ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΨΗΦΙΑΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ
ΓΕΝΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ ΑΞΙΟΛΟΓΗΣΗΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Οδηγίες συμπλήρωσης

Αρχείο Αλλαγών

Έκδοση	Ημερομηνία	Περιγραφή	Ενότητες
2.1	23/02/2009	2η Έκδοση, Υποέκδοση 1	
2.15	17/03/2009	2η Έκδοση, Υποέκδοση 5	
2.16	03/09/2010	2η Έκδοση, Υποέκδοση 6	
3	25/08/2010	3η Έκδοση	
3.1	13/09/2010	3η Έκδοση, Υποέκδοση 1	
3.17	11/10/2011	3η Έκδοση, Υποέκδοση 7	
3.18	22/11/2012	3η Έκδοση, Υποέκδοση 8	
3.19	31/01/2013	3η Έκδοση, Υποέκδοση 9	
3.3	08/10/2013	3η Έκδοση, Υποέκδοση 3	
3.4	04/02/2014	3η Έκδοση, Υποέκδοση 4	
3.5	23/12/2014	3η Έκδοση, Υποέκδοση 5	
4	25/01/2016	4η Έκδοση	
4.1	22/02/2018	4η Έκδοση, Υποέκδοση 1	
4.2	09/07/2019	4η Έκδοση, Υποέκδοση 2	

Πίνακας περιεχομένων

Κεφάλαιο 1:

Εισαγωγή

Κεφάλαιο 2:

Δομή της Μεθόδου

Κεφάλαιο 3:

Οδηγίες Υλοποίησης της Μεθόδου

Σημείωση:

Το παρόν έντυπο αφορά στις οδηγίες συμπλήρωσης του Ερωτηματολογίου/Εκθεσης Αξιολόγησης Ασφάλειας των Πληροφοριακών Συστημάτων στην περίπτωση εταιριών που αιτούνται για **Άδεια Εγκεκριμένου Οικονομικού Φορέα**, καθώς και την περίπτωση εταιριών που αιτούνται για έκδοση **Άδειας Χρήσης Απλουστευμένης Διασάφησης και Άδειας για τον Εκτελωνισμό στον οριζόμενο τόπο**.

ΚΕΦΑΛΑΙΟ 1

Εισαγωγή

Η ανάγκη διασφάλισης των συναλλαγών που διέπονται από την τελωνειακή νομοθεσία, τόσο εντός της Ευρωπαϊκής Ένωσης (ΕΕ), όσο και με τρίτες χώρες, καθώς και η αναγκαιότητα της συμμόρφωσης των οικονομικών φορέων με συγκεκριμένους κανόνες προστασίας και ασφάλειας οδήγησε την ΕΕ στη δημιουργία του θεσμού του Εγκεκριμένου Οικονομικού Φορέα (ΕΟΦ).

Πρόθεση της ΕΕ είναι η χορήγηση της ιδιότητας του ΕΟΦ σε αξιόπιστους οικονομικούς φορείς, οι οποίοι θα επωφελούνται, τόσο σε επίπεδο απλουστεύσεων που προβλέπονται από την τελωνειακή νομοθεσία, όσο και σε επίπεδο τελωνειακών διευκολύνσεων που αφορούν τελωνειακούς ελέγχους.

Ο στόχος της έννοιας του ΕΟΦ είναι να παρέχει αμοιβαία αναγνώριση σε διεθνές επίπεδο. Αυτό σημαίνει ταχύτερο τελωνισμό των εμπορευμάτων και αποφυγή χρονοβόρων διαδικασιών. Η αναγνώριση ενός οικονομικού φορέα ως εγκεκριμένου θα αποτελεί σημαντικό πλεονέκτημα, καθώς η ιδιότητα αυτή θα συνεπάγεται τη συμμόρφωση του φορέα με αυστηρά κριτήρια. Εάν δε ο φορέας είναι εγκεκριμένος και ως προς τις προϋποθέσεις ασφάλειας και προστασίας, τότε η ιδιότητα αυτή θα μπορεί να αποτελεί πιστοποίηση συναλλακτικής φερεγγυότητας και αξιοπιστίας.

Αρμόδιες υπηρεσίες και αρχές έχουν την αρμοδιότητα και ευθύνη της αξιολόγησης των υ-ΕΟΦ, ως προς το εάν τηρούν τα καθοριζόμενα κριτήρια. Με βάση τα αποτελέσματα της αξιολόγησης σε έναν υ-ΕΟΦ μπορεί να χορηγηθούν οι εξής Άδειες: (α). Άδεια ΕΟΦ - Τελωνειακές απλουστεύσεις (AEOC), (β). Άδεια ΕΟΦ - Ασφάλεια και Προστασία (AEOS) και (γ). Άδεια ΕΟΦ - Τελωνειακές απλουστεύσεις/Ασφάλεια και Προστασία (AEOF).

Τα συγκεκριμένα κριτήρια που πρέπει να πληροί ένας οικονομικός φορέας προκειμένου να του χορηγηθεί η Άδεια του ΕΟΦ καθορίζονται αναλυτικότερα στο άρ. 5α του Κανονισμού 648/2005. Μεταξύ των κριτηρίων αυτών υπάρχουν αυτά που αφορούν φυσική ασφάλεια εγκαταστάσεων, έλεγχο προσπέλασης σε σχετικούς χώρους, προστασία υλικών, έλεγχο ασφάλειας των υπαλλήλων, ασφάλεια της Τεχνολογίας της Πληροφορικής, προστασία μηχανογραφικών συστημάτων από μη εξουσιοδοτημένες παρεισφρύσεις, ευαισθητοποίηση και εκπαίδευση των εργαζομένων σε θέματα ασφάλειας κλπ.

Το παρόν έργο αναφέρεται και αφορά, αποκλειστικά και μόνον, την αξιολόγηση των μέτρων που εφαρμόζει ένας υ-ΕΟΦ για την ασφάλεια και την προστασία των (αυτοματοποιημένων) Πληροφοριακών Συστημάτων του (λογιστικών, διοικητικών κλπ.), στο πλαίσιο του ελέγχου των σχετικών προϋποθέσεων που πρέπει να πληροί ο υ-ΕΟΦ, όπως αυτές περιγράφονται στα κεφάλαια “Σύστημα Διαχείρισης Εμπορικών Καταχωρήσεων” και “Προδιαγραφές Ασφάλειας και Προστασίας”.

Ειδικότερα, το παρόν παραδοτέο εισαγάγει και περιγράφει τη μεθοδο ΓΓΠΣ-ΕΟΦ-ESMI[1] (**E**valuation of **S**ecurity **M**easures **I**mplementation), η οποία σχεδιάσθηκε για να χρησιμοποιηθεί για το σκοπό αυτό. Με τη χρήση της ΓΓΠΣ-ΕΟΦ-ESMI τα αρμόδια στελέχη της Διοίκησης μπορούν να αξιολογούν αν τα Μετρα Ασφάλειας των Πληροφοριακών Συστημάτων που λαμβάνει ένας υ-ΕΟΦ εφαρμόζονται ορθώς και πλήρως και συνεπώς να εισηγηθούν (ενδεχομένως μετά και από επιτόπιο έλεγχο στις εγκαταστασεις του υ-ΕΟΦ) αιτιολογημένα αν ο υ-ΕΟΦ αυτός πληροί τα συγκεκριμένα σχετικά κριτήρια.

Η επιλογή των κριτηρίων που σχετίζονται και αφορούν την Ασφάλεια των Πληροφοριακών Συστημάτων των υ-ΕΟΦ έγινε με βάση και σημείο αναφοράς το σχετικό ερωτηματολόγιο αυτο-αξιολόγησης που εκπόνησε η ΕΕ, σε συνεργασία με τα Κράτη-Μέλη. Το ερωτηματολόγιο αυτό είχε σκοπό να υποβοηθήσει τους υ-ΕΟΦ, στο πλαίσιο της σχετικής διεθνούς καλής πρακτικής, να (προ)αξιολογήσουν την εταιρεία τους, προκειμένου να αποκομίσουν μια πρώτηάποψη για το εάν πληρούν τα κριτήρια χορήγησης μιας Άδειας ΕΟΦ ή όχι.

Η ΓΓΠΣ-ΕΟΦ-ESMI είναι συνεργατική μέθοδος και βασίζεται στην πρόσφορη διεθνώς πρακτική της αυτο-αξιολόγησης μέσω δομημένων ερωτηματολογίων. Συνεπώς, για την εφαρμογή της είναι αναγκαία η ανταλαγή πληροφόρησης ή/και η δια ζώσης συνεργασία των αξιολογητών με τα αρμόδια στελέχη και τους συνεργάτες του υ-ΕΟΦ που εφαρμόζουν τα Μέτρα Ασφαλείας. Περαιτέρω, η μεθοδος αυτή διευκολύνει την ταχεία και ορθή αποτύπωση του τρόπου εφαρμογής των Μέτρων Ασφάλειας (δεδομενου ότι η εφαρμογή τους ενδείκνυται να περιγράφεται, καταρχήν, από όσους τα εφαρμόζουν), με αποτέλεσμα την αντικειμενικότερη, συνεπέστερη και ταχύτερη αξιολόγηση του υ-ΕΟΦ.

---

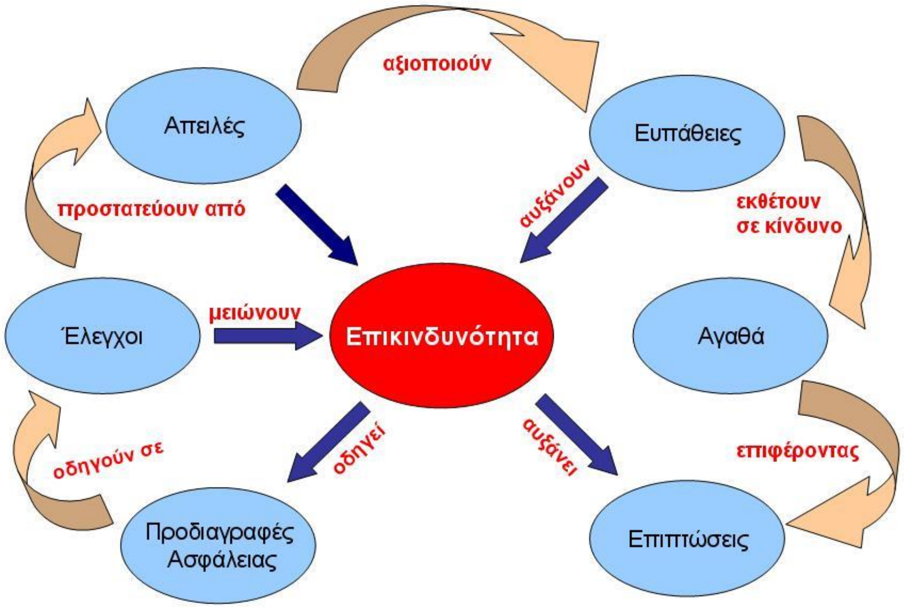
[1] Η μέθοδος ΓΓΠΣ-ΕΟΦ-ESMI αποτελεί εξειδίκευση και ειδική προσαρμογή της πρωτότυπης μεθόδου CIS-ESMI (βλ. Δ. Γκρίτζαλη, *Μέθοδος CIS-ESMI:Αξιολόγηση της εφαρμογής των Μέτρων Ασφάλειας σε Πληροφοριακά Συστήματα και Κρίσιμες Υποδομές*, Τεχνική Αναφορά No. 2 (2006), Τμήμα Πληροφορικής, Οικονομικό Πανεπιστήμιο Αθηνών, Αθήνα 2006 (www.cis.aueb.gr).

ΚΕΦΑΛΑΙΟ 2

Δομή της Μεθόδου

Η μέθοδος ΓΓΠΣ-ΕΟΦ-ESMI σχεδιάσθηκε για να χρησιμοποιηθεί για την αξιολόγηση της εφαρμογής των Μέτρων Ασφάλειας των (αυτοματοποιημένων) Πληροφοριακών Συστημάτων των υποψήφιων Εγκεκριμένων Οικονομικών Φορέων (υ-ΕΟΦ).

Όπως είναι γνωστό από τη βιβλιογραφία, τα Μέτρα Ασφάλειας ενός Πληροφοριακού Συστήματος προκύπτουν, σύμφωνα με την πιο πρόσφορη μεθοδολογία, ως αποτέλεσμα της ανάλυσης και αποτίμησης της επικινδυνότητάς του (risk analysis/assessment) (βλ. Διάγραμμα 1).



Διάγραμμα 1: Ανάλυση Επικινδυνότητας Πληροφοριακού Συστήματος

Η ΓΓΠΣ-ΕΟΦ-ESMI αποτελείται από δύο επάλληλες Πράξεις (Actions). Κάθε πράξη υλοποιείται με τη χρήση ενός ειδικά σχεδιασμένου δομημένου έντυπου ερωτηματολογίου (structured questionnaire).

1. Η περιγραφή της εφαρμογής του Μέτρου Ασφάλειας αποτελεί την πρώτη Πράξη και υλοποιείται κατά κανόνα μια φορά, εκτός αν υπάρξει ανάγκη αναλυτικότερης περιγραφής του, οπότε μπορεί να επαναληφθεί και άλλες φορές, κατά την απόλυτη κρίση του Αξιολογητή.
2. Η αξιολόγηση της εφαρμογής του Μέτρου Ασφάλειας αποτελεί τη δεύτερη Πράξη και μπορεί να επαναληφθεί περισσότερες της μιας φορές, εάν και εφόσον η εφαρμογή κάποιων Μέτρων Ασφάλειας από έναν υ-ΕΟΦ δεν κριθεί αποδεκτή.

Ο Πίνακας 1 περιγράφει, επιγραμματικά, τις δύο Πράξεις που απαρτίζουν τη Μέθοδο, τους Φορείς που συμμετέχουν σε καθεμία, καθώς και το Ρόλο καθενός από τους συμμετέχοντες φορείς.

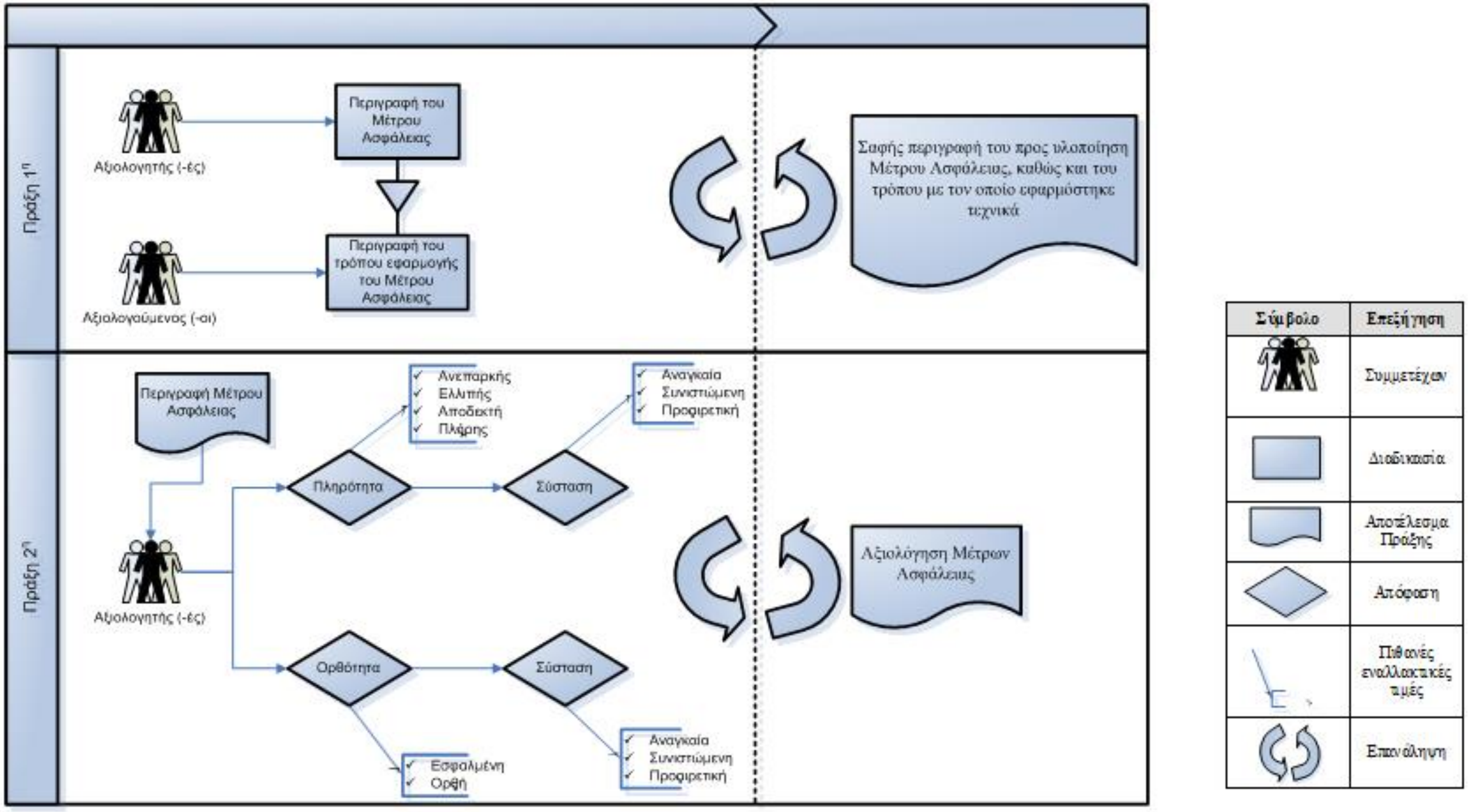
<table>
<tr><th colspan="2">ΠΕΡΙΓΡΑΦΗ ΜΕΘΟΔΟΥ ΓΓΠΣ-ΕΟΦ-ESMI©</th></tr>
<tr><td colspan="2">ΠΡΑΞΗ 1: Περιγραφή της εφαρμογής του Μέτρου Ασφάλειας</td></tr>
<tr><td><i>Συμμετέχων</i></td><td><i>Ρόλος</i></td></tr>
<tr><td>Αξιολογητής Ασφάλειας
(Αξιολογητής)</td><td>Ο ρόλος του Αξιολογητή είναι να περιγράψει[2] το Μέτρο Ασφάλειας, το οποίο πρέπει να εφαρμόσει ο αξιολογούμενος.</td></tr>
<tr><td>Υλοποιητής Μέτρων Ασφάλειας
(υ-ΕΟΦ, Αξιολογούμενος)</td><td>Ο ρόλος του Αξιολογούμενου, δηλαδή του υ-ΕΟΦ είναι να περιγράψει, με συνεκτικό, αλλά περιεκτικό και σαφή, τρόπο πώς εφάρμοσε το Μέτρο Ασφάλειας.</td></tr>
<tr><td><i>Επαναληπτικότητα Πράξης</i></td><td>Υπάρχει δυνατότητα επανάληψης της πράξης εάν πχ. διαπιστωθεί ότι η περιγραφή του Μέτρου Ασφάλειας δεν ήταν επαρκώς αναλυτική, ώστε να είναι αδιαμφισβήτητα σαφής για τον Αξιολογούμενο. Η επανάληψη είναι στην απόλυτη κρίση του Αξιολογητή.</td></tr>
<tr><td><i>Αποτέλεσμα Πράξης</i></td><td>Σαφής περιγραφή (της μη τεχνολογικά περιοριστικής προδιαγραφής) του προς υλοποίηση Μέτρου Ασφάλειας, καθώς και του τρόπου με τον οποίο εφαρμόστηκε τεχνικά από τον υ-ΕΟΦ.</td></tr>
<tr><td colspan="2">ΠΡΑΞΗ 2: Αξιολόγηση της εφαρμογής του Μέτρου Ασφάλειας</td></tr>
<tr><td><i>Συμμετέχων</i></td><td><i>Ρόλος</i></td></tr>
<tr><td>Αξιολογητής Ασφάλειας
(Αξιολογητής)</td><td>Ο ρόλος του Αξιολογητή είναι να εκτιμήσει εάν η εφαρμογή του Μέτρου Ασφάλειας έγινε με τον ενδεδειγμένο τρόπο. Αν δεν έγινε έτσι, τότε πρέπει να περιγράψει σε ποια σημεία αποκλίνει η προδιαγραφή του Μέτρου Ασφάλειας από την εφαρμογή του.</td></tr>
<tr><td><i>Επαναληπτικότητα Πράξης</i></td><td>Υπάρχει δυνατότητα επανάληψης της Πράξης, εφόσον εκτιμηθεί ότι η εφαρμογή του Μέτρου Ασφάλειας δεν καλύπτει κάποια από τις σχετικές απαιτήσεις πληρότητας ή/και ορθότητας.</td></tr>
<tr><td><i>Αποτέλεσμα Πράξης</i></td><td>Η στοιχειοθετημένη εκτίμηση (αξιολόγηση) του Αξιολογητή για την ορθότητα και πληρότητα της εφαρμογής του Μέτρου Ασφάλειας από τον Αξιολογούμενο.</td></tr>
</table>

Πίνακας 1: Συνοπτική περιγραφή μεθόδου αξιολόγησης ΓΓΠΣ-ΕΟΦ-ESMI

Συμπληρωματικά, το Διάγραμμα 2 παρέχει μια εποπτική περιγραφή της μεθόδου ΓΓΠΣ-ΕΟΦ-ESMI.

---

[2] Η περιγραφή των Μέτρων Ασφάλειας είναι αντίστοιχη με την αναφερόμενη στο ερωτηματολόγιο αυτο-αξιολόγησης ενός υ-ΕΟΦ. Σημειώνεται ότι η μορφή της περιγραφής αποτελεί λειτουργική προδιαγραφή (functional specification) του Μέτρου Ασφάλειας και δεν εξειδικεύει την τεχνολογία εφαρμογής κάθε Μέτρου.



Διάγραμμα 2: ΓΓΠΣ-ΕΟΦ-ESMI: Διαδικασία εφαρμογής της

ΚΕΦΑΛΑΙΟ 3

Οδηγίες Υλοποίησης της Μεθόδου

Όπως προαναφέρθηκε, η υλοποίηση κάθε μιας από τις δύο Πράξεις της ΓΓΠΣ-ΕΟΦ-ESMI βασίζεται στη συμπλήρωση, από τον αξιολογούμενο (καταρχήν) και τον αξιολογητή (στη συνέχεια), ενός κατάλληλα σχεδιασμένου και δομημένου έντυπου ερωτηματολογίου.

Το ερωτηματολόγιο που χρησιμοποιείται κατά την Πράξη 1 περιγράφεται στον Πίνακα 2. Αυτό που χρησιμοποιείται κατά την Πράξη 2 περιγράφεται στον Πίνακα 3.

ΓΓΠΣ-ΕΟΦ-ESMI©	**Περιγραφή εφαρμογής μέτρου ασφάλειας** (Πράξη 1 από 2)					
α/α Ερώτησης:	**1**					
1. Κωδικός μέτρου:		**2. Τμήμα - Υποτμήμα:**				
3. Περιγραφή μέτρου:						
4. Ποιόν αφορά:	Αξιολογούμενο		Τρίτο φορέα		Και τους δύο	
5. Κείμενο και μέθοδος αναφοράς:	Απάντηση Αξιολογούμενου					
6. Συνοπτική περιγραφή υλοποίησης μετρου:	Απάντηση Αξιολογούμενου					
7. Παραπομπές:	Απάντηση Αξιολογούμενου					
8. Αρμόδιοι για την υλοποίηση:	Απάντηση Αξιολογούμενου					
9. Σχόλια και παρατηρήσεις Αξιολογητή:						
10. Σημειώσεις και παραπομπές:						

Πίνακας 2: Πράξη 1: Ερωτηματολόγιο

Τα ερωτήματα που τίθενται κατά την Πράξη 1 απαντώνται από τον Αξιολογητή ή/και τον Αξιολογούμενο (όσα αφορούν τον αξιολογούμενο αναφέρονται ρητά στο ερωτηματολόγιο) είναι τα εξής:

[1]. Κωδικός μέτρου: Αναγράφεται από τον Αξιολογητή ο κωδικός αριθμός του Μέτρου Ασφάλειας, όπως αναφέρεται στο ερωτηματολόγιο αυτο-αξιολόγησης.

[2]. Τμήμα - Υποτμήμα: Αναγράφεται από τον Αξιολογητή το Τμήμα και το Υπο-τμήμα, όπως προκύπτει από το ερωτηματολόγιο αυτο-αξιολόγησης.

[3]. Περιγραφή του μέτρου: Αναγράφεται από τον Αξιολογητή η περιγραφή (λειτουργική προδιαγραφή) του Μέτρου Ασφάλειας, όπως αναφέρεται στο ερωτηματολόγιο αυτοαξιολόγησης. Εάν το Μέτρο Ασφάλειας αναλύεται σε περισσότερα των δύο επιπέδων, τότε κάθε επιμέρους Μέτρο Ασφάλειας καλύπτεται από ξεχωριστό έντυπο ερωτηματολόγιο.

[4]. Ποιόν αφορά: Αναγράφεται αν το Μέτρο Ασφάλειας αφορά τον Αξιολογούμενο (έτσι συμβαίνει κατά κανόνα) ή κάποιον τρίτο φορέα ή και τους δύο (ειδικές περιπτώσεις).

[5]. Κείμενο αναφοράς: Αναφέρεται από τον Αξιολογούμενο η ονομασία του εντύπου/κανονισμού-/διαδικασίας του υ-ΕΟΦ όπου περιγράφονται τα Μέτρα Ασφάλειας. Επίσης, αναφέρεται η μέθοδος με βάση την οποία εντοπίστηκε ως αναγκαίο το συγκεκριμένο Μέτρο Ασφάλειας (πχ. με ανάλυση επικινδυνότητας, από ειδικό εμπειρογνώμονα, μέσω ισομορφισμού με αντίστοιχο πληροφοριακό σύστημα, εμπειρικά κλπ.)

[6]. Συνοπτική περιγραφή υλοποίησης του μέτρου: Αναγράφεται από τον Αξιολογούμενο η τεχνολογία που επέλεξε για την εφαρμογή του Μέτρου Ασφάλειας, καθώς και ο τρόπος της (τεχνικής) εφαρμογής του. Η περιγραφή αυτή πρέπει να είναι συνοπτική, αλλά σαφής και περιεκτική.

[7]. Κείμενα παραπομπής: Αναφέρονται από τον Αξιολογούμενο τα κείμενα εκείνα στα οποία είτε υπάρχει περαιτέρω εξειδίκευση του τρόπου εφαρμογής του Μέτρου Ασφάλειας (πχ. Τεχνικό Εγχειρίδιο), είτε τα κείμενα όπου παρέχονται οδηγίες στους χρήστες των εφαρμογών για το πώς θα εφαρμόζουν το συγκεκριμένο Μέτρο Ασφάλειας (πχ. Οδηγός Χρήσης).

[8]. Αρμόδιοι για την υλοποίηση: Αναφέρονται από τον Αξιολογούμενο τα ονόματα και οι ιδιότητες των βασικών στελεχών (key persons) που σχεδίασαν την εφαρμογή και υλοποίησαν το Μέτρο Ασφάλειας.

[9]. Σχόλια και παρατηρήσεις αξιολογητή: Αναφέρονται από τον Αξιολογητή, συνοπτικά αλλά περιεκτικά, οι βασικές διαπιστώσεις που αφορούν τον τρόπο εφαρμογής του Μέτρου Ασφάλειας.

[10]. Σχόλια και παραπομπές: Στο χώρο αυτό υπάρχει η δυνατότητα να γίνουν ελεύθερα σχόλια από τον Αξιολογητή ή τον Αξιολογούμενο, κατά την κρίση τους. Για παράδειγμα, μπορεί να επισημανθεί (πράγμα που συμβαίνει αρκετές φορές) ότι το συγκεκριμένο Μέτρο Ασφαλείας δεν αφορά μόνο πληροφοριακά συστήματα, αλλά ενδεχομένως και φυσικές εγκαταστάσεις ή/και την

εφοδιαστική αλυσσίδα, οπότε θα πρέπει να αξιολογηθεί και από αντίστοιχους ειδικούς και όχι μόνο από ειδικούς Ασφάλειας Πληροφοριακών Συστημάτων.

Για τη διευκόλυνση του Αξιολογούμενου, οι ερωτήσεις στις οποίες πρέπει να απαντήσει (δηλαδή οι ερωτήσεις 5, 6, 7, 8 και ενδεχομένως η 10) είναι διαφορετικά γραμμοσκιασμένες στο έντυπο.

ΓΓΠΣ-ΕΟΦ-ESMI©	**Αξιολόγηση εφαρμογής μέτρου ασφάλειας** (Πράξη 2 από 2)			
α/α Ερώτησης:				
1. Κωδικός:		**2. Τμήμα - Υποτμήμα:**		
3. Ιστορικό της προσαρμογής μέτρου:	Αρχική αξιολόγηση		Επιπρόσθετη αξιολόγηση	Ιστορικότητα sn/safeguard-code/evaluation-date/ evaluator-name/recommend[cor(a,k),com(b,k)]

4. Αξιολόγηση της ορθότητας εφαρμογής του μέτρου:	**Εσφαλμένη**		**Ορθή**			
4Α. Σχόλια και παρατηρήσεις:						
4Β. Σκοπιμότητα περαιτέρω προσαρμογής μέτρου:	**Αναγκαία**		**Συνιστώμενη**		**Προαιρετική**	

5. Αξιολόγηση της πληρότητας εφαρμογής του μέτρου:	**Ανεπαρκής**		**Ελλιπής**		**Αποδεκτή**		**Πλήρης**	
5Α. Σχόλια και παρατηρήσεις:								
5Β. Σκοπιμότητα περαιτέρω προσαρμογής μέτρου:	**Αναγκαία**		**Συνιστώμενη**		**Προαιρετική**			

6Α. Πρώτος Αξιολογητής:	**6Β. Δεύτερος Αξιολογητής:**	**6Γ. Επόπτης Αξιολόγησης:**

Πίνακας 3: Πράξη 2: Ερωτηματολόγιο

Τα ερωτήματα που τίθενται κατά την Πράξη 2 απαντώνται, στο σύνολό τους, από τον Αξιολογητή και είναι τα εξής:

[1]. Κωδικός μέτρου: Αναγράφεται από τον Αξιολογητή ο κωδικός αριθμός του Μέτρου Ασφάλειας, όπως αναφέρεται στο ερωτηματολόγιο αυτο-αξιολόγησης.

[2]. Τμήμα - Υποτμήμα: Αναγράφεται από τον Αξιολογητή το Τμήμα και το Υπο-τμήμα του ερωτηματολογίου αυτο-αξιολόγησης, όπως αυτά είναι κωδικοποιημένα.

[3]. Ιστορικό της προσαρμογής του μέτρου: Εάν πρόκειται για την αρχική αξιολόγηση γίνεται σχετική αναφορά (tick). Αλλοιώς, υπάρχει προηγούμενο ερωτηματολόγιο που αναφέρεται στο ίδιο Μέτρο Ασφάλειας και σημειώνεται το ιστορικό των αλλαγών. Το ιστορικό έχει την εξής δομή:

sn: αύξων αριθμός αξιολόγησης του μέτρου

safeguard-code: κωδικός μέτρου

evaluation-date: ημερομηνία προηγούμενης αξιολόγησης

evaluator-name: όνομα Αξιολογητή

recommend [cor(a,k),com(b,k)]: αξιολόγηση ορθότητας και πληρότητας

[4]. Αξιολόγηση ορθότητας μέτρου: Αξιολογείται αν η εφαρμογή του Μέτρου Ασφάλειας έγινε με δόκιμο και επιστημονικά ενδεδειγμένο τρόπο.

Η διαπίστωση μπορεί να έχει μια από τις τιμές: {Εσφαλμένη, Ορθή}, συνοδεύεται από σχετική επιγραμματική τεκμηρίωση, καθώς και από ενδεχόμενη σύσταση για περαιτέρω ενέργειες, η οποία μπορεί να έχει μια από τις τιμές: {Αναγκαία, Συνιστώμενη, Προαιρετική}. Αν η τιμή της σύστασης είναι “Αναγκαία”, τότε ο Αξιολογούμενος οφείλει να προσαρμόσει την εφαρμογή του Μέτρου Ασφάλειας σύμφωνα με τη σύσταση του Αξιολογητή.

Σημειώνεται ότι ορισμένοι συνδυασμοί τιμών δεν είναι αποδεκτοί (πχ. {Ορθή, Αναγκαία}).

[5]. Αξιολόγηση πληρότητας μέτρου: Αξιολογείται αν η εφαρμογή του Μέτρου Ασφάλειας έγινε με τρόπο που καλύπτει πλήρως την αντίστοιχη προδιαγραφή του.

Η διαπίστωση μπορεί να έχει μια από τις τιμές: {Ανεπαρκής, Ελλιπής, Αποδεκτή, Πλήρης}, συνοδεύεται από σχετική συνοπτική τεκμηρίωση, καθώς και από ενδεχόμενη σύσταση για περαιτέρω ενέργειες, η οποία μπορεί να έχει μια από τις τιμές: {Αναγκαία, Συνιστώμενη, Προαιρετική}. Αν η τιμή της σύστασης είναι “Αναγκαία”, τότε ο Αξιολογούμενος οφείλει να επικαιροποιήσει την εφαρμογή του Μέτρου Ασφάλειας σύμφωνα με τη σύσταση του Αξιολογητή.

Σημειώνεται ότι ορισμένοι συνδυασμοί τιμών δεν είναι δυνατοί (πχ. {Πλήρης, Αναγκαία}).

[6]. Αξιολογητές: Αναφέρονται τα ονόματα όλων των Αξιολογητών, καθώς και το όνομα του επόπτη της Αξιολόγησης (αν υπάρχει).

Το αποτέλεσμα της αξιολόγησης είναι οι τιμές που αποδίδουν οι Αξιολογητές στην ορθότητα και την πληρότητα της εφαρμογής του Μέτρου Ασφάλειας. Οι περιπτώσεις μη θετικής αξιολόγησης (“απόρριψης” της εφαρμογής του Μέτρου Ασφάλειας) είναι οι εξής:

1. Ορθότητα: {Εσφαλμένη, Αναγκαία} ή {Εσφαλμένη, Συνιστώμενη}, συνδυαζόμενη με οποιαδήποτε τιμή Πληρότητας[3].
2. Πληρότητα: {Ανεπαρκής, Αναγκαία} ή {Ανεπαρκής, Συνιστώμενη} ή {Ελλιπής, Αναγκαία} ή {Ελλιπής, Συνιστώμενη}, συνδυαζόμενη με οποιαδήποτε τιμή Ορθότητας.

Σημειώνεται ότι η αξιολόγηση της ορθότητας και της πληρότητας της εφαρμογής ενός Μέτρου Ασφάλειας γίνεται “σειριακά”, τυπικά προηγούμενης της αξιολόγησης της ορθότητας της εφαρμογής του, αλλά χωρίς αυτό να έχει σημαντικό χαρακτήρα.

Όπως προαναφέρθηκε, το αποτέλεσμα των δύο πράξεων είναι η διαπίστωση εάν η εφαρμογή καθενός από τα Μέτρα Ασφάλειας έγινε με κάποιον αποδεκτό τρόπο, σύμφωνα με τις σχετικές κανονιστικές διατάξεις και τους κανόνες της Επιστήμης.

Για να διευκολυνθεί η διαδικασία αυτή, οι δύο πράξεις συνοδεύονται από ένα συγκεντρωτικό πίνακα, στον οποίον καταγράφεται επιγραμματικά το ιστορικό της επικαιροποίησης όσων Μέτρων Ασφάλειας αξιολογήθηκε ότι χρειάζεται τροποποίηση της εφαρμογής τους.

Μέσω του πίνακα αυτού είναι δυνατή η συνολική παρακολούθηση της εφαρμογής των Μέτρων Ασφάλειας, καθώς και η διαπίστωση της ολοκλήρωσης της αξιολόγησης, μέσω των τελικών αποτελεσμάτων της. Η δομή και τα συγκεκριμένα περιεχόμενα του πίνακα αυτού (πριν την αξιολόγηση) περιγράφεται στον Πίνακα 4.

Ένας υ-ΕΟΦ θεωρείται ότι αξιολογήθηκε θετικά ως προς την Ασφάλεια των (αυτοματοποιημένων) Πληροφοριακών Συστημάτων του, εάν διαπιστωθεί ότι ισχύει ένα από τα παρακάτω:

(α). Ελαβε όλα τα Μέτρα Ασφάλειας που όφειλε να λάβει και τα εφαρμόζει κατά τρόπο ορθό και πλήρη/αποδεκτό.

(β). Οι (όσες και όποιες) συστάσεις του υποδείχτηκαν είναι μόνον προαιρετικής μορφής.

---

[3] Ο συνδυασμός {Εσφαλμένη, Προαιρετική} καλύπτει μια ειδική συγκυρία. Ειδικότερα, αν ο Αξιολογούμενος υλοποίησε με εσφαλμένο τρόπο μια λειτουργικότητα ενός Μέτρου Ασφάλειας, η οποία δεν ζητείτο, τότε η προαιρετικότητα της επικαιροποίησής του Μέτρου Ασφάλειας σημαίνει ότι μπορεί είτε να διορθώσει την υλοποίηση της λειτουργικότητας αυτής, είτε να την αφαιρέσει (εφόσον είναι επιπλέον όσων απαιτούνται).

ΓΓΠΣ-ΕΟΦ-ESMI: Αξιολόγηση ασφάλειας πληροφοριακών συστημάτων

Ερώτηση	**α/α Ερώτησης**	**Αξιολόγηση Ορθότητας**		**Αξιολόγηση Πληρότητας**	
		Τιμή	*Σύσταση*	*Τιμή*	*Σύσταση*
Πιστοποιήσεις ασφάλειας Πληροφοριακών Συστημάτων	**1**				
	Ιστορικότητα[4]:				
Στοιχεία λογιστικού και αποθηκευτικού συστήματος	**2**				
	Ιστορικότητα:				
Διαθεσιμότητα πρωτότυπων on-line δεδομένων	**3**				
	Ιστορικότητα:				
Διαδικασίες εφεδρικής αποθήκευσης και ανάκτησης των δεδομένων. Διαδικασίες καταχώρησης/αποθήκευσης εγγράφων και πληροφοριών	**4**				
	Ιστορικότητα:				
Ύπαρξη σχεδίου ασφάλειας για αντιμετώπιση μη εξουσιοδοτημένης πρόσβασης, καταστροφής και απώλειας,	**5**				
	Ιστορικότητα:				
Ύπαρξη και έλεγχος διασυνδεσεων με απομακρυσμένα πληροφοριακά συστήματα	**6**				
	Ιστορικότητα:				
Υπεύθυνος ασφάλειας πληροφοριακού συστήματος	**7**				
	Ιστορικότητα:				
Έγκριση προσπέλασης στο πληροφοριακό σύστημα, κανόνες διαχείρισης κωδικών χρηστών, μεταφορά, διατήρηση, επικαιροποίηση στοιχείων χρήστη	**8**				
	Ιστορικότητα:				
Χρήση ειδικών προϊόντων ασφάλειας πληροφοριακών συστημάτων	**9**				
	Ιστορικότητα:				
Διαδικασία ελέγχου, καταγραφής και αντιμετώπισης συμβάντων	**10**				
	Ιστορικότητα:				
Ύπαρξη σχεδίου ανάκαμψης (DRP)	**11**				
	Ιστορικότητα:				

---

[4] Η ιστορικότητα έχει σημασία για την αξιολόγηση στις περιπτώσεις εκείνες στις οποίες η εφαρμογή του Μέτρου Ασφάλειας διορθώθηκε από τον Αξιολογούμενο, μετά από την αρχική (αρνητική) αξιολόγηση.

ΓΓΠΣ-ΕΟΦ-ESMI: Αξιολόγηση ασφάλειας πληροφοριακών συστημάτων

Τμήμα - Υποτμήμα	α/α Ερώτησης	Αξιολόγηση Ορθότητας		Αξιολόγηση Πληρότητας	
		Τιμή	*Σύσταση*	*Τιμή*	*Σύσταση*
Διαδικασίες συντήρησης εξοπλισμού / εφαρμογών. Προϋποθέσεις ασφάλειας σε συμβάσεις με συνεργάτες	**12**				
	Ιστορικότητα:				
Διαδικασίας αξιολόγησης ασφάλειας πληροφοριακών συστημάτων	**13**				
	Ιστορικότητα:				
Ειδικές διαδικασίες ασφάλειας από τρίτους	**14**				
	Ιστορικότητα:				
Πολιτική Ορθής Χρήσης. Σεμινάρια εκπαίδευσης/ευαισθητοποίησης σε ασφάλεια πληροφοριακών συστημάτων	**15**				
	Ιστορικότητα:				

Υπόμνημα	**Τιμή**	**Σύσταση**
Ορθότητα	Εσφαλμένη (**Ε**) Ορθή (**Ο**) Δεν έχει εφαρμογή (**Χ**)	Αναγκαία (**Α**) Συνιστώμενη (**Σ**) Προαιρετική (**Π**)
Πληρότητα	Ανεπαρκής (**ΑΝ**) Ελλιπής (**Ε**) Αποδεκτή (**ΑΠ**) Πλήρης (**Π**) Δεν έχει εφαρμογή (**Χ**)	

Πίνακας 1: Συνοπτικά αποτελέσματα αξιολόγησης της ασφάλειας των πληροφοριακών συστημάτων του υποψήφιου