μία πιθανή διακοπή λειτουργίας.

# Βασικοί όροι ασφάλειας

- **Κόστος** (cost)
  - Οποιαδήποτε επιβάρυνση προκύπτει από:
    - Την αγορά/εγκατάσταση ενός μέτρου ασφάλειας
    - Την χρήση/συντήρηση ενός μέτρου ασφάλειας

- Η διαδικασία προσδιορισμού, αξιολόγησης και επιλογής των κατάλληλων μέτρων ασφάλειας υποστηρίζεται από μεθοδολογίες και εργαλεία διαχείρισης επικινδυνότητας (risk management)

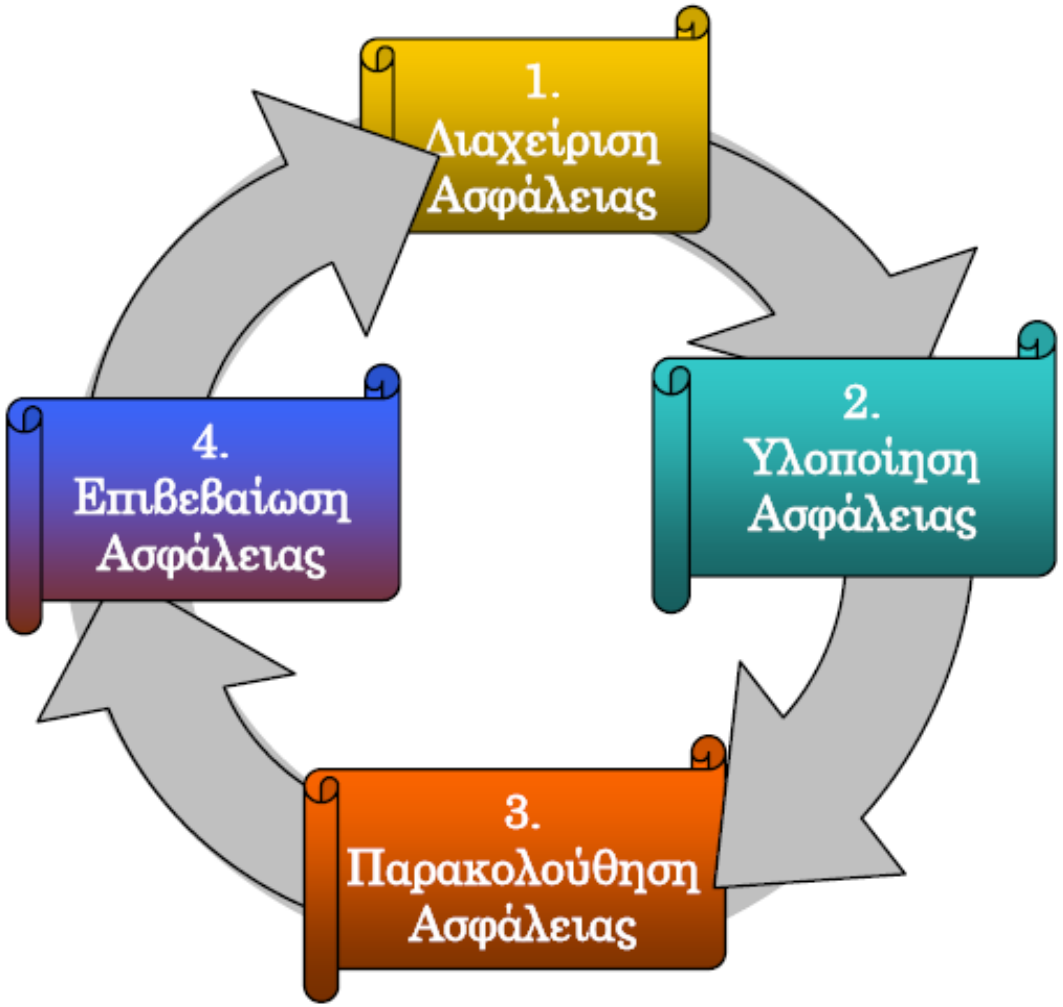
# Λειτουργική σύνδεση όρων ασφάλειας



# *1. Διαχείριση Ασφάλειας και Ιδιωτικότητας*

1. Βασικές έννοιες διαχείρισης ασφάλειας Π.Σ.
2. **Ο κύκλος ζωής της Ασφάλειας – Συστήματα διαχείρισης ασφάλειας**
3. Ανάλυση Επικινδυνότητας – Μεθοδολογίες και Πρότυπα
4. Πολιτική Ασφάλειας και Πρότυπα
5. Σχέδιο Επιχειρησιακής Συνέχειας / Σχέδιο Ανάκαμψης Καταστροφών και Πρότυπα
6. Εργαλεία Διαχείρισης Ασφάλειας

# Ο «κύκλος ζωής» της ασφάλειας



# Διαχείριση Ασφάλειας (Security Management) – 1/2

- Η φάση αυτή αποτελεί το **στρατηγικό σχεδιασμό της ασφάλειας**
- Καθορισμός των γενικών κατευθύνσεων και της για την επαρκή προστασία του Π.Σ.
- Ανάλυση απαιτήσεων ασφάλειας
  - συστημάτων
  - εφαρμογών
  - υποδομών
  - πληροφοριών ενός οργανισμού
- Εντοπισμός των ευαίσθητων από πλευράς ασφάλειας σημείων
  - ανάλογα με βαθμό κρισιμότητας των επιχειρηματικών λειτουργιών που υποστηρίζουν

# Διαχείριση Ασφάλειας (Security Management) – 2/2

- Η φάση της Διαχείρισης Ασφάλειας περιλαμβάνει δραστηριότητες όπως:
  1. Διενέργεια Ανάλυσης και Διαχείρισης Κινδύνου (Risk Analysis and Risk Management)
  2. Σύνταξη Πολιτικής Ασφάλειας (Security Policy)
  3. Σύνταξη Σχεδίου Συνέχειας Λειτουργιών (Business Continuity Plan)
  4. Σύνταξη Σχεδίου Ανάκαμψης Συστημάτων (Disaster Recovery Plan)

# Υλοποίηση Ασφάλειας (Security Implementation) – 1/3

- Σχεδιασμός και προδιαγραφές τεχνικών ή άλλων λύσεων που απαιτούνται για την τεχνική υλοποίηση των απαιτήσεων ασφάλειας.
- Σχεδιασμός της αρχιτεκτονικής ασφάλειας του δικτύου
  - τοπολογία του δικτύου
  - καθορισμός των σημείων ελέγχου εισόδου και εξόδου
  - σχεδιασμός του ελέγχου πρόσβασης
  - διαχωρισμός του δικτύου σε εικονικά ιδιωτικά δίκτυα (VPN) ή ανεξάρτητες ζώνες

# Υλοποίηση Ασφάλειας (Security Implementation) – 2/3

- Καθορισμός προδιαγραφών του δικτυακού και λοιπού εξοπλισμού ασφάλειας, όπως:
  - Firewall, IDS, Anti-virus κτλ.
  - Δρομολογητές (router)
  - Σημεία ασύρματης πρόσβασης
  - Υποδομές διαχείρισης κλειδιών κτλ.

# Υλοποίηση Ασφάλειας (Security Implementation) – 3/3

- Πραγματοποιείται η υλοποίηση, εγκατάσταση και λειτουργία:
  - του απαιτούμενου εξοπλισμού ασφάλειας (υλικού και λογισμικού)
    - π.χ η εγκατάσταση και παραμετροποίηση firewall, IDS, anti-virus, PKI, κτλ.
  - η παραμετροποίηση των συστημάτων και των εφαρμογών
    - π.χ. η διαμόρφωση των χρηστών Λ.Σ. και εφαρμογών, των δικαιωμάτων πρόσβασης κτλ.

# Παρακολούθηση Ασφάλειας (Security Monitoring)

- Περιλαμβάνει εργασίες όπως:
  - την καθημερινή παρακολούθηση ορθής λειτουργίας των συστημάτων
    - αρχεία καταγραφής (log files) Λ.Σ./εφαρμογών
    - Έλεγχος χρηστών και δικαιωμάτων
  - την τακτική ενημέρωση/ επικαιροποίηση των εφαρμογών και συστημάτων ασφάλειας
    - π.χ. κανόνων πρόσβασης του firewall, IDS
    - ενημέρωση (update) του anti-virus, IDS, κτλ.
  - την παρακολούθηση των εξειδικευμένων μηχανισμών εντοπισμού πιθανών προβλημάτων ασφάλειας όπως
    - firewall/IDS/ani-virus alerts, κτλ

# Επιβεβαίωση Ασφάλειας (Security Assurance) – 2/2

- Στο στάδιο αυτό πραγματοποιούνται έλεγχοι για:
  - την διασφάλιση της πλήρους και ορθής εφαρμογής των επιλεγμένων μέτρων
  - της αποτελεσματικότητας των μέτρων να αντιμετωπίσουν τα πραγματικά και πιθανώς μεταβαλλόμενα προβλήματα ασφάλειας

- Οι έλεγχοι αυτοί μπορεί να είναι
  - εσωτερικοί (internal audits) ή
  - εξωτερικοί έλεγχοι από ανεξάρτητους φορείς (external or independent audits)

# Επιβεβαίωση Ασφάλειας (Security Assurance) – 1/2

- Η διεξαγωγή των ελέγχων μπορεί να στηρίζεται σε
  - ερωτηματολόγια ελέγχου διαδικασιών (checklists)
  - τεχνικούς ελέγχους, penetration tests κτλ.

- Ανάλογα με τα αποτελέσματα των ελέγχων ενδέχεται να προκύψει η ανάγκη για αναθεώρηση της στρατηγικής ασφάλειας.

- Ο έλεγχος της αναθεώρησης θα πρέπει να πραγματοποιείται ανεξάρτητα από το εάν θα γίνουν τελικά οι αλλαγές ή όχι.

# Σύστημα Διαχείρισης Ασφάλειας Π.Σ. (ΣΔΑΠ)

- Ένα Σύστημα Διαχείρισης Ασφάλειας Π.Σ. (Information Security Management System – ISMS) ορίζεται ως:
  - Ένα (υπο-) σύστημα διοίκησης (management system) το οποίο βασίζεται σε μία προσέγγιση επικινδυνότητας (risk-based approach), με σκοπό τον ορισμό, την εφαρμογή, λειτουργία, παρακολούθηση, επικαιροποίηση και βελτίωση της ασφάλειας ενός Π.Σ.
- Το βασικό πρότυπο για τη δημιουργία ενός ΣΔΑΠ είναι το πρότυπο ISO 27001) (πρώην ISO 17799)

# Σύστημα Διαχείρισης Ασφάλειας ISO 27001

- Είναι de facto standard για τον καθορισμό ενός ΣΔΑΠ
- Ακολουθεί τη δομή προτύπων συστημάτων διοίκησης
- Είναι συμβατό με άλλα ISO πρότυπα συστημάτων διοίκησης όπως ISO 9001, 14001, 18001, κτλ.
- Ακολουθεί ένα «κύκλο ζωής», το μοντέλο PDCA (Plan-Do-Check-Act)

# Μοντέλο PDCA του προτύπου ISO 27001

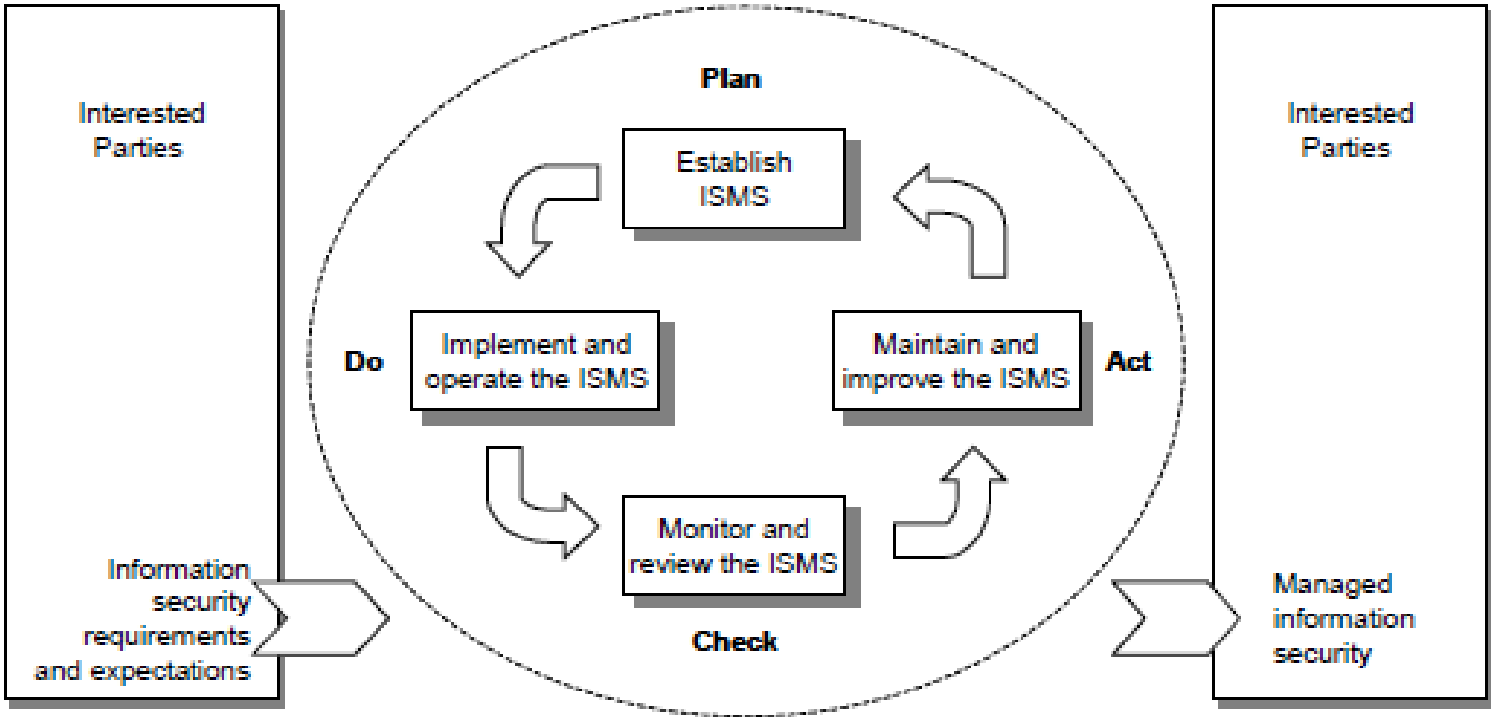



Figure 1 — PDCA model applied to ISMS processes

Πηγή: ISO 27001:2005

# *1. Διαχείριση Ασφάλειας και Ιδιωτικότητας*

1. Βασικές έννοιες διαχείρισης ασφάλειας Π.Σ.
2. Ο κύκλος ζωής της Ασφάλειας – Συστήματα διαχείρισης ασφάλειας
3. **Ανάλυση Επικινδυνότητας – Μεθοδολογίες και Πρότυπα**
4. Πολιτική Ασφάλειας και Πρότυπα
5. Σχέδιο Επιχειρησιακής Συνέχειας / Σχέδιο Ανάκαμψης Καταστροφών και Πρότυπα
6. Εργαλεία Διαχείρισης Ασφάλειας

# Ανάλυση Επικινδυνότητας

- Ως ***Επικινδυνότητα ή Πληροφοριακός Κίνδυνος (Information Risk)*** ενός Π.Σ. ορίζεται ως συνάρτηση τριών παραγόντων, που είναι:
  1. Οι ***απειλές*** που αντιμετωπίζουν τα επιμέρους πληροφοριακά αγαθά του Π.Σ.
  2. οι πιθανές ***αδυναμίες*** του Π.Σ. έναντι των απειλών και
  3. οι ***συνέπειες*** ή οι ***επιπτώσεις*** που θα υπάρξουν από την πραγματοποίηση των απειλών
- Η ***Ανάλυση Επικινδυνότητας*** αφορά τον προσδιορισμό του κινδύνου του Π.Σ. και την εκτίμηση του μεγέθους του κινδύνου για κάθε επιμέρους αγαθό.

# Διαχείριση Επικινδυνότητας

- Η **Διαχείριση Επικινδυνότητας** επιτρέπει την επιλογή των κατάλληλων μέτρων προστασίας. Οι κίνδυνοι μπορεί να:
  - ***αντιμετωπιστούν*** από μέτρα ασφάλειας,
  - ***παραβλεφθούν***, αναλαμβάνοντας τον κίνδυνο,
  - ή ***μεταφερθούν*** π.χ. μέσω ασφάλισης.

- Η απόφαση αυτή λαμβάνεται από τη Διοίκηση μετά από **ανάλυση «κόστους/ οφέλους»** (cost/benefit analysis).

# Ποσοτική Ανάλυση Κινδύνου (1/2)

- Λαμβάνει υπόψη δύο βασικά στοιχεία:
  - Την πιθανότητα (probability) να συμβεί ένα γεγονός και
  - την ενδεχόμενη συνέπεια (impact) που θα μπορούσε να προκαλέσει το γεγονός
- Χρησιμοποιεί το Εκτιμώμενο Ετήσιο Κόστος – ΕΕΚ (Annual Loss Expectancy)
  - ΕΕΚ = πιθανότητα Χ συνέπεια
- Παράδειγμα
  - πιθανή συνέπεια αποκάλυψης αρχείου πελατών: 10.000 €
  - πιθανότητα αποκάλυψης αρχείων: 5%

**ΕΕΚ = 10.000 × 5/100 = 500 €**

# Ποσοτική Ανάλυση Κινδύνου (2/2)

- Με βάση το ΕΕΚ μπορούν να ταξινομηθούν οι κίνδυνοι
- Προβλήματα:
  - Αναξιοπιστία στον υπολογισμό της πιθανότητας να συμβεί ένα γεγονός και
  - Δεν συσχετίζει τα διάφορα γεγονότα αλλά τα αντιμετωπίζει μεμονωμένα
- Λόγω της απλότητας, χρησιμοποιείται ακόμα από ορισμένους μικρούς/ μεσαίους οργανισμούς

# Ποιοτική Ανάλυση Κινδύνου

- Προσπάθεια περισσότερο «αντικειμενικής» ανάλυσης
- Δεν χρησιμοποιεί στατικά δεδομένα πιθανότητας αλλά χρησιμοποιεί στη θέση τους
  - Επίπεδα Απειλής και
  - Επίπεδα Αδυναμίας έναντι της απειλής
- Εξακολουθεί να χρησιμοποιεί την εκτίμηση της συνέπειας

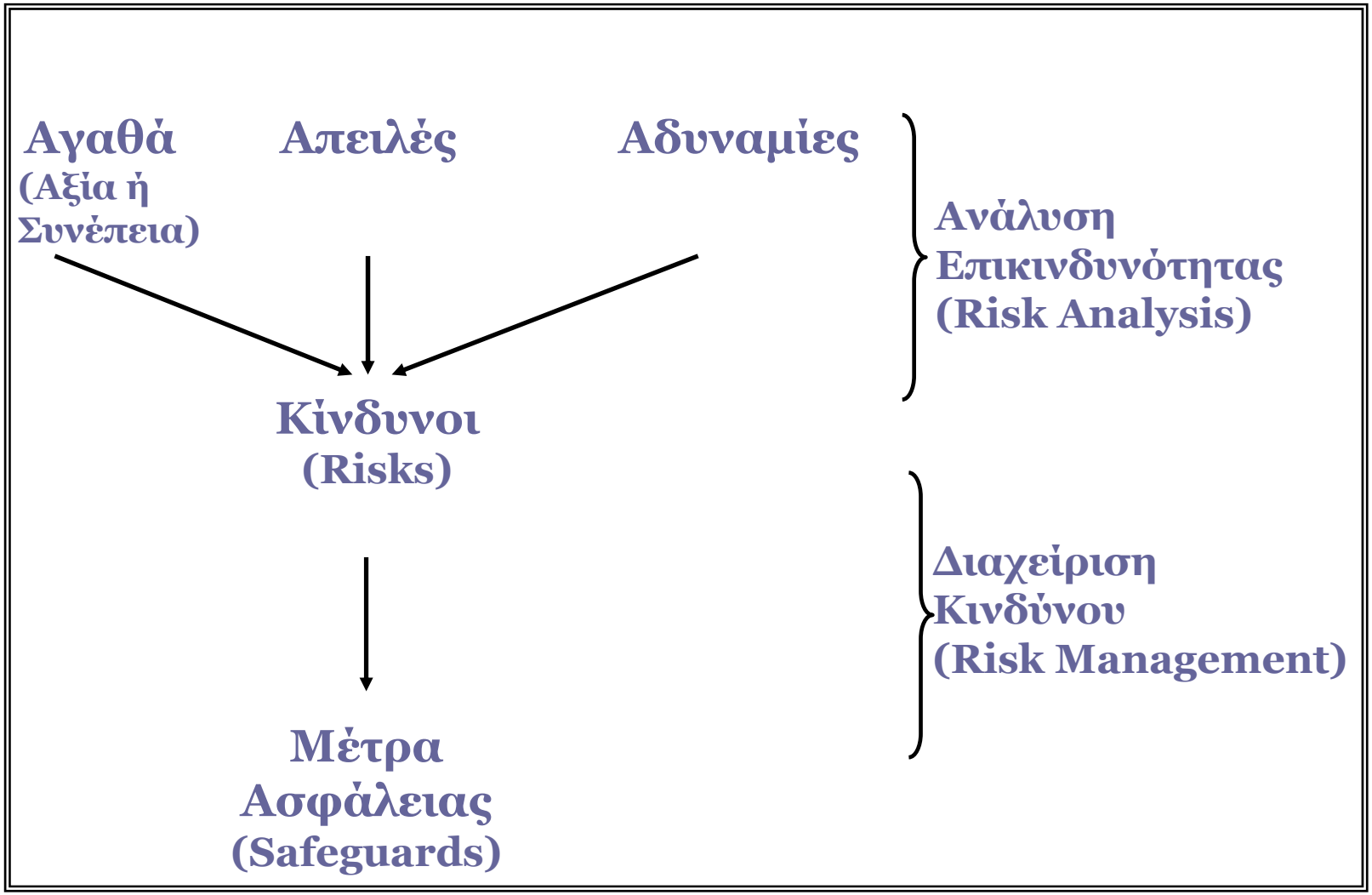
# Α. Φάση Ανάλυσης Κινδύνου

- Περιλαμβάνει:
  1. Τον καθορισμό των **στόχων**
  2. Τη σύσταση της **ομάδας έργου**
  3. Την επιλογή της **μεθοδολογίας** και των **εργαλείων**
  4. Τον προσδιορισμό και τη **μέτρηση του κινδύνου**. Αυτό το στάδιο περιλαμβάνει τις παρακάτω επιμέρους εργασίες:
     - Τον καθορισμό των ορίων του έργου
     - Την καταγραφή των αγαθών και την εκτίμηση των Συνεπειών
     - Την ανάλυση και εκτίμηση Απειλών
     - Την ανάλυση και εκτίμηση Αδυναμιών
     - Τον υπολογισμό και τη μέτρηση των πληροφοριακών Κινδύνων

# Β. Φάση Διαχείρισης Κινδύνου

- Περιλαμβάνει:
  5. Τον καθορισμό **κριτηρίων αποδοχής κινδύνων**
  6. Την **αντιμετώπιση των κινδύνων**. Αυτό το στάδιο περιλαμβάνει τις παρακάτω επιμέρους εργασίες:
     - Την επιλογή των κατάλληλων μέτρων ασφάλειας που περιορίζουν τη συνολική επικινδυνότητα στα ανεκτά επίπεδα
     - Την ανάλυση κόστους-οφέλους
     - Την τελική έκθεση για τη λήψη αποφάσεων

# Λειτουργική σύνδεση



# Α1. Καθορισμός Στόχων και Σύσταση Ομάδας Έργου

- Οι στόχοι πρέπει να καθορίζονται στο ανώτατο διοικητικό επίπεδο
- Η διοίκηση ορίζει επίσης τους αναγκαίους οικονομικούς πόρους και τους υπεύθυνους υλοποίησης
- Η Ομάδα Έργου έχει την ευθύνη για την επίτευξη των στόχων
  - Μπορεί να συσταθεί από υπάρχων προσωπικό με σχετική πείρα σε θέματα πληροφορικής
  - Ο επικεφαλής της Ομάδας Έργου θα πρέπει να έχει ευρεία γνώση θεμάτων ασφάλειας ΠΣ.

# Α2. Επιλογή Μεθοδολογίας και Εργαλείων Ανάλυσης & Διαχείρισης Κινδύνου

- Υπάρχει μεγάλη γκάμα μεθοδολογιών και αυτοματοποιημένων εργαλείων
  - CRAMM
  - OCTAVE
  - COBRA
  - EBIOS
  - …
- Βασικοί παράμετροι κάθε μεθοδολογίας:
  - Να λαμβάνει υπόψη την τρέχουσα κατάσταση ασφάλειας
  - Να οδηγεί σε καθορισμό στρατηγικής και στόχους ασφάλειας ώστε με βάση αυτά να εκτιμάται η αποτελεσματικότητα κάθε μέτρου ασφάλειας πριν την επιλογή του.

# Α3. Προσδιορισμός και Μέτρηση Κινδύνου

- Θα πρέπει να έχει όσο το δυνατό πιο μεγάλο εύρος ώστε
  1. η διοίκηση να έχει καλή επίγνωση της παρούσας κατάστασης της ασφάλειας πληροφοριών και
  2. η διοίκηση να έχει επαρκείς βάσεις για τον καθορισμό κριτηρίων αποδοχής κινδύνου και προτεραιοτήτων αντιμετώπισης κινδύνου.

# Α3.1. Καθορισμός των ορίων του έργου

- Απαραίτητος για την αποτελεσματικότητα και ταχύτητα της μέτρησης του κινδύνου

- Καταγράφεται το εύρος του έργου (τι περιλαμβάνεται στη μελέτη)
  - Επιχειρησιακές λειτουργίες
  - Οργανωτικά τμήματα
  - Συστήματα (υλικό, λογισμικό, δεδομένα)

- Καταγράφονται περιορισμοί (τι δεν περιλαμβάνεται)
  - Αποφεύγεται η σπατάλη ανθρώπινων και οικονομικών πόρων για προβλήματα ασφάλειας εκτός των ορίων που έχει θέσει η διοίκηση.

# Α3.2. Καταγραφή αγαθών και εκτίμηση συνεπειών (1/3)

- Καταγράφονται όλα τα αγαθά που ανήκουν στο εύρος του έργου
  - Φυσικά αγαθά (κτήρια, υπολογιστικά συστήματα κτλ)
  - Λογισμικά Αγαθά
  - Αγαθά Δεδομένων
- Γίνεται εκτίμηση των άμεσων και έμμεσων συνεπειών
  - Άμεσες συνέπειες (κόστος επαναγοράς)
  - Έμμεσες Συνέπειες
    - Παρεμπόδιση Λειτουργίας
    - Νομικές Συνέπειες
    - Δυσφήμιση
    - ...

# Α3.2. Καταγραφή αγαθών και εκτίμηση συνεπειών (2/3)

- Γίνεται εκτίμηση των συνεπειών για κάθε αγαθό, ως προς πιθανές απώλειες ασφάλειας
  - Αποκάλυψη αγαθού (απώλεια εμπιστευτικότητας)
  - Τροποποίηση αγαθού (απώλεια ακεραιότητας)
  - Μη διαθεσιμότητα αγαθού (απώλεια διαθεσιμότητας)
- Κάθε συνέπεια λαμβάνει κάποιου είδους βαθμολογία
  - Σε οικονομικές τιμές ή
  - Σε κάποια ποιοτική κλίμακα
    - Υψηλές συνέπειες
    - Μέτριες συνέπειες
    - Χαμηλές συνέπειες

# Α3.2. Καταγραφή αγαθών και εκτίμηση συνεπειών (3/3)

- Για την αντικειμενική και αξιόπιστη εκτίμηση των συνεπειών, πραγματοποιούνται συνεντεύξεις με τους Ιδιοκτήτες των αγαθών
- Οι Ιδιοκτήτες αγαθών ενδέχεται να υποδείξουν και κατάλληλους χρήστες οι οποίοι έχουν κατάλληλη γνώση της αξίας των αγαθών
- Μεγάλη σημασία έχει η εμπειρία του αναλυτή

# Α3.3. Ανάλυση και εκτίμηση απειλών

- Καθορίζονται και εκτιμώνται οι απειλές που μπορούν να πλήξουν το Π.Σ.
- Και σε αυτό το βήμα απαιτούνται συνεντεύξεις με τους Ιδιοκτήτες ή/και χρήστες των αγαθών
- Πηγές πιθανών απειλών
  - Πίνακες από αυτοματοποιημένα εργαλεία
  - Διαθέσιμες στατιστικές μελέτες (π.χ. από το Internet)
  - Εσωτερικές στατιστικές / καταγραφή περιστατικών
  - Αρχεία καταγραφής συστημάτων (Log files)

# Παραδείγματα απειλών ασφάλειας

| | Απειλή |
|---|---|
| 1. | Πλαστοπροσωπία Χρήστη από κακόβουλους Εσωτερικούς Χρήστες |
| 2. | Πλαστοπροσωπία Χρήστη από κακόβουλους Συνεργάτες |
| 3. | Πλαστοπροσωπία Χρήστη από κακόβουλους Εξωτερικούς Χρήστες |
| 4. | Μη εξουσιοδοτημένη χρήση Εφαρμογής |
| 5. | Παρακολούθηση Επικοινωνίας |
| 6. | Παραποίηση Επικοινωνίας |
| 7. | Αποποίηση πράξης από Χρήστη |
| 8. | Αποτυχία Επικοινωνίας |
| 9. | Είσοδος κακόβουλου κώδικα (virus, Trojan, spam, hoaxes κτλ) |
| 10. | Τυχαίο λάθος δρομολόγησης επικοινωνίας |
| 11. | Εσκεμμένη τροποποίηση δρομολόγησης επικοινωνίας |
| 12. | Λανθασμένη χρήση συστήματος |
| 13. | Τεχνική βλάβη υπολογιστή |
| 14. | Βλάβη κλιματισμού |
| 15. | Βλάβη λογισμικού συστήματος |
| 16. | Βλάβη λογισμικού διαχείρισης δικτύου |
| 17. | Λάθος διαχείρισης συστήματος ή δικτύου |
| 18. | Λάθος συντήρησης υλικού (hardware) |
| 19. | Λάθος συντήρησης λογισμικού (software) |
| | |
| 20. | Έλλειψη προσωπικού |
| 21. | Τεχνική βλάβη εγκατάστασης (παροχή ρεύματος, τηλεφώνου κτλ) |
| 22. | Τεχνική βλάβη εκτυπωτών |
| 23. | Τεχνική βλάβη δικτυακού εξοπλισμού (hub, router, switch κτλ) |
| 24. | Τεχνική βλάβη Gateway |
| 25. | Τεχνική βλάβη συστήματος ελέγχου πρόσβασης (firewall) |
| 26. | Τεχνική βλάβη συστήματος εντοπισμού εισβολών (IDS) |
| 27. | Τεχνική βλάβη υπολογιστή διαχείρισης δικτύου ή λειτουργιών |
| 28. | Τεχνική βλάβη υπηρεσίας πρόσβασης διαδικτύου (Internet access) |
| 29. | Τεχνική βλάβη άλλης δικτυακής υπηρεσίας (ftp, web mail κτλ) |
| 30. | Τεχνική βλάβη υπηρεσίας e-mail |
| 31. | Βλάβη λογισμικού εφαρμογών (application software) |
| 32. | Λάθος χειρισμού δεδομένων |

# Α3.4. Ανάλυση και εκτίμηση αδυναμιών

- Γίνεται εκτίμηση τεχνικών και οργανωτικών αδυναμιών ασφάλειας, δηλαδή χαρακτηριστικά του Π.Σ. τα οποία επιτρέπουν την εμφάνιση απειλών με:
  - Μεγαλύτερη συχνότητα
  - Μεγαλύτερες συνέπειες
  - Συνδυασμό των παραπάνω
- Και σε αυτό το βήμα απαιτούνται συνεντεύξεις με τους Ιδιοκτήτες ή/και χρήστες των αγαθών
- Είναι χρήσιμη σε αυτή τη φάση η καταγραφή των υφισταμένων μέτρων ασφάλειας
  - Τα υφιστάμενα μέτρα ασφάλειας μειώνουν τις αδυναμίες ασφάλειας
  - Πιθανή έλλειψη μέτρων αυξάνει τις αδυναμίες ασφάλειας

# Παραδείγματα επιπέδων απειλής και επιπέδων αδυναμίας

| Επίπεδο Απειλής | Περιγραφή |
|---|---|
| Χαμηλό | Αυτή η εκτίμηση απειλής δίδεται σε γεγονότα τα οποία αναμένεται να συμβούν το πολύ μέχρι 1 φορά το χρόνο. |
| Μεσαίο | Αυτή η εκτίμηση απειλής δίδεται σε γεγονότα τα οποία αναμένεται να συμβούν το από 2 μέχρι 5 φορές το χρόνο |
| Υψηλό | Αυτή η εκτίμηση απειλής δίδεται σε γεγονότα τα οποία αναμένεται να συμβούν πάνω από 5 φορές το χρόνο. |

| Επίπεδο Αδυναμίας | Περιγραφή |
|---|---|
| Χαμηλό | Σε περίπτωση που συνέβαινε μία απειλή, θα υπήρχε το πολύ 30% πιθανότητα να εκδηλωθεί το χειρότερο σενάριο συνεπειών, με βάση την εκτίμηση συνέπειας που έχει πραγματοποιηθεί. |
| Μεσαίο | Σε περίπτωση που συνέβαινε μία απειλή, θα υπήρχε από 30% μέχρι 70% πιθανότητα να εκδηλωθεί το χειρότερο σενάριο συνεπειών, με βάση την εκτίμηση συνέπειας που έχει πραγματοποιηθεί. |
| Υψηλό | Σε περίπτωση που συνέβαινε μία απειλή, θα υπήρχε πάνω από 70% πιθανότητα να εκδηλωθεί το χειρότερο σενάριο συνεπειών, με βάση την εκτίμηση συνέπειας που έχει πραγματοποιηθεί. |

# Α3.5. Υπολογισμός και μέτρηση κινδύνου

- Αξιολογούνται και συσχετίζονται όλες οι προηγούμενες πληροφορίες
- Για κάθε πιθανό συνδυασμό αγαθού - συνέπειας – απειλής – αδυναμίας
- Για κάθε συνδυασμό, κάθε κίνδυνος μπορεί να έχει είτε ποιοτική είτε ποσοτική μέτρηση
  - Χαμηλός – Μέτριος – Υψηλός κίνδυνος
  - Κλίμακα 1 – 2 – 3 – 4 – 5 – 6 – 7 – 8

# Παράδειγμα πίνακα εκτίμησης κινδύνου

| ΕΠΙΠΕΔΟ ΑΠΕΙΛΗΣ | | Χαμηλό | | | Μεσαίο | | | Μεγάλο | | |
|---|---|---|---|---|---|---|---|---|---|---|
| ΕΠΙΠΕΔΟ ΑΔΥΝΑΜΙΑΣ | | Χαμηλό | Μεσαίο | Μεγάλο | Χαμηλό | Μεσαίο | Μεγάλο | Χαμηλό | Μεσαίο | Μεγάλο |
| ΑΞΙΑ ή ΣΥΝΕΠΕΙΑ ΑΓΑΘΟΥ | Ε | 0 | 1 | 2 | 1 | 2 | 3 | 2 | 3 | 4 |
| | Δ | 1 | 2 | 3 | 2 | 3 | 4 | 3 | 4 | 5 |
| | Γ | 2 | 3 | 4 | 3 | 4 | 5 | 4 | 5 | 6 |
| | Β | 3 | 4 | 5 | 4 | 5 | 6 | 5 | 6 | 7 |
| | Α | 4 | 5 | 6 | 5 | 6 | 7 | 6 | 7 | 8 |

# Β4. Καθορισμός κριτηρίων αποδοχής κινδύνων

- Η αντιμετώπιση όλων των κινδύνων, συνήθως δεν είναι εφικτή, ούτε και αποδοτική
- Η διοίκηση του οργανισμού σε συνεργασία με τον επικεφαλής ή/και την Ομάδα Έργου καθορίζει κριτήρια αποδοχής κινδύνων
- Παράδειγμα
  - Επίπεδα κινδύνων με βαθμολογία **<3** είναι αποδεκτά

# Β5. Αντιμετώπιση κινδύνων

- Περιλαμβάνει
  - Την πρόταση συγκεκριμένων μέτρων ασφάλειας και την κοστολόγησή τους
  - Την ανάλυση κόστους-οφέλους
  - Την τελική έκθεση και τη λήψη αποφάσεων

# Β5.1. Επιλογή μέτρων ασφάλειας

- Περιλαμβάνει μέτρα που μειώνουν τους κίνδυνους που έχουν εντοπιστεί
  - Είτε μειώνοντας την πιθανότητα εκδήλωσης της απειλής
  - Είτε μειώνοντας την αδυναμία του αγαθού (αγαθών) έναντι της απειλής
- Για κάθε μέτρο ασφάλειας γίνεται κοστολόγηση ώστε να χρησιμοποιηθεί στο επόμενο στάδιο
- Τα αυτοματοποιημένα εργαλεία περιλαμβάνουν λίστες προτεινόμενων μέτρων ασφάλειας και πιθανώς εκτίμηση κόστους και οφέλους για κάθε μέτρο

# B5.2. Ανάλυση κόστους- οφέλους

- Περιλαμβάνει την εκτίμηση του βαθμού μείωσης του κινδύνου μετά την εφαρμογή ενός προτεινόμενου μέτρου ασφάλειας σε συνδυασμό με το κόστος εφαρμογής των μέτρων.
- Παράδειγμα. Έστω ότι:
  - b: Καθαρό Όφελος Μέτρου
  - B: Ακαθάριστο Όφελος Μέτρου λόγω εκτιμώμενης μείωσης κινδύνου
  - C: Κόστος Εφαρμογής Μέτρου (ανά έτος)
- Τότε η ανάλυση κόστους-οφέλους για κάθε μέτρο υπολογίζεται από τη σχέση

$$b = B - C$$

# Β5.3. Τελική έκθεση και λήψη αποφάσεων

- Περιλαμβάνει συνοπτικά τα αποτελέσματα όλων των προηγούμενων φάσεων
  - Σημαντικότερους κινδύνους, απειλές, αδυναμίες
  - Επιλογή μέτρων ασφάλειας και ανάλυση κόστους-οφέλους
  - Προτάσεις για τη λήψη μέτρων ασφάλειας
    - Τα μέτρα με τον καλύτερο δυνατό βαθμό καθαρού οφέλους
    - Τα μέτρα που μειώνουν όλους του κινδύνους κάτω από το επίπεδο αποδοχής που έχει τεθεί στη φάση Β4 (Καθορισμός κριτηρίων αποδοχής κινδύνων)
- Οι τελικές αποφάσεις λαμβάνονται από τη Διοίκηση του οργανισμού

# Παράδειγμα προτεινόμενων μέτρων διαχείρισης κινδύνων

| Αγαθό | Απειλή | Επικινδυνό-τητα απειλής | Προτεινόμενο Μέτρο Ασφάλειας | Εκτίμηση Κόστους Μέτρου Ασφάλειας | Νέο επίπεδο επικινδυνό-τητας | Παρατηρήσεις |
|---|---|---|---|---|---|---|
| Web server (Apache web server) | Τροποποίηση ιστοσελίδας (Web defacement) | 5 | Patching και αλλαγή configuration | 0 (περιλαμβά-νεται στους όρους συντήρησης) | 2 | Χρειάζεται εκπαίδευση προσωπικού για τη συντήρηση μετά το λήξη της σύμβασης |
| | | | | | | |

# Πρότυπα και μεθοδολογίες ανάλυσης επικινδυνότητας

- ISO 27005:2008
  - Πρότυπο για την ανάλυση και διαχείριση επικινδυνότητας
  - Περιγράφει γενικές απαιτήσεις και όχι συγκεκριμένη μεθοδολογία
- Μεθοδολογίες και εργαλεία
  - CRAMM
    - Μεθοδολογία και εργαλείο
    - Εμπορικό προϊόν
  - COBRA (http://www.riskworld.net/)
    - Μεθοδολογία και εργαλείο
    - (Μέχρι πρόσφατα) δωρεάν δοκιμαστική έκδοση
  - EBIOS (http://www.ssi.gouv.fr/archive/en/confidence/ebiospresentation.html)
    - Μεθοδολογία και εργαλείο
    - Δωρεάν λογισμικό
  - OCTAVE (http://www.cert.org/octave/)
    - Μεθοδολογία και εργαλείο
    - Εμπορικό προϊόν (παρέχει δωρεάν οδηγό εφαρμογής – implementation guide)
  - MEGERIT (http://www.csi.map.es/csi/pg5m20.htm)
    - Μεθοδολογία και εργαλείο
    - Εμπορικό προϊόν (δωρεάν δοκιμαστική έκδοση εφαρμογής – https://www.ccn-cert.cni.es/publico/herramientas/pilar43/tools/index.html)

# *1. Διαχείριση Ασφάλειας και Ιδιωτικότητας*

1. Βασικές έννοιες διαχείρισης ασφάλειας Π.Σ.
2. Ο κύκλος ζωής της Ασφάλειας – Συστήματα διαχείρισης ασφάλειας
3. Ανάλυση Επικινδυνότητας – Μεθοδολογίες και Πρότυπα
4. **Πολιτική Ασφάλειας και Πρότυπα**
5. Σχέδιο Επιχειρησιακής Συνέχειας / Σχέδιο Ανάκαμψης Καταστροφών και Πρότυπα
6. Εργαλεία Διαχείρισης Ασφάλειας

# Τι είναι Πολιτική;

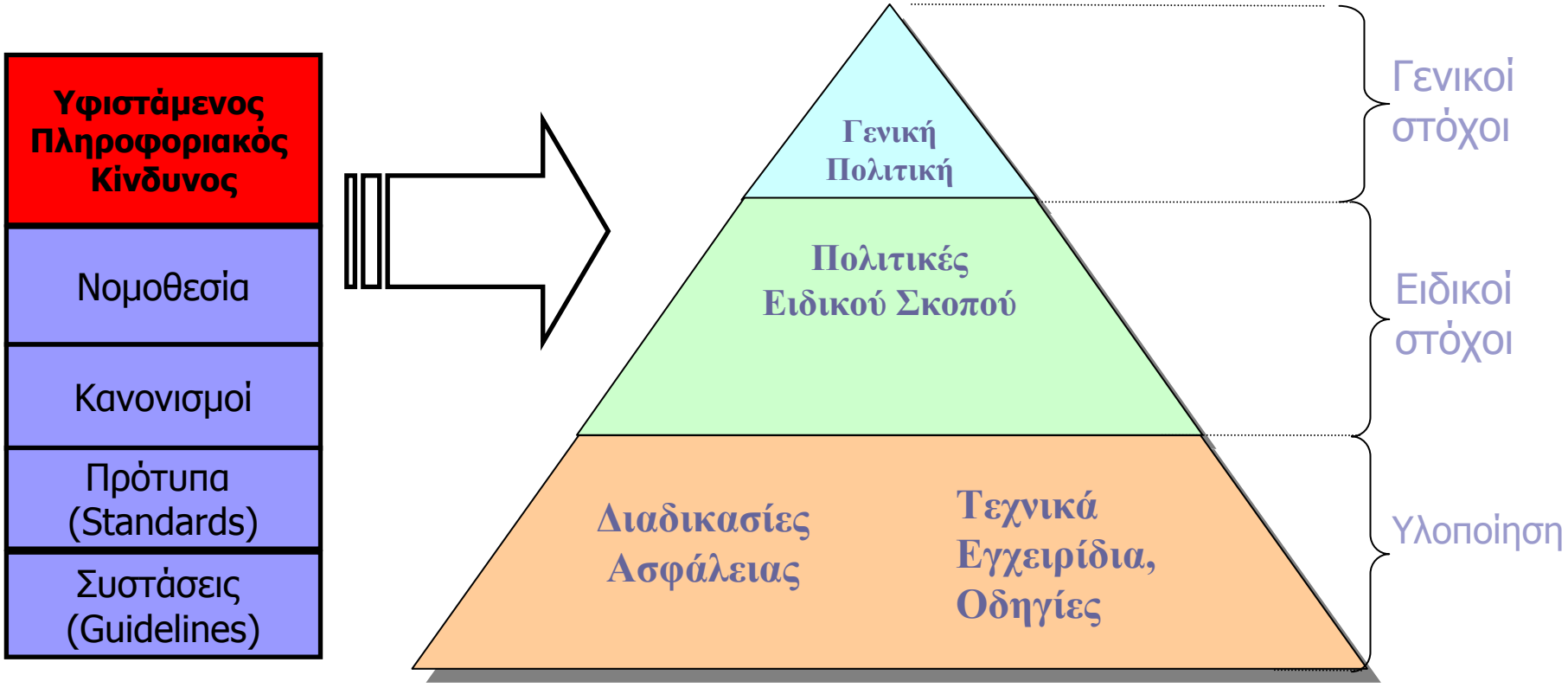
- **Πολιτική (Policy):** *«Ένα σύνολο από* ***γενικές αρχές, πεποιθήσεις*** *και* ***στόχους****, το οποίο καθορίζει ένα ευρύτερο πλαίσιο υποχρεώσεων, δεσμεύσεων και απαγορεύσεων για την επίτευξη ενός σκοπού».*
- Δεν περιλαμβάνει λεπτομέρειες υλοποίησης.

# Πολιτική Ασφάλειας Πληροφοριακού Συστήματος

- Έγγραφο το οποίο περιλαμβάνει τον καθορισμό των γενικών αρχών που πρέπει να ισχύουν για την ασφάλεια των:
  - Πληροφοριών
  - Υπολογιστικών συστημάτων και λογισμικού
  - Δικτύων και υποδομών

  ενός οργανισμού και την επαρκή προστασία από τους υφιστάμενους πληροφοριακούς κινδύνους
- Η Πολιτική Ασφάλειας είναι έγγραφο με **ιεραρχική δομή** και **top-down προσέγγιση**

# Δομή Πολιτικής Ασφάλειας



# Γενική Πολιτική Ασφάλειας (1/3)

1. Θέτει τους **στρατηγικούς στόχους** και τις κατευθύνσεις του οργανισμού.

2. Περιλαμβάνει σαφή **δέσμευση** της **ανώτατης διοίκησης**

3. Δεσμεύει **πόρους** για την επίτευξή των στόχων

# Γενική Πολιτική Ασφάλειας (2/3)

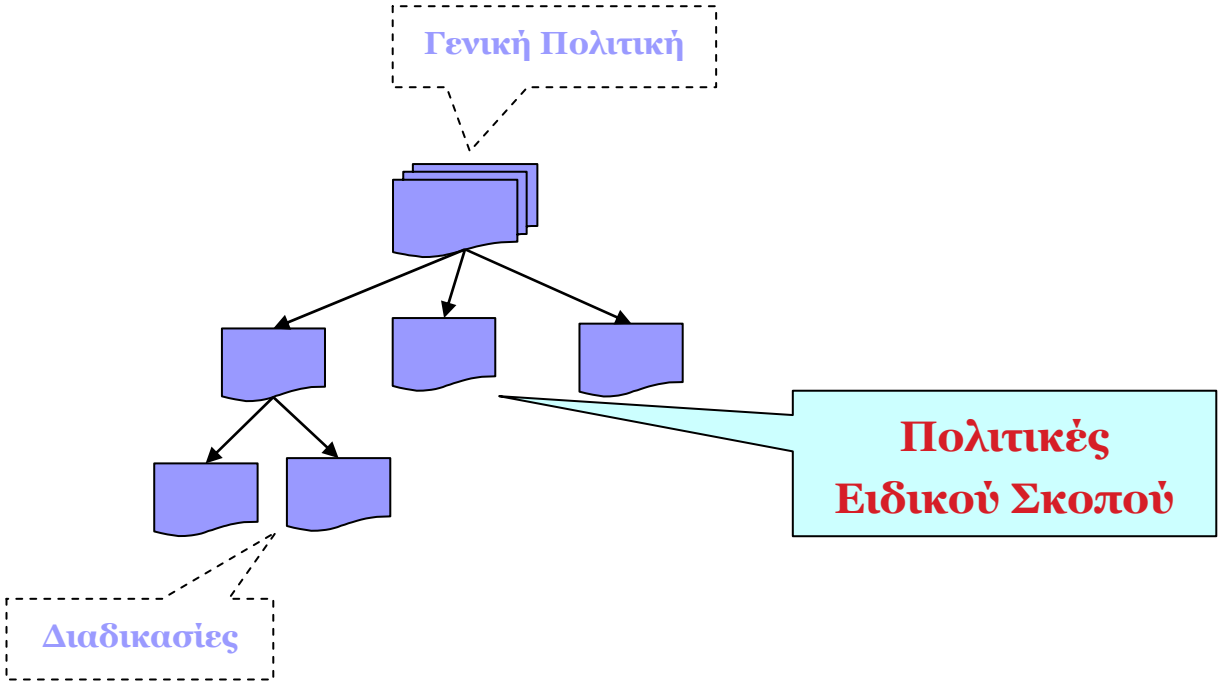
4. Ορίζει τους **ρόλους** που εμπλέκονται στο σύνολο της Πολιτικής, καθώς και τις σχετικές τους **αρμοδιότητες**

Παραδείγματα:

- Υπεύθυνος Ασφάλειας Π.Σ
- Υπεύθυνος Συστήματος
- Διαχειριστής Συστήματος
- Ομάδα Αντιμετώπισης Περιστατικών Ασφάλειας

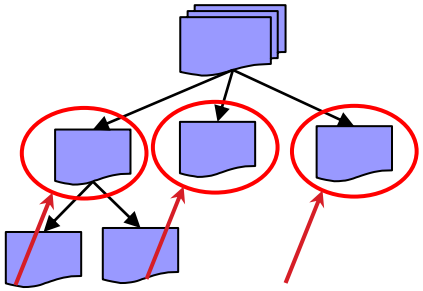
# Γενική Πολιτική Ασφάλειας (3/3)

5. Ορίζει τις **Πολιτικές Ειδικού Σκοπού**, οι οποίες και αποτελούν τμήμα της Πολιτική Ασφάλειας του οργανισμού (**modular approach**)



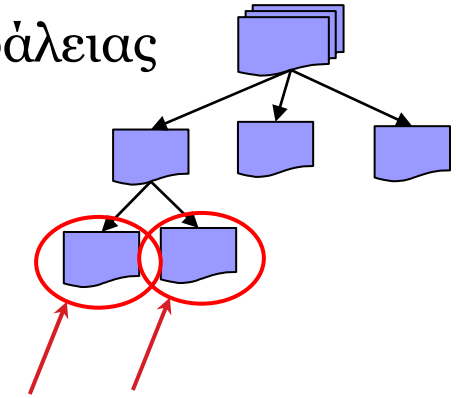
# Πολιτικές Ειδικού Σκοπού

- Αντιμετωπίζουν τα προβλήματα ασφάλειας που αφορούν **επιμέρους περιοχές** της ασφάλειας ή **ειδικά συστήματα**
- *Παραδείγματα:*
  - Πολιτική Λογικής Πρόσβασης
  - Πολιτική Φυσικής Πρόσβασης
  - Πολιτική Ανάπτυξης Συστημάτων και Εφαρμογών
  - Πολιτική Προστασίας από Ιούς
  - Πολιτική Αντιμετώπισης Περιστατικών Ασφάλειας
  - Πολιτική Συνέχειας Επιχειρηματικών Λειτουργιών



# Διαδικασίες Ασφάλειας

- Έγγραφα που περιγράφουν με **μεγάλο βαθμό λεπτομέρειας** συγκεκριμένες ενέργειες και εργασίες.
- Είναι μέρος της **υλοποίησης** της πολιτικής ασφάλειας
- Περιγράφουν:
  - *Τη ροή εργασιών και*
  - *τους εμπλεκόμενους ρόλους για μία εργασία*
- Παραδείγματα διαδικασιών
  - Διαδικασία εισαγωγής/διαγραφής χρηστών
  - Διαδικασία αντιμετώπισης περιστατικών ασφάλειας
  - Διαδικασία λήψης και διατήρησης εφεδρικών αρχείων
  - Διαδικασία ελέγχου φυσικής πρόσβασης



# Παράδειγμα: Διαδικασία χειρισμού περιστατικών ασφάλειας

# Πρότυπα Ασφάλειας

- Το ISO 27001 είναι πρότυπο για τον καθορισμό απαιτήσεων ασφάλειας και συστήματος διαχείρισης ασφάλειας (ΣΔΑΠ)
- Υπάρχουν πρότυπα για πολλούς τομείς της ασφάλειας. Μερικά βασικά πρότυπα είναι:
  - ISO 27002: Πρότυπο για την εφαρμογή ΣΔΑΠ με βάση τις απαιτήσεις ασφάλειας του 27001
  - ISO 27005: Πρότυπο για τη διαχείριση πληροφοριακού κινδύνου
  - ISO/IEC 7498-2 και ITU-T X.800: Πρότυπα ασφάλειας δικτύων

# Το πρότυπο ISO 27002

- Το ISO 27001 θέτει τις απαιτήσεις ασφάλειας, όχι τον τρόπο εφαρμογής τους
- ISO 27002:2005 – Κώδικας εφαρμογής
- Διεξοδικός κατάλογος κοινώς αποδεκτών μέτρων ασφάλειας
- Ανάλυση των μέτρων ασφάλειας του ISO 27001
- Αποτελεί βάση για την εφαρμογή του ISO 27001
- Μη πιστοποιήσιμο

# Το πρότυπο ISO 27005

- Το ISO 27005:2008 (Information security risk management) περιλαμβάνει οδηγίες για τη διαχείριση πληροφοριακού κινδύνου σε έναν οργανισμό
- Δεν παρέχει κάποια συγκεκριμένη μεθοδολογία
- Μπορούν να χρησιμοποιηθούν διάφορες μεθοδολογίες ανάλυσης και διαχείρισης πληροφοριακού κινδύνου, σύμφωνα με το πρότυπο 27005.

# Τα πρότυπα ISO 7498-2, ITU-T X.800

- Καθορίζει στόχους ασφάλειας για κάθε επίπεδο δικτύου
- Οι στόχοι ασφάλειας επιτυγχάνονται μέσω πολιτικών ασφάλειας (security policies):
  - το σύνολο κριτηρίων το οποίο ορίζει την παροχή υπηρεσιών ασφάλειας
- υπηρεσίες ασφάλειας (security services):
  - υπηρεσία η οποία παρέχεται από ένα επίπεδο δικτύου, προκειμένου να εξασφαλιστεί η επαρκής προστασία των συστημάτων ή των μεταδιδόμενων δεδομένων
- Μία υπηρεσία ασφάλειας υλοποιείται με τη βοήθεια κατάλληλων μηχανισμών ασφάλειας (security mechanisms)
  - μηχανισμοί που μπορούν να χρησιμοποιηθούν για να επιβάλουν τεχνικά την εφαρμογή μια υπηρεσίας ασφάλειας

# *1. Διαχείριση Ασφάλειας και Ιδιωτικότητας*

1. Βασικές έννοιες διαχείρισης ασφάλειας Π.Σ.
2. Ο κύκλος ζωής της Ασφάλειας – Συστήματα διαχείρισης ασφάλειας
3. Ανάλυση Επικινδυνότητας – Μεθοδολογίες και Πρότυπα
4. Πολιτική Ασφάλειας
5. **Σχέδιο Επιχειρησιακής Συνέχειας / Σχέδιο Ανάκαμψης Καταστροφών και Πρότυπα**
6. Εργαλεία Διαχείρισης Ασφάλειας

# Σχέδιο Επιχειρησιακής Συνέχειας
# Σχέδιο Ανάκαμψης από Καταστροφές

**Εισαγωγή**

Παρουσίαση εννοιών

Σχέση Σχεδίου Επιχειρησιακής Συνέχειας

και Σχεδίου Ανάκαμψης

**Διαχείριση Επιχειρησιακής Συνέχειας**

Ανάλυση

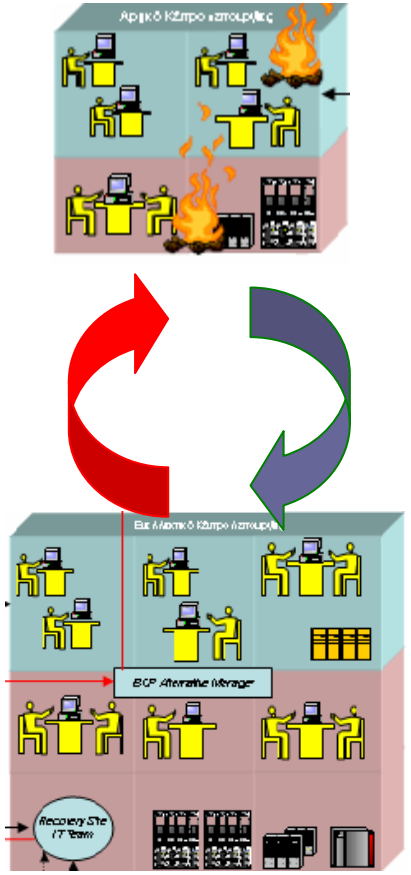
Σχεδιασμός

Υλοποίηση

Έλεγχος & Αποδοχή

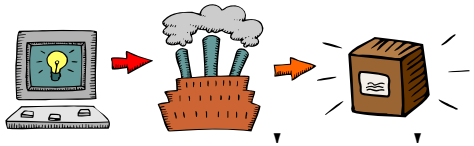
Συντήρηση

**Πηγές**

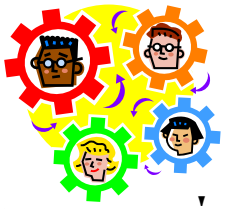


# Ορισμοί

- Επιχειρησιακή Λειτουργία



  - Το σύνολο των δραστηριοτήτων ενός οργανισμού που έχουν σχεδιαστεί για την παροχή μία αυτόνομης λειτουργίας του. Π.χ.
    - Πωλήσεις
    - Υποστήριξη δικτύου καταστημάτων
    - Marketing
    - Η-πωλήσεις



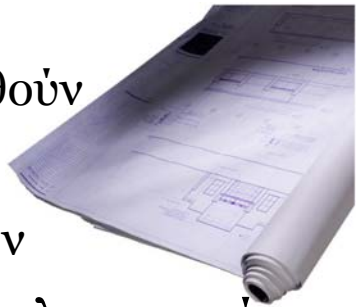
- Επιχειρησιακή Συνέχεια
  1. Η δυνατότητα ενός οργανισμού να συνεχίσει να παρέχει τις επιχειρησιακές λειτουργίες του, πρακτικά χωρίς σημαντικές συνέπειες, μετά από κάποια διακοπή ή κατά τη διάρκεια αυτής.
  2. Η μη διακοπή των κρίσιμων επιχειρησιακών λειτουργιών του οργανισμού.

# Γεγονότα πρόκλησης διακοπής λειτουργίας (Καταστροφές)

- Η διακοπή λειτουργίας μπορεί να οφείλεται σε:
  - ✓ Φυσική καταστροφή
    - Πλημμύρα
    - Πυρκαγιά
    - Σεισμός
  - ✓ Τεχνική βλάβη
    - Αστοχία υλικού, λογισμικού
    - Απώλεια δεδομένων
    - Απώλεια παροχών ενέργειας
  - ✓ Ανθρώπινη ενέργεια
    - Εσκεμμένη
      - Κακόβουλος κώδικας
      - Τρομοκρατική ενέργεια
      - Παρεμπόδιση εργασίας
      - Δολιοφθορά
    - Τυχαία
      - Λάθος χειρισμός εφαρμογής ή συστήματος
      - Λάθος συντήρησης εξοπλισμού

# Σχέδιο Επιχειρησιακής Συνέχειας (Business Continuity Plan)

- Ένα καταγεγραμμένο εγχειρίδιο το οποίο περιλαμβάνει
  - πλήρης οδηγίες για δράσεις (actions)
  - τις διαδικασίες (procedures) που πρέπει να ακολουθηθούν
  - τους πόρους (resources) που θα απαιτηθούν
  - τις συμφωνίες (agreements) που πρέπει να προηγηθούν



με σκοπό να διασφαλίσει ένας οργανισμός τη συνέχεια λειτουργίας των κρίσιμων επιχειρησιακών λειτουργιών πριν, κατά τη διάρκεια ή μετά από κάποια καταστροφή.

- Το Σχέδιο Επιχειρησιακής Συνέχειας είναι συνεχώς ενεργό – δεν απαιτείται κάποια διακοπή λειτουργίας για την ενεργοποίησή του.

# Σχέδιο Ανάκαμψης Συστημάτων (Disaster Recovery Plan)

- Ένα καταγεγραμμένο εγχειρίδιο το οποίο περιλαμβάνει πλήρης οδηγίες σχετικά με τα:
  - τεχνικά
  - οργανωτικά
  - και άλλα μέτρα

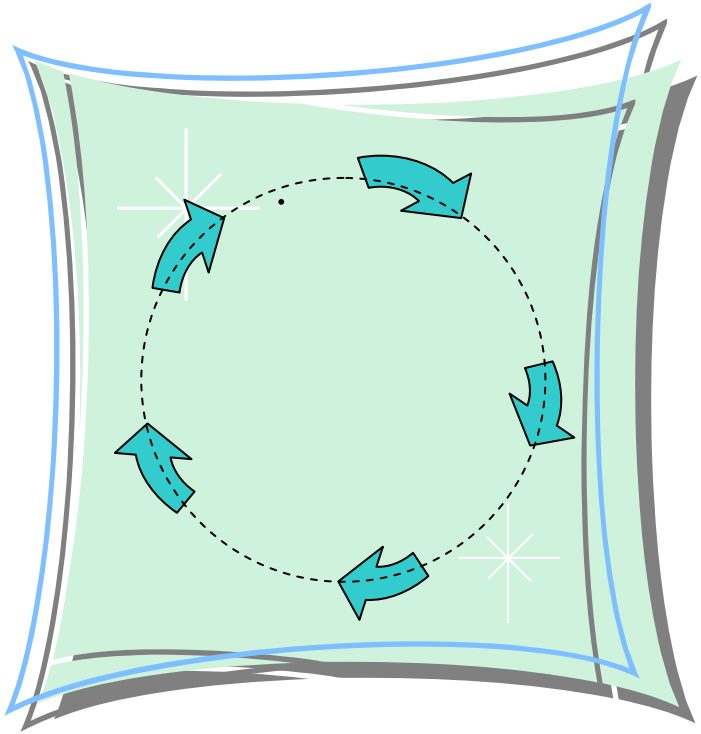
που ακολουθεί ένας οργανισμός με σκοπό να διασφαλίσει την έγκαιρη ανάκαμψη των συστημάτων του μετά από διακοπή λειτουργίας και την επαναφορά τους σε κανονική κατάσταση λειτουργίας.

- Το Σχέδιο Ανάκαμψης Συστημάτων ενεργοποιείται μετά από κάποια διακοπή λειτουργίας συστήματος

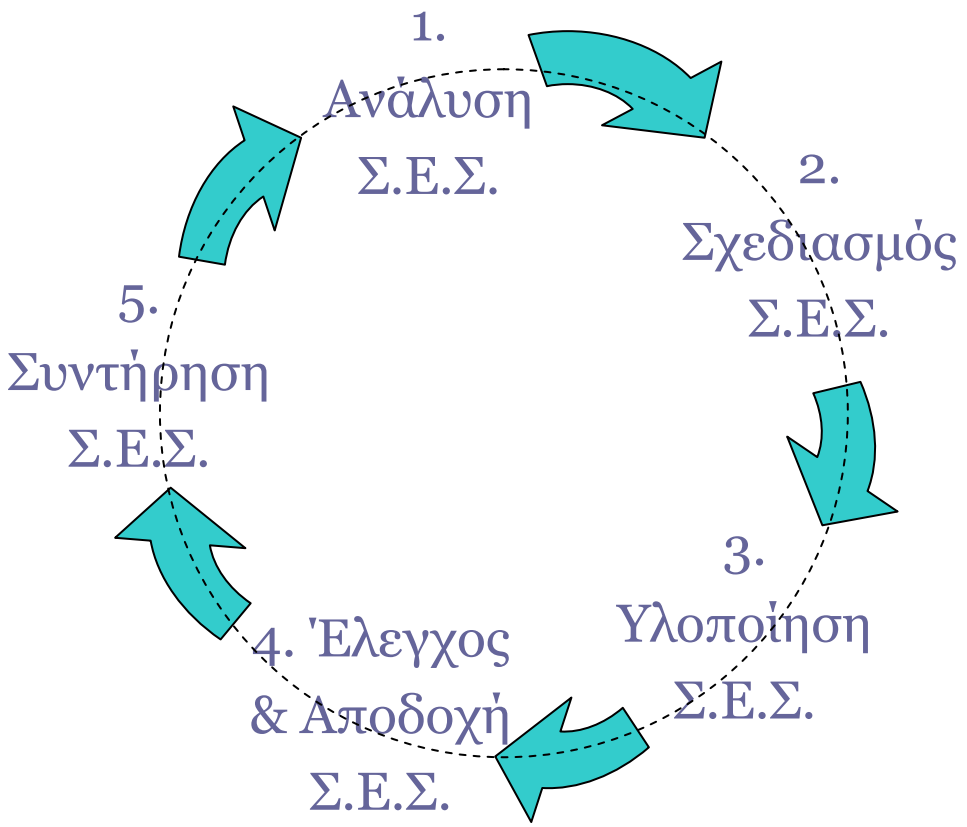
# Διαφορές Σχεδίων

- Σχέδιο Επιχειρησιακής Συνέχειας
  - Εστιάζει στις επιχειρησιακές λειτουργίες
  - Λαμβάνει υπόψη πολλές συνιστώσες όπως ανθρώπινο δυναμικό, παροχή ενέργειας, υγεία και ασφάλεια εργασίας, δημόσιες σχέσεις και επικοινωνία, κτλ.
  - Είναι πάντοτε ενεργοποιημένο
  - Περιλαμβάνει το Σχέδιο Ανάκαμψης Συστημάτων
- Σχέδιο Ανάκαμψης Συστημάτων
  - Εστιάζει στα πληροφοριακά συστήματα
  - Αφορά μόνο τεχνολογικά ζητήματα (αντίγραφα ασφαλείας, εναλλακτική λειτουργία, κτλ.)
  - Ενεργοποιείται μετά από κάποια διακοπή λειτουργίας συστήματος
  - Αποτελεί μέρος του Σχεδίου Επιχειρησιακής Συνέχειας

# Σχέδιο Επιχειρησιακής Συνέχειας



# Δομή Σχεδίου Επιχειρησιακής Συνέχειας



# 1. Ανάλυση Σχεδίου Επιχειρησιακής Συνέχειας

- Η φάση αυτή να περιλαμβάνει εργασίες όπως:
  1. την *ανάλυση επιχειρησιακών επιδράσεων* (business impact analysis)
  2. την *ανάλυση απειλών* (threat analysis) και
  3. τα *σενάρια επιδράσεων* (impact scenarios)

- Αποτέλεσμα της φάσης: καταγραφή των απαιτήσεων για το Σ.Ε.Σ.

# 1. 1. Ανάλυση Επιχειρησιακών Επιδράσεων

- Ταξινόμηση των επιχειρησιακών λειτουργιών σε επίπεδα κρισιμότητας
  - *Κρίσιμη Λειτουργία:* η διακοπή της λειτουργίας θα μπορούσε να βλάψει τον οργανισμό σε μη αποδεκτό για την επιβίωση του βαθμό
  - *Σημαντική Λειτουργία:* η διακοπή της λειτουργίας θα προκαλούσε πολύ σημαντικές αλλά όχι καταστροφικές συνέπειες στον οργανισμό
  - *Απαιτούμενη Λειτουργία:* η διακοπή της λειτουργίας θα προκαλούσε σχετικά μικρής κλίμακας συνέπειες στον οργανισμό

# Κριτήρια για την κρισιμότητα λειτουργιών

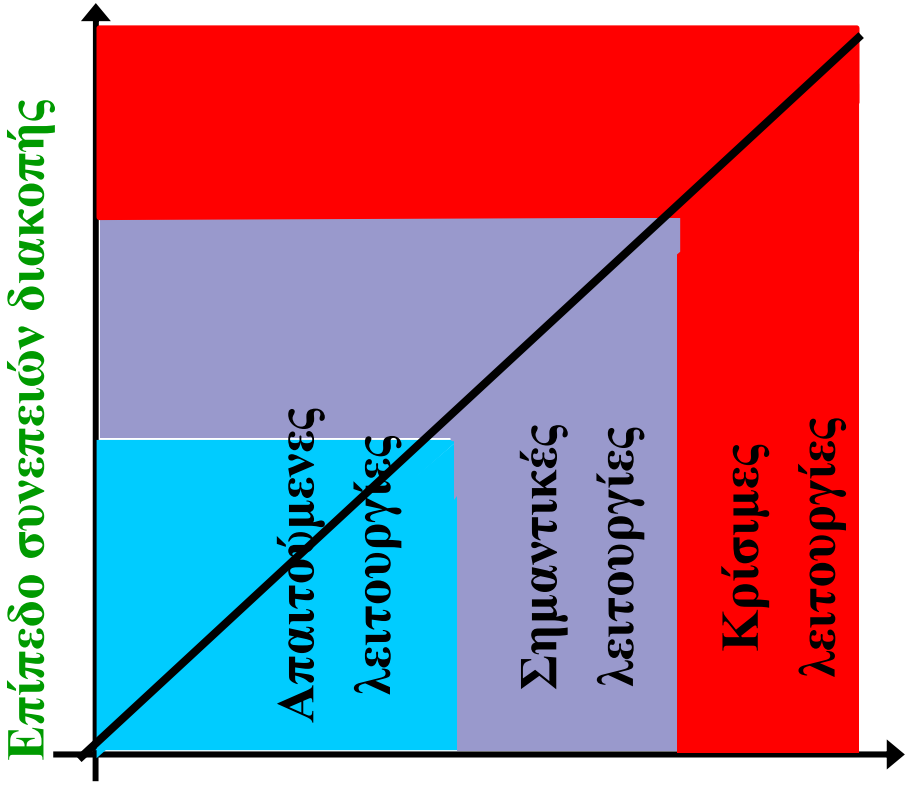
## 1ο κριτήριο για την ταξινόμηση κρισιμότητας

- *οι άμεσες ή/ και έμμεσες συνέπειες από τη μη διαθεσιμότητα.*
  - *π.χ. οικονομικές απώλειες*
  - *απώλεια αξιοπιστίας*
  - *νομικές επιπτώσεις κτλ*

## 2ο κριτήριο για την ταξινόμηση κρισιμότητας

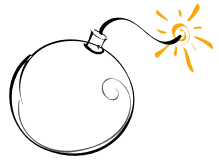
- *το κόστος που δαπανάται για τη λήψη κατάλληλων μέτρων ανάκαμψης.*
  - *επιχειρησιακών*
  - *οργανωτικών και*
  - *τεχνικών μέτρων*

# Κρισιμότητα Λειτουργιών



# 1.2. Ανάλυση Απειλών (Threat analysis)

- Ακολουθεί μετά την καταγραφή των απαιτήσεων ανάκαμψης
- Καταγραφή των απειλών για κάθε αγαθό



- Σκοπός: να γίνει λεπτομερής καταγραφή των απαραίτητων βημάτων ανάκαμψης για κάθε συγκεκριμένη απειλή.
- Οι απειλές μπορεί να αφορούν:
  - φυσικές υποδομές
  - οργανωτικές υποδομές
  - προσωπικό

# 1.2. Ανάλυση Απειλών (Threat analysis)

- Για την καταγραφή των απειλών είναι πολύ χρήσιμα (αν υπάρχουν) τα αποτελέσματα μίας *ανάλυσης πληροφοριακού κινδύνου*
- Οι απειλές έναντι του προσωπικού απαιτούν συνήθως οργανωτικά αλλά και τεχνικά μέτρα.
  - *Παράδειγμα, ιός SARS (2002-2003): Ομαδοποίηση του προσωπικού σε ανεξάρτητες ομάδες και κυκλική αλλαγή ομάδων μεταξύ των κεντρικών και των εναλλακτικών εγκαταστάσεων λειτουργίας. Η συχνότητα εναλλαγής ήταν ίση με την περίοδο επώασης του ιού.*

# 1.3. Σενάρια επιδράσεων (Impact scenarios)

- Μετά των καθορισμό των πιθανών απειλών, γίνεται μελέτη σεναρίων επιδράσεων
- Αποτελούν τη βάση για το σχέδιο ανάκαμψης

- Είναι προτιμότερο να γίνεται σχεδιασμός για τα ευρύτερης έκτασης πιθανά προβλήματα αντί για μικρής έκτασης προβλήματα
- Τα μικρότερης έκτασης προβλήματα αποτελούν συνήθως στοιχεία μεγαλύτερων καταστροφών

# Παραδείγματα Σεναρίων Επιδράσεων

- Ένα τυπικό σενάριο:
  - *Η απώλεια ενός κτηρίου*
    - Θα επηρεάσει όλες τις κρίσιμες λειτουργίες (;)
    - Χρειάζεται ένα σενάριο επιδράσεων για κάθε κτήριο του οργανισμού (;)
- Άλλα σενάρια:
  - *Η προσωρινή ή μόνιμη απώλεια ενός συγκεκριμένου ορόφου*
  - *Η προσωρινή ή μόνιμη απώλεια του κεντρικού database server*
    - περιλαμβάνεται στο προηγούμενο (;)

# Αποτέλεσμα 1ης φάσης: Καθορισμός απαιτήσεων συνέχειας

1. Καθορισμός εύρους έργου – λειτουργιών (project sizing)
2. Ταξινόμηση κρισιμότητας λειτουργιών
3. Καθορισμός κύριων απειλών και εκτίμηση επιδράσεων
4. Καθορισμός μέγιστου χρόνου διακοπής για κάθε λειτουργία
5. Καθορισμός πόρων που απαιτεί κάθε (κρίσιμη) λειτουργία σε Κανονικές Συνθήκες
   - Προσωπικού
   - Συστημάτων
   - Υποδομών
   - Εφαρμογών
   - Δεδομένων

# 2. Σχεδιασμός Σχεδίου Επιχειρησιακής Συνέχειας

- Καταγράφονται απαιτήσεις σχεδιασμού με σκοπό να εφαρμοστούν και να υλοποιηθούν στην επόμενη φάση.
  1. Επιχειρησιακές απαιτήσεις
  2. Τεχνικές απαιτήσεις

- Στόχος: ο εντοπισμός της περισσότερο συμφέρουσας λύσης Ανάκαμψης Συστημάτων και Λειτουργιών (Disaster Recovery)

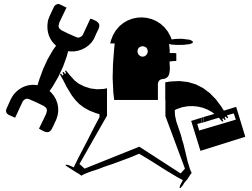
# Επιχειρησιακές απαιτήσεις ανάκαμψης (1/2)

- Περιλαμβάνουν (μη τεχνικά) ζητήματα που αφορούν τη συνέχεια των λειτουργιών όπως:
  1. Καθορισμός οργανωτικής δομής διαχείρισης συνέχειας
     - Υπεύθυνος Συνέχειας Λειτουργίας
     - Υπεύθυνος Εναλλακτικού Κέντρου
     - Υπεύθυνος Επικοινωνίας με το προσωπικό
     - Υπεύθυνος Επικοινωνίας με Πελάτες, Αρχές και τα Μ.Μ.Ε.
     - Υπεύθυνος Μεταφοράς Προσωπικού και Εξοπλισμού
     - Συντονιστής Σχεδίου Συνέχειας Λειτουργίας
  2. Διατήρηση τηλεφωνικού καταλόγου εμπλεκομένων: Τα άτομα που εμπλέκονται στο Σ.Ε.Σ. και τα στοιχεία επικοινωνίας τους
     - Τηλέφωνο επικοινωνίας για την ενημέρωση του αρμόδιου προσωπικού ανάλογα με το πρόβλημα

# Επιχειρησιακές απαιτήσεις ανάκαμψης (2/2)

3. Καθορισμός ατόμου και στρατηγικής επικοινωνίας με τρίτους
   - ειδοποίηση πελατών, αρμόδιων Αρχών, μέσων για το πρόβλημα με σκοπό την αποφυγή δημιουργίας πανικού.
4. Καθορισμός μέτρων ενθάρρυνσης προσωπικού
   - κατά την ανάκαμψη από κάποια καταστροφή πιθανόν να απαιτηθούν επιπλέον ώρες εργασίας σε πιεστικές συνθήκες.
   - Για αυτό το λόγο θα πρέπει να υπάρχει κάποιο σύστημα για την υποστήριξη του προσωπικού.
5. Σύνταξη απαιτούμενων διαδικασιών
   - Εκκένωση κτηρίων
   - Ανάκαμψη συστημάτων
   - Μεταφορά προσωπικού στο εναλλακτικό κέντρο
   - Λήψη και διατήρηση εφεδρικών αρχείων
   - Επαναφορά εφεδρικών αρχείων

# Τεχνικές απαιτήσεις ανάκαμψης



## 1. Εγκαταστάσεις εναλλακτικής λειτουργίας

- Διατήρηση εναλλακτικών κέντρων
- Απαιτήσεις εναλλακτικού κέντρου

## 2. Εφεδρικά αρχεία

- Μέθοδος λήψης και επαναφοράς εφεδρικών αρχείων

## 3. Άλλα θέματα

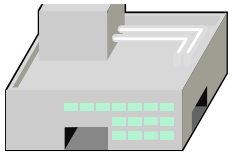
- Τον αριθμό και το είδος των γραφείων τα οποία απαιτούνται για το εναλλακτικό κέντρο λειτουργίας.
- Τις ανάγκες σε αναλώσιμα και περιφερειακές συσκευές (χαρτί, γραφική ύλη, εκτυπωτές, αντιγραφικά, fax, κτλ)
- Χρήση συστημάτων αδιάλειπτης τροφοδοσίας (UPS)
- συστήματα πρόληψης πυρκαγιάς, π.χ. συναγερμοί, συστήματα πυρόσβεσης, πυροσβεστήρες κτλ.
- Χρήση προγράμματος anti-virus
- Εφαρμογή ασφαλιστικών προγραμμάτων για εγκαταστάσεις και εξοπλισμό

# i. Εγκαταστάσεις εναλλακτικής λειτουργίας

1) Ορισμός της τοποθεσίας του εναλλακτικού κέντρου
2) Σχεδιασμός αρχιτεκτονικής τηλεπικοινωνιών μεταξύ βασικής εγκατάστασης και εναλλακτικού κέντρου
3) Ορισμός τεχνικών απαιτήσεων για την ενεργοποίηση των κρίσιμων λειτουργιών στο εναλλακτικό κέντρο
   - απαιτήσεις συστημάτων
   - απαιτήσεις εφαρμογών
   - απαιτήσεις δεδομένων
4) Ορισμός μέγιστου ανεκτού χρόνου διακοπής (down-time) για κάθε εφαρμογή για κάθε εφαρμογή
   - Προσοχή! Αφορά τις ίδιες τις εφαρμογές, όχι τις λειτουργίες
5) Ορισμός των εναλλακτικών χειρόγραφων λειτουργιών

# Τύποι εναλλακτικών κέντρων (1/3)

1. «Ψυχρό» Κέντρο (Cold Site)
   - Η πιο φτηνή λύση εναλλακτικού κέντρου
   - Περιλαμβάνει:
     - Ελάχιστες υποδομές γραφείου
     - Παροχή ρεύματος
   - **Δεν** περιλαμβάνει:
     - Συστήματα
     - Δικτυακές υποδομές
     - Δεδομένα
   - Απαιτείται πολύς χρόνος για την μεταφορά των λειτουργιών και την έναρξη λειτουργίας του
   - Καλύτερο από το τίποτα



# Τύποι εναλλακτικών κέντρων (2/3)

2. «Χλιαρό» Κέντρο (Warm Site)
   - Ενδιάμεσου κόστους λύση
   - Περιλαμβάνει:
     - Υποδομές γραφείου
     - Παροχή ρεύματος
     - Εξοπλισμό
     - Υπολογιστές
     - Δικτυακές υποδομές
     - Ελάχιστο (ή καθόλου) προσωπικό
   - **Δεν** περιλαμβάνει:
     - Δεδομένα
     - Προσωπικό
   - Απαιτείται χρόνος για την μεταφορά των δεδομένων, προσωπικού και την έναρξη λειτουργίας του

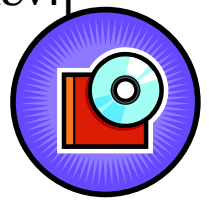
# Τύποι εναλλακτικών κέντρων (3/3)

## 3. «Θερμό» Κέντρο (Hot Site)

- Υψηλού κόστους λύση
- Σχεδόν πλήρες αντίγραφο της Βασικής Εγκατάστασης
- Περιλαμβάνει:
  - Υποδομές γραφείου
  - Παροχή ρεύματος
  - Εξοπλισμό
  - Υπολογιστές
  - Δικτυακές υποδομές
  - Δεδομένα
  - Προσωπικό
- **Δεν** περιλαμβάνει:
  - Δεν υποστηρίζει τις δευτερεύουσες λειτουργίες
- Απαιτείται ελάχιστος χρόνος για την έναρξη λειτουργίας του

# ii. Εφεδρικά Αρχεία (1/2)

- Μέθοδος λήψης εφεδρικών αρχείων τους σε περίπτωση καταστροφής
  - Χρήση αυτοματοποιημένου συστήματος εξ αποστάσεως λήψης εφεδρικών αρχείων (remote backup).
  - Χρήση περιοχών αποθήκευσης (Storage Area Networks – SANs) σε πολλαπλές τοποθεσίες για άμεση διάθεση των δεδομένων χωρίς την ανάγκη συγχρονισμού.
  - Χειροκίνητη (manual) λήψη εφεδρικών αρχείων
- Μέθοδος επαναφοράς εφεδρικών αρχείων
  - Για αυτοματοποιημένο σύστημα απαιτείται η ύπαρξη δικτυακής σύνδεσης μέχρι την απομακρυσμένη τοποθεσία.
  - Για χειρονακτική λήψη, η ανάκτηση από την απομακρυσμένη τοποθεσία.
- Μέσα αποθήκευσης
  - CD, DVD, Tape library, RAID



- Απομακρυσμένη διατήρηση εφεδρικών εφαρμογών

# ii. Εφεδρικά Αρχεία (2/2)

- Προγραμματισμός Λήψης Εφεδρικών Αρχείων
  - Πλήρης και Αυξητική Αποθήκευση (Full + Incremental)
    - Αρχικά λαμβάνεται ένα πλήρες backup
    - Στη συνέχεια, λαμβάνονται αυξητικά εφεδρικά αρχεία (μόνο των αρχείων που έχουν τροποποιηθεί από το προηγούμενο backup)
    - Προσφέρει μεγαλύτερη αξιοπιστία
    - Έχει μεγάλες απαιτήσεις αποθήκευσης
    - Απαιτεί αρκετό χρόνο για επαναφορά

# iii. Άλλες τεχνικές απαιτήσεις ανάκαμψης

- Περιλαμβάνει ζητήματα όπως:
  - Τις ανάγκες σε αναλώσιμα και περιφερειακές συσκευές (χαρτί, γραφική ύλη, εκτυπωτές, αντιγραφικά, fax, κτλ)
  - Χρήση συστημάτων αδιάλειπτης τροφοδοσίας (Uninterruptible Power Supply – UPS)
  - Συστήματα πρόληψης πυρκαγιάς, π.χ. συναγερμοί, συστήματα πυρόσβεσης, πυροσβεστήρες κτλ.

  - Χρήση προγράμματος anti-virus
  - Εφαρμογή ασφαλιστικών προγραμμάτων για εγκαταστάσεις και εξοπλισμό
  - Τον αριθμό και το είδος των γραφείων τα οποία απαιτούνται για το εναλλακτικό κέντρο λειτουργίας

# 3. Υλοποίηση Σχεδίου Επιχειρησιακής Συνέχειας

- Η φάση υλοποίησης είναι με απλά λόγια η εκτέλεση των στοιχείων σχεδιασμού που έχουν εντοπιστεί στην φάση σχεδιασμού.
- Περιλαμβάνει:
  - Τη συγγραφή του Σ.Ε.Σ., των διαδικασιών, των τηλεφωνικών καταλόγων κτλ
  - Την ενεργοποίηση των διαδικασιών λήψης και επαναφοράς εφεδρικών αρχείων
  - Την υλοποίηση των μηχανισμών λήψης εφεδρικών αρχείων
  - Την υλοποίηση των εναλλακτικών κέντρων

- Ο έλεγχος της υλοποίησης μπορεί να ξεκινήσει από αυτή τη φάση

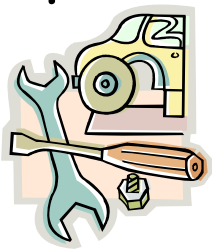
# 4. Έλεγχος και Αποδοχή Σχεδίου Επιχειρησιακής Συνέχειας

- Στόχος: η οργανωτική αποδοχή ότι το Σ.Ε.Σ. ικανοποιεί τις απαιτήσεις συνέχειας και ανάκαμψης του οργανισμού.
- Το Σ.Ε.Σ. μπορεί να αποτύχει λόγω:
  - ελλιπών ή εσφαλμένων απαιτήσεων ανάκαμψης,
  - σφαλμάτων σχεδιασμού
  - σφαλμάτων υλοποίησης

- Ο έλεγχος περιλαμβάνει:
  - Σενάρια σε χαρτί (paper-based what-if scenarios)
  - Έλεγχο κλήσης της ομάδας διαχείρισης κινδύνου
  - Τεχνικός έλεγχος μετάβασης από το βασικό στο εναλλακτικό κέντρο λειτουργίας.
  - Έλεγχος εφαρμογών
  - Έλεγχος λήψης και επαναφοράς αρχείων

# 5. Συντήρηση Σχεδίου Επιχειρησιακής Συνέχειας

- Στόχος: Η επικαιροποίηση (update) του Σ.Ε.Σ. ανάλογα με τις αλλαγές στον ίδιο τον οργανισμό
- Διακρίνεται σε τρεις περιοδικές ενέργειες
  - Επιβεβαίωση του περιεχομένου του εγχειριδίου
  - Έλεγχο και επαλήθευση των τεχνικών λύσεων ανάκαμψης
  - Έλεγχο και την επαλήθευση των καταγεγραμμένων διαδικασιών ανάκαμψης.
- Ένας τυπικός κύκλος συντήρησης είναι κάθε ένα με δύο χρόνια



# 5.1. Ανανέωση και έλεγχος περιεχομένου

- Αφορά μεταβολές του οργανισμού, οι οποίες αφορούν και το περιεχόμενο του Σ.Ε.Σ.
- Μερικοί τύποι μεταβολών που θα πρέπει να εντοπιστούν και να ανανεωθούν είναι:
  - ✓Αλλαγές προσωπικού
  - ✓Αλλαγές σε στοιχεία επικοινωνίας καταλόγου Σ.Ε.Σ.
  - ✓Αλλαγές σε σημαντικούς προμηθευτές και τα στοιχεία επικοινωνίας τους
  - ✓Αλλαγές στην οργανωτική δομή του οργανισμού

# 5.2 Έλεγχος και επαλήθευση τεχνικών λύσεων

- Κάθε εξειδικευμένο τεχνικό μέρος θα πρέπει να ελεγχθεί και να επαληθευτεί ως προς την λειτουργικότητά του.
- Μερικοί τέτοιο έλεγχοι περιλαμβάνουν:
  - ✓ Διανομή και εγκατάσταση ανανεώσεων antivirus
  - ✓ Διανομή και εγκατάσταση διορθώσεων (updates, patches) σε Λ.Σ. και εφαρμογές
  - ✓ Έλεγχος λειτουργίας Hardware
  - ✓ Έλεγχος λειτουργίας εφαρμογών
  - ✓ Επαλήθευση δεδομένων
  - ✓ Επαλήθευση μεθόδου λήψης και επαναφοράς

# 5. 3 Έλεγχος και επαλήθευση καταγεγραμμένων διαδικασιών ανάκαμψης

- Καθώς οι διαδικασίες τροποποιούνται με το χρόνο, οι καταγεγραμμένες διαδικασίες ανάκαμψης ενδέχεται να μην είναι κατάλληλες.
- Μερικοί έλεγχοι σε αυτό το στάδιο περιλαμβάνουν:
  - ✓ Είναι όλες οι διαδικασίες των κρίσιμων λειτουργιών καταγεγραμμένες;
  - ✓ Έχουν αλλάξει τα συστήματα που έχουν χρησιμοποιηθεί σε κρίσιμες εφαρμογές;
  - ✓ Οι καταγεγραμμένες διαδικασίες ανάκαμψης είναι ικανές να επιτρέψουν την ανάκαμψη των λειτουργιών εντός των προκαθορισμένων χρόνων ανάκαμψης;
- Υπάρχει άμεση σχέση μεταξύ των φάσεων συντήρησης και ανάλυσης επιχειρησιακών επιδράσεων.
- Τα στοιχεία που προκύπτουν από τη φάση του ελέγχου και της συντήρησης μπορούν να χρησιμοποιηθούν στη φάση της ανάλυσης.

# Ερωτήσεις;

# Παραδείγματα εργαλείων ΣΔΑΠ – www.ISO27001security.com

- ISO27k_ISMS_implementation_and_certification_process_v3.pdf
- ISO27k_FMEA_spreadsheet.xls
- ISO27k_SOA_sample.xls

# Βιβλιογραφία


1. Δ. Πολέμη, Χ. Δημητριάδης, Σ. Παπαστεργίου, Α. Καλιαντζόγλου, Εργαστηριακά θέματα ασφάλειας, 2006.
2. Σ. Κάτσικας Δ. Γκρίτζαλης, Σ. Γκρίτζαλης, «Ασφάλεια Πληροφοριακών Συστημάτων», Εκδόσεις Νέων Τεχνολογιών, 2003.
3. International Standardization Organization, ISO/IEC 27001, Information Technology – Security Techniques – Information security management systems – Requirements, 2005.
4. International Standardization Organization, ISO/IEC 27002:2005, Information technology – Security techniques – Code of Practice for Information Security Management, 2007.
5. International Standardization Organization, ISO/IEC 27005:2008, Information technology – Security techniques Information security risk management, 2008.)
6. "Information Security Policies, Procedures and Standrards – Guideline for Effective Information Security Management:, Tomas R. Peltier, Auerbach publications, ISBN: 0-8493-1137-3, CRC Press, 2002.
7. "Information Security Risk Analysis", Publisher: Auerbach Publications; 1st edition (January 23, 2001), ISBN: 0849308801
8. "Writing Information Security Policies", Publisher: Sams; 1st edition (November 9, 2001), ISBN: 157870264X
9. www.iso27001security.com
10. Business Continuity Planning / Disaster Recovery Planning - An Online Guide http://www.yourwindow.to/business-continuity/bcpindex.htm?bcp5_2_6
11. Business Continuity: Best Practices – World-Class Business Continuity Management, Second Edition, Andrwe Hiles, ISBN-13: 978-0973372502
12. Business Continuity Planning Methodology, Akhtar Syed, Afsar Syed, ISBN-13: 978-0973372502
13. Disaster Recovery: Principles and Practices (Prentice Hall Security Series), April Wells, Charlyne Walker, and Timothy Walker, ISBN-13: 978-0131711273