STORM-RM: A Collaborative Risk Management Methodology

T. Ntouskas, D. Gritzalis

January 2017

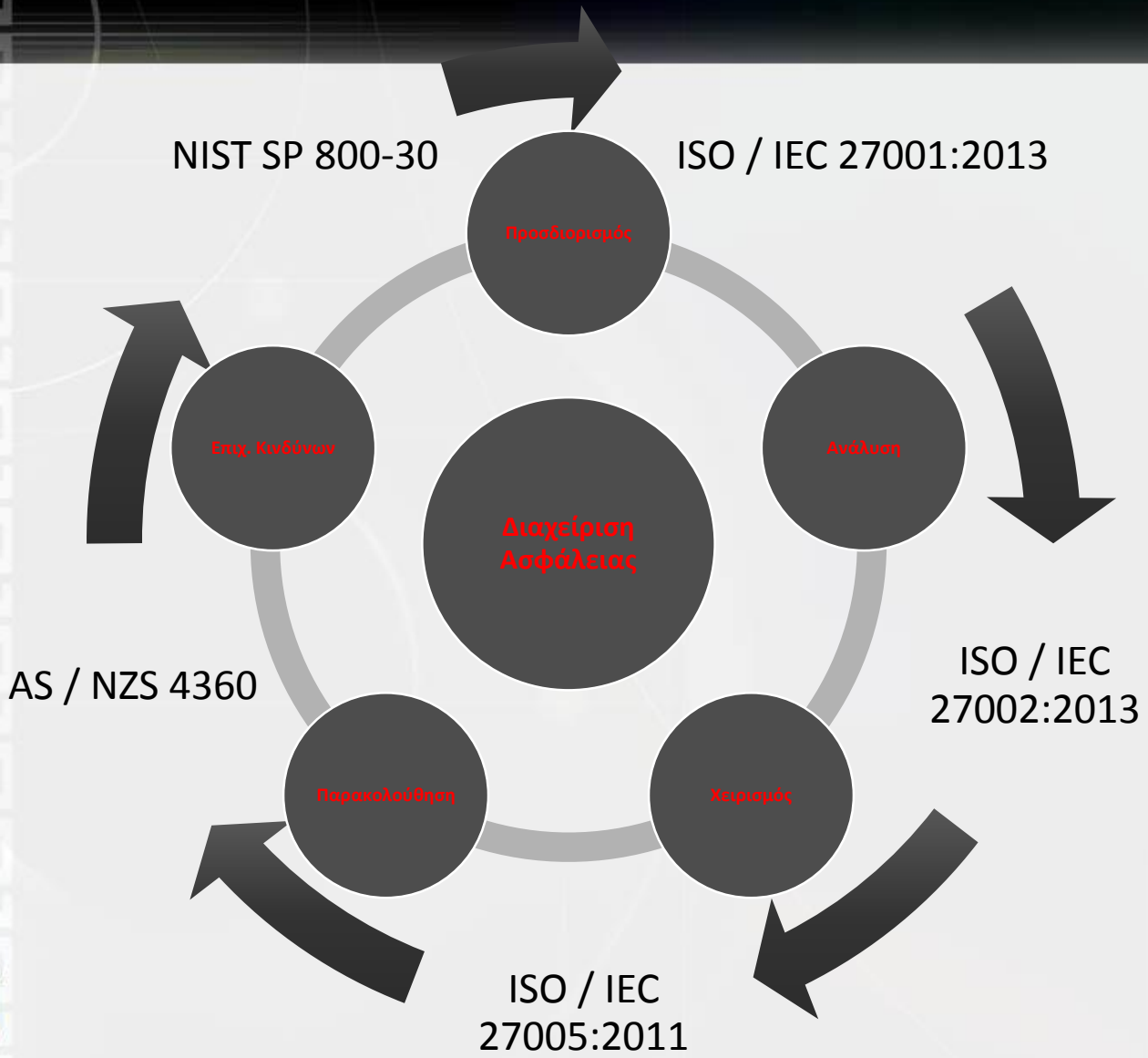
Συνεργατική Μεθοδολογία ΑΔΕ STORM-RM

T. Ntouskas, D. Gritzalis
Information Security & Critical Infrastructure Protection Laboratory
Dept. of Informatics | Athens University of Economics & Business

Εισαγωγή


Πολύπλοκες αρχιτεκτονικές
Κατανεμημένα
Αλληλεξαρτώνται από ΠΣ συνεργαζόμενων φορέων
Πολλοί χρήστες
Σύνθετες η /κ-υπηρεσίες - εφαρμογές
Απαιτήσεις χρηστών
Σημερινά
Πληροφοριακά Συστήματα


www
@


NIST SP 800-30
ISO / IEC 27001:2013
Προσδιορισμός
Ανάλυση
Διαχείριση Ασφάλειας
Επιχ. Κινδύνων
Παρακολούθηση
Χειρισμός
AS / NZS 4360
ISO / IEC 27002:2013
ISO / IEC 27005:2011


www
@

Μεθοδολογίες / Κριτήρια	CRAMM	EBIOS	OCTAVE	Mehari	MAGERIT
Κόστος	Εμπορικό	Δωρεάν	Δωρεάν	Εμπορικό	Δωρεάν
Εργαλείο/ Κόστος	Ναι/ Εμπορικό	Ναι/ Δωρεάν	Ναι/ Εμπορικό	Ναι/ Εμπορικό	Ναι/ Εμπορικό
Συνεργατικότητα	Όχι	Όχι	Ναι	Όχι	Όχι
Συμβατότητα με πρότυπα	Ναι	Ναι	Όχι	Ναι	Ναι
Παραμετροποιήσιμες	Όχι	Όχι	Ναι	Ναι	Ναι
Πολυγλωσικότητα	Μόνο Αγγλικά	Ναι	Μόνο Αγγλικά	Μόνο Γαλλικά	Αγγλικά, Ισπανικά

Ανοιχτά προβλήματα

i. Η διαχείριση ασφάλειας ΔΕΝ αντιμετωπίζεται ως ένα πολυκριτηριακό πρόβλημα.

ii. Οι υφιστάμενες μεθοδολογίες ΑΔΕ δεν ανταποκρίνονται στις σημερινές ανάγκες και δεν ικανοποιούν συγκεκριμένα κριτήρια:
   - μη παραμετροποιήσιμες, μη συνεργατικές, πολύπλοκες, ακριβές (απαιτούν πόρους)

iii. Τα εργαλεία ΑΔΕ είναι:
   - Δύσχρηστα, εξειδικευμένα (απαιτούν τεχνογνωσία), ακριβά (κόστος, ανθρωποπροσπάθεια), εμπορικά, μη συνεργατικά

iv. Έλλειψη ολοκληρωμένων συνεργατικών συστημάτων ΑΔΕ:
   - παροχή υπηρεσιών ΑΔΕ , συνεργασία, εκπαίδευση, ενημέρωση σε θέματα ασφάλειας.

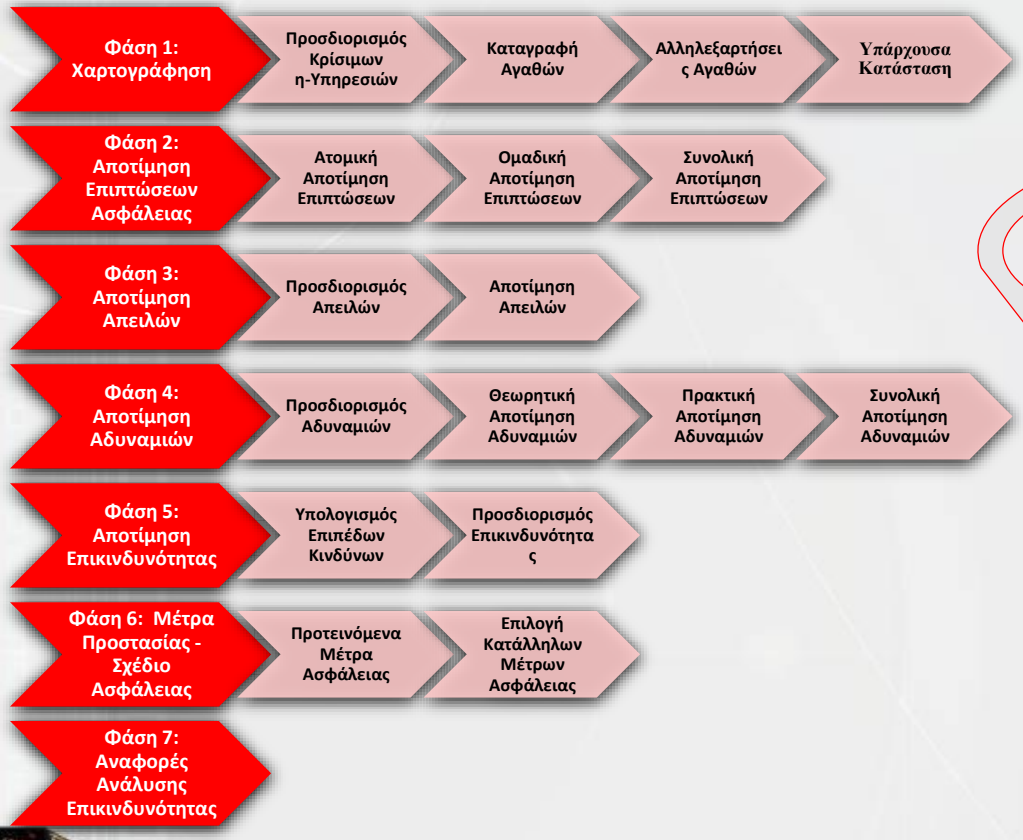
Συνεισφορές

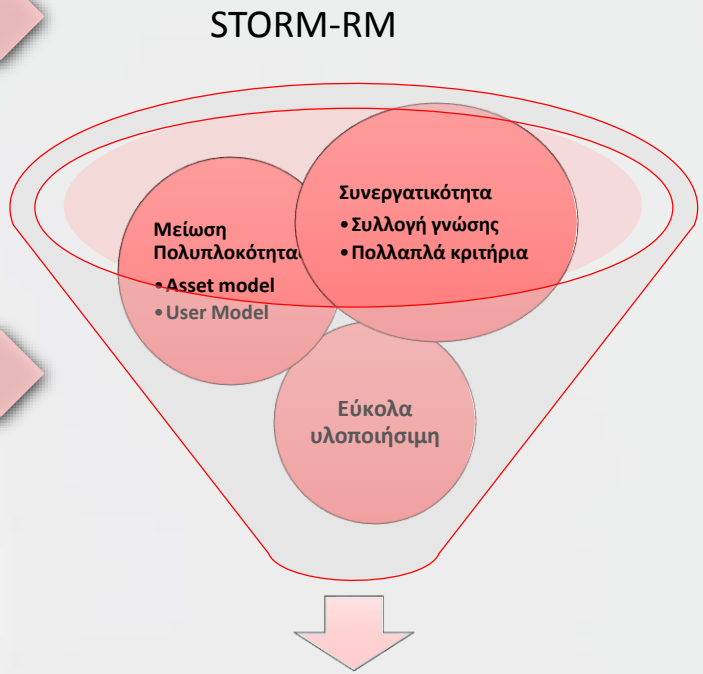
i. Αντιμετωπίζεται η ΑΔΕ ως πολυκριτηριακό πρόβλημα, λαμβάνοντας υπόψη της τα εξής κριτήρια:
   - τεχνολογικά,
   - επιχειρησιακά,
   - νομικά

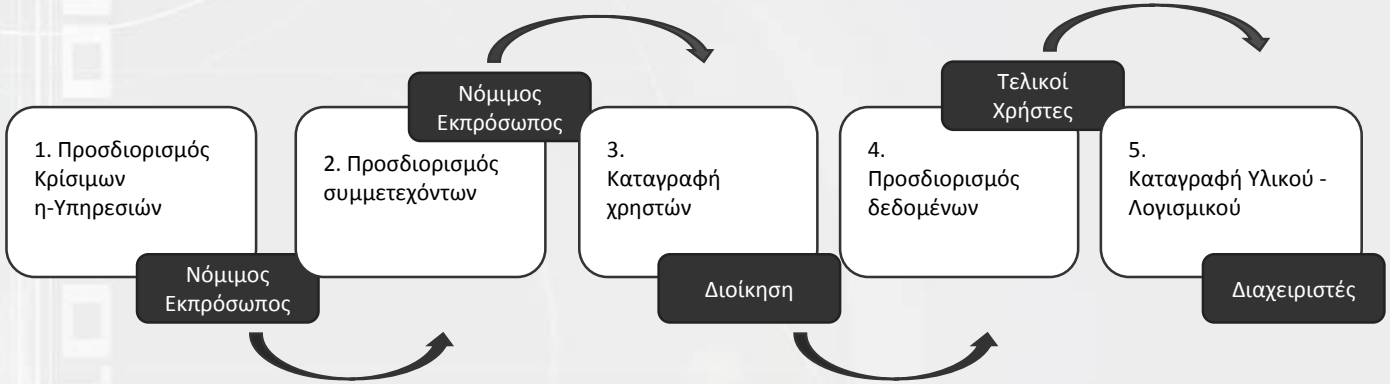
ii. Αναπτύσσεται ή συνεργατική, πολυκριτηριακή, παραμετροποιήσιμη μεθοδολογία ΑΔΕ, STORM-RM

iii. Προδιαγράφονται και αναπτύσσονται συνεργατικές STORM - υπηρεσίες για τη ΑΔΕ, που υλοποιούν τα βήματα της STORM-RM

Φάσεις της STORM-RM

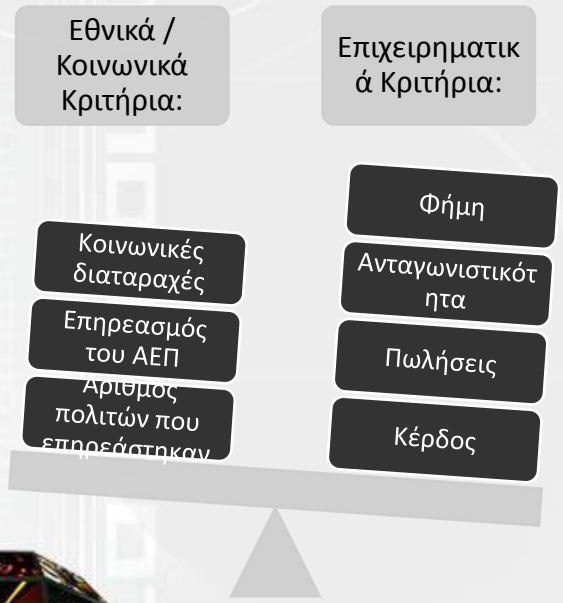


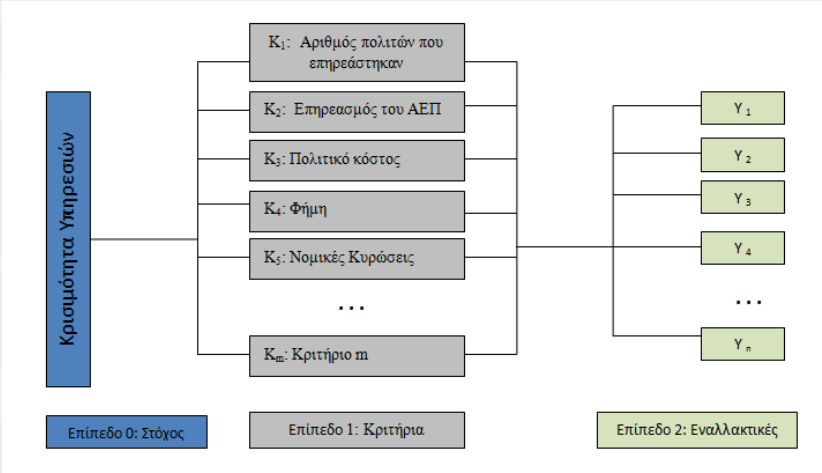



1. Προσδιορισμός Κρίσιμων η-Υπηρεσιών
Νόμιμος Εκπρόσωπος
2. Προσδιορισμός συμμετεχόντων
Νόμιμος Εκπρόσωπος
3. Καταγραφή χρηστών
Διοίκηση
4. Προσδιορισμός δεδομένων
Τελικοί Χρήστες
5. Καταγραφή Υλικού - Λογισμικού
Διαχειριστές

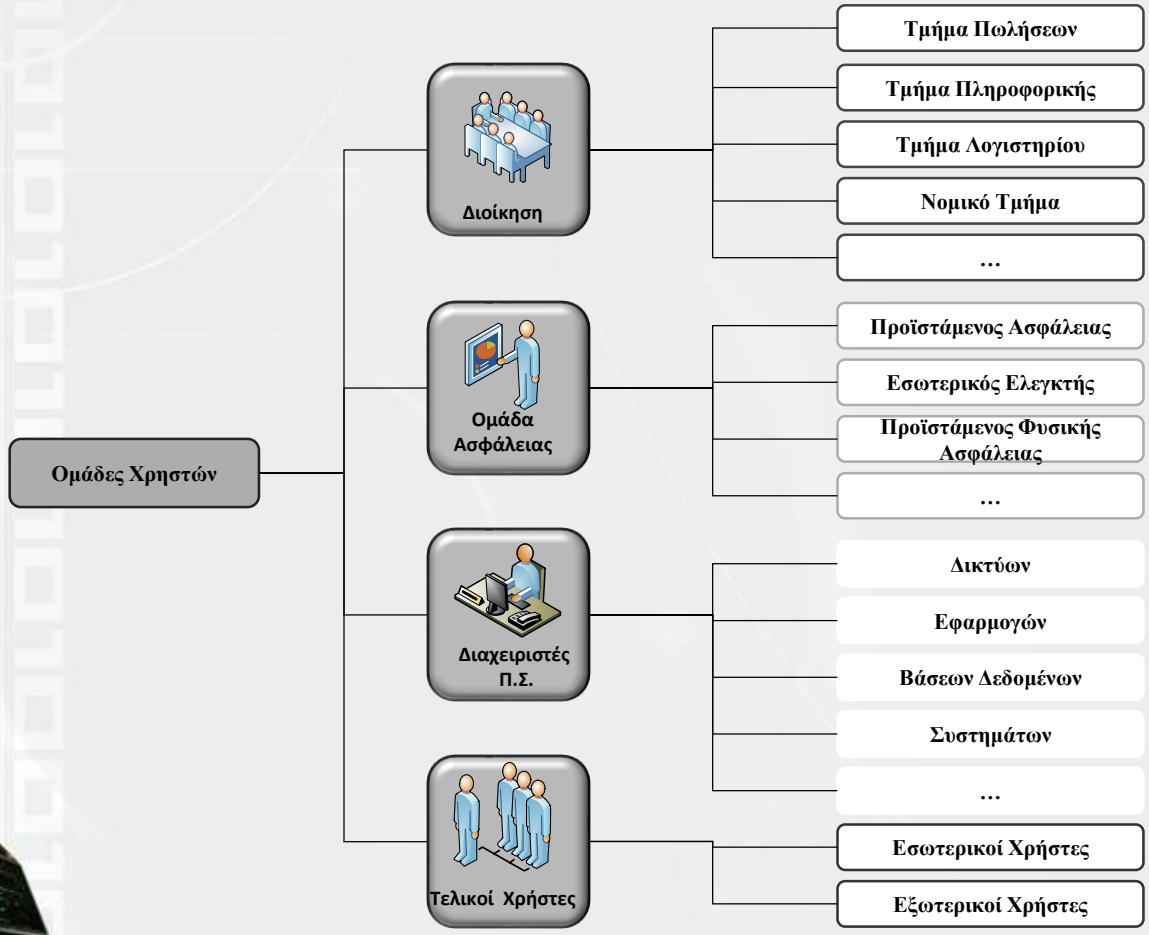

www
@

- Καταγραφή των η-υπηρεσιών
- Αξιολόγηση της κρισιμότητας των η-υπηρεσιών (με την βοήθεια της AHP)

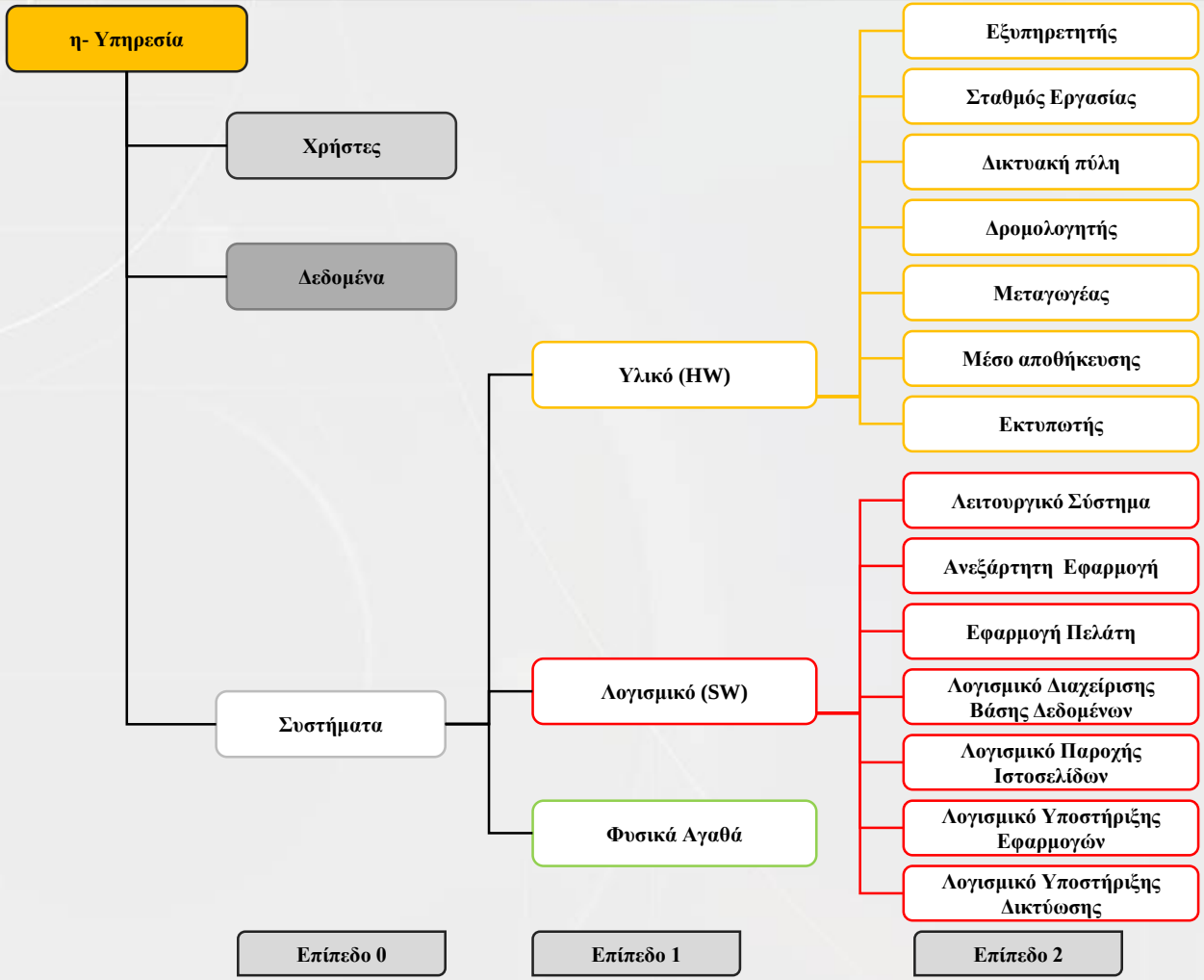




- η- Υπηρεσίες
  - E_1
  - E_n
- Φυσικά αγαθά
  - Κτίρια
  - Δωμάτια
- Υλικό
  - Υπολογιστής εξυπηρετητής
  - Σταθμός εργασίας
  - Δικτυακή πύλη
  - Δρομολογητής
  - Μεταγωγέας
  - Μέσο αποθήκευσης
  - Εκτυπωτής
- Λογισμικό
  - Λειτουργικό σύστημα
  - Ανεξάρτητη εφαρμογή
  - Εφαρμογή πελάτη
  - Λογισμικό διαχείρισης βάσης δεδομένων
  - Λογισμικό παροχής ιστοσελίδων
  - Λογισμικό υποστήριξης εφαρμογών
  - Ενσωματωμένο λογισμικό
  - Λογισμικό υποστήριξης δικτύωσης
- Δεδομένα
  - Οικονομικά
  - Προσωπικά


Ομάδες Χρηστών
Διοίκηση
Τμήμα Πωλήσεων
Τμήμα Πληροφορικής
Τμήμα Λογιστηρίου
Νομικό Τμήμα
…
Ομάδα Ασφάλειας
Προϊστάμενος Ασφάλειας
Εσωτερικός Ελεγκτής
Προϊστάμενος Φυσικής Ασφάλειας
…
Διαχειριστές Π.Σ.
Δικτύων
Εφαρμογών
Βάσεων Δεδομένων
Συστημάτων
…
Τελικοί Χρήστες
Εσωτερικοί Χρήστες
Εξωτερικοί Χρήστες


WWW
@


η- Υπηρεσία
Χρήστες
Δεδομένα
Συστήματα
Υλικό (HW)
Λογισμικό (SW)
Φυσικά Αγαθά
Εξυπηρετητής
Σταθμός Εργασίας
Δικτυακή πύλη
Δρομολογητής
Μεταγωγέας
Μέσο αποθήκευσης
Εκτυπωτής
Λειτουργικό Σύστημα
Ανεξάρτητη Εφαρμογή
Εφαρμογή Πελάτη
Λογισμικό Διαχείρισης Βάσης Δεδομένων
Λογισμικό Παροχής Ιστοσελίδων
Λογισμικό Υποστήριξης Εφαρμογών
Λογισμικό Υποστήριξης Δικτύωσης
Επίπεδο 0
Επίπεδο 1
Επίπεδο 2

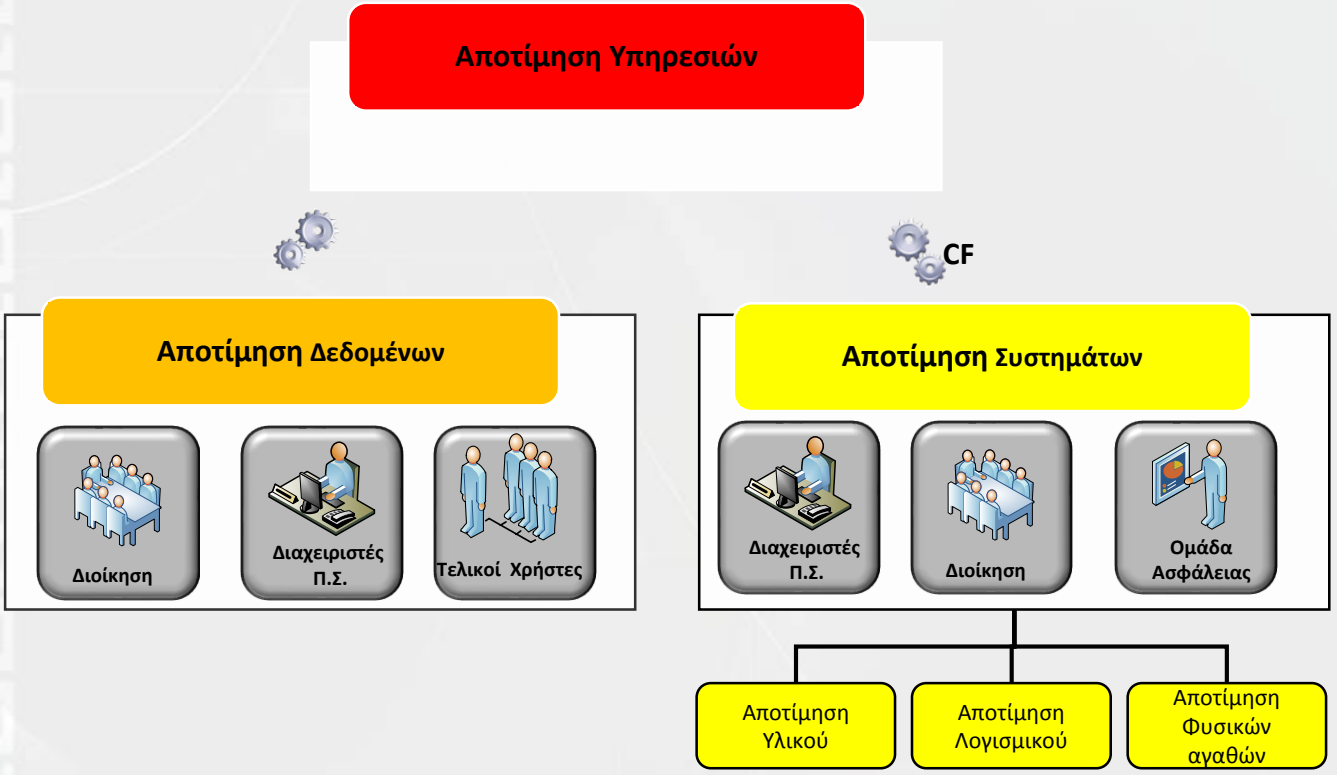

WWW

- **Βαθμός Συσχέτισης (Correlation Factor – CF)** του Συστήματος **S** και της η-υπηρεσίας **E**:
  - **CF** (System S, Service E)
- ποσοστό με το οποίο επηρεάζεται η Εμπιστευτικότητα, Ακεραιότητα και Διαθεσιμότητα της η-υπηρεσίας

- Καταγράφονται όλα τα υφιστάμενα μέτρα προστασίας του υπό εξέταση ΠΣ.

- Για κάθε ένα αγαθό γίνεται ο έλεγχος με βάση τα μέτρα που ορίζει το ISO 27001 και χαρακτηρίζονται:
  - Πλήρως εγκατεστημένα,
  - Μερικώς Εγκατεστημένα,
  - Μη Εγκατεστημένα.

- Τα αποτελέσματα του συγκεκριμένου Βήματος θα χρησιμοποιηθούν στο Βήμα 4.1: Ανάλυση Αδυναμιών καθώς και στο Βήμα 6.1 Προτεινόμενα μέτρα ασφάλειας


Αποτίμηση Υπηρεσιών
CF
Αποτίμηση Δεδομένων
Διοίκηση
Διαχειριστές Π.Σ.
Τελικοί Χρήστες
Αποτίμηση Συστημάτων
Διαχειριστές Π.Σ.
Διοίκηση
Ομάδα Ασφάλειας
Αποτίμηση Υλικού
Αποτίμηση Λογισμικού
Αποτίμηση Φυσικών αγαθών


www
@

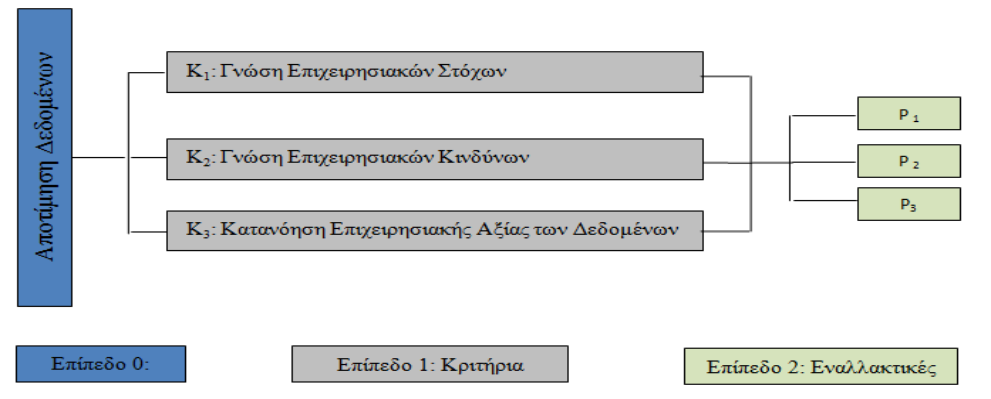
Επίπεδο Επίπτωσης	Βαθμός	Περιγραφή	Οικονομική Απώλεια	Απώλεια Κύκλου Εργασιών
Πολύ Υψηλό (ΠΥ)	5	Καταστροφική Επίπτωση	> 10.000.000 €	100% του κύκλου εργασιών
Υψηλό (Υ)	4	Σημαντική Επίπτωση	έως 10.000.000 €	75% του κύκλου εργασιών
Μέτριο (Μ)	3	Μέτρια Επίπτωση	έως 1.000.000 €	50% του κύκλου εργασιών
Χαμηλό (Χ)	2	Χαμηλή Επίπτωση	έως 100.000 €	25% του κύκλου εργασιών
Πολύ Χαμηλό (ΠΧ)	1	Ασήμαντη Επίπτωση	έως 10.000 €	5% του κύκλου εργασιών

Κάθε χρήστης U_j , **j=1,...n**, από μια Ομάδα Χρηστών G_k , **k=1,..., m** δίνει το δικό του Impact Value για όλες τις πιθανές επιπτώσεις ασφάλειας
(βάσει της STORM-RM κλίμακας)

User Impact Value:

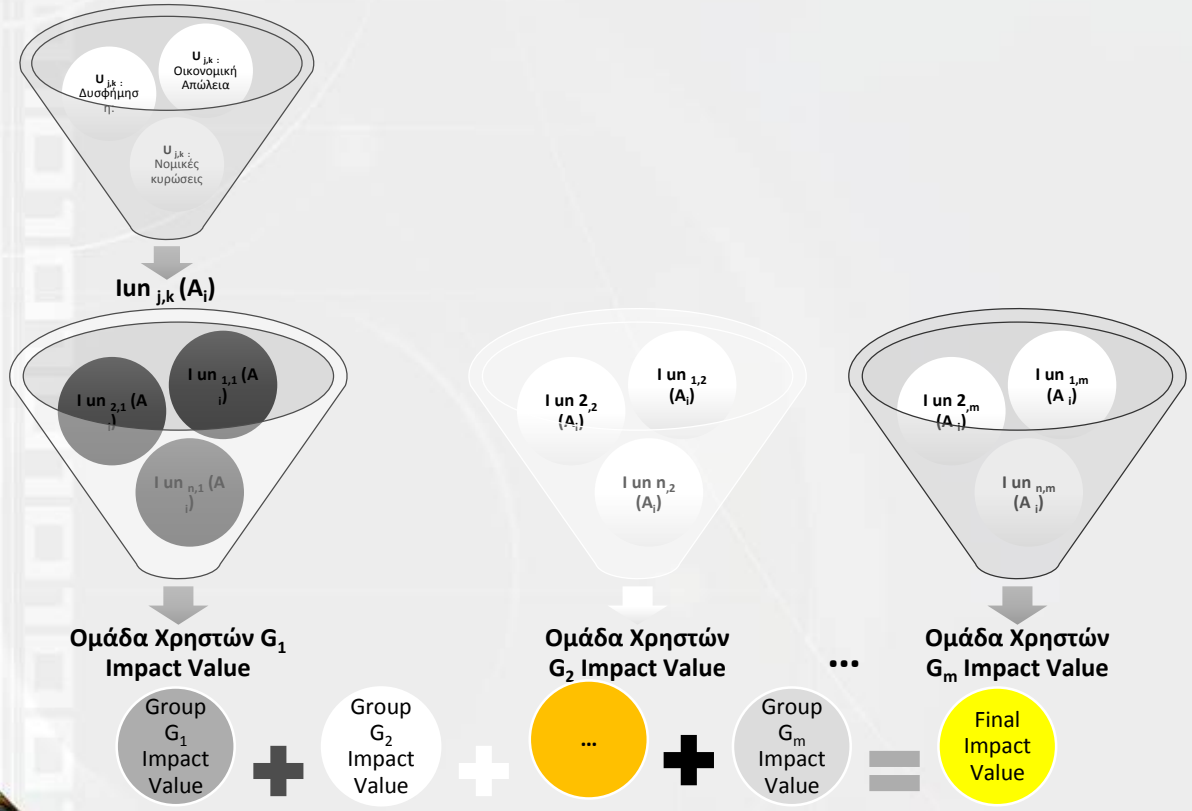
- Απώλεια Διαθεσιμότητας : $I_{un\ j,k}(A_i)$,
- Απώλεια Εμπιστευτικότητας: $I_{dis\ j,k}(A_i)$,
- Απώλεια Ακεραιότητας: $I_{mod\ j,k}(A_i)$.

$$I_{un\ j,k}(A_i) = \max(5,4,..,3)$$



K_1: Γνώση Επιχειρησιακών Στόχων	**P_1**	**P_2**	**P_3**	**Βάρη (w_i)**
P_1 : Διοίκηση	1	3	3	0,600
P_2 : Διαχειριστές	1/3	1	1	0,200
P_3 : Τελικοί Χρήστες	1/3	1	1	0,200
Λόγος Ευαισθησίας (Consistency ratio): 0.00				

Κριτήρια	**K_1**	**K_2**	**K_3**	
Προτεραιότητες Κριτηρίων	**0,333**	**0,333**	**0,333**	**Βάρη (w_i)**
P_1 : Διοίκηση	0,600	0,685	0,574	0,620
P_2 : Διαχειριστές	0,200	0,179	0,286	0,222
P_3 : Τελικοί Χρήστες	0,200	0,136	0,140	0,159
Λόγος Ευαισθησίας (Consistency ratio): 0.00				



$$Iun_k(A_i) = \left(\frac{\sum_{j=1}^{n} Iun_{j,k}(A_i)}{n}\right) * W_k$$

$$Idis_k(A_i) = \left(\frac{\sum_{j=1}^{n} Idis_{j,k}(A_i)}{n}\right) * W_k$$

$$Imod_k(A_i) = \left(\frac{\sum_{j=1}^{n} Imod_{j,k}(A_i)}{n}\right) * W_k$$

$$I_{un}(A_i) = \sum_{k=1}^{m} Iun_k(A_i)$$

$$I_{dis}(A_i) = \sum_{k=1}^{m} Idis_k(A_i)$$

$$I_{mod}(A_i) = \sum_{k=1}^{m} Imod_k(A_i).$$

Αποτίμηση Υπηρεσιών

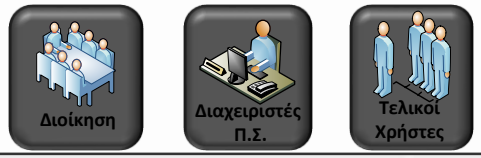
$I_{un}(E_e) = \max(I_{un}(A_1), I_{un}(A_2), I_{un}(A_3), \ldots)$

$I_{dis}(E_e) = \max(I_{dis}(A_1), I_{dis}(A_2), I_{dis}(A_3), \ldots)$

$I_{mod}(E_e) = \max(I_{mod}(A_1), I_{mod}(A_2), I_{mod}(A_3), \ldots)$

CF

Αποτίμηση Δεδομένων



$I_{un}(A_i) = \sum_{k=1}^{m} Iun_k(A_i)$

$I_{dis}(A_i) = \sum_{k=1}^{m} Idis_k(A_i)$

$I_{mod}(A_i) = \sum_{k=1}^{m} Imod_k(A_i)$

Αποτίμηση Συστημάτων

- Αποτίμηση Υλικού
- Αποτίμηση Λογισμικού
- Αποτίμηση Φυσικών αγαθών

$I_{un} = I_{un}(H_h) * CF_{un}(S_s, E_e)$

$I_{dis} = I_{dis}(H_h) * CF_{dis}(S_s, E_e)$

$I_{mod} = I_{mod}(H_h) * CF_{mod}(S_s, E_e)$

ΕΙΔΟΣ ΑΓΑΘΟΥ	ΑΠΕΙΛΕΣ (OCTAVE, CRAMM, NIST)
ΦΥΣΙΚΑ ΑΓΑΘΑ	Πυρκαγιά
	Σεισμός
	Πλημμύρα
ΥΛΙΚΟ	Διακυμάνσεις Ηλεκτρικής Ισχύος
	Τεχνικές Βλάβες
	Ηλεκτρονικές Παρεμβολές
ΑΓΑΘΑ ΛΟΓΙΣΜΙΚΟΥ	Μη εξουσιοδοτημένες αλλαγές σε λογισμικό
	Κακόβουλο Λογισμικό
	Άρνηση Υπηρεσίας
ΑΓΑΘΑ ΔΕΔΟΜΕΝΩΝ	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα
	Σφάλμα χειρισμού
	Κακόβουλη καταστροφή δεδομένων
ΔΙΚΥΑΚΟΣ ΕΞΟΠΛΙΣΜΟΣ	Σφάλματα μετάδοσης
	Μη ορθή δρομολόγηση επικοινωνιών
	Εξαπάτηση διεύθυνσης δικτύου (IP Spoofing)

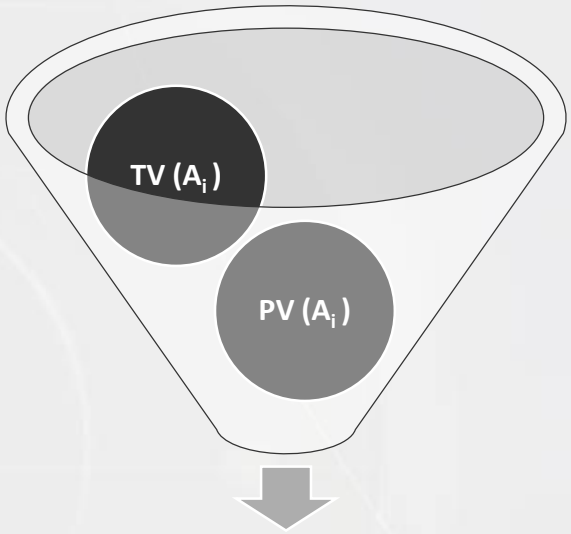
Συνολική αποτίμηση απειλών	Επίπεδο Απειλής	Βαθμός Αποτίμησης Απειλής	Συνολική αποτίμηση απειλών
≥ 80	Πολύ Υψηλό (ΠΥ)	1	Μία φορά τον μήνα
60-79	Υψηλό (Υ)	0,33	Μία φορά κάθε 4 μήνες
40-59	Μέτριο (Μ)	0,1	Μία φορά τον χρόνο
20-39	Χαμηλό (Χ)	0,034	Μία φορά κάθε 3 χρόνια
≤ 19	Πολύ Χαμηλό (ΠΧ)	0,01	Το πολύ μία φορά τα 10 χρόνια

Είδος Αγαθού	**Απειλές- (T_i)**	**Αδυναμίες - (V_i)**
Φυσικό Αγαθό	$T_{1:}$ Φωτιά	V_{11}: Ύπαρξη εύφλεκτων υλικών V_{12} : Αστοχία Συστημάτων ανίχνευσης φωτιάς V_{13} : Αστοχία φυσικής ασφάλειας $V_{1\ n}$: Αδυναμία - (για T_1)
	T_m	V_{m1}....V_{mn}
Υλικό	$T_{2:}$ Αστοχία Υλικού	V_{21} : Λανθασμένη Συντήρηση V_{22}: Έλλειψη συντήρησης V_{2n}: Αδυναμία - (για T_2)
	T_m	V_{m1}...V_{mn}
Λογισμικό	T3: Κακόβουλος κώδικας	V_{31}: Απουσία Αντι-ικού λογισμικού V_{32}: Αποτυχημένη ενημέρωση Αντι-ικού λογισμικού V_{33}: Ανεπαρκής εκπαίδευση του προσωπικού για τους ιούς V_{3n}: Αδυναμία - (για T_3)
	T_m	V_{m1}....V_{mn}

Προτεραιότητα αδυναμιών	Επίπεδο Αδυναμιών	Βαθμός Αποτίμησης Αδυναμιών	Περιγραφή (Πιθανότητα να συμβεί το χειρότερο σενάριο)
>66	Υψηλό (Υ)	1	>66%
33-66	Μέτριο (Μ)	0,66	33% - 66%
<33	Χαμηλό (Χ)	0,33	< 33%

- Καταγραφή ευρημάτων/αποτελεσμάτων από εργαλεία πρακτικής αξιολόγησης.
- Αντιστοίχιση αδυναμιών με εξεταζόμενα αγαθά και ανάθεση βαθμού αποτίμησης κάθε αδυναμίας.
- Από την ανάθεση του βαθμού αποτίμησης προκύπτει για κάθε αδυναμία και κάθε αγαθό το **επίπεδο της πρακτικής αποτίμησης** αδυναμιών, **Practical Vulnerability Assessment PV(A_i).**

Τελικός επίπεδο αποτίμησης Αδυναμιών (Final Vulnerability Level)



$$FV(A_i) = \max\left(TV(A_i), PV(A_i)\right)$$

Κίνδυνος ως προς απώλεια Διαθεσιμότητας:

$$R_{un}(A_i) = I_{un}(A_i) \times T(A_i) \times FV(A_{i,})$$

Κίνδυνος ως προς απώλεια Εμπιστευτικότητας:

$$R_{dis}(A_i) = I_{dis}(A_i) \times T(A_i) \times FV(A_i)$$

Κίνδυνος ως προς απώλεια Ακεραιότητας:

$$R_{mod}(A_i) = I_{mod}(A_i) \times T(A_i) \times FV(A_i)$$

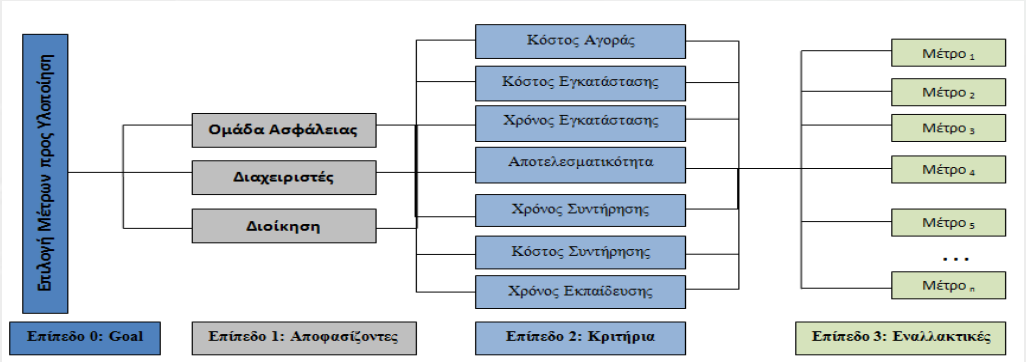
Συνολικός Κίνδυνος:

$$R(A_i) = I(A_i) \times T(A_i) \times FV(A_i) \text{ , όπου } I(A_i) = \max (I_{un}(A_i) , I_{dis}(A_i) , I_{mod}(A_i))$$

Επίπεδο Επικινδυνότητας	Βαθμός	Περιγραφή
Πολύ Χαμηλή (ΠΧ)	1	R < 1.000
Χαμηλή (Χ)	2	1.000 ≤ R < 10.000
Μέτρια (Μ)	3	10.000 ≤ R < 150.000
Υψηλή (Υ)	4	150.000 ≤ R < 5.000.000
Πολύ Υψηλή (ΠΥ)	5	αν R ≥ 5.000.000

ΕΠΙΠΕΔΟ ΑΠΕΙΛΗΣ		ΠΧ	ΠΧ	ΠΧ	Χ	Χ	Χ	Μ	Μ	Μ	Υ	Υ	Υ	ΠΥ	ΠΥ	ΠΥ
ΕΠΙΠΕΔΟ ΑΔΥΝΑΜΙΑΣ		Χ	Μ	Υ	Χ	Μ	Υ	Χ	Μ	Υ	Χ	Μ	Υ	Χ	Μ	Υ
ΕΠΙΠΤΩΣΗ	ΠΧ	ΠΧ	ΠΧ	ΠΧ	ΠΧ	ΠΧ	ΠΧ	ΠΧ	ΠΧ	Χ	Χ	Χ	Χ	Χ	Χ	Μ
	Χ	ΠΧ	ΠΧ	Χ	Χ	Χ	Χ	Χ	Χ	Μ	Μ	Μ	Μ	Μ	Μ	Μ
	Μ	Χ	Χ	Μ	Μ	Μ	Μ	Μ	Μ	Μ	Μ	Υ	Υ	Υ	Υ	Υ
	Υ	Μ	Μ	Μ	Μ	Υ	Υ	Υ	Υ	Υ	Υ	Υ	Υ	Υ	ΠΥ	ΠΥ
	ΠΥ	Υ	Υ	Υ	Υ	Υ	Υ	Υ	ΠΥ	ΠΥ	ΠΥ	ΠΥ	ΠΥ	ΠΥ	ΠΥ	ΠΥ

- Προτείνονται μέτρα ασφάλειας για όλα τα αγαθά και για κάθε συνδυασμό Αγαθού – Απειλής
- Τα μέτρα προστασίας χωρίζονται σε ομάδες, ανάλογα με το είδος των απειλών που καλούνται να αντιμετωπίσουν και ανάλογα με το είδος των αγαθών που καλούνται να προστατέψουν.
- Προτεινόμενα μέτρα:
  - Τεχνικά
  - Διοικητικά
  - Οργανωτικά



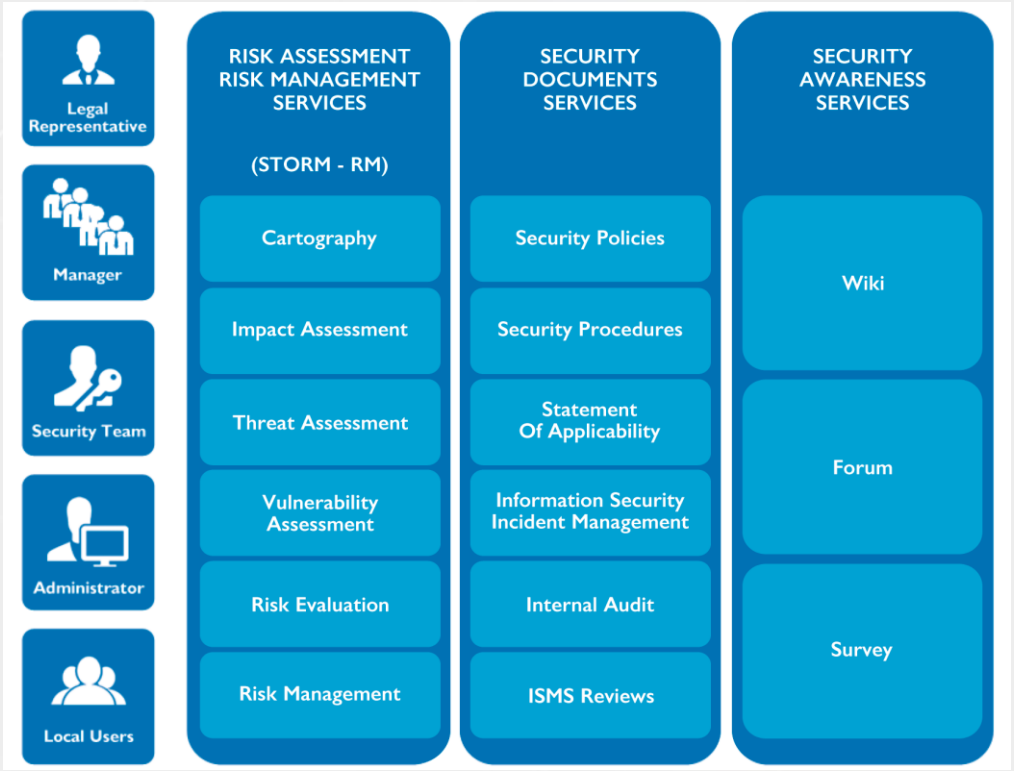
Τα αποτελέσματα της παραπάνω διαδικασίας είναι μια λίστα με όλα τα μέτρα ανάλογα με τον *βαθμό υλοποίησής* τους ως εξής:

- άμεση υλοποίηση,
- προτεινόμενο για υλοποίηση,
- υπό συζήτηση,
- μη εφαρμόσιμο.

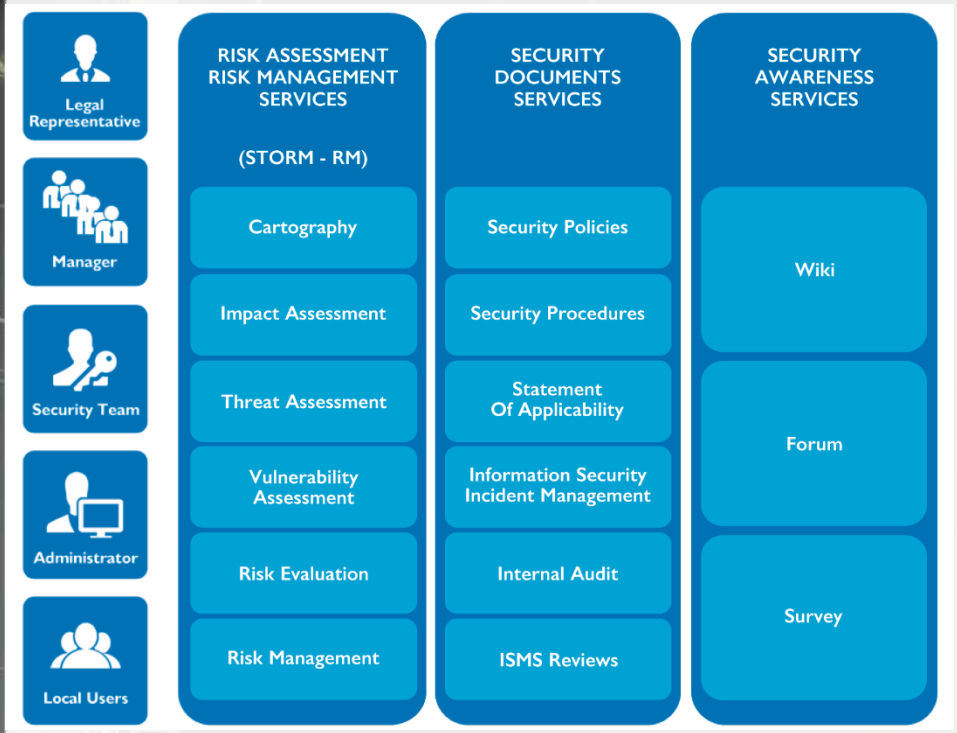
Στην τελευταία αυτή Φάση υπάρχει η δυνατότητα δημιουργίας όλων των αποτελεσμάτων από κάθε Φάση και επιμέρους Βήμα της μεθοδολογίας με μορφή αναφοράς:

- Η λίστα αγαθών και των αλληλεξαρτήσεων,
- Η Αναφορά Ανάλυσης Επικινδυνότητας,
- Η Αναφορά κατάλληλων μέτρων προστασίας.

STORM™ - Secure TOol for Risk Management



STORM
Secure TOol for Risk Management



- Innovative, collaborative, cost effective and user friendly security consultancy environment.
- Can be used by different type of organizations in order to collaboratively manage their information security.
- Offers a bundle of targeted services to the ICT users in order to guide them to securely manage their ICT systems.
- Based on the PDCA model of the ISO27001 security standard.

STORM SERVICES
Υπηρεσία Χαρτογράφησης (Cartography Service)

- Προσδιορισμός και καταγραφή όλων των Πληροφοριακών Αγαθών (φυσικά αγαθά, υλικό, λογισμικό, δεδομένα, χρήστες) του υπό εξέταση ΠΣ.
- Μέσω της συγκεκριμένης υπηρεσίας, οι χρήστες είναι σε θέση να αποθηκεύσουν με την βοήθεια των ειδικά διαμορφωμένων φορμών αλλά και κα να κατεβάσουν σε μορφή PDF αρχείων τις εξής αναφορές (reports):
  - Λίστα Υποδομών (List of Physical Assets)
  - Λίστα Υπηρεσιών (List of Services)
  - Λίστα Χρηστών (List of Users)
  - Λίστα Αγαθών (Asset Inventory)
  - Λίστα Αγαθών και Αλληλεξαρτήσεων (STORM-RM Asset Model)

STORM SERVICES
Υπηρεσία Αποτίμησης Επιπτώσεων Ασφάλειας (Impact Assessment Service)

- Προσδιορισμός, καταγραφή και ανάλυση των επιπτώσεων απώλειας ασφάλειας (απώλεια διαθεσιμότητας, εμπιστευτικότητας ή/και ακεραιότητας) όλων των αγαθών του υπό εξέταση ΠΣ, με την βοήθεια ηλεκτρονικών ερωτηματολογίων (σύμφωνα με την κλίμακα της μεθοδολογίας STORM-RM).
- Προβολή αποτελεσμάτων μέσω ειδικά διαμορφωμένων γραφημάτων
- Εξαγωγή αποτελεσμάτων σε μορφή εγγράφων PDF / Excel

STORM SERVICES
Υπηρεσία Αποτίμησης Απειλών (Threat Assessment Service)

- Προσδιορισμός και αξιολόγηση των απειλών που αντιμετωπίζει κάθε αγαθό του υπό εξέταση ΠΣ, με τη βοήθεια ηλεκτρονικών ερωτηματολογίων.
- Για κάθε αγαθό (ανάλογα με το είδος του) υπάρχει αντιστοίχιση ομάδων απειλών και δίνεται η δυνατότητα αποτίμησης του επιπέδου αποτίμησης απειλών, σύμφωνα με την κλίμακα της μεθοδολογίας STORM-RM.
- Προβολή αποτελεσμάτων μέσω ειδικά διαμορφωμένων γραφημάτων
- Εξαγωγή αποτελεσμάτων σε μορφή εγγράφων PDF / Excel

STORM SERVICES
Υπηρεσία Αποτίμησης Αδυναμιών (Vulnerability Assessment Service)

- Προσδιορισμός και αξιολόγηση των αδυναμιών ως προς τις απειλές που αντιμετωπίζει κάθε αγαθό του υπό εξέταση ΠΣ, με τη βοήθεια ηλεκτρονικών ερωτηματολογίων (σύμφωνα με την κλίμακα της μεθοδολογίας STORM-RM).
- Για κάθε απειλή υπάρχει η αντιστοίχιση των αδυναμιών ασφάλειας που σχετίζονται με αυτή την απειλή.
- Προβολή αποτελεσμάτων μέσω ειδικά διαμορφωμένων γραφημάτων
- Εξαγωγή αποτελεσμάτων σε μορφή εγγράφων PDF / Excel

STORM SERVICES

Υπηρεσία Αποτίμησης Επικινδυνότητας (Risk Evaluation Service)

- Γίνεται ο υπολογισμός του επιπέδου επικινδυνότητας κάθε αγαθού και παρουσιάζονται όλα τα αποτελέσματα με τη βοήθεια γραφημάτων.
- Προβολή αποτελεσμάτων μέσω ειδικά διαμορφωμένων γραφημάτων
- Εξαγωγή αποτελεσμάτων σε μορφή εγγράφων PDF / Excel:
  - Αποτελέσματα αποτίμησης επιπτώσεων (Impact Assessment Report)
  - Αποτελέσματα αποτίμησης απειλών (Threat Assessment Report)
  - Αποτελέσματα αποτίμησης αδυναμιών (Vulnerability Assessment Report)
  - Αποτέλεσμα ανάλυσης επικινδυνότητας (STORM Risk Assessment Report)

STORM SERVICES
Υπηρεσία Διαχείρισης Επικινδυνότητας (Risk Management Service)

- Επιλογή κατάλληλων μέτρων ασφάλειας, με σκοπό τη βέλτιστη προστασία των πληροφοριακών αγαθών.
- Για κάθε συνδυασμό αγαθού-απειλής προτείνονται διαφορετικά μέτρα (π.χ. τεχνικά, οργανωτικά κλπ.)
- Δημιουργία του Σχεδίου Διαχείρισης Επικινδυνότητας (Risk Treatment Report).
- Ανάθεση ενεργειών σε χρήστες του οργανισμού

STORM SERVICES

Υπηρεσία Διαχείρισης εγγράφων ασφάλειας (Security Documents Services)

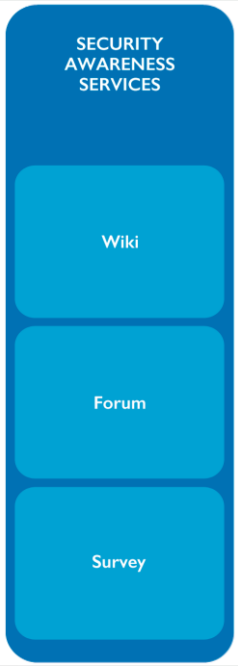
- Δημιουργία, ανανέωση, αποθήκευση και εκτύπωση των **Σχεδίου Ασ*φάλειας*** του υπό εξέταση ΠΣ (βασισμένη στο πρότυπο ασφάλειας ISO 27001:2013),
- Δημιουργία, ανανέωση, αποθήκευση και εκτύπωση των **Πολιτικών Ασφάλειας** του υπό εξέταση ΠΣ (βασισμένη στο πρότυπο ασφάλειας ISO 27001:2013),
- Δημιουργία, ανανέωση, αποθήκευση και εκτύπωση των **Διαδικασιών Ασ*φάλειας*** του υπό εξέταση ΠΣ (βασισμένη στο πρότυπο ασφάλειας ISO 27001:2013),
- Δημιουργία, ανανέωση, αποθήκευση και εκτύπωση του **Statement Of Applicability** του υπό εξέταση ΠΣ (βασισμένη στο πρότυπο ασφάλειας ISO 27001:2013),
- Αναφορά και διαχείριση των **Περιστατικών Ασφάλειας** του υπό εξέταση ΠΣ. Στην υπηρεσία αυτή, οι χρήστες είναι σε θέση να καταγράψουν όλα τα περιστατικά ασφάλειας με λεπτομέρειες όπως το αγαθό που επηρεάστηκε, την ημερομηνία εκδήλωσης του περιστατικού, το επίπεδο επίπτωσης, τις διορθωτικές και προληπτικές ενέργειες κλπ, ενώ ταυτόχρονα μπορεί να αποθηκεύσουν και εκτυπώσουν τόσο την φόρμα καταγραφής περιστατικών ασφάλειας όσο και την λίστα με τα υπάρχοντα περιστατικά.
- Καταγραφή όλων των **Ευρημάτων** που προκύπτουν από τις εσωτερικές επιθεωρήσεις (internal audits) καθώς και η ανάθεση των διορθωτικών ενεργειών στους κατάλληλους χρήστες προς υλοποίηση μέσω του μηχανισμού task της εφαρμογής.

Καταγραφή των **Πρακτικών Συναντήσεων της Ομάδας Ασφάλειας**

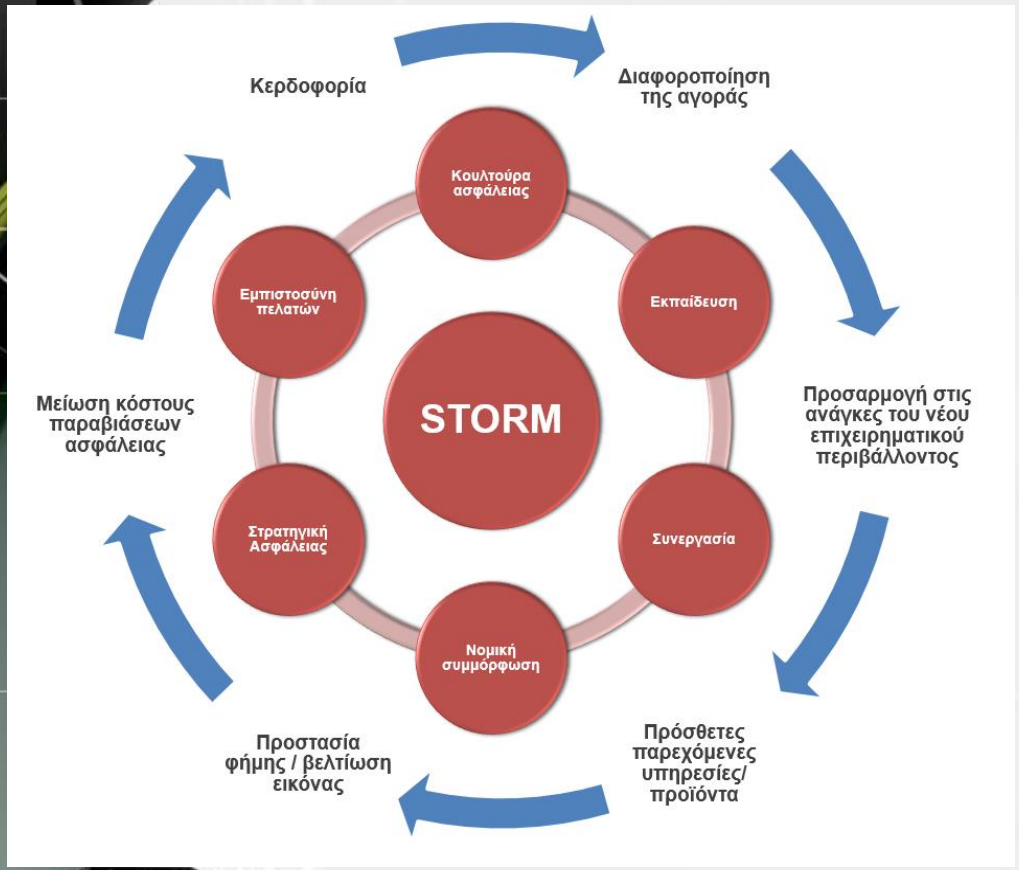
STORM SERVICES

Υπηρεσίες Εκπαίδευσης και Επαγρύπνησης Ασφάλειας (Security Awareness)

- Πρόκειται για μια ομάδα συνεργατικών υπηρεσιών (όπως Wiki/Forum/ η-Βιβλιοθήκη /ερωτηματολόγια) οι οποίες ως στόχο έχουν να διευκολύνουν την συνεργατικότητα και την ανταλλαγή απόψεων και ιδεών σε θέματα ασφάλειας ΠΣ, ενώ ταυτόχρονα θα είναι σε θέση να βοηθήσουν τους χρήστες στην άμεση εύρεση λύσεων τυχόν καθημερινών προβλημάτων ασφάλειας.
- Επιπρόσθετα, οι εν λόγω υπηρεσίες έχουν ως στόχο την συνεχή εκπαίδευση και ενημέρωση των χρηστών πάνω σε θέματα ασφάλειας ώστε να είναι διαρκώς ενημερωμένοι με τις διαδικασίες και πολιτικές που εφαρμόζονται στον οργανισμό τους



STORM advantages



- αποτελεσματικότερη αποτύπωση και καταγραφή των κρίσιμων υπηρεσιών της υποκείμενης υποδομής, των εξαρτώμενων αγαθών όπως, επίσης, και των εφαρμοζόμενων μέτρων ασφάλειας,
- ευέλικτη αποτίμηση των επιπτώσεων που επιφέρει η παραβίαση της ασφάλειας (απώλεια διαθεσιμότητας, εμπιστευτικότητας ή/και ακεραιότητας) των επιμέρους συστατικών της υποδομής,
- ακριβέστερη αποτίμηση της τρωτότητας των σύνθετων συστημάτων και υποδομών,
- σαφής καθορισμός των απειλών που αντιμετωπίζουν οι υποδομές,
- καθορισμός της επικινδυνότητας και της κρισιμότητας των επιμέρους συστατικών της υποδομής με αντικειμενικότερα κριτήρια, και
- προσδιορισμός των μέτρων ασφάλειας που ικανοποιούν σε μεγαλύτερο βαθμό τις απαιτήσεις ασφάλειας των συστημάτων, ενώ, παράλληλα αντιμετωπίζουν με αποτελεσματικότερο τρόπο τους κινδύνους στους οποίους είναι εκτεθειμένα τα αγαθά.
- στην αύξηση της κουλτούρας ασφάλειας ΠΣ,
- στην υιοθέτηση μιας στρατηγικής ασφάλειας η οποία μπορεί να ενσωματωθεί στην υπάρχουσα επιχειρησιακή λειτουργία και λογική των εταιριών.

References

1. Gritzalis D., “Insider threat prevention through Open Source Intelligence based on Online Social Networks”, Keynote address, *13th European Conference on Cyber Warfare and Security* (ECCWS-2014), Greece, 2014.
2. Kotzanikolaou P., Theoharidou M., Gritzalis D., “Risk assessment of multi-order interdependencies between critical information and communication infrastructures”, Critical Information Infrastructure Protection and Resilience in the ICT Sector, pp. 151-170, IGI Global, 2013.
3. Kotzanikolaou P., Theoharidou M., Gritzalis D., “Accessing n-order dependencies between critical infrastructures”, International Journal of Critical Infrastructure Protection, Vol. 9, Nos, 1-2, pp. 93-110, 2013.
4. Kotzanikolaou P., Theoharidou M., Gritzalis D., “Cascading effects of common-cause failures on Critical Infrastructures, in Proc. of the 7th IFIP International Conference on Critical Infrastructure Protection, pp. 171-182, Springer (AICT 417), USA, March 2013.
5. Kotzanikolaou P., Theoharidou M., Gritzalis D., “Interdependencies between Critical Infrastructures: Analyzing the Risk of Cascading Effects”, in Proc. of the 6th International Workshop on Critical Infrastructure Security, pp. 107-118, Springer (LNCS 6983), Switzerland, September 2011.
6. Ntouskas, T., Pentafronimos G., Papastergiou, S., "STORM - Collaborative Security Management Environment", in Proc. of WISTP-2011, Springer, LNCS 6633, pp. 320-335, 2011.
7. Ntouskas, T., Polemi, N., "STORM-RM: a collaborative and multicriteria risk management methodology", Int. Journal of Multicriteria Decision Making, Vol. 2, No. 2, pp. 159–177, 2012.
8. Ntouskas T., Kotzanikolaou P., Polemi N., "Impact Assessment through Collaborative Asset Modeling: The STORM-RM approach", in Proc. of the 1st International Symposium & 10th Balkan Conference on Operational Research, Thessaloniki, Greece, 2011.
9. Polemi D., Ntouskas T., Georgakakis E., Douligeris C., Theoharidou M., Gritzalis D., “S-Port: Collaborative security management of Port Information Systems”, in Proc. of the 4th International Conference on Information, Intelligence, Systems and Applications, IEEE Press, Greece, 2013.
10. Theoharidou M., Kotzanikolaou P., Gritzalis D., “Risk-based Criticality Analysis”, in Proc. of the 3rd IFIP International Conference on Critical Infrastructure Protection, Springer, USA, March 2009.
11. Theoharidou M., Kotzanikolaou P., Gritzalis D., “A multi-layer criticality assessment methodology based on interdependencies”, Computers & Security, Vol. 29, No. 6, pp. 643-658, 2010.
12. Theoharidou M., Kotzanikolaou P., Gritzalis D., “Risk assessment methodology for interdependent Critical Infrastructures”, International Journal of Risk Assessment and Management, Vol. 15, Nos. 2/3, pp. 128-148, 2011.
13. Theoharidou M., Kandias M., Gritzalis D., “Securing Transportation-Critical Infrastructures: Trends and Perspectives”, in Proc. of the 7th IEEE International Conference in Global Security, Safety and Sustainability, pp. 171-178, Springer (LNICST 99), Greece, 2012.
14. Stergiopoulos G., Theocharidou M., Kotzanikolaou P., Gritzalis D., “Using centrality measures in dependency risk graphs for efficient risk mitigation”, in Critical Infrastructure Protection IX, pp. 25-40, Springer, 2015.
15. Stergiopoulos G., Kotzanikolaou P., Theoharidou M., Gritzalis D., "Risk mitigation strategies for Critical Infrastructures based on graph centrality analysis", International Journal of Critical Infrastructure Protection, September 2015.
16. Stergiopoulos G., Theoharidou M., Gritzalis D., "Using logical error detection in remote-terminal units to predict initiating events of Critical Infrastructures failures", Proc. of the 3rd International Conference on Human Aspects of Information Security, Privacy & Trust, Springer, USA, 2015.