ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ
ΠΛΗΡΟΦΟΡΙΚΗΣ και ΥΠΟΛΟΓΙΣΤΩΝ
ΔΙΙΔΡΥΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
«ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ»
2021-2022

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

«Διοίκηση Επικινδυνότητας Πληροφοριακών Συστημάτων: Σύγκριση πλαισίων, μεθοδολογιών και εργαλείων»

Συγγραφέας

ΜΑΡΙΛΕΝΑ ΤΣΕΣΜΕΛΗ

ΑΜ: 21036

Επιβλέπων: Στέφανος Γκρίτζαλης

Αιγάλεω, Μάιος 2023

ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ

ΠΛΗΡΟΦΟΡΙΚΗΣ και ΥΠΟΛΟΓΙΣΤΩΝ

ΔΙΙΔΡΥΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

«ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ»

2021-2022

«Διοίκηση Επικινδυνότητας Πληροφοριακών Συστημάτων: Σύγκριση πλαισίων, μεθοδολογιών και εργαλείων»

Μέλη Εξεταστικής Επιτροπής συμπεριλαμβανομένου και του Εισηγητή

Η μεταπτυχιακή διπλωματική εργασία εξετάστηκε επιτυχώς από την κάτωθι Εξεταστική Επιτροπή:

Α/α	ΟΝΟΜΑ ΕΠΩΝΥΜΟ	ΒΑΘΜΙΔΑ/ΙΔΙΟΤΗΤΑ	ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ
1	Στέφανος Γκρίτζαλης	Εισηγητής - Επιβλέπων	STEFANOS GKRITZALIS 01/06/2023 17:03
2	Παναγιώτης Γιαννακόπουλος	Μέλος Εξεταστικής Επιτροπής	Panagiotis Giannakopoulos Digitally signed by Panagiotis Giannakopoulos Date: 2023.08.22 11:11:54 +03'00'
3	Δημήτριος Κόγιας	Μέλος Εξεταστικής Επιτροπής	

Αιγάλεω, Μάιος 2023

Η παρούσα διπλωματική εργασία εκπονήθηκε στο πλαίσιο των απαιτήσεων του Διιδρυματικού Προγράμματος Μεταπτυχιακών Σπουδών στην Κυβερνοασφάλεια του τμήματος Μηχανικών Πληροφορική και Υπολογιστών του Πανεπιστημίου Δυτικής Αττικής. Η έγκρισή της δεν υποδηλώνει απαραιτήτως και την αποδοχή των απόψεων του συγγραφέα εκ μέρους του Μηχανικών Πληροφορική και Υπολογιστών.

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Η κάτωθι υπογεγραμμένη Μαριλένα Τσεσμελή του Στυλιανού με αριθμό μητρώου 21036 φοιτήτρια του Προγράμματος Μεταπτυχιακών Σπουδών «ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ» του Τμήματος Μηχανικών Πληροφορικής και Υπολογιστών της Σχολής Μηχανικών του Πανεπιστημίου Δυτικής Αττικής, δηλώνω ότι:

«Είμαι συγγραφέας αυτής της Διπλωματικής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από μένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος.

Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου».

Η Δηλούσα

Ευχαριστίες

Θα ήθελα να ευχαριστήσω θερμά τον σύμβουλο και επιβλέπων καθηγητή μου κύριο Στέφανο Γκρίτζαλη για την υποστήριξη, καθοδήγηση και ενθάρρυνση που μου παρείχε καθ' όλη τη διάρκεια εκπόνησης αυτής της διπλωματικής εργασίας. Θα ήθελα επίσης να ευχαριστήσω την οικογένειά μου για την αγάπη και την αμέριστη υποστήριξή της στην ακαδημαϊκή μου πορεία. Τέλος θα ήθελα να εκφράσω την ευγνωμοσύνη μου σε αυτούς που με την ύπαρξή τους, στην άλλη άκρη του πλανήτη, ήταν πηγή έμπνευσης και δημιουργικότητας για μένα τα τελευταία χρόνια.

Για τη Λίλη

ΠΕΡΙΛΗΨΗ

Η διαχείριση επικινδυνότητας της ασφάλειας πληροφοριών αποτελεί κρίσιμη πτυχή των σύγχρονων οργανισμών και επιχειρήσεων και έχει αποκτήσει ιδιαίτερη σημασία τα τελευταία χρόνια λόγω της αυξανόμενης πολυπλοκότητας των απειλών στον κυβερνοχώρο. Η παρούσα διπλωματική εργασία έχει ως στόχο να παράσχει μια συγκριτική αξιολόγηση των πλαισίων, μεθοδολογιών και εργαλείων που χρησιμοποιούνται στη διαχείριση της επικινδυνότητας της ασφάλειας πληροφοριών. Η μεθοδολογία που υιοθετήθηκε στην παρούσα διατριβή περιλαμβάνει μία ανασκόπηση των υφιστάμενων πλαισίων, μεθοδολογιών και εργαλείων που χρησιμοποιούνται στη διαχείριση κινδύνων ασφάλειας πληροφοριών. Στη συνέχεια, τα πλαίσια, οι μεθοδολογίες και τα εργαλεία αξιολογήθηκαν και συγκρίθηκαν με βάση τα κριτήρια που επιλέχθηκαν και ορίστηκαν κατάλληλα, στο πλαίσιο της παρούσας εργασίας ,όπως η χρηστικότητά και το επίπεδο τεχνικότητας, η ευκολία χρήσης και η ενσωμάτωσή τους στις υφιστάμενες διαδικασίες και συστήματα, ο χρόνος εφαρμογής και το κόστος του καθενός κλπ.. Τα αποτελέσματα της συγκριτικής αξιολόγησης αναδεικνύουν τα δυνατά και αδύνατα σημεία των διαφόρων πλαισίων, μεθοδολογιών και εργαλείων και παρέχουν πληροφορίες σχετικά με τις βέλτιστες πρακτικές για την αποτελεσματική διαχείριση της επικινδυνότητας της ασφάλειας πληροφοριών. Η παρούσα διατριβή αναμένεται να είναι ένα χρηστικό εργαλείο για τους οργανισμούς που επιθυμούν να εφαρμόσουν ή να βελτιώσουν τις διαδικασίες διαχείρισης κινδύνων ασφάλειας πληροφοριών, καθώς και για τους ερευνητές που ενδιαφέρονται να διερευνήσουν περαιτέρω το θέμα. Επίσης η παρούσα μελέτη αναμένεται να συμβάλει στην πρόοδο του τομέα της διαχείρισης επικινδυνότητας της ασφάλειας πληροφοριών, παρέχοντας μια βαθύτερη κατανόηση των διαφόρων διαθέσιμων πλαισίων, μεθοδολογιών και εργαλείων και των αντίστοιχων δυνατών και αδύνατων σημείων τους.

Λέξεις - κλειδιά: Πλαίσια – Μεθοδολογίες – Εργαλεία διαχείρισης επικινδυνότητας , Ασφάλεια πληροφοριών, Συγκριτικά κριτήρια αξιολόγησης, Βέλτιστες πρακτικές, Τεχνολογία Πληροφοριών, Κυβερνοασφάλεια , Διοίκηση επικινδυνότητας.

ABSTRACT

Information security risk management is a critical aspect of modern organisations and businesses and has become particularly important in recent years due to the increasing complexity of cyber threats. This thesis aims to provide a comparative assessment of the frameworks, methodologies and tools used in information security risk management. The methodology adopted in this thesis includes a review of existing frameworks, methodologies and tools used in information security risk management. The frameworks, methodologies and tools were then evaluated and compared based on the criteria selected and appropriately defined, in the context of this thesis, such as usability and level of technicality, ease of use and integration into existing processes and systems, implementation time and cost of each, etc. The results of the benchmarking evaluation highlight the strengths and weaknesses of the different frameworks, methodologies and tools and provide information on the best practices for the implementation of the various frameworks, methodologies and tools. This thesis is expected to be a useful tool for organizations wishing to implement or improve their information security risk management processes, as well as for researchers interested in further exploring the topic. This study is also expected to contribute to the advancement of the field of information security risk management by providing a deeper understanding of the various frameworks, methodologies and tools available and their respective strengths and weaknesses.

Key-words: Frameworks - Methodologies - Risk management tools, Information security, Benchmarking criteria, Best practices, Information technology, Cybersecurity, Risk management.

Περιεχόμενα

Συντομογραφίες

ATP	Advanced Threat Protection
CERT	Computer Emergency Response Team
COBIT	Control Objectives for Information Technologies
COSO	Committee of Sponsoring Organizations
CS	Control Strength
CSF	Cybersecurity Framework
CVE	Common Vulnerabilities and Exposures
ERM	Enterprise Risk Management
EU	European Union
FABOK	FAIR Analysis Body of Knowledge
FAIR	Factor Analysis of Information Risk
GSM	Greenbone Security Manager
IC-IF	Internal Control-Integrated Framework
IEC	International Electrotechnical Commission
IoT	Internet of Things
ISA	Information Security Assessment
ISACA	Information Systems Audit and Control Association
ISMS	Information Security Management System
ISO	International Organization for Standardization
ITSRM²	IT Security Risk Management Methodology
LEF	Loss Event Frequency
MSAT	Microsoft Security Assessment Tool
MSRSAT	Microsoft Security Risk Self-Assessment Tool
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
OWASP	Open Web Application Security Project
PLM	Primary Loss Magnitude
SCM	Security Compliance Manager
TCap	Threat Capability
Vuln	Vulnerability
ATP	Advanced Threat Protection

1. Εισαγωγή

1.1 Ιστορικό και κίνητρα της μελέτης

Η σημασία της ασφάλειας των πληροφοριών έχει αυξηθεί σημαντικά τα τελευταία χρόνια, καθώς οι οργανισμοί βασίζονται όλο και περισσότερο σε ψηφιακά συστήματα και δίκτυα για την αποθήκευση και επεξεργασία ευαίσθητων και μη πληροφοριών. Ως αποτέλεσμα, η διαχείριση της επικινδυνότητας για την ασφάλεια των πληροφοριών έχει καταστεί ένα ζωτικής σημασίας ζήτημα για τους οργανισμούς όλων των μεγεθών και όλων των κλάδων. Ο κίνδυνος στον κυβερνοχώρο, ο οποίος αρχικά ήταν τεχνολογικός κίνδυνος, έχει πλέον μετατραπεί σε επιχειρησιακό κίνδυνο και σήμερα πλέον, επηρεάζει όλα τα επίπεδα μιας εταιρείας, μέχρι και τον διευθύνοντα σύμβουλο.
Με την αυξανόμενη απειλή των επιθέσεων στον κυβερνοχώρο, των παραβιάσεων δεδομένων και άλλων περιστατικών ασφαλείας, θα πρέπει απαραίτητα να λαμβάνονται προληπτικά μέτρα για την προστασία των πληροφοριακών συστημάτων και των δεδομένων από τους οργανισμούς και τις επιχειρήσεις. Αυτό είχε ως αποτέλεσμα την ανάπτυξη μίας πληθώρας πλαισίων ,μεθοδολογιών και εργαλείων για τη διαχείριση της επικινδυνότητας της ασφάλειας των πληροφοριών των οργανισμών και των επιχειρήσεων.

Το κίνητρο για αυτή την έρευνα προέρχεται από την αυξανόμενη σημασία της ασφάλειας των πληροφοριών στον σημερινό ψηφιακό κόσμο και την ανάγκη των οργανισμών να διαθέτουν μια αξιόπιστη και αποτελεσματική μέθοδο διαχείρισης της επικινδυνότητας. Με τη συνεχή εξέλιξη της τεχνολογίας και την αυξανόμενη πολυπλοκότητα των απειλών, είναι απαραίτητο να υπάρχει ένα ισχυρό πλαίσιο διαχείρισης επικινδυνότητας που να μπορεί να συμβαδίζει με το μεταβαλλόμενο τοπίο. Η συγκριτική αξιολόγηση των πλαισίων και των μεθοδολογιών θα παράσχει πολύτιμες γνώσεις και συστάσεις σε αυτούς που επιθυμούν να βελτιώσουν τις πρακτικές τους στον τομέα της ασφάλειας των πληροφοριών και να προστατεύσουν καλύτερα τα περιουσιακά τους στοιχεία.

Η παρούσα μελέτη λοιπόν, αποσκοπεί στη συγκριτική αξιολόγηση των πλαισίων και των μεθοδολογιών και εργαλείων που διατίθενται στην αγορά για τη διαχείριση της επικινδυνότητας της ασφάλειας των πληροφοριών. Η μελέτη θα διερευνήσει και θα συγκρίνει ορισμένα από τα υπάρχοντα πλαίσια και μεθοδολογίες και θα στοχεύσει στην παροχή ενός πίνακα αξιολόγησης που οι οργανισμοί μπορούν να χρησιμοποιήσουν για να αξιολογήσουν την καταλληλότητα των διαφόρων πλαισίων, μεθοδολογιών και εργαλείων για τις συγκεκριμένες ανάγκες τους. Η μελέτη θα συμβάλει στη συνεχιζόμενη συζήτηση σχετικά με την αναζήτηση της χρήσης βέλτιστων πρακτικών στη διαχείριση της επικινδυνότητας και θα ενθαρρύνει την περαιτέρω έρευνα στον τομέα αυτό.

1. 2 Ερευνητικό ερώτημα και στόχοι

Το ερευνητικό ερώτημα της παρούσας μελέτης είναι: "Ποια είναι τα πλαίσια, οι μεθοδολογίες και τα εργαλεία διαχείρισης επικινδυνότητας της ασφάλειας πληροφοριών που όταν συγκριθούν με κοινά συγκριτικά κριτήρια καλύπτουν καλύτερα/περισσότερο τις απαιτήσεις του χώρου;"

Για να απαντηθεί αυτό το ερευνητικό ερώτημα, τέθηκαν οι ακόλουθοι στόχοι:

1.

Ορισμός και επιλογή των κατάλληλων κριτηρίων συγκριτικής αξιολόγησης . Αναλυτική επεξήγηση του κάθε κριτηρίου αξιολόγησης έτσι ώστε ο αναγνώστης να εξοικειωθεί με τις έννοιες που πραγματεύονται στην παρούσα μελέτη και να είναι ξεκάθαρο στη συνέχεια αν κάποιο πλαίσιο, μεθοδολογία και εργαλείο πληροί το εκάστοτε κριτήριο και σε ποιο βαθμό.

2.

Επισκόπηση των υφιστάμενων πλαισίων και μεθοδολογιών και εργαλείων διαχείρισης επικινδυνότητας της ασφάλειας πληροφοριών που επιλέχθηκαν για τη συγκεκριμένη μελέτη και τα οποία είναι :

1. COSO Internal Control-Integrated Framework
2. "The FAIR Methodology"
3. ISACA RiskIT Framework
4. ISO 27005 Framework
5. EU ITSRM^2, IT Security Risk Management Methodology V1.2
6. Microsoft Security Assessment Tool
7. NIST Special Publication 800-30
8. OCTAVE Allegro methodology
9. Verinice - Risk Management Tool

3.

Δημιουργία συγκριτικού πίνακα με τα επιλεγμένα κριτήρια ως γραμμές και τις επιλεγμένες μεθοδολογίες , πλαίσια και εργαλεία ως στήλες.

4.

Σχολιασμός των ευρημάτων του πίνακα σε σχέση με τα κριτήρια αξιολόγησης.

1.3 Μεθοδολογία

Η μεθοδολογία που θα χρησιμοποιηθεί στην παρούσα μελέτη έχει βασιστεί στη χρήση συγκριτικών κριτηρίων αξιολόγησης για να αξιολογήσει και να συγκρίνει τα διάφορα πλαίσια/μεθοδολογίες/εργαλεία που σχετίζονται με τη διαχείριση κινδύνου ασφάλειας πληροφοριών.

Το πρώτο βήμα της μεθοδολογίας θα είναι ο προσδιορισμός κατάλληλων κριτηρίων αξιολόγησης τα οποία καλύπτουν , αλλά δεν εξαντλούν, τις πτυχές της διαχείρισης της επικινδυνότητας της ασφάλειας των πληροφοριών και θα περιλαμβάνουν παράγοντες όπως η πληρότητα των πλαισίων/μεθοδολογιών/εργαλείων, η ευκολία χρήσης, το επίπεδο της παρεχόμενης λεπτομέρειας, η ακρίβεια των αποτελεσμάτων και το επίπεδο της διαθέσιμης υποστήριξης και άλλα χρηστικά χαρακτηριστικά.

Το επόμενο βήμα της μεθοδολογίας θα είναι η παρουσίαση των μεθοδολογιών που θα αξιολογηθούν. Οι μεθοδολογίες έχουν επιλεγεί με βάση τη δημοτικότητα και την ευρεία χρήση τους, καθώς και τη συνάφεια τους με τον τομέα της διαχείρισης επικινδυνότητας ασφάλειας πληροφοριών. Τα δεδομένα για τη μελέτη θα συλλεχθούν μέσω ενός συνδυασμού διαδικτυακών ερευνών, και ανασκόπησης της υπάρχουσας βιβλιογραφίας και θα αποδοθούν με έναν ομοιόμορφο τρόπο κατά την περιγραφή έκαστου εκ των πλαισίων,

μεθοδολογιών και εργαλείων για να προκύπτουν με σαφήνεια τα χαρακτηριστικά και οι ιδιαιτερότητές τους.
Το επόμενο βήμα θα είναι να παραχθεί ένας πίνακας συγκριτικής αξιολόγησης του οποίου το περιεχόμενο θα περιλαμβάνει ως γραμμές τα κριτήρια αξιολόγησης και ως στήλες τα επιλεγμένα πλαίσια/μεθοδολογίες/εργαλεία και θα απεικονίζει τα συμπεράσματα της αξιολόγησης που θα προκύψουν από το προηγούμενο βήμα.
Τέλος θα υπάρξει σχολιασμός των αποτελεσμάτων σε σχέση με το κάθε κριτήριο. Τα αποτελέσματα θα μπορούν να χρησιμοποιηθούν για την παροχή συστάσεων προς τους ενδιαφερόμενου που επιθυμούν να υιοθετήσουν μια αποτελεσματική μεθοδολογία διαχείρισης επικινδυνότητας ασφάλειας πληροφοριών.

1.4 Ορισμοί

Διαχείριση επικινδυνότητας της ασφάλειας πληροφοριών

Η διαχείριση επικινδυνότητας της ασφάλειας των πληροφοριών, ή ISRM, είναι η διαδικασία διαχείρισης των κινδύνων που συνδέονται με τη χρήση της τεχνολογίας των πληροφοριών. Περιλαμβάνει τον εντοπισμό, την αξιολόγηση και την αντιμετώπιση των κινδύνων για την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των περιουσιακών στοιχείων ενός οργανισμού. Ο τελικός στόχος αυτής της διαδικασίας είναι η αντιμετώπιση της επικινδυνότητας σύμφωνα με τη συνολική ανοχή κινδύνου ενός οργανισμού. Οι επιχειρήσεις δεν θα πρέπει να περιμένουν να εξαλείψουν όλους τους κινδύνους- μάλλον, θα πρέπει να επιδιώκουν να προσδιορίσουν και να επιτύχουν ένα αποδεκτό επίπεδο κινδύνου για τον οργανισμό τους.

ISMS (Information Security Management System)

Το Σύστημα διαχείρισης της ασφάλειας των πληροφοριών, είναι μια συστηματική προσέγγιση για τη διαχείριση ευαίσθητων και εμπιστευτικών πληροφοριών σε έναν οργανισμό. Στόχος του ISMS είναι η προστασία των πληροφοριών από μη εξουσιοδοτημένη πρόσβαση, χρήση, αποκάλυψη, διατάραξη, τροποποίηση ή καταστροφή. Περιλαμβάνει διαδικασίες, πολιτικές και ελέγχους για την εξασφάλιση των πληροφοριών μέσω της αξιολόγησης επικινδυνότητας, της προστασίας δεδομένων, του ελέγχου πρόσβασης και της διαχείρισης περιστατικών.

Πλαίσιο

Ένα πλαίσιο είναι ένα σύνολο κατευθυντήριων γραμμών ή αρχών που παρέχουν μια δομή για την οργάνωση και την υλοποίηση μιας συγκεκριμένης διαδικασίας ή εργασίας. Στο πλαίσιο της διαχείρισης κινδύνων για την ασφάλεια των πληροφοριών, ένα πλαίσιο μπορεί να παρέχει ένα γενικό περίγραμμα για τον τρόπο εντοπισμού, αξιολόγησης και διαχείρισης της επικινδυνότητας σε έναν οργανισμό. Τα πλαίσια μπορούν επίσης να παρέχουν καθοδήγηση σχετικά με τον τρόπο οργάνωσης και υλοποίησης των διαδικασιών διαχείρισης κινδύνων και μπορούν επίσης να χρησιμεύσουν ως σημείο αναφοράς για την αξιολόγηση της αποτελεσματικότητας του προγράμματος διαχείρισης κινδύνων.

Μεθοδολογία

Μια μεθοδολογία είναι μια συγκεκριμένη προσέγγιση ή μέθοδος για την εκτέλεση μιας διαδικασίας ή μιας εργασίας. Στο πλαίσιο της διαχείρισης κινδύνων για την ασφάλεια των

πληροφοριών, μια μεθοδολογία μπορεί να παρέχει μια διαδικασία βήμα προς βήμα για τον εντοπισμό, την αξιολόγηση και τη διαχείριση της επικινδυνότητας. Οι μεθοδολογίες μπορούν να προσαρμοστούν στις συγκεκριμένες ανάγκες ενός οργανισμού και να χρησιμοποιηθούν για την υποστήριξη της εφαρμογής ενός πλαισίου

Εργαλεία

Τα εργαλεία είναι λογισμικό ή υλικό που μπορεί να χρησιμοποιηθεί για να βοηθήσει στην εφαρμογή ενός πλαισίου ή μιας μεθοδολογίας. Στο πλαίσιο της διαχείρισης κινδύνου ασφάλειας πληροφοριών, τα εργαλεία μπορούν να περιλαμβάνουν λογισμικό για την αξιολόγηση κινδύνου, τη διαχείριση ευπαθειών, την αντιμετώπιση περιστατικών και τη διαχείριση συμμόρφωσης. Τα εργαλεία μπορούν να βοηθήσουν τους οργανισμούς να αυτοματοποιήσουν πολλές από τις διαδικασίες που εμπλέκονται στη διαχείριση κινδύνων και μπορούν επίσης να βοηθήσουν τους οργανισμούς να παραμείνουν συμβατοί με διάφορους κανονισμούς και πρότυπα.

2. Κριτήρια συγκριτικής αξιολόγησης

2.1 Σκοπός της συγκριτικής αξιολόγησης

Ο σκοπός της συγκριτικής αξιολόγησης των πλαισίων, μεθοδολογιών και εργαλείων που χρησιμοποιούνται για τη διαχείριση κινδύνων ασφάλειας πληροφοριών είναι η αξιολόγηση και η σύγκριση της αποτελεσματικότητας και της καταλληλότητας τους στη διαχείριση της επικινδυνότητας ασφάλειας πληροφοριών που μπορεί να αντιμετωπίσει ο εκάστοτε οργανισμός ή επιχείρηση.
Με τη χρήση προκαθορισμένων κοινών κριτηρίων ,όπως έχουμε κάνει στην παρούσα μελέτη, πετυχαίνουμε την εξάλειψη των υποκειμενικών αντιλήψεων κατά τη σύγκριση διαφορετικών μεθοδολογιών ,πλαισίων και εργαλείων .
Χρησιμοποιώντας καλά ορισμένα κριτήρια , στο πλαίσιο που εξετάζει η παρούσα μελέτη , καθίσταται ευκολότερη η πραγματοποίηση έγκυρων συγκρίσεων μεταξύ διαφορετικών μεθοδολογιών/πλαισίων/εργαλείων καθώς και ο εντοπισμός δυνατών και αδύνατων σημείων κάθε μεθοδολογίας και πλαισίου, επιτρέποντας τη λήψη τεκμηριωμένων αποφάσεων σχετικά με την καταλληλότητα του καθενός για μια συγκεκριμένη εργασία ή διαδικασία.

2.2 Τα Κριτήρια

Τα κριτήρια επιλέχτηκαν με σκοπό να καλύψουν τις περισσότερε πτυχές των ερωτημάτων που εγείρονται κατά την επιλογή του κατάλληλου πλαισίου, μεθοδολογίας και εργαλείου. Μέσω της επιλογής των κριτηρίων επίσης γίνεται μία προσπάθεια να παρουσιαστούν τόσο τα ποιοτικά χαρακτηριστικά του κάθε πλαισίου/μεθοδολογίας/εργαλείου, όσο και τα πρακτικά/χρηστικά χαρακτηριστικά του καθενός , προβαίνοντας ταυτόχρονα και στην αντίστοιχη αξιολόγηση.
Η περιγραφή που ακολουθεί , αναλύει πλήρως τα κριτήρια που θα χρησιμοποιηθούν για την συγκριτική αξιολόγηση , στο πλαίσιο που πραγματεύεται η παρούσα εργασία, έτσι ώστε να είναι ευκολότερο στον αναγνώστη να κατανοήσει τα χαρακτηριστικά του κάθε πλαισίου, μεθοδολογίας ή εργαλείου που παρουσιάζονται στη συνέχεια.

Η λίστα με τα κριτήρια που ακολουθεί δεν είναι εξαντλητική, έγινε προσπάθεια να συμπεριληφθεί μία ποικιλία κριτηρίων τόσο ποιοτικών όσο και χρηστικών για να είναι πιο σφαιρική η εικόνα που παρουσιάζουμε.

2.2.1 Χρηστικότητα (Usability)

Όταν αναφερόμαστε στη **"χρηστικότητα"** στο πλαίσιο μιας μεθοδολογίας ενός πλαισίου ή ενός εργαλείου, σημαίνει ότι είναι εύκολα στην κατανόηση, τη χρήση και την εφαρμογή. Με άλλα λόγια, μια μεθοδολογία, ένα πλαίσιο ή ένα εργαλείο θεωρούνται εύχρηστα εάν είναι **φιλικά προς τον χρήστη**, **εύκολα στην παρακολούθηση** και **δεν απαιτούν εκτεταμένη εκπαίδευση** ή εμπειρογνωμοσύνη για την εκτέλεσή τους.

Στο πλαίσιο της διαχείρισης επικινδυνότητας της ασφάλειας των πληροφοριών, μια χρηστική μεθοδολογία θα πρέπει επιπλέον να έχει σαφείς οδηγίες και κατευθυντήριες

γραμμές για τον εντοπισμό, την αξιολόγηση και τον μετριασμό της επικινδυνότητας. Θα διαθέτει επίσης ένα **φιλικό προς το χρήστη περιβάλλον για την τεκμηρίωση και την υποβολή εκθέσεων** σχετικά με τη διαδικασία διαχείρισης κινδύνων και θα **ενσωματώνεται εύκολα στις υφιστάμενες διαδικασίες και συστήματα του οργανισμού.**

Η χρηστικότητα είναι σημαντική, διότι συμβάλλει στη διασφάλιση ότι η μεθοδολογία ή το πλαίσιο ή το εργαλείο χρησιμοποιούνται πραγματικά και ότι εφαρμόζονται αποτελεσματικά, αντί να αγνοούνται ή να μην γίνονται κατανοητά. Μια χρηστική μεθοδολογία είναι πιο πιθανό να υιοθετηθεί και να χρησιμοποιηθεί από έναν οργανισμό, γεγονός που αυξάνει τις πιθανότητες επιτυχίας στην επίτευξη των επιθυμητών στόχων.

Η συγκριτική αξιολόγηση θα κυμανθεί μεταξύ του αν το πλαίσιο, η μεθοδολογία ή το εργαλείο είναι πλήρως , μερικώς ή καθόλου χρηστικό οπότε και το κριτήριο θα καλύπτεται πλήρως , μερικώς ή καθόλου.

2.2.2 Ευελιξία (Flexibility)

Όταν αναφερόμαστε στην "ευελιξία" στο πλαίσιο μιας μεθοδολογίας , ενός πλαισίου ή ενός εργαλείου, σημαίνει ότι μπορούν να προσαρμοστούν και να εφαρμοστούν σε διαφορετικές καταστάσεις και πλαίσια. Με άλλα λόγια, μια μεθοδολογία, ένα πλαίσιο ή ένα εργαλείο θεωρούνται ευέλικτα εάν **μπορούν να προσαρμοστούν ώστε να ανταποκρίνονται στις συγκεκριμένες ανάγκες και απαιτήσεις διαφορετικών οργανισμών και καταστάσεων,** ενώ παράλληλα επιτυγχάνουν τον ίδιο στόχο.

Στο πλαίσιο της διαχείρισης επικινδυνότητας για την ασφάλεια των πληροφοριών, μια ευέλικτη μεθοδολογία, θα μπορούσε **να λάβει υπόψη της τα μοναδικά χαρακτηριστικά ενός οργανισμού**, όπως το μέγεθος, τον κλάδο και το προφίλ κινδύνου, και **να προσαρμόσει ανάλογα τη διαδικασία διαχείρισης επικινδυνότητας**. Επιπλέον, μια ευέλικτη μεθοδολογία **επιτρέπει να γίνονται προσαρμογές** καθώς το τοπίο κινδύνου του οργανισμού αλλάζει με την πάροδο του χρόνου.

Η ευελιξία είναι σημαντική επειδή οι οργανισμοί και τα περιβάλλοντά τους είναι δυναμικά και μια μεθοδολογία , πλαίσιο ή εργαλείο που μπορεί να προσαρμόζεται στις μεταβαλλόμενες συνθήκες θα είναι πιο αποτελεσματικά στην επίτευξη των στόχων της. Μια ευέλικτη μεθοδολογία , πλαίσιο ή εργαλείο , επιτρέπει επίσης στους οργανισμούς να χρησιμοποιούν ίδια αντιμετώπιση για διαφορετικά έργα και μπορεί να τους εξοικονομήσει χρόνο και χρήμα, καθώς αποφεύγεται η ανάγκη ανάπτυξης νέων μεθοδολογιών για κάθε έργο.

Μερικά από τα βασικά στοιχεία που συμβάλλουν στην ευελιξία ενός πλαισίου ή μιας μεθοδολογίας περιλαμβάνουν:

- Γενικές κατευθυντήριες γραμμές αντί για συγκεκριμένους κανόνες: Τα πλαίσια και οι μεθοδολογίες που παρέχουν γενικές κατευθυντήριες γραμμές και όχι συγκεκριμένους κανόνες επιτρέπουν στους οργανισμούς να προσαρμόζουν την εφαρμογή τους στις συγκεκριμένες ανάγκες και περιστάσεις τους.
- Επιλογές προσαρμογής: Ορισμένα πλαίσια και μεθοδολογίες περιλαμβάνουν επιλογές προσαρμογής που επιτρέπουν στους οργανισμούς να προσαρμόσουν το

πλαίσιο ή τη μεθοδολογία στις συγκεκριμένες ανάγκες τους. Για παράδειγμα, ένα πλαίσιο ασφάλειας πληροφοριών μπορεί να περιλαμβάνει επιλογές για διαφορετικά επίπεδα ασφάλειας ή διαφορετικούς τύπους διαχείρισης κινδύνων.

- Επεκτασιμότητα: Τα πλαίσια και οι μεθοδολογίες που μπορούν να κλιμακωθούν σε διαφορετικά μεγέθη και τύπους οργανισμών είναι πιο ευέλικτα. Αυτό σημαίνει ότι το ίδιο πλαίσιο ή η ίδια μεθοδολογία μπορεί να χρησιμοποιηθεί από μικρούς, μεσαίους και μεγάλους οργανισμούς και μπορεί να προσαρμοστεί σε διαφορετικούς τύπους οργανισμών.

Η συγκριτική αξιολόγηση θα κυμανθεί μεταξύ του αν το πλαίσιο, η μεθοδολογία ή το εργαλείο καλύπτει πλήρως , μερικώς ή καθόλου το ως άνω κριτήριο.

2.2.3 Διαχείριση περιουσιακών στοιχείων (Asset management)

Όταν αναφερόμαστε στη "διαχείριση περιουσιακών στοιχείων" στο πλαίσιο μιας μεθοδολογίας, πλαισίου ή εργαλείου, εννοούμε τη **διαδικασία εντοπισμού, ταξινόμησης και διαχείρισης των περιουσιακών στοιχείων ενός οργανισμού.** Η διαχείριση περιουσιακών στοιχείων αποτελεί αναπόσπαστο μέρος της διαχείρισης επικινδυνότητας της ασφάλειας των πληροφοριών, καθώς παρέχει μια ολοκληρωμένη κατανόηση των περιουσιακών στοιχείων που πρέπει να προστατευθούν και της αξίας τους για τον οργανισμό.

Στο πλαίσιο της διαχείρισης επικινδυνότητας της ασφάλειας των πληροφοριών, η διαχείριση περιουσιακών στοιχείων περιλαμβάνει **τον εντοπισμό και την καταγραφή όλων των περιουσιακών στοιχείων σχετικών με της ασφάλεια πληροφοριών, συμπεριλαμβανομένου του υλικού, του λογισμικού και των δεδομένων.** Οι πληροφορίες αυτές θα χρησιμοποιηθούν στη συνέχεια για την **ταξινόμηση των περιουσιακών στοιχείων με βάση την κρισιμότητά τους** και **για την αξιολόγηση των κινδύνων που ενέχουν για τον οργανισμό.** Μόλις εντοπιστούν οι κίνδυνοι, μπορούν να εφαρμοστούν τα κατάλληλα μέτρα για τον μετριασμό τους.
Η διαχείριση περιουσιακών στοιχείων είναι σημαντική, διότι **επιτρέπει στους οργανισμούς να κατανοήσουν τα περιουσιακά στοιχεία τους και την αξία τους**, ώστε να μπορούν να ιεραρχήσουν τις προσπάθειες προστασίας και διαχείρισης κινδύνων εκεί όπου θα έχουν τον μεγαλύτερο αντίκτυπο. Επιπλέον, καταγράφοντας και ταξινομώντας τα περιουσιακά στοιχεία**, οι οργανισμοί μπορούν να κατανοήσουν καλύτερα το τοπίο της ασφάλειας πληροφοριών και να εντοπίσουν πιθανές ευπάθειες.** Οι πληροφορίες αυτές βοηθούν τους οργανισμούς να λαμβάνουν τεκμηριωμένες αποφάσεις σχετικά με τη διαχείριση κινδύνων και να εφαρμόζουν τους πιο αποτελεσματικούς ελέγχους για την προστασία των περιουσιακών τους στοιχείων.

Η συγκριτική αξιολόγηση θα κυμανθεί μεταξύ του αν το πλαίσιο, η μεθοδολογία ή το εργαλείο καλύπτει πλήρως , μερικώς ή καθόλου το ως άνω κριτήριο.

2.2.4 Βάση δεδομένων για απειλές (Database for threats)

Όταν αναφερόμαστε στη "βάση δεδομένων για απειλές" στο πλαίσιο μιας μεθοδολογίας, πλαισίου ή εργαλείου, εννοούμε **τη διαδικασία συλλογής και αποθήκευσης πληροφοριών**

σχετικά με πιθανές απειλές για την ασφάλεια που μπορεί να αντιμετωπίσει ένας οργανισμός. Αυτή η βάση δεδομένων χρησιμοποιείται για τον εντοπισμό και την ιεράρχηση των πιο σημαντικών απειλών και την ανάπτυξη στρατηγικών για τον μετριασμό τους.
Στο πλαίσιο της διαχείρισης της επικινδυνότητας της ασφάλειας των πληροφοριών, μια βάση δεδομένων για τις απειλές θα μπορούσε να περιλαμβάνει πληροφορίες σχετικά με διάφορους τύπους απειλών, όπως κακόβουλο λογισμικό, phishing, κοινωνική μηχανική και άλλες απειλές στον κυβερνοχώρο. Η βάση δεδομένων θα περιλάμβανε επίσης **πληροφορίες σχετικά με την πιθανότητα εμφάνισης μιας απειλής**, τις **πιθανές επιπτώσεις** στον οργανισμό και **τα μέτρα που εφαρμόζονται** για τον μετριασμό της απειλής.

Μια βάση δεδομένων για τις απειλές είναι ένα σημαντικό εργαλείο για τη διαχείριση της επικινδυνότητας της ασφάλειας των πληροφοριών, **διότι επιτρέπει στους οργανισμούς να εντοπίζουν προληπτικά και να ιεραρχούν τις πιο σημαντικές απειλές και να αναπτύσσουν στρατηγικές για τον μετριασμό τους.** Οι πληροφορίες αυτές μπορούν να χρησιμοποιηθούν για τη δημιουργία προφίλ απειλών και για την ανάπτυξη σχεδίων αντιμετώπισης περιστατικών. Επιπλέον, μια βάση δεδομένων για τις απειλές μπορεί να χρησιμοποιηθεί για την παρακολούθηση της αποτελεσματικότητας των μέτρων ασφαλείας με την πάροδο του χρόνου, η οποία μπορεί να χρησιμοποιηθεί για τη βελτίωση της συνολικής κατάστασης ασφαλείας του οργανισμού.

Η συγκριτική αξιολόγηση θα κυμανθεί μεταξύ του αν το πλαίσιο, η μεθοδολογία ή το εργαλείο καλύπτει πλήρως , μερικώς ή καθόλου το ως άνω κριτήριο.

2.2.5 Βάση δεδομένων για ευπάθειες (Database for vulnerabilities)

Μια “βάση δεδομένων ευπαθειών” αναφέρεται σε μια συλλογή πληροφοριών σχετικά με γνωστές ευπάθειες σε λογισμικό, υλικό και άλλα συστήματα. Οι πληροφορίες αυτές μπορεί να περιλαμβάνουν **λεπτομέρειες σχετικά με την ευπάθεια**, όπως **η σοβαρότητά της** και τα **συγκεκριμένα συστήματα ή το λογισμικό που επηρεάζει**, καθώς και πληροφορίες σχετικά με **τον τρόπο επιδιόρθωσης ή μετριασμού της ευπάθειας.**
Αυτή η βάση δεδομένων μπορεί να χρησιμοποιηθεί ως μέρος μιας μεθοδολογίας ή ενός πλαισίου διαχείρισης της επικινδυνότητας της ασφάλειας πληροφοριών, για να βοηθήσει τους οργανισμούς να εντοπίσουν και να αντιμετωπίσουν πιθανές ευπάθειες στα συστήματά τους. Η βάση δεδομένων μπορεί να χρησιμοποιηθεί για τη διενέργεια αξιολογήσεων επικινδυνότητας, την ιεράρχηση των προσπαθειών αποκατάστασης και την παρακολούθηση της προόδου των προσπαθειών μετριασμού.

Η συγκριτική αξιολόγηση θα κυμανθεί μεταξύ του αν το πλαίσιο, η μεθοδολογία ή το εργαλείο καλύπτει πλήρως , μερικώς ή καθόλου το ως άνω κριτήριο.

2.2.6 Βάση δεδομένων για μέτρα ασφαλείας. (Database for controls)

Όταν αναφερόμαστε στη "βάση δεδομένων για μέτρα" στο πλαίσιο μιας μεθοδολογίας, εννοούμε **τη διαδικασία συλλογής και αποθήκευσης πληροφοριών σχετικά με τα μέτρα ασφαλείας που έχει εφαρμόσει ένας οργανισμός για την προστασία από πιθανές απειλές ασφαλείας**. Αυτή η βάση δεδομένων χρησιμοποιείται για τον **εντοπισμό και την**

αξιολόγηση της αποτελεσματικότητας των εφαρμοζόμενων μέτρων και για την ανάπτυξη στρατηγικών για τη βελτίωσή τους.

Στο πλαίσιο της διαχείρισης επικινδυνότητας της ασφάλειας των πληροφοριών, μια βάση δεδομένων για τα μέτρα θα μπορούσε να περιλαμβάνει πληροφορίες σχετικά με διάφορους τύπους μέτρων ασφαλείας, όπως τείχη προστασίας, συστήματα ανίχνευσης και πρόληψης εισβολών, λογισμικό προστασίας από ιούς και άλλες τεχνολογίες ασφαλείας. Η βάση δεδομένων θα περιλάμβανε επίσης **πληροφορίες σχετικά με τη διαμόρφωση των μέτρων**, **το επίπεδο προστασίας που παρέχουν** και **τυχόν ευπάθειες ή αδυναμίες που έχουν εντοπιστεί.**

Μια βάση δεδομένων για τα μέτρα αποτελεί σημαντικό εργαλείο, διότι επιτρέπει στους οργανισμούς **να εντοπίζουν και να αξιολογούν προληπτικά την αποτελεσματικότητα των υφιστάμενων μέτρων και να αναπτύσσουν στρατηγικές για τη βελτίωσή τους.** Οι πληροφορίες αυτές μπορούν να χρησιμοποιηθούν για τον εντοπισμό περιοχών στις οποίες απαιτούνται πρόσθετα μέτρα και για την ιεράρχηση της εφαρμογής νέων μέτρων.

Η συγκριτική αξιολόγηση θα κυμανθεί μεταξύ του αν το πλαίσιο, η μεθοδολογία ή το εργαλείο καλύπτει πλήρως , μερικώς ή καθόλου το ως άνω κριτήριο.

2.2.7 Πλοήγηση σε περιστατικά (Incident navigation)

Όταν αναφερόμαστε στην «πλοήγηση σε περιστατικά» στο πλαίσιο μίας μεθοδολογίας , ενός πλαισίου ή ενός εργαλείου αναφερόμαστε **στη διαδικασία διαχείρισης του εντοπισμού, αντιμετώπισης και επίλυσης περιστατικών ασφαλείας σε έναν οργανισμό.** Αυτή η διαδικασία περιλαμβάνει συνήθως **ένα σύνολο καθορισμένων διαδικασιών και κατευθυντήριων γραμμών για τον εντοπισμό, την ταξινόμηση και τη διαχείριση περιστατικών ασφαλείας, καθώς και πρωτόκολλα επικοινωνίας για το συντονισμό με τους σχετικούς ενδιαφερόμενους φορείς, όπως οι ομάδες πληροφορικής και ασφάλειας, οι νομικοί σύμβουλοι και οι εξωτερικοί συνεργάτες.**
Ο στόχος της πλοήγησης σε συμβάντα στο πλαίσιο της διαχείρισης κινδύνου ασφάλειας πληροφοριών είναι να ελαχιστοποιηθούν οι επιπτώσεις των συμβάντων ασφάλειας στον οργανισμό, στα περιουσιακά του στοιχεία και τους πελάτες του και να επανέλθει ο οργανισμός στην κανονική του λειτουργία το συντομότερο δυνατό.

Ένα πλαίσιο ή μια μεθοδολογία για την πλοήγηση σε περιστατικά περιγράφει συνήθως ένα **σύνολο βέλτιστων πρακτικών και διαδικασιών** που πρέπει να ακολουθούν οι ομάδες αντιμετώπισης περιστατικών και μπορεί επίσης να περιλαμβάνει εργαλεία και τεχνολογίες που βοηθούν στον εντοπισμό, την ταξινόμηση και τη διαχείριση περιστατικών. Ευθυγραμμίζεται επίσης με το συνολικό πλαίσιο, τις μεθοδολογίες και τα εργαλεία διαχείρισης κινδύνων για τον οργανισμό. Αυτό περιλαμβάνει τον εντοπισμό πιθανών απειλών και ευπαθειών, την αξιολόγηση της πιθανότητας και του αντίκτυπου αυτών των απειλών και ευπαθειών και την εφαρμογή ελέγχων για τον μετριασμό ή τη διαχείριση του κινδύνου.

Η συγκριτική αξιολόγηση θα κυμανθεί μεταξύ του αν το πλαίσιο, η μεθοδολογία ή το εργαλείο καλύπτει πλήρως , μερικώς ή καθόλου το ως άνω κριτήριο.

2.2.8 Έλεγχος επιχειρησιακών διαδικασιών (Business process control)

Όταν αναφερόμαστε στον "έλεγχο επιχειρησιακών διαδικασιών" στο πλαίσιο μιας μεθοδολογίας, εννοούμε **τη διαδικασία διασφάλισης ότι οι επιχειρησιακές διαδικασίες ενός οργανισμού εκτελούνται σωστά, αποτελεσματικά και με ασφάλεια.** Ο έλεγχος επιχειρηματικών διαδικασιών είναι ένας τρόπος αξιολόγησης και διαχείρισης της επικινδυνότητας που σχετίζεται με τις επιχειρηματικές διαδικασίες και εφαρμογής μέτρων για τον μετριασμό τους.

Στο πλαίσιο της διαχείρισης της επικινδυνότητας της ασφάλειας των πληροφοριών, ο έλεγχος επιχειρηματικών διαδικασιών **θα περιλάμβανε τον εντοπισμό και την αξιολόγηση της επικινδυνότητας που σχετίζονται με τις επιχειρηματικές διαδικασίες και την εφαρμογή μέτρων για τον μετριασμό τους. Αυτό θα περιελάμβανε την κατανόηση του τρόπου ροής των δεδομένων μέσω του οργανισμού, το πού αποθηκεύονται τα ευαίσθητα δεδομένα και ποιος έχει πρόσβαση σε αυτά.** Θα περιλάμβανε επίσης την αξιολόγηση των μέτρων ασφαλείας που εφαρμόζονται για την προστασία των δεδομένων, όπως τείχη προστασίας, συστήματα ανίχνευσης και πρόληψης εισβολών και έλεγχοι πρόσβασης.

Ο έλεγχος των επιχειρηματικών διαδικασιών είναι σημαντικός, διότι **συμβάλλει στη διασφάλιση της ορθής, αποτελεσματικής και ασφαλούς εκτέλεσης των επιχειρηματικών διαδικασιών, η οποία με τη σειρά της συμβάλλει στην προστασία των περιουσιακών στοιχείων και της φήμης του οργανισμού**. Επιπλέον, ο έλεγχος των επιχειρηματικών διαδικασιών μπορεί να χρησιμοποιηθεί για τη βελτίωση της συνολικής αποδοτικότητας του οργανισμού, με τον εντοπισμό και την εξάλειψη περιττών διαδικασιών και με την αυτοματοποίηση επαναλαμβανόμενων εργασιών.

Η συγκριτική αξιολόγηση θα κυμανθεί μεταξύ του αν το πλαίσιο, η μεθοδολογία ή το εργαλείο καλύπτει πλήρως , μερικώς ή καθόλου το ως άνω κριτήριο.

2.2.9 Αναφορές και αναλύσεις (Reporting and analytics)

Όταν λέμε ότι μια μεθοδολογία, πλαίσιο, εργαλείο "υποστηρίζει την υποβολή αναφορών και αναλύσεων", σημαίνει ότι περιλαμβάνει τη **δυνατότητα συλλογής, ανάλυσης και υποβολής εκθέσεων** σχετικά με τα δεδομένα, προκειμένου να εντοπίζονται τάσεις, πρότυπα και περιοχές για βελτίωση και να λαμβάνονται τεκμηριωμένες αποφάσεις.

Στο πλαίσιο της διαχείρισης επικινδυνότητας της ασφάλειας πληροφοριών, μια μεθοδολογία που υποστηρίζει την υποβολή αναφορών και την ανάλυση περιλαμβάνει τη **δυνατότητα συλλογής δεδομένων σχετικά με τους κινδύνους και τα μέτρα που υπάρχουν, την ανάλυση των δεδομένων αυτών για τον εντοπισμό προτύπων και τάσεων και την υποβολή εκθέσεων σχετικά με τα αποτελέσματα.**

Οι πληροφορίες αυτές μπορούν να χρησιμοποιηθούν για τον εντοπισμό των περιοχών στις οποίες ο οργανισμός είναι πιο ευάλωτος, για την παρακολούθηση της

αποτελεσματικότητας των μέτρων ασφαλείας με την πάροδο του χρόνου και για τον εντοπισμό περιοχών στις οποίες απαιτούνται πρόσθετα μέτρα. **Η μεθοδολογία θα πρέπει επίσης να παρέχει έναν εύκολο τρόπο πρόσβασης σε αυτά τα δεδομένα και να μπορεί να δημιουργηθεί εύκολα μια έκθεση.**

Η ύπαρξη μιας μεθοδολογίας που υποστηρίζει αναφορές και αναλύσεις είναι σημαντική, διότι **βοηθά τους οργανισμούς να λαμβάνουν πιο τεκμηριωμένες αποφάσεις, παρέχοντάς τους μια βαθύτερη κατανόηση της κατάστασης ασφαλείας τους και της επικινδυνότητας που αντιμετωπίζουν.**

Η συγκριτική αξιολόγηση θα κυμανθεί μεταξύ του αν το πλαίσιο, η μεθοδολογία ή το εργαλείο καλύπτει πλήρως , μερικώς ή καθόλου το ως άνω κριτήριο.

2.2.10 Επίπεδο τεχνικότητας (Technicality)

Το "επίπεδο τεχνικότητας" στο πλαίσιο της διαχείρισης επικινδυνότητας της ασφάλειας πληροφοριών αναφέρεται **στο επίπεδο πολυπλοκότητας και εμπειρογνωμοσύνης που απαιτείται για την κατανόηση, την εφαρμογή και τη χρήση** μιας μεθοδολογίας, ενός πλαισίου ή ενός εργαλείου.

Μια μεθοδολογία, ένα πλαίσιο ή ένα εργαλείο με υψηλό επίπεδο τεχνικότητας θα απαιτούσε υψηλό βαθμό τεχνικών γνώσεων και δεξιοτήτων για την πλήρη αξιοποίησή τους, ενώ μια μεθοδολογία, ένα πλαίσιο ή ένα εργαλείο με χαμηλό επίπεδο τεχνικότητας θα μπορούσε να γίνει πιο εύκολα κατανοητή και να χρησιμοποιηθεί από άτομα με λιγότερη τεχνική εμπειρία. Αυτό περιλαμβάνει **την πολυπλοκότητα των χρησιμοποιούμενων μεθόδων**, **το επίπεδο της απαιτούμενης προσαρμογής**, **το επίπεδο αυτοματοποίησης** και **το επίπεδο διεπαφής με τον χρήστη**.

Για παράδειγμα, μια μεθοδολογία που χρησιμοποιεί πολλά μαθηματικά μοντέλα και στατιστικές αναλύσεις θεωρείται ότι έχει υψηλό επίπεδο τεχνικότητας, ενώ μια μεθοδολογία που χρησιμοποιεί απλές λίστες ελέγχου και ερωτηματολόγια θεωρείται ότι έχει χαμηλό επίπεδο τεχνικότητας. Το ίδιο ισχύει και για τα πλαίσια ή τα εργαλεία που μπορεί να έχουν πολλά προηγμένα χαρακτηριστικά και επιλογές για έμπειρους χρήστες ή μια πιο απλή διεπαφή χρήστη για λιγότερο έμπειρους χρήστες.

Θα πρέπει να λαμβάνεται υπόψη το επίπεδο τεχνικότητας κατά την επιλογή μιας μεθοδολογίας, ενός πλαισίου ή ενός εργαλείου για τη διαχείριση κινδύνων, καθώς μπορεί να επηρεάσει την ικανότητα ενός οργανισμού να το εφαρμόσει και να το χρησιμοποιήσει αποτελεσματικά, και μπορεί επίσης να επηρεάσει τη συνολική αποτελεσματικότητα της μεθοδολογίας, του πλαισίου ή του εργαλείου.

Η συγκριτική αξιολόγηση θα κυμανθεί μεταξύ του αν το πλαίσιο, η μεθοδολογία ή το εργαλείο έχει υψηλό , μέτριο ή χαμηλό επίπεδο τεχνικότητας.

Όταν λέμε ότι το κριτήριο της τεχνικότητας καλύπτεται πλήρως, εννοούμε ότι το πλαίσιο, η μεθοδολογία ή το εργαλείο έχουν χαμηλό επίπεδο τεχνικότητας.
Όταν λέμε ότι καλύπτεται μερικώς, εννοούμε ότι το επίπεδο της τεχνικότητας είναι μέτριο.

Όταν λέμε ότι το κριτήριο δεν καλύπτεται καθόλου εννοούμε ότι το επίπεδο της τεχνικότητας είναι υψηλό.

2.2.11 Υποστήριξη και πόροι (Support and resources)

Όταν αναφερόμαστε στην "υποστήριξη και τους πόρους" στο πλαίσιο μιας μεθοδολογίας, πλαισίου ή εργαλείου, εννοούμε **τη βοήθεια που είναι διαθέσιμη έτσι ώστε οι χρήστες να κατανοήσουν, να εφαρμόσουν ορθά και να συντηρήσουν κατάλληλα τη μεθοδολογία , το πλαίσιο ή το εργαλείο.**

Στο πλαίσιο της διαχείρισης επικινδυνότητας της ασφάλειας πληροφοριών, ο όρος «υποστήριξη» **περιλαμβάνει εγχειρίδια χρήσης, οδηγούς βήμα προς βήμα, εκπαιδευτικό υλικό και πρόσβαση σε ειδικούς τεχνικής υποστήριξης.** Επιπλέον, μπορεί να περιλαμβάνει ενημερώσεις λογισμικού, διορθώσεις σφαλμάτων και πρόσβαση σε μια βάση γνώσεων ή σε μια διαδικτυακή κοινότητα όπου οι χρήστες θα μπορούν να θέτουν ερωτήσεις και να μοιράζονται τις εμπειρίες τους.

Ο όρος «πόροι» περιλαμβάνει τα υλικά και τα εργαλεία που είναι διαθέσιμα για να βοηθήσουν τους χρήστες να εφαρμόσουν και να χρησιμοποιήσουν αποτελεσματικά μια μεθοδολογία, πλαίσιο ή εργαλείο. Αυτοί οι πόροι μπορεί να περιλαμβάνουν εκπαιδευτικό υλικό, πρότυπα και εργαλεία λογισμικού.

Μία μεθοδολογία που διαθέτει ένα ευρύ φάσμα πόρων και υποστήριξης, όπως βήμα προς βήμα διαδικασίες, εκπαιδευτικό υλικό και εργαλεία λογισμικού, θα θεωρηθεί ότι είναι πιο φιλική προς το χρήστη και προσβάσιμη, καθώς οι πόροι αυτοί μπορούν να βοηθήσουν τους χρήστες να κατανοήσουν και να εφαρμόσουν τη μεθοδολογία πιο εύκολα. Από την άλλη πλευρά, μια μεθοδολογία που δεν διαθέτει επαρκείς υποστηρικτικούς πόρους μπορεί να είναι πιο δύσκολο να κατανοηθεί και να χρησιμοποιηθεί αποτελεσματικά.

Συνολικά, η διαθεσιμότητα πόρων και υποστήριξης μπορεί να επηρεάσει σε μεγάλο βαθμό την ευκολία εφαρμογής και χρήσης μιας μεθοδολογίας, ενός πλαισίου ή ενός εργαλείου και μπορεί να συμβάλει σημαντικά στην επιτυχία του προγράμματος διαχείρισης κινδύνων.

Η συγκριτική αξιολόγηση θα κυμανθεί μεταξύ του αν το πλαίσιο, η μεθοδολογία ή το εργαλείο καλύπτει πλήρως , μερικώς ή καθόλου το ως άνω κριτήριο.

2.2.12 Πληρότητα (Completeness)

Όταν αναφερόμαστε στην "πληρότητα" στο πλαίσιο μιας μεθοδολογίας, πλαισίου ή εργαλείου, σημαίνει ότι η **μεθοδολογία περιλαμβάνει όλα τα απαραίτητα βήματα και εκτιμήσεις για την αποτελεσματική αντιμετώπιση ενός συγκεκριμένου προβλήματος ή την επίτευξη ενός συγκεκριμένου στόχου.** Με άλλα λόγια, μια μεθοδολογία/πλαίσιο/εργαλείο θεωρείται πλήρης **εάν καλύπτει όλες τις πτυχές ενός προβλήματος ή στόχου και εάν δεν παραλείπει τίποτα που είναι απαραίτητο για την επίτευξη ενός επιτυχημένου αποτελέσματος.**

Στο πλαίσιο της διαχείρισης επικινδυνότητας της ασφάλειας πληροφοριών, μια πλήρης μεθοδολογία/πλαίσιο/εργαλείο θα περιλάμβανε **βήματα για τον εντοπισμό, την**

αξιολόγηση και τον μετριασμό της επικινδυνότητας, καθώς και μια διαδικασία για συνεχή παρακολούθηση και αναθεώρηση. Επιπλέον, μια πλήρης μεθοδολογία θα λάμβανε υπόψη τις συγκεκριμένες ανάγκες και τους στόχους του οργανισμού, προκειμένου να προσαρμόσει ανάλογα την προσέγγιση διαχείρισης κινδύνων.

Είναι σημαντικό να σημειωθεί ότι μια πλήρης μεθοδολογία δεν σημαίνει ότι είναι τέλεια, αλλά ότι **καλύπτει όλα τα απαραίτητα βήματα και εκτιμήσεις** για την επίτευξη ενός συγκεκριμένου στόχου.

Η συγκριτική αξιολόγηση θα κυμανθεί μεταξύ του αν το πλαίσιο, η μεθοδολογία ή το εργαλείο καλύπτει πλήρως , μερικώς ή καθόλου το ως άνω κριτήριο.

2.2.13 Χρόνος/Διάρκεια (Time /Duration)

Όταν αναφερόμαστε στο "χρόνο" στο πλαίσιο μιας μεθοδολογίας, ενός πλαισίου ή ενός εργαλείου, εννοούμε τη διάρκεια που απαιτείται για την ολοκλήρωση του καθενός, από την αρχή έως το τέλος. Η χρονική πτυχή μιας μεθοδολογίας/πλαισίου/εργαλείου λαμβάνει υπόψη πόσος χρόνος απαιτείται για την ολοκλήρωση κάθε βήματος, τη συνολική διάρκεια και τη συχνότητα εκτέλεσης .

Στο πλαίσιο της διαχείρισης επικινδυνότητας για την ασφάλεια πληροφοριών, η χρονική πτυχή μιας μεθοδολογίας/πλαισίου/εργαλείου, εξετάζει πόσος **χρόνος απαιτείται για την ολοκλήρωση της αξιολόγησης κινδύνων**, **πόσο συχνά πρέπει να διεξάγεται η αξιολόγηση κινδύνων** και **πόσος χρόνος απαιτείται για την εφαρμογή και την παρακολούθηση των μέτρων** που έχουν τεθεί σε εφαρμογή για τον μετριασμό της επικινδυνότητας. Μια μεθοδολογία με μικρότερο χρονικό πλαίσιο για την ολοκλήρωση και την εκτέλεση θα μπορούσε να είναι πιο ελκυστική για οργανισμούς που έχουν στενά χρονοδιαγράμματα ή περιορισμένους πόρους.

Ο χρόνος είναι σημαντικός , διότι βοηθά τους οργανισμούς **να σχεδιάζουν και να κατανέμουν αποτελεσματικά τους πόρους τους**. Μια μεθοδολογία/πλαίσιο/εργαλείο που απαιτεί λιγότερο χρόνο για την εκτέλεσή της μπορεί να είναι πιο οικονομικά αποδοτική και να διαταράσσει λιγότερο τις καθημερινές δραστηριότητες του οργανισμού. Επιπλέον, μπορεί να ενσωματωθεί ευκολότερα στις υφιστάμενες διαδικασίες και τα συστήματα του οργανισμού, γεγονός που αυξάνει τις πιθανότητες επιτυχίας.

Η συγκριτική αξιολόγηση θα κυμανθεί μεταξύ του αν το πλαίσιο, η μεθοδολογία ή το εργαλείο καλύπτει πλήρως , μερικώς ή καθόλου το ως άνω κριτήριο.

Όταν είναι χρονικά αποδοτικό για τη χρήση που προορίζεται (από εβδομάδες έως και μήνες), θεωρούμε ότι καλύπτεται πλήρως το κριτήριο του χρόνου.
Όταν είναι σχετικά χρονοβόρο (από μήνες έως και χρόνο) για τη χρήση που προορίζεται θεωρούμε ότι το κριτήριο καλύπτεται μερικώς.
Όταν λέμε ότι δεν είναι χρονικά αποδοτικό ή αρκετά χρονοβόρο θεωρούμε ότι το κριτήριο δεν καλύπτεται καθόλου.

2.2.14 Οικονομικό κόστος (Financial Cost)

Όταν αναφερόμαστε στο "κόστος" για μια μεθοδολογία, αναφερόμαστε στα έξοδα που προκύπτουν από την εφαρμογή και τη συντήρηση της συγκεκριμένης μεθοδολογίας, πλαισίου ή εργαλείου. **Τα έξοδα αυτά μπορεί να περιλαμβάνουν πράγματα όπως η κατάρτιση και η εκπαίδευση των εργαζομένων, η αγορά οποιουδήποτε απαραίτητου εξοπλισμού ή λογισμικού, καθώς και ο χρόνος και οι πόροι που απαιτούνται για την εφαρμογή της μεθοδολογίας στην πράξη**.

Το κόστος ενός πλαισίου αναφέρεται στις χρηματικές δαπάνες που σχετίζονται με την εφαρμογή και τη χρήση ενός συγκεκριμένου πλαισίου για τη διαχείριση της επικινδυνότητας ασφαλείας. Αυτό μπορεί να **περιλαμβάνει δαπάνες όπως η εκπαίδευση των εργαζομένων, η αγορά λογισμικού ή εργαλείων που υποστηρίζουν το πλαίσιο και οι αμοιβές συμβούλων για εμπειρογνώμονες που θα βοηθήσουν στην εφαρμογή του.**
Το κόστος ενός εργαλείου αναφέρεται στις χρηματικές δαπάνες που σχετίζονται με την αγορά, την αδειοδότηση, την εφαρμογή και τη χρήση ενός συγκεκριμένου εργαλείου για την υποστήριξη των επιχειρήσεων ασφαλείας. Αυτό μπορεί να περιλαμβάνει το κόστος του ίδιου του εργαλείου, καθώς και κάθε πρόσθετο κόστος, όπως η εκπαίδευση των υπαλλήλων για τη χρήση του εργαλείου, τα τέλη συντήρησης και υποστήριξης και τυχόν αναβαθμίσεις ή ενημερώσεις του εργαλείου.
Η συγκριτική αξιολόγηση θα κυμανθεί μεταξύ του αν το πλαίσιο, η μεθοδολογία ή το εργαλείο καλύπτει πλήρως , μερικώς ή καθόλου το ως άνω κριτήριο.

Όταν το συνολικό κόστος χρήσης , απόκτησης , εφαρμογής και συντήρησης είναι χαμηλό θεωρούμε ότι καλύπτεται πλήρως το κριτήριο του κόστους.
Όταν το συνολικό κόστος είναι μέτριο, θεωρούμε ότι το κριτήριο καλύπτεται εν μέρει.
Όταν το συνολικό κόστος είναι υψηλό, θεωρούμε ότι το κριτήριο δεν καλύπτεται καθόλου.

3. Πλαίσια, Μεθοδολογίες και Εργαλεία

Για την παρούσα μελέτη επιλέχθηκαν τα παρακάτω πλαίσια, μεθοδολογίες και εργαλεία προς εξέταση, λόγω της δημοτικότητάς τους και της ευρείας υιοθέτησής του, τα οποία και θα περιγραφούν ομοιοτρόπως για να μπορέσει να είναι σαφέστερη η σύγκριση τους :

1. COSO Internal Control-Integrated Framework
2. The FAIR Methodology
3. ISACA RiskIT Framework
4. ISO 27005 Framework
5. EU ITSRM2, IT Security Risk Management Methodology V1.2
6. Microsoft Security Assessment Tool
7. NIST Special Publication 800-30
8. OCTAVE Allegro methodology
9. Verinice - Risk Management Tool

Ο αναγνώστης μπορεί να συμβουλευθεί τη λίστα με τα προαναφερόμενα κριτήρια συγκριτικής αξιολόγησης για να αποσαφηνίσει οποιαδήποτε στιγμή το τι αντιπροσωπεύει το καθένα χαρακτηριστικό που περιγράφεται για κάθε πλαίσιο/μεθοδολογία/εργαλείο.

3.1 Αναλυτική παρουσίαση

Ακολουθεί αναλυτική παρουσίαση του κάθε επιλεγμένου πλαισίου, μεθοδολογίας, εργαλείου , η οποία περιλαμβάνει μία σύντομη παρουσίαση του ιστορικού και της λειτουργίας του κάθε πλαισίου/μεθοδολογίας/εργαλείου και στη συνέχεια παρουσιάζονται τα χαρακτηριστικά του καθενός περιγεγραμμένα μέσω των κριτηρίων αξιολόγησης που έχουμε αναφέρει στην προηγούμενη ενότητα της παρούσας μελέτης.

1) COSO Internal Control-Integrated Framework

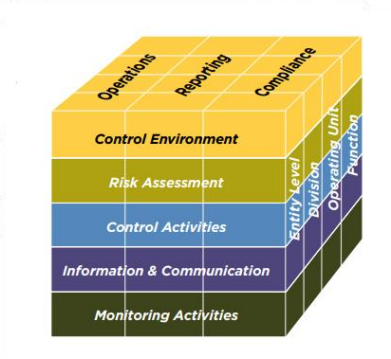
Ιστορικό

Το COSO είναι ακρωνύμιο της Επιτροπής Χορηγών Οργανισμών (Committee of Sponsoring Organizations). Η επιτροπή αυτή δημιούργησε το πλαίσιο το 1992, με επικεφαλής τον Εκτελεστικό Αντιπρόεδρο και Γενικό Σύμβουλο, James Treadway, Jr. μαζί με άλλους οργανισμούς του ιδιωτικού τομέα.
Το πλαίσιο COSO επικαιροποιήθηκε το 2013 με την ονομασία Internal Control-Integrated Framework, για να συμπεριλάβει τον κύβο COSO, ένα τρισδιάστατο διάγραμμα που καταδεικνύει πώς όλα τα στοιχεία ενός συστήματος εσωτερικού ελέγχου συνδέονται μεταξύ τους (εικόνα 1). Το 2017, η επιτροπή εισήγαγε το πλαίσιο COSO για τη διαχείριση επιχειρηματικών κινδύνων με όνομα COSO Enterprise Risk Management framework.

Επισκόπηση

Το πλαίσιο COSO είναι ένα σύστημα που χρησιμοποιείται για **τη δημιουργία εσωτερικών ελέγχων που πρέπει να ενσωματωθούν στις επιχειρηματικές διαδικασίες**. Από κοινού, οι έλεγχοι αυτοί παρέχουν την **επαρκή διασφάλιση ότι ο οργανισμός λειτουργεί με ηθική, διαφάνεια και σύμφωνα με τα καθιερωμένα πρότυπα του κλάδου.**

Το Πλαίσιο COSO ERM έχει ως στόχο **να βοηθήσει τους οργανισμούς να κατανοήσουν και να ιεραρχήσουν τους κινδύνους και να δημιουργήσουν μια ισχυρή σύνδεση μεταξύ της επικινδυνότητας, της στρατηγικής και του τρόπου με τον οποίο μια επιχείρηση αποδίδει.**



Εικόνα 1: COSO ERM framework 2013

Τα πέντε συστατικά στοιχεία του ολοκληρωμένου πλαισίου εσωτερικού ελέγχου της COSO είναι:

1. **Περιβάλλον ελέγχου:** Η συνολική στάση, η ευαισθητοποίηση και οι ενέργειες της ηγεσίας, της διοίκησης και των εργαζομένων ενός οργανισμού σχετικά με τον εσωτερικό έλεγχο και τη σημασία του για τον οργανισμό.
2. **Αξιολόγηση κινδύνων:** Ο εντοπισμός και η ανάλυση πιθανών γεγονότων που θα μπορούσαν να επηρεάσουν αρνητικά την ικανότητα του οργανισμού να επιτύχει τους στόχους του.

3. **Δραστηριότητες ελέγχου:** Οι πολιτικές και οι διαδικασίες που συμβάλλουν στη διασφάλιση της εκτέλεσης των οδηγιών της διοίκησης, όπως οι εγκρίσεις, οι εξουσιοδοτήσεις, οι επαληθεύσεις, οι συμφωνίες και ο διαχωρισμός των καθηκόντων.
4. **Πληροφόρηση και επικοινωνία:** Ο προσδιορισμός, η καταγραφή και η ανταλλαγή πληροφοριών που είναι απαραίτητες για την υποστήριξη της λειτουργίας του εσωτερικού ελέγχου.
5. **Παρακολούθηση:** Η διαδικασία αξιολόγησης της ποιότητας της απόδοσης του εσωτερικού ελέγχου με την πάροδο του χρόνου, συμπεριλαμβανομένης της συνεχούς παρακολούθησης και των ξεχωριστών αξιολογήσεων.

Οι πέντε συνιστώσες του πλαισίου COSO αποτελούν τη βάση για τον εσωτερικό έλεγχο. Δημιουργούν επίσης το πλαίσιο για τον ορισμό του εσωτερικού ελέγχου μέσω **τριών στόχων.**

1. **Επιχειρησιακοί στόχοι :** Αφορά δραστηριότητες που εξασφαλίζουν την αποδοτική και αποτελεσματική λειτουργία των επιχειρησιακών διαδικασιών.
2. **Στόχοι αναφοράς :**Αφορούν εσωτερικές και εξωτερικές αναφορές χρηματοοικονομικών και μη χρηματοοικονομικών δραστηριοτήτων.
3. **Στόχοι συμμόρφωσης :**Αυτοί οι στόχοι αφορούν τη συμμόρφωση και τους κανονισμούς.

Χρηστικότητα

Το COSO IC-IF , θεωρείται ένα ολοκληρωμένο πλαίσιο **που καλύπτει ένα ευρύ φάσμα θεμάτων εσωτερικού ελέγχου**, αλλά **μπορεί να είναι αρκετά λεπτομερές και πολύπλοκο, γεγονός που μπορεί να δυσχεράνει την κατανόηση και την εφαρμογή του από ορισμένους οργανισμούς**, κάτι που το καθιστά εν μέρει δύσχρηστο.

Χρησιμοποιείται συνήθως από μεγαλύτερους οργανισμούς και από οργανισμούς με πιο σύνθετα συστήματα εσωτερικού ελέγχου, οι οποίοι ενδέχεται να απαιτούν ένα ορισμένο επίπεδο εμπειρογνωμοσύνης για την πλήρη κατανόηση και εφαρμογή του πλαισίου. Επιπλέον δεν έχει σχεδιαστεί ως οδηγός βήμα προς βήμα, οπότε οι οργανισμοί **ενδέχεται να χρειαστεί να επενδύσουν χρόνο και πόρους για την ερμηνεία και την προσαρμογή του πλαισίου ώστε να ανταποκρίνεται στις συγκεκριμένες ανάγκες τους.**

Όσον αφορά τη συντήρηση και τις ενημερώσεις, το πλαίσιο δεν είναι ένα ζωντανό έγγραφο, οπότε ενδέχεται να μην ενημερώνεται τόσο συχνά όσο άλλα πλαίσια. Ωστόσο, ο οργανισμός COSO εκδίδει ενημερώσεις και οδηγίες για να βοηθήσει τους οργανισμούς στην κατανόηση και την εφαρμογή του πλαισίου.

Συνολικά, η χρηστικότητα του ενοποιημένου πλαισίου εσωτερικού ελέγχου COSO μπορεί να θεωρηθεί μέτρια.

Ευελιξία

Το COSO **έχει σχεδιαστεί ώστε να μπορεί να προσαρμόζεται στις συγκεκριμένες ανάγκες και συνθήκες των διαφόρων οργανισμών και επιχειρήσεων και θεωρείται γενικά ευέλικτο.** Παρέχει καθοδήγηση σχετικά με τον τρόπο ενσωμάτωσης του ERM (Enterprise Risk Management) στη συνολική στρατηγική και τις διαδικασίες λήψης αποφάσεων ενός

οργανισμού και μπορεί να εφαρμοστεί σε οργανισμούς διαφορετικών μεγεθών και κλάδων τόσο για την αξιολόγηση των χρηματοοικονομικών όσο και των μη χρηματοοικονομικών εσωτερικών ελέγχων.
Επιτρέπει στους οργανισμούς να εντοπίζουν και να αξιολογούν τους κινδύνους με τρόπο που να συνάδει με τη συνολική στρατηγική τους για τη διαχείριση της επικινδυνότητας. Επιπλέον, επιτρέπει στους οργανισμούς **να εφαρμόζουν δραστηριότητες εσωτερικού ελέγχου για τον μετριασμό της επικινδυνότητας με βάση το δικό τους εσωτερικό περιβάλλον, τους στόχους και τους εξωτερικούς παράγοντες κάτι που το κάνει ένα ευέλικτο πλαίσιο.**

Διαχείριση περιουσιακών στοιχείων

Το COSO IC - IF **δεν διαθέτει ειδική διαδικασία για τη διαχείριση περιουσιακών στοιχείων**, αλλά παρέχει οδηγίες για το πώς οι οργανισμοί μπορούν να διαχειριστούν τους κινδύνους που σχετίζονται με τα περιουσιακά τους στοιχεία. Προτείνει στους οργανισμούς να αναπτύσσουν πολιτικές και διαδικασίες για να διασφαλίζουν ότι τα περιουσιακά στοιχεία διασφαλίζονται, καταγράφονται με ακρίβεια και χρησιμοποιούνται σύμφωνα με την εξουσιοδότηση της διοίκησης και να διενεργούν τακτικές αξιολογήσεις κινδύνου για τον εντοπισμό και τη διαχείριση της επικινδυνότητας που σχετίζεται με τα περιουσιακά τους στοιχεία**,** αλλά δεν περιλαμβάνει συγκεκριμένα μια διαδικασία για τη διαχείριση περιουσιακών στοιχείων. Θεωρούμε ότι το κριτήριο δεν καλύπτεται από το COSO IC-IF.

Βάση δεδομένων για απειλές

Το πλαίσιο COSO IC-IF επικεντρώνεται στην παροχή καθοδήγησης για το σχεδιασμό και την εφαρμογή συστημάτων εσωτερικού ελέγχου **και όχι στον εντοπισμό και την παρακολούθηση συγκεκριμένων απειλών.** Το πλαίσιο COSO περιλαμβάνει αρχές και σημεία εστίασης που σχετίζονται με την αξιολόγηση της επικινδυνότητας, τα οποία περιλαμβάνουν **τον εντοπισμό και την αξιολόγηση των απειλών που αντιμετωπίζει ένας οργανισμός και τον καθορισμό του τρόπου αντιμετώπισης αυτών των απειλών** ωστόσο, δεν παρέχει ούτε παράγει κάποια βάση δεδομένων για απειλές.
Αντ' αυτού, οι οργανισμοί μπορούν να χρησιμοποιούν διάφορες πηγές πληροφοριών, όπως εκθέσεις του κλάδου και πληροφορίες για την ασφάλεια στον κυβερνοχώρο, για να εντοπίζουν και να αξιολογούν τις συγκεκριμένες απειλές που αντιμετωπίζουν. Στη συνέχεια, μπορούν να χρησιμοποιήσουν το πλαίσιο COSO IC-IF για να τους βοηθήσει να σχεδιάσουν και να εφαρμόσουν συστήματα εσωτερικού ελέγχου που είναι αποτελεσματικά για τον μετριασμό αυτών των απειλών και την επίτευξη των στόχων τους. Συνολικά, επειδή περιλαμβάνει τον εντοπισμό και την αξιολόγηση των απειλών, θα λέγαμε ότι καλύπτει μερικώς το κριτήριο.

Βάση δεδομένων για ευπάθειες

Το COSO IC-IF παρέχει ένα πλαίσιο για τους οργανισμούς ώστε να αξιολογούν και να κατανοούν τους εσωτερικούς τους ελέγχους και να αξιολογούν την αποτελεσματικότητά τους όσον αφορά την αντιμετώπιση πιθανών κινδύνων και ευπαθειών **και δεν περιέχει ούτε παρέχει βάση δεδομένων για τις ευπάθειες.** Το πλαίσιο περιλαμβάνει

κατευθυντήριες γραμμές και βέλτιστες πρακτικές για τον εντοπισμό, την αξιολόγηση και τη διαχείριση της επικινδυνότητας, αλλά εναπόκειται στον οργανισμό να εντοπίσει και να αξιολογήσει τις συγκεκριμένες ευπάθειες και τους πιθανούς κινδύνους του.

Βάση δεδομένων για μέτρα ασφαλείας.

Οι έλεγχοι και τα αντίμετρα αποτελούν βασική πτυχή του πλαισίου, καθώς είναι τα μέσα με τα οποία ένας οργανισμός μπορεί να μετριάσει τους κινδύνους που αντιμετωπίζει. Ωστόσο, το πλαίσιο COSO **δεν παρέχει κατάλογο ή βάση δεδομένων συγκεκριμένων ελέγχων ή αντιμέτρων**. Αντ' αυτού**,** εστιάζει στην παροχή μιας ολοκληρωμένης, βασισμένης στην επικινδυνότητα , προσέγγισης για τον εντοπισμό, την αξιολόγηση και τη διαχείριση της επικινδυνότητας σε ολόκληρο τον οργανισμό. Το COSO παρέχει έναν οδηγό για τη διοίκηση ώστε να αναπτύξει μέτρα που ανταποκρίνονται στους συγκεκριμένους κινδύνους του οργανισμού, και **παρέχει επίσης οδηγίες για τη διατήρηση, την αξιολόγηση και τη δοκιμή της αποτελεσματικότητας των μέτρων αυτών. Συνολικά το κριτήριο καλύπτεται εν μέρει από το COSO.**

Πλοήγηση σε περιστατικά

Το COSO **δεν περιλαμβάνει συγκεκριμένα μια διαδικασία πλοήγησης σε περιστατικά, αλλά περιλαμβάνει μια συνιστώσα για τις δραστηριότητες ελέγχου, όπου θα μπορούσε να εφαρμοστεί η διαδικασία πλοήγησης σε περιστατικά.**
Οι δραστηριότητες ελέγχου είναι πολιτικές και διαδικασίες που συμβάλλουν στη διασφάλιση της εκτέλεσης των οδηγιών της διοίκησης και της λήψης των απαραίτητων μέτρων για την αντιμετώπιση της επικινδυνότητας που απειλεί την επίτευξη των στόχων της οντότητας. Οι δραστηριότητες αυτές περιλαμβάνουν μια σειρά από ενέργειες, όπως εγκρίσεις, εξουσιοδοτήσεις, επαληθεύσεις, συμφωνίες, επισκοπήσεις της λειτουργικής απόδοσης, ασφάλεια των περιουσιακών στοιχείων και διαχωρισμό των καθηκόντων. Έτσι, η διαδικασία πλοήγησης περιστατικών θα μπορούσε να είναι μία από τις δραστηριότητες ελέγχου που μπορούν να καθιερώσουν οι οργανισμοί προκειμένου να συμβάλουν στον μετριασμό της επικινδυνότητας και στην πρόληψη περιστατικών. Θεωρούμε ότι το κριτήριο καλύπτεται εν μέρει.

Έλεγχος επιχειρησιακών διαδικασιών

Το πλαίσιο COSO **περιλαμβάνει οδηγίες σχετικά με το σχεδιασμό και την εφαρμογή εσωτερικών ελέγχων, συμπεριλαμβανομένων των ελέγχων επί των επιχειρηματικών διαδικασιών.** Το πλαίσιο παρέχει στους οργανισμούς μια δομή για την αξιολόγηση και τη βελτίωση των συστημάτων εσωτερικού ελέγχου, συμπεριλαμβανομένου του εντοπισμού και της αντιμετώπισης της επικινδυνότητας, της εφαρμογής πολιτικών και διαδικασιών και της παρακολούθησης της αποτελεσματικότητάς τους. **Η συνιστώσα "Δραστηριότητες ελέγχου"** του πλαισίου και συγκεκριμένα η Αρχή 10 : «Ο οργανισμός επιλέγει και αναπτύσσει δραστηριότητες ελέγχου που συμβάλλουν στον μετριασμό της επικινδυνότητας για την επίτευξη των στόχων σε αποδεκτά επίπεδα», **ασχολείται συγκεκριμένα με τους ελέγχους επί των επιχειρηματικών διαδικασιών, συμπεριλαμβανομένου του διαχωρισμού των καθηκόντων, των εξουσιοδοτήσεων και εγκρίσεων, των φυσικών**

ελέγχων και των διαδικασιών παρακολούθησης και συμφωνίας των συναλλαγών. Το κριτήριο καλύπτεται πλήρως.

Αναφορές και αναλύσεις

Το COSO (IC-IF) παρέχει καθοδήγηση σχετικά με την υποβολή εκθέσεων και την ανάλυση ως μέρος της συνιστώσας "Πληροφόρηση και επικοινωνία" , ειδικότερα στις Αρχές 13 και 14. Το πλαίσιο αναφέρει ότι οι οργανισμοί θα πρέπει να αναπτύσσουν και να διατηρούν ένα σύστημα για τον εντοπισμό, την καταγραφή και την ανταλλαγή σχετικών πληροφοριών που είναι απαραίτητες για την υποστήριξη της λειτουργίας του εσωτερικού ελέγχου. Αυτό περιλαμβάνει πληροφορίες που χρησιμοποιούνται για την υποβολή εκθέσεων προς τη διοίκηση και τους υπεύθυνους για τη διακυβέρνηση, καθώς και πληροφορίες που χρησιμοποιούνται για τη λήψη αποφάσεων. Επιπλέον, το πλαίσιο τονίζει τη σημασία της επικοινωνίας και την ανάγκη για ανοικτές γραμμές επικοινωνίας σε ολόκληρο τον οργανισμό, συμπεριλαμβανομένης της αποτελεσματικής επικοινωνίας των πληροφοριών που σχετίζονται με τον έλεγχο και της επικοινωνίας των ελλείψεων του εσωτερικού ελέγχου. Συνολικά καλύπτεται πλήρως το κριτήριο.

Επίπεδο τεχνικότητας

Το πλαίσιο COSO έχει σχεδιαστεί έτσι ώστε να είναι ευέλικτο και προσαρμόσιμο σε διαφορετικούς οργανισμούς και κλάδους και **δεν απαιτεί υψηλό επίπεδο τεχνικών γνώσεων για την εφαρμογή του**, όμως οι ιδιαιτερότητες της εφαρμογής ποικίλλουν ανάλογα με το μέγεθος, την πολυπλοκότητα και τη φύση του οργανισμού.
Το πλαίσιο βασίζεται στις αρχές του εσωτερικού ελέγχου και παρέχει μια κοινή γλώσσα και δομή για την αξιολόγηση των συστημάτων εσωτερικού ελέγχου, δεν προδιαγράφει συγκεκριμένες μεθόδους ή διαδικασίες για την εφαρμογή**. Η εφαρμογή των αρχών του πλαισίου μπορεί να γίνει από τη διοικητική ομάδα του οργανισμού και τους υπαλλήλους με γνώση των λειτουργιών της εταιρείας, ανεξάρτητα από το τεχνικό τους υπόβαθρο.** Ωστόσο, όπως και σε κάθε άλλο πλαίσιο, είναι σημαντικό **να υπάρχει καλή κατανόηση των αρχών και των στοιχείων του πλαισίου για να μπορέσει να εφαρμοστεί αποτελεσματικά και αποδοτικά**. Συνιστάται επίσης η συνεργασία με εμπειρογνώμονες, όπως επαγγελματίες του εσωτερικού ελέγχου, της διαχείρισης κινδύνων ή της συμμόρφωσης, για την παροχή **καθοδήγησης και υποστήριξης** κατά την εφαρμογή του πλαισίου. Η τεχνικότητα που απαιτείται θεωρείται μέτρια.

Υποστήριξη και πόροι

Το COSO (IC-IF**) περιλαμβάνει υποστηρικτικό υλικό και βοηθητικούς πόρους για να βοηθήσει τους οργανισμούς να κατανοήσουν και να χρησιμοποιήσουν σωστά το πλαίσιο.** Περιλαμβάνει έναν **οδηγός χρήσης**, ο οποίος παρέχει μια επισκόπηση του πλαισίου, συμπεριλαμβανομένων των στοιχείων και των αρχών του, και καθοδήγηση σχετικά με τον τρόπο χρήσης του πλαισίου.
Το υποστηρικτικό υλικό και οι πόροι περιλαμβάνουν **διάφορα εργαλεία και πρότυπα, καθώς και μελέτες περιπτώσεων και παραδείγματα για το πώς το πλαίσιο έχει εφαρμοστεί σε διαφορετικούς τύπους οργανισμών και κλάδων**. Επιπλέον, ο δικτυακός τόπος του COSO παρέχει πρόσβαση σε πρόσθετους πόρους, όπως whitepapers,

διαδικτυακά σεμινάρια και άλλο εκπαιδευτικό υλικό για την υποστήριξη της κατανόησης και της εφαρμογής του πλαισίου.
Επιπλέον, υπάρχουν και τρίτοι πάροχοι που προσφέρουν πρόσθετους πόρους, όπως εκπαίδευση, λογισμικό και συμβουλευτικές υπηρεσίες για την ορθή εφαρμογή του πλαισίου COSO.

Πληρότητα

Το πλαίσιο COSO δεν καλύπτει όλους τους σχετικούς τομείς της διαχείρισης επικινδυνότητας της ασφάλειας πληροφοριών. Το πλαίσιο επικεντρώνεται σε πέντε βασικές συνιστώσες του εσωτερικού ελέγχου όπως έχει ήδη προαναφερθεί , ωστόσο , η διαχείριση επικινδυνότητας της ασφάλειας πληροφοριών **απαιτεί μια πιο ολοκληρωμένη προσέγγιση** που περιλαμβάνει πρόσθετες συνιστώσες κινδύνου, όπως η διαχείριση περιουσιακών στοιχείων, η πιστοποίηση και εξουσιοδότηση, ο έλεγχος πρόσβασης, η προστασία δεδομένων και η ασφάλεια συστημάτων.
Το πλαίσιο COSO αν και καλύπτει πολλές πτυχές της διαχείρισης κινδύνων, δεν ασχολείται ειδικά με τους κινδύνους ασφάλειας πληροφοριών. Οι οργανισμοί που βασίζονται σε μεγάλο βαθμό στην τεχνολογία και τα συστήματα πληροφορικής ενδέχεται να χρειαστεί να συμπληρώσουν το πλαίσιο COSO με πρόσθετους ελέγχους και πρακτικές διαχείρισης κινδύνων που αφορούν ειδικά την ασφάλεια. Για παράδειγμα, ένα πλαίσιο ασφάλειας όπως το NIST CSF (Cybersecurity Framework) ή το ISO/IEC 27001 θα μπορούσε να χρησιμοποιηθεί για να συμπληρώσει το πλαίσιο COSO στην αντιμετώπιση της επικινδυνότητας της ασφάλειας πληροφοριών. Συνολικά το κριτήριο της πληρότητας καλύπτεται εν μέρει.

Χρόνος

Η εφαρμογή του πλαισίου μπορεί να είναι χρονοβόρα, καθώς απαιτεί από τους οργανισμούς να έχουν σαφή κατανόηση των εσωτερικών τους ελέγχων και των διαδικασιών διαχείρισης κινδύνων και να είναι σε θέση να αξιολογούν και να αντιμετωπίζουν αποτελεσματικά τους κινδύνους. **Επιπλέον, μπορεί να απαιτήσει από τους οργανισμούς να προβούν σε σημαντικές αλλαγές στις τρέχουσες διαδικασίες τους, οι οποίες μπορεί να είναι δύσκολες και χρονοβόρες.** Οι οργανισμοί θα πρέπει να επενδύσουν χρόνο για να κατανοήσουν, να τεκμηριώσουν και να εφαρμόσουν το πλαίσιο, καθώς και για να επανεξετάζουν, να επικαιροποιούν και να παρακολουθούν τους εσωτερικούς ελέγχους, τη διαχείριση κινδύνων και την ασφάλεια πληροφοριών.
Αν και τα οφέλη από τη χρήση του πλαισίου μπορεί μακροπρόθεσμα να είναι σημαντικά θεωρούμε ότι το κριτήριο δεν καλύπτεται καθόλου, αφού είναι μία αρκετά χρονοβόρα διαδικασία.

Οικονομικό κόστος

Το COSO δεν είναι δωρεάν. Το πλαίσιο ανήκει και συντηρείται από την Επιτροπή Χορηγικών Οργανισμών της Επιτροπής Treadway και **η πρόσβαση στο πλαίσιο, η εκπαίδευση και η πιστοποίηση έχει κάποια οικονομική επιβάρυνση**. Η COSO προσφέρει διάφορους πόρους, όπως οδηγίες και διαδικτυακά σεμινάρια, τα οποία μπορούν να αγοραστούν ή να αποκτήσουν πρόσβαση σε αυτά με συνδρομή επί πληρωμή. Ωστόσο, **το ίδιο το έγγραφο**

του πλαισίου μπορεί να μεταφορτωθεί δωρεάν από τον ιστότοπο της COSO, οπότε το κόστος του ίδιου του πλαισίου είναι μηδενικό. Εάν ένας οργανισμός επιθυμεί να συμμετάσχει σε προγράμματα κατάρτισης ή πιστοποίησης, αυτά θα έχουν κάποιο κόστος. Επιπλέον, ορισμένοι οργανισμοί μπορεί να επιλέξουν να αγοράσουν πρόσθετους πόρους ή υλικό καθοδήγησης, τα οποία επίσης θα έχουν κόστος που συνδέεται με αυτά. Σε γενικές γραμμές**, το κόστος χρήσης του πλαισίου COSO μπορεί να θεωρηθεί μέτριο, καθώς δεν απαιτεί μεγάλη επένδυση, αλλά μπορεί να απαιτεί κάποιο κόστος για την πρόσβαση σε ορισμένους πόρους ή πιστοποιήσεις, οπότε το κριτήριο καλύπτεται εν μέρει.**

2) The FAIR™ Methodology for Cyber Risks

Ιστορικό

Η μεθοδολογία Factor Analysis of Information Risk (FAIR) εισήχθη για πρώτη φορά το 2000 από τον Jack Jones, ιδρυτή και επικεφαλής έρευνας της Risk Management Insight, LLC. Το FAIR Institute, είναι ένας μη κερδοσκοπικός οργανισμός, ιδρύθηκε το 2016 με σκοπό την προώθηση της χρήσης του FAIR και την παροχή εκπαίδευσης και πόρων σε επαγγελματίες και οργανισμούς.

Το FAIR βοηθά τους οργανισμούς να κατανοήσουν, να μετρήσουν και να αναλύσουν τον κίνδυνο της κυβερνοασφάλειας και να λαμβάνουν έγκαιρα και τεκμηριωμένα αποφάσεις σχετικά με τον τρόπο πρόληψης και αποκατάστασης διαφόρων μορφών επιθέσεων στον κυβερνοχώρο σε κρίσιμα δεδομένα και συστήματα.

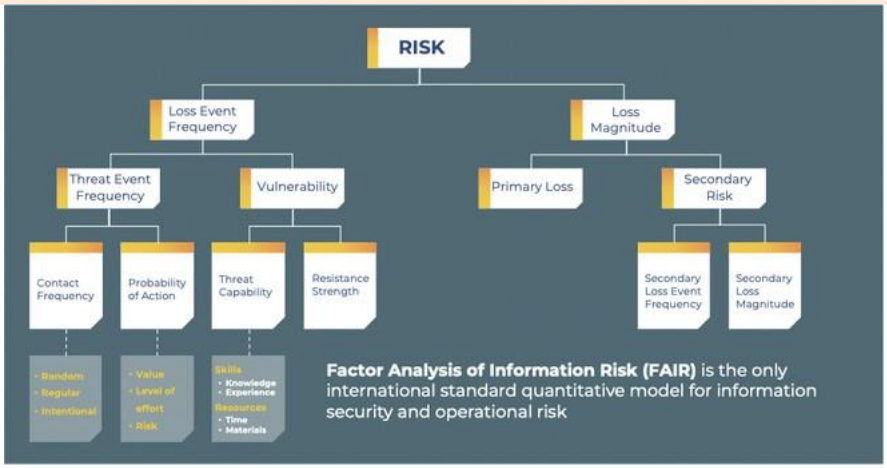
Η πιο ισχυρή πτυχή της μεθοδολογίας FAIR είναι ότι ποσοτικοποιεί τις διάφορες μορφές κινδύνου με μια χρηματική ή νομισματική αξία. Αυτό βοηθά τις επιχειρήσεις να μεταφράσουν τον κίνδυνο στον κυβερνοχώρο σε εφαρμόσιμες, οικονομικά ορθές αποφάσεις.

Πώς λειτουργεί η μεθοδολογία FAIR;

Η αξιολόγηση κινδύνων με τη μεθοδολογία FAIR αξιολογεί συστηματικά τους κινδύνους ασφάλειας με :

- Κατηγοριοποίηση του συστήματος που διατρέχει κίνδυνο από απειλές
- Προσδιορισμό των διαφόρων απειλών που μπορεί να αντιμετωπίσει ένα σύστημα
- Βαθμολόγηση του επιπέδου επιπτώσεων για κάθε κατηγορία κινδύνου
- Αξιολόγηση του περιβάλλοντος ελέγχου
- Υπολογισμός της βαθμολογίας κινδύνου

Η ταξινόμηση της επικινδυνότητας με βάση την οποία μπορεί να σχηματοποιηθεί το FAIR™ φαίνεται στην εικόνα 2:



Εικόνα 2: Factor Analysis of Information Risk (FAIR)

Η ανάλυση κινδύνου πραγματοποιείται σε τέσσερα στάδια.

Στάδιο 1.

Προσδιορισμός των στοιχείων του σεναρίου

- Προσδιορισμός του περιουσιακού στοιχείου που διατρέχει κίνδυνο
- Προσδιορισμός της εξεταζόμενης ομάδας απειλών

Στάδιο 2 -

Αξιολόγηση της συχνότητας συμβάντων απώλειας (LEF)

- Εκτίμηση της πιθανής συχνότητας συμβάντων απειλής (TEF)
- Εκτίμηση της ικανότητας απειλής (TCap)
- Εκτίμηση της δύναμης του ελέγχου (CS)
- Παραγωγή ευπάθειας (Vuln)
- Εξαγωγή της συχνότητας συμβάντων απώλειας (LEF)

Στάδιο 3 -

Αξιολόγηση του πιθανού μεγέθους απώλειας (PLM)

- Εκτίμηση απώλειας χειρότερης περίπτωσης
- Εκτίμηση πιθανής απώλειας

Στάδιο 4 -

Παραγωγή και διατύπωση κινδύνων

- Παραγωγή και διατύπωση της επικινδυνότητας

Η ολοκλήρωση και των τεσσάρων σταδίων της μεθοδολογίας κινδύνου FAIR δίνει στους οργανισμούς μια σαφή εικόνα των σημείων στα οποία είναι ευάλωτοι, του εν δυνάμει κόστους των επιθέσεων στον κυβερνοχώρο και των φορέων επίθεσης που πρέπει ενδεχομένως να ενισχύσουν**. Ο κίνδυνος ορίζεται από την αξιολόγηση FAIR ως "Η πιθανή συχνότητα και το πιθανό μέγεθος μελλοντικής απώλειας".**

Χρηστικότητα

Η μεθοδολογία FAIR έχει σχεδιαστεί έτσι ώστε να είναι πολύ φιλική προς το χρήστη και είναι εύκολη στη συντήρηση και την ενημέρωση. Η διαδικασία βασίζεται σε μερικά απλά βήματα, όπως ο καθορισμός των στόχων, η συλλογή δεδομένων, η ανάπτυξη ενός μοντέλου και η δοκιμή του μοντέλου. Η μεθοδολογία FAIR περιλαμβάνει επίσης έναν οδηγό βήμα προς βήμα που βοηθά τους χρήστες να δημιουργούν και να δοκιμάζουν μοντέλα με ελάχιστη προσπάθεια, εξασφαλίζοντας ακρίβεια και συνέπεια. Επιπλέον, το FAIR επιτρέπει στους χρήστες να ενημερώνουν γρήγορα τα μοντέλα τους χωρίς να χρειάζεται να τα ανακατασκευάσουν πλήρως.
Το πλαίσιο παρέχει μια κοινή γλώσσα για τη διαχείριση της επικινδυνότητας και επιτρέπει την ποσοτικοποίηση και τη σύγκριση της επικινδυνότητας σε διάφορα τμήματα ενός οργανισμού. **Η χρηστικότητά του θεωρείται υψηλή λόγω της σαφούς, συνεπούς και ολοκληρωμένης προσέγγισής του στη διαχείριση κινδύνων και της ικανότητάς του να ενσωματώνεται με τις υφιστάμενες διαδικασίες και πλαίσια διαχείρισης κινδύνων.**

Ευελιξία

Το FAIR είναι ευέλικτο υπό την έννοια ότι μπορεί να εφαρμοστεί σε ένα ευρύ φάσμα κινδύνων ασφάλειας πληροφοριών, σε διαφορετικούς τύπους οργανισμών και κλάδων. Το πλαίσιο παρέχει μια κοινή γλώσσα και ένα σύνολο εννοιών για την περιγραφή και την ανάλυση της επικινδυνότητας, το οποίο μπορεί να χρησιμοποιηθεί για τη διευκόλυνση της επικοινωνίας και της συνεργασίας μεταξύ των διαφόρων ενδιαφερομένων σε έναν οργανισμό. Επιπλέον, επιτρέπει στους οργανισμούς να συγκρίνουν και να ιεραρχούν τους κινδύνους σε συνεπή βάση.

Ωστόσο, οι αρχές της FAIR προορίζονται να είναι καθολικά εφαρμόσιμες και οι κατευθυντήριες γραμμές προορίζονται να ακολουθούνται όσο το δυνατόν στενότερα για να διασφαλιστεί ότι τα δεδομένα είναι όσο το δυνατόν ορθότερα. Επίσης επειδή το FAIR είναι ένα ποσοτικό πλαίσιο και ακολουθεί μια συγκεκριμένη μεθοδολογία και διαδικασία, μπορεί να απαιτεί κάποια εκπαίδευση και τεχνογνωσία για τη σωστή εφαρμογή του.

Συνολικά, το FAIR **δεν παρέχει υψηλό επίπεδο ευελιξίας που θα επέτρεπε στους οργανισμούς να προσαρμόζονται στις μεταβαλλόμενες συνθήκες ή απαιτήσεις εν εξελίξει.** Θεωρούμε ότι το κριτήριο καλύπτεται μερικώς.

Διαχείριση περιουσιακών στοιχείων

Στη μεθοδολογία FAIR, τα περιουσιακά στοιχεία αποτελούν σημαντικό παράγοντα στη διαδικασία ανάλυσης κινδύνων. Η μεθοδολογία **προτείνει τον εντοπισμό και την ταξινόμηση των περιουσιακών στοιχείων που είναι σημαντικά** για τον οργανισμό και την κατανόηση της αξίας τους για τον οργανισμό. Αυτό περιλαμβάνει τόσο υλικά περιουσιακά στοιχεία, όπως διακομιστές και συσκευές, όσο και άυλα περιουσιακά στοιχεία, όπως ευαίσθητα δεδομένα και πνευματική ιδιοκτησία. Συνιστά επίσης **την εξέταση των απειλών και των ευπαθειών που θα μπορούσαν να επηρεάσουν τα εν λόγω περιουσιακά στοιχεία** και την πιθανότητα και τον αντίκτυπο της πραγματοποίησης αυτών των απειλών και των ευπαθειών.

Η διαδικασία **εντοπισμού και χαρακτηρισμού των περιουσιακών στοιχείων** αποτελεί **σημαντικό βήμα στη μεθοδολογία FAIR**, καθώς βοηθά τους οργανισμούς να ιεραρχήσουν τις προσπάθειές τους για τη διαχείριση κινδύνων και να επικεντρωθούν στην προστασία των περιουσιακών στοιχείων που είναι πιο κρίσιμα για τις δραστηριότητές τους, οπότε θεωρούμε ότι το FAIR καλύπτει πλήρως αυτό το κριτήριο.

Βάση δεδομένων για απειλές

Η μεθοδολογία FAIR **δεν περιλαμβάνει μια συγκεκριμένη διαδικασία για τη δημιουργία ή τη διατήρηση μιας βάσης δεδομένων απειλών**. Ωστόσο, περιλαμβάνει μια διαδικασία για τον εντοπισμό και την ανάλυση πιθανών απειλών για τα περιουσιακά στοιχεία ενός οργανισμού.

Η διαδικασία αυτή περιλαμβάνει **τον εντοπισμό πιθανών απειλών,** όπως εξωτερικές επιθέσεις, εσωτερικές παραβιάσεις και φυσικές καταστροφές, και στη συνέχεια **την ανάλυση της πιθανότητας και των επιπτώσεων αυτών των απειλών στα περιουσιακά στοιχεία του οργανισμού.** Οι πληροφορίες αυτές μπορούν στη συνέχεια να χρησιμοποιηθούν για την **ιεράρχηση των προσπαθειών διαχείρισης κινδύνων και την εστίαση στην προστασία των περιουσιακών στοιχείων που κινδυνεύουν περισσότερο.**

Το FAIR δεν προδιαγράφει κάποιον συγκεκριμένο τρόπο συλλογής των πληροφοριών σχετικά με τις απειλές, οι οργανισμοί μπορούν να χρησιμοποιούν τις δικές τους τροφοδοσίες πληροφοριών για απειλές, εσωτερικούς και εξωτερικούς ελέγχους, αναφορές περιστατικών, penetration testing και σαρώσεις ευπαθειών κ.λπ. για να συλλέγουν πληροφορίες που θα τροφοδοτήσουν τη μεθοδολογία FAIR, οπότε θεωρούμε ότι καλύπτει εν μέρει αυτό το κριτήριο.

Βάση δεδομένων για ευπάθειες

Η μεθοδολογία FAIR δεν περιλαμβάνει κάποια βάση δεδομένων με ευπάθειες, αντ' αυτού περιλαμβάνει μια διαδικασία για τον εντοπισμό και την ανάλυση πιθανών ευπαθειών στα περιουσιακά στοιχεία ενός οργανισμού, αλλά δεν καθορίζει τον τρόπο με τον οποίο θα πρέπει να αποθηκεύονται ή να διαχειρίζονται οι πληροφορίες αυτές για τις ευπάθειες.
Η διαδικασία αυτή περιλαμβάνει **α)** τον εντοπισμό πιθανών ευπαθειών, όπως τρωτά σημεία λογισμικού, ζητήματα διαμόρφωσης και ανθρώπινα λάθη, και **β)** την ανάλυση, της πιθανότητας και του αντίκτυπου αυτών των ευπαθειών στα περιουσιακά στοιχεία του οργανισμού. Οι πληροφορίες αυτές μπορούν στη συνέχεια να χρησιμοποιηθούν για την ιεράρχηση των προσπαθειών διαχείρισης κινδύνου και την εστίαση στον μετριασμό των ευπαθειών που είναι πιο κρίσιμες για τις λειτουργίες του οργανισμού.
Εναπόκειται στον οργανισμό να αποφασίσει πώς θα αποθηκεύσει και θα διαχειριστεί τις ευπάθειες που εντοπίζονται κατά τη διαδικασία. Οι οργανισμοί μπορούν να χρησιμοποιήσουν διάφορες πηγές πληροφοριών, όπως σαρώσεις ευπαθειών, δοκιμές διείσδυσης, αναφορές συμβάντων, εσωτερικούς και εξωτερικούς ελέγχους κ.λπ. για να συλλέξουν πληροφορίες σχετικά με τις ευπάθειες και να τις τροφοδοτήσουν στη μεθοδολογία FAIR, αλλά η ίδια η μεθοδολογία FAIR δεν περιλαμβάνει μια συγκεκριμένη βάση δεδομένων ευπαθειών. Σύμφωνα με τα παραπάνω θεωρούμε ότι το κριτήριο καλύπτεται εν μέρει, διότι υπάρχει διαδικασία εντοπισμού και διαδικασία ανάλυσης των ευπαθειών.

Βάση δεδομένων για μέτρα ασφάλειας

Η μεθοδολογία FAIR δεν περιλαμβάνει ούτε παρέχει συγκεκριμένη βάση δεδομένων μέτρων ασφαλείας ή αντιμέτρων όπως το έχουμε προσδιορίσει στην παρούσα μελέτη , περιλαμβάνει όμως μια διαδικασία για τον εντοπισμό και την ανάλυση της αποτελεσματικότητας των υφιστάμενων μέτρων ασφαλείας ή αντιμέτρων που εφαρμόζονται για τον μετριασμό της επικινδυνότητας.
Η διαδικασία αυτή περιλαμβάνει τον εντοπισμό των υφιστάμενων μέτρων ασφαλείας ή αντιμέτρων, την αξιολόγηση της αποτελεσματικότητάς τους όσον αφορά τον μετριασμό της επικινδυνότητας και την ανάλυση του υπολειπόμενου κινδύνου που παραμένει μετά την εφαρμογή των ελέγχων ή των αντιμέτρων. Οι πληροφορίες αυτές μπορούν στη συνέχεια να χρησιμοποιηθούν για την ιεράρχηση των προσπαθειών διαχείρισης κινδύνου και την εστίαση στην εφαρμογή πρόσθετων μέτρων ή αντιμέτρων για την περαιτέρω μείωση της επικινδυνότητας.
Αξίζει να σημειωθεί ότι η FAIR επικεντρώνεται στη διαχείριση επικινδυνότητας και, ως εκ τούτου, δεν καθορίζει μέτρα ασφαλείας ή τα αντίμετρα που πρέπει να χρησιμοποιηθούν για τον μετριασμό της επικινδυνότητας, εξαρτάται από τον οργανισμό να αποφασίσει ποια

μέτρα ή αντίμετρα πρέπει να χρησιμοποιηθούν με βάση τη διάθεση ανάληψης κινδύνου, τις απειλές και τις ευπάθειες που έχουν εντοπιστεί, τις απαιτήσεις συμμόρφωσης, τις κανονιστικές απαιτήσεις κ.λπ. Σύμφωνα με τα παραπάνω το κριτήριο καλύπτεται μερικώς, εφ' όσον προβλέπεται διαδικασία εντοπισμού και αξιολόγησης των μέτρων ασφαλείας.

Πλοήγηση σε περιστατικά

Το FAIR επικεντρώνεται κυρίως στην ανάλυση και τον ποσοτικό προσδιορισμό του κινδύνου και όχι στην αντιμετώπιση περιστατικών. Ωστόσο, οι οργανισμοί μπορούν να χρησιμοποιήσουν το πλαίσιο για να ενημερώσουν τις διαδικασίες αντιμετώπισης συμβάντων. Μια προσέγγιση θα μπορούσε να είναι η χρήση του πλαισίου FAIR για τον εντοπισμό και την ιεράρχηση πιθανών κινδύνων και, στη συνέχεια, η χρήση αυτών των πληροφοριών για την ανάπτυξη και εφαρμογή αποτελεσματικών σχεδίων αντιμετώπισης συμβάντων και διαδικασιών διαχείρισης συμβάντων. Από τα παραπάνω προκύπτει ότι το FAIR δεν καλύπτει αυτό το κριτήριο.

Έλεγχος επιχειρηματικών διαδικασιών

Η μεθοδολογία περιλαμβάνει μια τυποποιημένη ταξινόμηση και λεξιλόγιο, καθώς και μια διαδικασία για την ανάλυση της επικινδυνότητας και τον προσδιορισμό του συνολικού επιπέδου σοβαρότητάς τους, **αλλά δεν περιλαμβάνει συγκεκριμένη διαδικασία για τον έλεγχο των επιχειρηματικών διαδικασιών.**
Ωστόσο, άλλες μεθοδολογίες, όπως το ISO 31000 ή το COBIT ,που περιλαμβάνουν ελέγχους επιχειρησιακών διαδικασιών, μπορούν να χρησιμοποιηθούν **σε συνδυασμό με το FAIR** για να παρέχουν μια πιο ολοκληρωμένη εικόνα της κατάστασης κινδύνου ενός οργανισμού, συμπεριλαμβανομένων τόσο της επικινδυνότητας της ασφάλειας πληροφοριών όσο και της επικινδυνότητας επιχειρηματικών διαδικασιών. Θεωρούμε ότι δεν καλύπτει αυτό το κριτήριο.

Αναφορές και αναλύσεις

Η μεθοδολογία FAIR περιλαμβάνει αναφορές και αναλύσεις ως μέρος της διαδικασίας διαχείρισης κινδύνων.
Το FAIR μέσω της διαδικασίας ανάλυσης κινδύνου παρέχει καθοδήγηση σχετικά με τον τρόπο χρήσης των μετρικών και των δεικτών για τη μέτρηση του κινδύνου και την αξιολόγηση της αποτελεσματικότητας των δραστηριοτήτων διαχείρισης κινδύνου. Τα δεδομένα που συλλέγονται **μέσω της διαδικασίας ανάλυσης κινδύνου χρησιμοποιούνται για τη δημιουργία διαφόρων εκθέσεων, συμπεριλαμβανομένων των χαρτών θερμότητας κινδύνου, των προφίλ κινδύνου και των μητρώων κινδύνου.** Οι εκθέσεις αυτές χρησιμοποιούνται για την κοινοποίηση της κατάστασης κινδύνου του οργανισμού στα ανώτερα διοικητικά στελέχη, το διοικητικό συμβούλιο και άλλα ενδιαφερόμενα μέρη. Συνολικά, το πλαίσιο FAIR περιλαμβάνει τη χρήση αναφορών και αναλύσεων για τη μέτρηση, την ανάλυση και την υποβολή εκθέσεων σχετικά με τους κινδύνους, καθώς και για την παροχή ανατροφοδότησης σχετικά με την αποτελεσματικότητα των δραστηριοτήτων της διαχείρισης κινδύνων και θεωρούμε ότι καλύπτει πλήρως το κριτήριο.

Επίπεδο τεχνικότητας

Η μεθοδολογία FAIR δεν είναι ένα απλό πλαίσιο και απαιτεί βαθιά κατανόηση των εννοιών και των υπολογισμών που εμπλέκονται, προκειμένου να χρησιμοποιηθεί σωστά. Βασίζεται σε μαθηματικές έννοιες και απαιτεί γνώσεις στατιστικής, πιθανοτήτων και άλλων συναφών θεμάτων που απαιτούν **ένα υψηλό επίπεδο τεχνικών γνώσεων.**
Η μεθοδολογία FAIR δεν συνιστάται για οργανισμούς που δεν διαθέτουν την τεχνογνωσία ή τους πόρους για την εφαρμογή της γιατί εφ' όσον απαιτεί υψηλό επίπεδο τεχνικών γνώσεων και εμπειρογνωμοσύνης προκειμένου να εφαρμοστεί σωστά, η χρήση του απαιτεί σοβαρή επένδυση σε εκπαίδευση, εργαλεία και πόρους.
Συνοψίζοντας, η μεθοδολογία FAIR είναι ένα πολύπλοκο και τεχνικό πλαίσιο για τη διαχείριση κινδύνων στον κυβερνοχώρο και απαιτεί υψηλό επίπεδο τεχνικών γνώσεων για την κατανόηση και την ορθή εφαρμογή της.

Υποστήριξη και πόροι

Η μεθοδολογία FAIR περιλαμβάνει διάφορους οδηγούς χρήσης, υλικό υποστήριξης και πόρους για να βοηθήσει τους χρήστες να κατανοήσουν και να εφαρμόσουν σωστά τη μεθοδολογία.
Το Ινστιτούτο FAIR, μια μη κερδοσκοπική επαγγελματική ένωση που υποστηρίζει τη χρήση της μεθοδολογίας FAIR, παρέχει διάφορους πόρους, όπως εκπαιδευτικό υλικό, διαδικτυακά σεμινάρια, προγράμματα πιστοποίησης και μια διαδικτυακή κοινότητα για να βοηθήσει άτομα και οργανισμούς να κατανοήσουν και να εφαρμόσουν τη μεθοδολογία.
Το Ινστιτούτο FAIR παρέχει επίσης το FAIR Analysis Body of Knowledge - FABOK, το οποίο περιέχει έναν ολοκληρωμένο οδηγό για τη μεθοδολογία FAIR, συμπεριλαμβανομένων λεπτομερών περιγραφών της ταξινομίας, της διαδικασίας και των τεχνικών FAIR. Περιλαμβάνει επίσης μελέτες περιπτώσεων, παραδείγματα και πρότυπα που βοηθούν τους χρήστες να εφαρμόσουν τη μεθοδολογία στους συγκεκριμένους κινδύνους τους.
Επιπλέον, το Ινστιτούτο FAIR διατηρεί έναν δικτυακό τόπο (www.fairinstitute.org) που προσφέρει διάφορους πόρους, όπως whitepapers, διαδικτυακά σεμινάρια και μελέτες περιπτώσεων για την παροχή πιο εμπεριστατωμένων πληροφοριών σχετικά με τη μεθοδολογία και την εφαρμογή της. Το FAIR καλύπτει πλήρως το κριτήριο.

Πληρότητα

Το FAIR είναι ένα πλαίσιο για την ποσοτική ανάλυση και διαχείριση της επικινδυνότητας της ασφάλειας πληροφοριών**, αλλά δεν έχει σχεδιαστεί ώστε να καλύπτει όλους τους συναφείς τομείς κινδύνου στο πλαίσιο της διαχείρισης επικινδυνότητας για την ασφάλεια πληροφοριών.** Επικεντρώνεται συγκεκριμένα στον εντοπισμό και την ανάλυση της επικινδυνότητας πιθανών απειλών και ευπαθειών, καθώς και στον προσδιορισμό της πιθανότητας και του αντίκτυπου των πιθανών συμβάντων απώλειας.
Άλλες σημαντικές πτυχές της διαχείρισης κινδύνων, όπως η αντιμετώπιση της επικινδυνότητας, η παρακολούθηση και η συμμόρφωση, δεν καλύπτονται μόνο από το πλαίσιο FAIR.
Επιπλέον, το FAIR δεν αποτελεί μεθοδολογία για την εφαρμογή μέτρων ασφαλείας ή την καθημερινή διαχείριση της επικινδυνότητας ασφάλειας πληροφοριών, τα οποία αποτελούν επίσης σημαντικά στοιχεία μιας πλήρους προσέγγισης διαχείρισης κινδύνων.

Επιπλέον, ορισμένοι οργανισμοί ενδέχεται να έχουν μοναδικούς κινδύνους που δεν καλύπτονται από τη μεθοδολογία FAIR, σε τέτοιες περιπτώσεις, θα πρέπει να χρησιμοποιηθούν άλλες μεθοδολογίες ή πλαίσια για την αξιολόγηση των εν λόγω κινδύνων. Ως εκ τούτου, συνήθως χρησιμοποιείται σε συνδυασμό με το ISO 27001 ή το NIST SP 800-30, για να παρέχει μια ολοκληρωμένη προσέγγιση στη διαχείριση της επικινδυνότητας της ασφάλειας πληροφοριών. Συνολικά, καλύπτει εν μέρει το κριτήριο.

Χρόνος/Διάρκεια

Η μεθοδολογία FAIR είναι ένα ολοκληρωμένο πλαίσιο και, ως εκ τούτου, μπορεί να χρειαστεί αρκετός χρόνος για την πλήρη εφαρμογή της. Η ακριβής διάρκεια της εφαρμογής εξαρτάται από διάφορους παράγοντες, όπως το μέγεθος και η πολυπλοκότητα του οργανισμού, ο αριθμός των σεναρίων κινδύνου που αναλύονται και το επίπεδο τεχνογνωσίας και εμπειρίας των εμπλεκόμενων ατόμων ή συμβουλευτικών εταιρειών.
Το Ινστιτούτο FAIR, η μη κερδοσκοπική επαγγελματική ένωση στην οποία ανήκει η μεθοδολογία, συνιστά στους οργανισμούς να προγραμματίζουν **μια αρχική περίοδο εφαρμογής 6-12 μηνών και συνεχή ετήσια ή εξαμηνιαία ανάλυση, προκειμένου να διατηρείται μια ακριβής εικόνα της επικινδυνότητας.**
Η εφαρμογή της μεθοδολογίας FAIR ξεκινά συνήθως με την αξιολόγηση των υφιστάμενων πρακτικών και διαδικασιών διαχείρισης κινδύνου του οργανισμού, ακολουθούμενη από τον προσδιορισμό και την ανάλυση σεναρίων κινδύνου. **Η διαδικασία αυτή μπορεί να διαρκέσει αρκετές εβδομάδες ή μήνες, ανάλογα με τον αριθμό των σεναρίων που αναλύονται και τη διαθεσιμότητα των δεδομένων.** Μετά τον εντοπισμό και την ανάλυση των σεναρίων κινδύνου, ο οργανισμός μπορεί να αρχίσει να αναπτύσσει ένα σχέδιο διαχείρισης κινδύνου και να εφαρμόζει επιλογές αντιμετώπισης του κινδύνου. Η διαδικασία αυτή μπορεί **επίσης να διαρκέσει αρκετές εβδομάδες ή μήνες**, ανάλογα με την πολυπλοκότητα των σεναρίων κινδύνου και τους πόρους που διαθέτει ο οργανισμός.
Συνολικά θεωρούμε ότι καλύπτεται εν μέρει το συγκεκριμένο κριτήριο εφ’ όσον κυμαίνεται μεταξύ μηνών και έτους η διαδικασία εφαρμογής της.

Οικονομικό κόστος

Το Ινστιτούτο FAIR, η μη κερδοσκοπική επαγγελματική ένωση στην οποία ανήκει η μεθοδολογία, **χρεώνει ετήσια συνδρομή μέλους για πρόσβαση στη μεθοδολογία, εκπαίδευση, πιστοποίηση και συνεχή υποστήριξη.** Επιπλέον, προσφέρονται διαδικτυακά μαθήματα κατάρτισης και πιστοποίησης, τα οποία έχουν διαφορετικό κόστος ανάλογα με το επίπεδο πιστοποίησης που επιθυμείτε.
Οι οργανισμοί μπορούν επίσης να συνεργαστούν με πιστοποιημένους επαγγελματίες FAIR ή εκπαιδευμένους συμβούλους FAIR για να τους βοηθήσουν να εφαρμόσουν τη μεθοδολογία στον οργανισμό τους. **Οι εν λόγω επαγγελματίες και σύμβουλοι ενδέχεται να χρεώνουν πρόσθετες αμοιβές για τις υπηρεσίες τους**, οι οποίες μπορεί να ποικίλλουν σε μεγάλο βαθμό ανάλογα με τις συγκεκριμένες υπηρεσίες που παρέχονται και την εμπειρία και την εξειδίκευση του επαγγελματία ή του συμβούλου.
Το οικονομικό κόστος θεωρείται μέτριο και κυμαινόμενο , οπότε θεωρούμε ότι το κριτήριο καλύπτεται εν μέρει, από το FAIR.

3) ISACA the RiskIT Framework

Ιστορικό

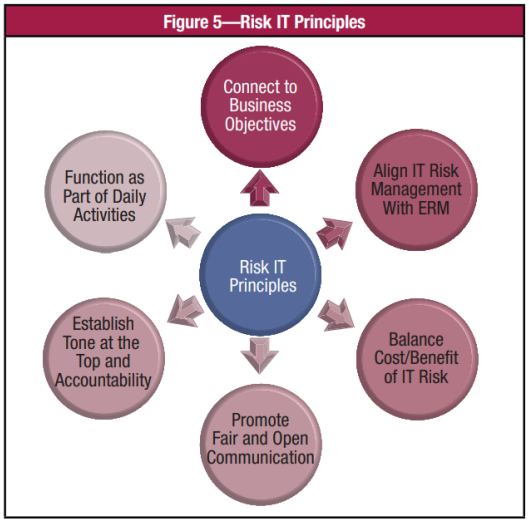
Το RiskIT Framework κυκλοφόρησε για πρώτη φορά το 2009. Αναπτύχθηκε από την ISACA (Information Systems Audit and Control Association) ως ένα ολοκληρωμένο πλαίσιο για τη διαχείριση και αξιολόγηση της επικινδυνότητας που σχετίζεται με τα συστήματα και τις διαδικασίες του τομέα της πληροφορικής (IT). Η τελευταία αναβάθμιση του πλαισίου ISACA "The RISK IT Framework 2nd edition" κυκλοφόρησε το 2020.

Το πλαίσιο παρέχει στους οργανισμούς μια δομημένη προσέγγιση για την ευθυγράμμιση της επικινδυνότητας του τομέα της πληροφορικής με τους συνολικούς επιχειρηματικούς κινδύνους τους και περιλαμβάνει κατευθυντήριες γραμμές και βέλτιστες πρακτικές για τη διακυβέρνηση, τη διαχείριση και την αξιολόγηση της επικινδυνότητας της πληροφορικής. Λειτουργεί στη διασταύρωση των Επιχειρήσεων και της Πληροφορικής και επιτρέπει στις επιχειρήσεις να διαχειρίζονται και ακόμη και να αξιοποιούν τον κίνδυνο κατά την επιδίωξη των στόχων τους.

Επεκτείνει το COBIT, το παγκοσμίως αναγνωρισμένο Πλαίσιο Διακυβέρνησης Πληροφορικής **και εξοικονομεί χρόνο, κόστος και προσπάθεια, παρέχοντας στις επιχειρήσεις έναν τρόπο να εστιάζουν αποτελεσματικά στους τομείς επιχειρηματικών κινδύνων** που σχετίζονται με την Πληροφορική, συμπεριλαμβανομένων της επικινδυνότητας που σχετίζεται με την καθυστερημένη παράδοση έργων, τη συμμόρφωση, την κακή ευθυγράμμιση, την παρωχημένη αρχιτεκτονική Πληροφορικής και τα προβλήματα παροχής υπηρεσιών Πληροφορικής.

Επισκόπηση

Το Risk IT ορίζει και βασίζεται σε μια σειρά κατευθυντήριων **αρχών** για την **αποτελεσματική διαχείριση της επικινδυνότητας στον τομέα της πληροφορικής**. Οι αρχές βασίζονται σε κοινά αποδεκτές αρχές του ERM , οι οποίες έχουν εφαρμοστεί στον τομέα της πληροφορικής , όπως φαίνεται στην παρακάτω εικόνα 3 :



Εικόνα 3: Οι βασικές αρχές του RISK IT

- Σύνδεση πάντα με τους επιχειρηματικούς στόχους.

- Ευθυγράμμιση της διαχείρισης των επιχειρηματικών κινδύνων που σχετίζονται με την πληροφορική με το συνολικό ERM.
- Εξισορρόπηση του κόστους και των οφελών της διαχείρισης της επικινδυνότητας IT
- Προώθηση της δίκαιης και ανοικτής επικοινωνίας της επικινδυνότητας IT
- Καθιέρωση του σωστού κλίματος από την κορυφή, με ταυτόχρονο καθορισμό και επιβολή της προσωπικής ευθύνης για τη λειτουργία εντός αποδεκτών και σαφώς καθορισμένων επιπέδων ανοχής.
- Λειτουργία που αποτελεί συνεχή διαδικασία και μέρος των καθημερινών Δραστηριοτήτων.

Το μοντέλο χωρίζεται επίσης σε τρεις τομείς: **Risk Governance**, **Risk Evaluation**, **Risk Response**, ο καθένας από τους οποίους περιλαμβάνει τρεις διεργασίες:

Διακυβέρνηση επικινδυνότητας

- Δημιουργία και διατήρηση κοινής άποψης κινδύνου
- Ενσωμάτωση με τη διαχείριση επιχειρηματικού κινδύνου ,
- Λήψη επιχειρηματικών αποφάσεων με επίγνωση του κινδύνου

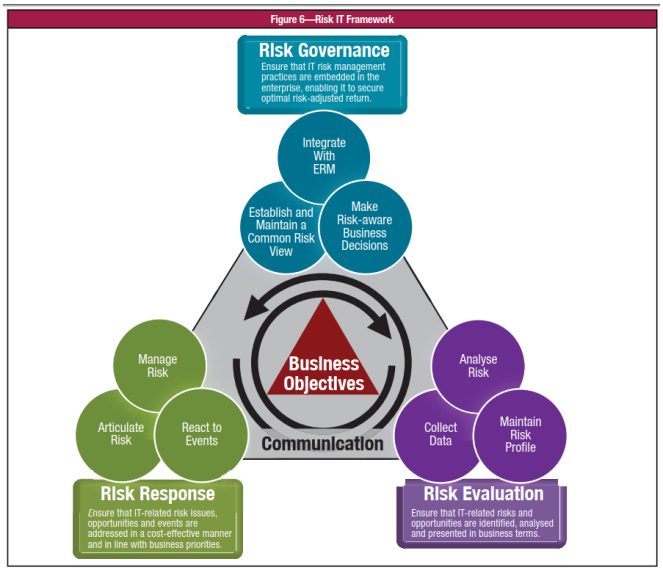
Αξιολόγηση επικινδυνότητας

- Συλλογή δεδομένων
- Ανάλυση κινδύνου
- Διατήρηση προφίλ κινδύνου

Απόκριση στην επικινδυνότητα

- Διατύπωση του κινδύνου
- Διαχείριση του κινδύνου
- Αντίδραση σε συμβάντα

Σχηματικά οι παραπάνω τρεις τομείς φαίνονται στην παρακάτω εικόνα 4.



Εικόνα 4: Οι τρείς τομείς του RiskIT Framework

Χρηστικότητα

Το RISK IT της ISACA έχει σχεδιαστεί ώστε να **είναι φιλικό προς το χρήστη και εύκολα κατανοητό για οργανισμούς κάθε μεγέθους**. Πρόκειται για ένα ολιστικό πλαίσιο που παρέχει καθοδήγηση για τη διαχείριση και τη διακυβέρνηση της επικινδυνότητας που σχετίζεται με την τεχνολογία πληροφοριών.
Παρέχει επίσης μια συνεπή προσέγγιση στη διαχείριση κινδύνων σε ολόκληρο τον οργανισμό, συμβάλλοντας στη διασφάλιση ότι όλοι οι τομείς της επιχείρησης είναι ευθυγραμμισμένοι και εργάζονται για τους ίδιους στόχους.
Η συντήρηση και η επικαιροποίηση του πλαισίου γίνεται από την ISACA, μια γνωστή και καταξιωμένη επαγγελματική ένωση στον τομέα της διακυβέρνησης, της διαχείρισης επικινδυνότητας και της συμμόρφωσης στον τομέα της πληροφορικής , που εκδίδει τακτικά ενημερώσεις του πλαισίου για να αντικατοπτρίζει τις αλλαγές στην τεχνολογία και τους κανονισμούς, και οι οργανισμοί μπορούν εύκολα να ενσωματώσουν αυτές τις ενημερώσεις στις υφιστάμενες διαδικασίες τους.
Βέβαια το πλαίσιο ,όπως προκύπτει και μέσα από την τεκμηρίωσή του, δεν είναι μια «χρυσή λύση» και **η εφαρμογή του απαιτεί εξειδικευμένους πόρους και χρόνο**. Μπορεί όμως να αποτελέσει ένα καλό σημείο εκκίνησης για τους οργανισμούς ώστε να δημιουργήσουν το δικό τους πρόγραμμα διαχείρισης κινδύνων με βάση τις βέλτιστες πρακτικές του κλάδου.
Συνολικά, το πλαίσιο ISACA RiskIT θεωρείται ότι έχει υψηλό επίπεδο χρηστικότητας για τη διαχείριση της επικινδυνότητας στον τομέα της ασφάλειας των πληροφοριών.

Ευελιξία

Το πλαίσιο ISACA RiskIT **έχει σχεδιαστεί ώστε να είναι ευέλικτο**, με την έννοια ότι μπορεί να προσαρμοστεί στις συγκεκριμένες ανάγκες ενός οργανισμού. Παρέχει μια γενική δομή και καθοδήγηση για τη διαχείριση της επικινδυνότητας, αλλά **μπορεί να προσαρμοστεί στις ιδιαίτερες συνθήκες και απαιτήσεις διαφορετικών οργανισμών**. Επιτρέπει επίσης στους οργανισμούς **να επιλέξουν το επίπεδο τυπικότητας και αυστηρότητας που είναι κατάλληλο για τις συγκεκριμένες ανάγκες και τους στόχους τους.**
Επιπλέον, το πλαίσιο παρέχει ένα σύνολο βέλτιστων πρακτικών, κατευθυντήριων γραμμών και εργαλείων που οι οργανισμοί μπορούν να χρησιμοποιήσουν για να εφαρμόσουν το πλαίσιο με τον καταλληλότερο για την περίπτωσή τους τρόπο. Το πλαίσιο δεν είναι κανονιστικό και επιτρέπει στους οργανισμούς να το χρησιμοποιούν με τον τρόπο που έχει νόημα για την επιχείρησή τους. Επίσης θεωρείται ευέλικτο υπό την έννοια ότι μπορεί να ενσωματωθεί σε υφιστάμενα πλαίσια όπως το COBIT και το ISO 27001/2 και μπορεί να εφαρμοστεί σε διάφορες βιομηχανίες και τομείς.
Συνολικά, το πλαίσιο RiskIT της ISACA έχει σχεδιαστεί για να είναι μια ευέλικτη και προσαρμόσιμη μεθοδολογία που οι οργανισμοί μπορούν να χρησιμοποιούν για την αποτελεσματική διαχείριση και αξιολόγηση της επικινδυνότητας με τρόπο που να ευθυγραμμίζεται με τις συγκεκριμένες ανάγκες και απαιτήσεις τους.

Διαχείριση περιουσιακών στοιχείων

Το πλαίσιο ISACA Risk IT **περιλαμβάνει μια συγκεκριμένη διαδικασία για τη διαχείριση περιουσιακών στοιχείων,** η οποία αποτελεί βασικό συστατικό του πλαισίου και χρησιμοποιείται για τον εντοπισμό, την ταξινόμηση και την προστασία των περιουσιακών στοιχείων του οργανισμού. Η διαδικασία περιγράφεται στο COBIT 5 με την ονομασία "Acquire and Implement" (Απόκτηση και υλοποίηση), και περιλαμβάνει βήματα όπως :

- Προσδιορισμό περιουσιακών στοιχείων: Προσδιορισμός και τεκμηρίωση όλων των περιουσιακών στοιχείων IT στον οργανισμό.
- Ταξινόμηση περιουσιακών στοιχείων: Ταξινόμηση των περιουσιακών στοιχείων με βάση την κρισιμότητά τους και την αξία τους για τον οργανισμό.
- Ιεράρχηση περιουσιακών στοιχείων: Ιεράρχηση των περιουσιακών στοιχείων με βάση την κρισιμότητα και την αξία τους για τον οργανισμό.
- Προστασία περιουσιακών στοιχείων: Εφαρμογή ελέγχων για την προστασία των περιουσιακών στοιχείων, όπως έλεγχοι πρόσβασης, κρυπτογράφηση και δημιουργία αντιγράφων ασφαλείας.
- Παρακολούθηση περιουσιακών στοιχείων: Παρακολούθηση των περιουσιακών στοιχείων για τον εντοπισμό τυχόν μη εξουσιοδοτημένης πρόσβασης ή αλλαγών και ανάληψη κατάλληλων ενεργειών σε περίπτωση εντοπισμού προβλημάτων.
- Αναθεώρηση και ενημέρωση περιουσιακών στοιχείων: Επανεξέταση του καταλόγου και ενημέρωσή του, εφόσον είναι απαραίτητο, ώστε να αντικατοπτρίζει τυχόν αλλαγές στα περιουσιακά στοιχεία του οργανισμού ή στη στάση ασφαλείας.

Επιπλέον, το πλαίσιο Risk IT της ISACA ευθυγραμμίζεται επίσης με το πρότυπο ISO/IEC 27001, το οποίο αναγνωρίζεται ευρέως ως βέλτιστη πρακτική στη διαχείριση επικινδυνότητας πληροφορικής και στα συστήματα διαχείρισης ασφάλειας πληροφοριών που περιλαμβάνει συγκεκριμένη διαδικασία και στόχους ελέγχου για τη διαχείριση περιουσιακών στοιχείων. Το κριτήριο καλύπτεται πλήρως από το RiskIT.

Βάση δεδομένων για απειλές

Το πλαίσιο RiskIT **δεν περιλαμβάνει βάση δεδομένων για τις απειλές και δεν αποτελεί εργαλείο για τον εντοπισμό συγκεκριμένων απειλών.**

Έχει σχεδιαστεί για να χρησιμοποιείται σε συνδυασμό με άλλες μεθοδολογίες και πρότυπα διαχείρισης επικινδυνότητας. Οι οργανισμοί που χρησιμοποιούν το πλαίσιο θα πρέπει να χρησιμοποιούν τις δικές τους εσωτερικές διαδικασίες και εργαλεία για τον εντοπισμό πιθανών απειλών και να χρησιμοποιούν το πλαίσιο για να καθοδηγούν τη στρατηγική διαχείρισης της επικινδυνότητας. Μπορούν να χρησιμοποιήσουν εξωτερικές πηγές πληροφοριών, όπως εκθέσεις του κλάδου και πληροφορίες για την κυβερνοασφάλεια, για να εντοπίσουν και να αξιολογήσουν τις συγκεκριμένες απειλές που αντιμετωπίζουν, και στη συνέχεια να χρησιμοποιήσουν το Risk IT Framework για να τους βοηθήσει να αναπτύξουν και να εφαρμόσουν στρατηγικές διαχείρισης που είναι αποτελεσματικές για τον μετριασμό αυτής της επικινδυνότητας και την επίτευξη των στόχων τους. Θεωρούμε ότι το κριτήριο δεν καλύπτεται καθόλου.

Βάση δεδομένων για ευπάθειες

Το πλαίσιο παρέχει καθοδήγηση σχετικά με τον τρόπο διεξαγωγής αξιολογήσεων ευπαθειών , δοκιμών διείσδυσης και άλλων μεθόδων για τον εντοπισμό ευπαθειών αλλά **δεν παράγει ούτε παρέχει βάση δεδομένων ευπαθειών**. Παρέχει καθοδήγηση σχετικά με τον τρόπο ιεράρχησης των ευπαθειών, την ανάπτυξη και την εφαρμογή στρατηγικών μετριασμού της επικινδυνότητας, καθώς και την παρακολούθηση και την υποβολή εκθέσεων σχετικά με την αποτελεσματικότητα αυτών των στρατηγικών. Υπάρχουν άλλες διαθέσιμες πηγές και εργαλεία, όπως το National Vulnerability Database (NVD), το Common Vulnerabilities and Exposures (CVE) και το Open Web Application Security Project (OWASP) που παρέχουν βάση δεδομένων ευπαθειών. Το κριτήριο θεωρούμε ότι δεν καλύπτεται.

Βάση δεδομένων για μέτρα ασφαλείας

Το RiskIT δεν περιλαμβάνει ούτε παρέχει συγκεκριμένο κατάλογο ή βάση δεδομένων μέτρων ασφαλείας ή αντιμέτρων. Ωστόσο, περιλαμβάνει καθοδήγηση σχετικά με τον τρόπο επιλογής και εφαρμογής των κατάλληλων μέτρων ασφαλείας ή αντιμέτρων για τον μετριασμό των κινδύνων που έχουν εντοπιστεί. Το πλαίσιο συνιστά στους οργανισμούς να χρησιμοποιούν μια προσέγγιση με βάση την επικινδυνότητα για τον εντοπισμό, την αξιολόγηση και την ιεράρχηση της και στη συνέχεια, να επιλέγουν τα κατάλληλα μέτρα ασφαλείας ή αντίμετρα με βάση το επίπεδο προτεραιότητάς τους και τον πιθανό αντίκτυπο μιας εκμετάλλευσης.

Το πλαίσιο συνιστά επίσης τη χρήση βιομηχανικών προτύπων, κατευθυντήριων γραμμών και βέλτιστων πρακτικών, όπως το ISO 27001 ή το πλαίσιο NIST, για τον εντοπισμό, το σχεδιασμό και την εφαρμογή μέτρων ασφαλείας.

Είναι σημαντικό να σημειωθεί ότι υπάρχουν διάφοροι τύποι μέτρων ασφαλείας ή αντίμετρων, όπως τεχνικά, διοικητικά, φυσικά και νομικά και το Risk IT παρέχει καθοδήγηση για τη χρήση όλων των τύπων μέτρων, **αλλά δεν παρέχει συγκεκριμένο κατάλογο ή βάση δεδομένων με μέτρα ασφαλείας .** Το κριτήριο θεωρούμε ότι δεν καλύπτεται .

*** τα μέτρα ασφαλείας** είναι τα προληπτικά μέτρα που τίθενται σε εφαρμογή για την πρόληψη παραβιάσεων ασφαλείας και **τα αντίμετρα** είναι τα αντιδραστικά μέτρα που λαμβάνονται μετά την εκδήλωση ενός περιστατικού ασφαλείας.

Πλοήγηση σε περιστατικά

Το πλαίσιο ISACA Risk IT **παρέχει οδηγίες για τον τρόπο διαχείρισης των περιστατικών καθ' όλη τη διάρκεια του κύκλου ζωής τους, από τον εντοπισμό έως την επίλυση.** Έχει σχεδιαστεί για να βοηθήσει τους οργανισμούς να διασφαλίσουν ότι είναι καλά προετοιμασμένοι για την αντιμετώπιση περιστατικών και να ελαχιστοποιήσουν τις επιπτώσεις των περιστατικών αυτών στις δραστηριότητές τους.

Η διαδικασία για την πλοήγηση σε συμβάντα περιλαμβάνει τα ακόλουθα βήματα:

- Προσδιορισμός του συμβάντος: Αυτό περιλαμβάνει τον εντοπισμό και την αναγνώριση του συμβάντος, καθώς και τον προσδιορισμό του αντίκτυπου και των πιθανών συνεπειών του συμβάντος.

- Αξιολόγηση του περιστατικού: Αυτό περιλαμβάνει τη συλλογή και ανάλυση πληροφοριών σχετικά με το περιστατικό για τον προσδιορισμό της κατάλληλης πορείας δράσης.
- Σχεδιασμός της αντίδρασης: Αυτό περιλαμβάνει την ανάπτυξη ενός σχεδίου για την αντιμετώπιση του συμβάντος, συμπεριλαμβανομένου του προσδιορισμού των πόρων και του προσωπικού που απαιτούνται για την αντιμετώπιση του συμβάντος.
- Εκτέλεση της αντίδρασης: Περιλαμβάνει την εφαρμογή του σχεδίου απόκρισης και τη λήψη των απαραίτητων μέτρων για την αντιμετώπιση του περιστατικού.
- Παρακολούθηση και επανεξέταση: Αυτό περιλαμβάνει την παρακολούθηση της κατάστασης για να διασφαλιστεί ότι το περιστατικό έχει αντιμετωπιστεί αποτελεσματικά και την επανεξέταση του περιστατικού για τον εντοπισμό τυχόν διδαγμάτων ή ευκαιριών βελτίωσης.

Το κριτήριο καλύπτεται πλήρως.

Έλεγχος επιχειρησιακών διαδικασιών

Το πλαίσιο Risk IT παρέχει καθοδήγηση σχετικά με τον τρόπο ευθυγράμμισης της επικινδυνότητας των συστημάτων πληροφορικής με τους επιχειρηματικούς στόχους και τις στρατηγικές**, αλλά δεν παρέχει έλεγχο των επιχειρηματικών διαδικασιών**. Ωστόσο, παρέχει καθοδήγηση σχετικά με τον τρόπο αντιμετώπισης της επικινδυνότητας για τις επιχειρηματικές διαδικασίες στο πλαίσιο της διαδικασίας διαχείρισης επικινδυνότητας. Παρέχει επίσης καθοδήγηση σχετικά με τον τρόπο με τον οποίο διασφαλίζεται η ενσωμάτωση των επιχειρηματικών διαδικασιών με τα συστήματα πληροφορικής, καθώς και με τον τρόπο παρακολούθησης και διαχείρισης της επικινδυνότητας που σχετίζεται με αυτές τις διαδικασίες.
Το πλαίσιο ISACA Risk IT δεν έχει σχεδιαστεί για τον έλεγχο της επιχειρηματικής διαδικασίας, αλλά για να διασφαλίσει ότι οι κίνδυνοι στον τομέα της πληροφορικής ευθυγραμμίζονται με την επιχειρηματική διαδικασία και ότι οι κίνδυνοι διαχειρίζονται σωστά, **άρα καλύπτει εν μέρει το εν λόγω κριτήριο.**

Αναφορές και αναλύσεις

Το πλαίσιο παρέχει μια διαδικασία διαχείρισης κινδύνων που περιλαμβάνει δραστηριότητες όπως ο εντοπισμός της επικινδυνότητας, η αξιολόγηση της επικινδυνότητας, η ιεράρχηση της επικινδυνότητας και, στη συνέχεια, **η εφαρμογή, η παρακολούθηση και η υποβολή εκθέσεων σχετικά με τους κινδύνους.**
Κατά τη διάρκεια αυτών των δραστηριοτήτων το πλαίσιο συνιστά την ανάλυση , τη χρήση μετρήσεων και δεικτών για τη μέτρηση **και την υποβολή εκθέσεων σχετικά με τους κινδύνους και παρέχει καθοδήγηση σχετικά με τον τρόπο χρήσης αυτών των μετρήσεων για την αξιολόγηση της αποτελεσματικότητας των δραστηριοτήτων διαχείρισης κινδύνων**. Αυτές οι μετρήσεις μπορούν να περιλαμβάνουν τόσο ποιοτικά όσο και ποσοτικά μέτρα και χρησιμοποιούνται για την παρακολούθηση της κατάστασης της επικινδυνότητας του οργανισμού, τον εντοπισμό τομέων προς βελτίωση και την παροχή ανατροφοδότησης σχετικά με την αποτελεσματικότητα της διαδικασίας διαχείρισης κινδύνου.

Το πλαίσιο παρείχε επίσης μεθοδολογίες σχετικά με τον τρόπο αναφοράς της επικινδυνότητας και την παροχή περίληψης των δραστηριοτήτων διαχείρισης κινδύνων στο διοικητικό συμβούλιο ή στην ανώτερη διοίκηση.
Συνολικά, το πλαίσιο Risk IT περιλαμβάνει τη χρήση αναφορών και αναλύσεων για τη μέτρηση και την υποβολή εκθέσεων σχετικά με τους κινδύνους, καθώς και για την παροχή ανατροφοδότησης σχετικά με την αποτελεσματικότητα των δραστηριοτήτων διαχείρισης κινδύνων και θεωρούμε ότι καλύπτει πλήρως το κριτήριο.

Επίπεδο τεχνικότητας

Το πλαίσιο Risk IT δεν είναι απαραίτητα τεχνικής φύσης, παρέχει καθοδήγηση σχετικά με τις βέλτιστες πρακτικές και αρχές για τη διαχείριση της επικινδυνότητας της ασφάλειας των πληροφοριών και **προορίζεται να χρησιμοποιηθεί από** ένα ευρύ φάσμα χρηστών, συμπεριλαμβανομένων εκείνων που ενδέχεται να μην έχουν υψηλό επίπεδο τεχνικών γνώσεων και **όχι μόνο από ειδικούς του τομέας της ασφάλειας πληροφοριών.**
Ωστόσο, η **εφαρμογή του πλαισίου μπορεί να απαιτεί κάποιες τεχνικές γνώσεις ανάλογα με τα συστήματα , την υποδομή και τις διαδικασίες της τεχνολογίας των πληροφοριών που χρησιμοποιεί ο οργανισμός.** Για παράδειγμα, εάν ένας οργανισμός εφαρμόζει μέτρα ασφάλειας στον τομέα της πληροφορικής , ενδέχεται να απαιτούνται γνώσεις τεχνολογιών και διαδικασιών ασφάλειας. **Όμως, το ίδιο το πλαίσιο δεν απαιτεί υψηλό επίπεδο τεχνικής εμπειρογνωμοσύνης και μπορεί να εφαρμοστεί με τη βοήθεια τόσο εσωτερικών όσο και εξωτερικών εμπειρογνωμόνων.**
Συνολικά, το πλαίσιο ISACA RiskIT δεν απαιτεί υψηλό επίπεδο τεχνικών γνώσεων για την κατανόηση και την εφαρμογή του, αλλά ενδέχεται να απαιτούνται κάποιες τεχνικές γνώσεις ανάλογα με τα συγκεκριμένα συστήματα και τις διαδικασίες που χρησιμοποιεί ο οργανισμός, οπότε θεωρούμε ότι καλύπτει μερικώς το κριτήριο.

Υποστήριξη και πόροι

Το Risk IT περιλαμβάνει οδηγό χρήσης, υποστηρικτικό υλικό και πόρους για να βοηθήσει τους χρήστες να κατανοήσουν και να χρησιμοποιήσουν σωστά το πλαίσιο. Η ISACA παρέχει ποικίλο υλικό και πόρους για την υποστήριξη των οργανισμών στην εφαρμογή του πλαισίου Risk IT, συμπεριλαμβανομένου **ενός οδηγού χρήστη, βέλτιστων πρακτικών, μελετών περιπτώσεων και προτύπων** ώστε να βοηθήσουν τους οργανισμούς να το κατανοήσουν , να το εφαρμόσουν αποτελεσματικά και να διασφαλίσουν τη συμμόρφωση με τους σχετικούς κανονισμούς και πρότυπα.
Ο οδηγός χρήστη παρέχει μια επισκόπηση του πλαισίου, συμπεριλαμβανομένης της μεθοδολογίας, της καθοδήγησης και των βέλτιστων πρακτικών, καθώς και παραδείγματα για τον τρόπο με τον οποίο το πλαίσιο μπορεί να εφαρμοστεί σε διαφορετικούς τύπους οργανισμών. Ο διαδικτυακός τόπος της ISACA παρέχει **επίσης μαθήματα κατάρτισης και πιστοποιήσεις** για όσους θέλουν να κατανοήσουν βαθύτερα το πλαίσιο και την εφαρμογή του. Επιπλέον παρέχει μια **κοινότητα όπου οι χρήστες μπορούν να ανταλλάσσουν γνώσεις και εμπειρίες**, καθώς και **πρόσβαση σε μια βάση γνώσεων** για την απόκτηση λεπτομερέστερης καθοδήγησης και βέλτιστων πρακτικών. Το κριτήριο καλύπτεται πλήρως από το RiskIT.

Πληρότητα

Το πλαίσιο παρέχει μια ολοκληρωμένη άποψη της διαχείρισης της επικινδυνότητας της ασφάλειας των πληροφοριών, καλύπτοντας θέματα όπως η διακυβέρνηση, το πλαίσιο της επικινδυνότητας, ο εντοπισμός, η αξιολόγηση και η μέτρηση της επικινδυνότητας, η αντιμετώπιση και η παρακολούθηση της επικινδυνότητας και η υποβολή εκθέσεων σχετικά με την επικινδυνότητα.
Καλύπτει ένα ευρύ φάσμα τομέων κινδύνου που σχετίζονται με την ασφάλεια των πληροφοριών, όπως :

- Προσδιορισμός της επικινδυνότητας: Το πλαίσιο παρέχει καθοδήγηση σχετικά με τον τρόπο εντοπισμού και κατηγοριοποίησης της επικινδυνότητας και τον τρόπο αξιολόγησης της πιθανότητας και των επιπτώσεών της.
- Διακυβέρνηση: Το πλαίσιο παρέχει καθοδήγηση σχετικά με τον τρόπο ευθυγράμμισης της επικινδυνότητας με τους επιχειρηματικούς στόχους και τις στρατηγικές και με τον τρόπο διασφάλισης της ενσωμάτωσης των συστημάτων ΤΠ στις επιχειρηματικές διαδικασίες.
- Αξιολόγηση επικινδυνότητας: Το πλαίσιο παρέχει καθοδήγηση σχετικά με τον τρόπο αξιολόγησης της πιθανότητας και του αντίκτυπου της επικινδυνότητας και τον τρόπο ιεράρχησής της για περαιτέρω ενέργειες.
- Αντιμετώπιση της επικινδυνότητας : Το πλαίσιο παρέχει καθοδήγηση σχετικά με τον τρόπο μετριασμού, μεταφοράς ή αποδοχής της επικινδυνότητας ΤΠ και τον τρόπο εφαρμογής των σχεδίων αντιμετώπισης της επικινδυνότητας.
- Παρακολούθηση: Το πλαίσιο παρέχει καθοδήγηση σχετικά με τον τρόπο παρακολούθησης της αποτελεσματικότητας των σχεδίων αντιμετώπισης κινδύνων και τον τρόπο υποβολής εκθέσεων σχετικά με τις δραστηριότητες διαχείρισης κινδύνων.

Το πλαίσιο καλύπτει επίσης τους κινδύνους που σχετίζονται με τη συμμόρφωση και τις κανονιστικές απαιτήσεις και καλύπτει τον τρόπο διαχείρισης της επικινδυνότητας που σχετίζεται με την εξωτερική ανάθεση, το cloud computing και άλλες αναδυόμενες τεχνολογίες, οπότε θεωρούμε ότι το κριτήριο καλύπτεται πλήρως από το Risk IT.

Χρόνος/Διάρκεια

Σε γενικές γραμμές, η εφαρμογή του πλαισίου ISACA Risk IT μπορεί να χωριστεί σε διάφορες φάσεις , όπως η φάση προετοιμασίας , η φάση υλοποίησης και η φάση παρακολούθησης και συντήρησης, οι οποίες μπορεί να διαρκέσουν από μερικές εβδομάδες έως αρκετούς μήνες ανάλογα με την πολυπλοκότητα των συστημάτων , τον αριθμό των κινδύνων που θα εντοπιστούν και τις απαραίτητες προσαρμογές που θα πρέπει να γίνουν. Η εκτιμώμενη συνολική διάρκεια της υλοποίησης/εφαρμογής του πλαισίου μπορεί να κυμαίνεται **από λίγες εβδομάδες έως μερικούς μήνες**, ανάλογα με το εύρος, την πολυπλοκότητα και το μέγεθος του οργανισμού και των συστημάτων πληροφορικής του. Είναι σημαντικό να σημειώσουμε ότι η διαχείριση της επικινδυνότητας είναι μια συνεχής διαδικασία και η εφαρμογή του πλαισίου Risk IT θα πρέπει να θεωρείται ως ένα συνεχές ταξίδι, με τακτικές αναθεωρήσεις και ενημερώσεις. Το κριτήριο καλύπτεται πλήρως.

Οικονομικό κόστος

Το πλαίσιο Risk IT δεν είναι δωρεάν και παρέχεται από την ISACA η οποία είναι μια επαγγελματική ένωση που παρέχει πόρους και καθοδήγηση σχετικά με τις βέλτιστες πρακτικές για τη διακυβέρνηση, τη διαχείριση κινδύνων και τη συμμόρφωση στον τομέα της πληροφορικής. Το πλαίσιο είναι διαθέσιμο στα μέλη της ISACA ως μέρος του πακέτου συνδρομής τους. Τα μη μέλη μπορούν επίσης να έχουν πρόσβαση στο πλαίσιο, αλλά αυτό εμπεριέχει κάποιο κόστος το οποίο για τα μη μέλη μπορεί να ποικίλλει ανάλογα με τη μορφή με την οποία είναι προσβάσιμο το πλαίσιο (π.χ. σε απευθείας σύνδεση, σε έντυπη μορφή) και τη χώρα. Επιπλέον, η ISACA παρέχει επίσης προγράμματα κατάρτισης και πιστοποίησης σχετικά με το πλαίσιο Risk IT, τα οποία επίσης έχουν κάποιο κόστος. Ωστόσο, η ISACA παρέχει ορισμένους δωρεάν πόρους για τη διαχείριση κινδύνων, όπως διαδικτυακά σεμινάρια, ερευνητικά έγγραφα, άρθρα και το ISACA Journal, τα οποία είναι διαθέσιμα από τον δικτυακό τόπο της ISACA. Αυτοί οι πόροι μπορούν να παρέχουν μια επισκόπηση του πλαισίου Risk IT και μπορούν να βοηθήσουν στην κατανόηση της μεθοδολογίας και των βέλτιστων πρακτικών για τη διαχείριση κινδύνων της επικινδυνότητας της ασφάλειας των πληροφοριών. Θεωρούμε ότι το κριτήριο καλύπτεται εν μέρει.

4) ISO/IEC 27005 framework

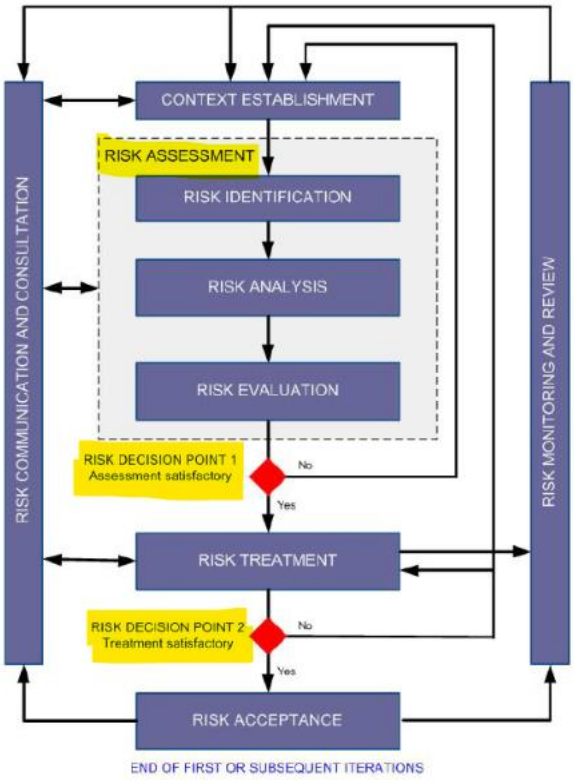
Ιστορικό

Το ISO/IEC 27005, μέρος μιας αυξανόμενης οικογένειας προτύπων ISO/IEC IRM, της "σειράς ISO/IEC 27000", είναι ένα πρότυπο ασφάλειας πληροφοριών που δημοσιεύθηκε από τον Διεθνή Οργανισμό Τυποποίησης (ISO) και το Διεθνή Ηλεκτροτεχνική Επιτροπή (IEC). Ο πλήρης τίτλος του είναι ISO/IEC 27005:2008 Information technology — Security techniques — Information security risk management - Τεχνολογίες πληροφοριών - Τεχνικές ασφάλειας - Διαχείριση επικινδυνότητας ασφάλειας πληροφοριών.
Η τρέχουσα έκδοση του είναι το ISO/IEC 27005:2022, το οποίο δημοσιεύθηκε ως έγγραφο καθοδήγησης για να βοηθήσει τους οργανισμούς να εκπληρώσουν τις απαιτήσεις του ISO/IEC 27001 σχετικά με τις ενέργειες για την αντιμετώπιση της επικινδυνότητας της ασφάλειας των πληροφοριών. Η προηγούμενη έκδοση του προτύπου ήταν το ISO/IEC 27005:2018, το οποίο παρείχε κατευθυντήριες γραμμές για τη διαχείριση επικινδυνότητας της ασφάλειας πληροφοριών.
Σκοπός του ISO/IEC 27005 είναι να παρέχει κατευθυντήριες γραμμές για τη διαχείριση επικινδυνότητας της ασφάλειας πληροφοριών, υποστηρίζει τις γενικές έννοιες που καθορίζονται στο ISO/IEC 27001 και δεν προσδιορίζει, δεν συνιστά ούτε καν ονοματίσει κάποια συγκεκριμένη μέθοδο ανάλυσης επικινδυνότητας, αν και καθορίζει μια δομημένη, συστηματική και αυστηρή διαδικασία από την ανάλυση της επικινδυνότητας έως τη δημιουργία του σχεδίου αντιμετώπισης της.

Επισκόπηση

Το ISO 27005 παρέχει κατευθυντήριες γραμμές και γενικές αρχές για την έναρξη, την εφαρμογή, τη διατήρηση και τη βελτίωση ενός συστήματος ISMS σε έναν οργανισμό. Ένα ISMS συνεπάγεται την καθιέρωση διαδικασιών και πολιτικών για την ασφάλεια στον κυβερνοχώρο, ενώ ταυτόχρονα βελτιώνει συνεχώς τη διαχείριση της επικινδυνότητας και λαμβάνει υπόψη τους ανθρώπινους και τεχνικούς παράγοντες κατά τη διαδικασία αυτή.
Η διαδικασία διαχείρισης της επικινδυνότητας περιλαμβάνει τις κάτωθι διεργασίες :

1. Καθορισμός περιεχομένου
2. Αποτίμηση επικινδυνότητας
    a. Προσδιορισμός επικινδυνότητας
    b. Ανάλυση επικινδυνότητας
    c. Αξιολόγηση επικινδυνότητας
3. Αντιμετώπιση επικινδυνότητας
    a. Τροποποίηση/Μείωση επικινδυνότητας
    b. Διατήρηση επικινδυνότητας
    c. Αποφυγή επικινδυνότητας
    d. Διαμοιρασμός επικινδυνότητας
4. Αποδοχή επικινδυνότητας
5. Επικοινωνία και διαβούλευση
6. Παρακολούθηση και αναθεώρηση



Εικόνα 5:Απεικόνιση της διαδικασίας διαχείρισης επικινδυνότητας της ασφάλειας των πληροφοριών

Πρώτα καθορίζεται το περιεχόμενο. Στη συνέχεια, διενεργείται αποτίμηση της επικινδυνότητας. Εάν αυτό παρέχει επαρκείς πληροφορίες για τον αποτελεσματικό προσδιορισμό των ενεργειών που απαιτούνται για την τροποποίηση της επικινδυνότητας σε αποδεκτό επίπεδο, τότε το έργο έχει ολοκληρωθεί και ακολουθεί η αντιμετώπιση της επικινδυνότητας. Εάν οι πληροφορίες είναι ανεπαρκείς, ακολουθεί μια άλλη επανάληψη της αξιολόγησης της επικινδυνότητας με αναθεωρημένο πλαίσιο (π.χ. κριτήρια αξιολόγησης της επικινδυνότητας, κριτήρια αποδοχής της επικινδυνότητας κριτήρια ή κριτήρια επιπτώσεων), ενδεχομένως σε περιορισμένα τμήματα του συνολικού πεδίου εφαρμογής (Risk Decision Point1).

Είναι πιθανό η αντιμετώπιση της επικινδυνότητας να μην οδηγήσει αμέσως σε αποδεκτό επίπεδο υπολειπόμενου κινδύνου. Στην περίπτωση αυτή, μια άλλη επανάληψη της αποτίμησης της επικινδυνότητας με αλλαγμένες παραμέτρους πλαισίου (π.χ. αξιολόγηση της επικινδυνότητας, κριτήρια αποδοχής επικινδυνότητας ή επιπτώσεων), εάν είναι απαραίτητο, μπορεί να απαιτηθεί, ακολουθούμενη από περαιτέρω εκτίμηση της επικινδυνότητας (Risk Decision Point 2).

Η δραστηριότητα αποδοχής επικινδυνότητας πρέπει να διασφαλίζει ότι οι υπολειπόμενοι κίνδυνοι γίνονται ρητά αποδεκτοί από τους διαχειριστές του οργανισμού. Αυτό είναι ιδιαίτερα σημαντικό σε μια κατάσταση όπου η εφαρμογή των μέτρων παραλείπεται ή αναβάλλεται, π.χ. λόγω κόστους.

Κατά τη διάρκεια ολόκληρης της διαδικασίας διαχείρισης επικινδυνότητας της ασφάλειας των πληροφοριών, είναι σημαντικό οι κίνδυνοι και οι αντιμετώπιση τους να κοινοποιούνται στους αρμόδιους διευθυντές και το επιχειρησιακό προσωπικό. Ακόμη και πριν από την αντιμετώπιση της επικινδυνότητας, οι πληροφορίες σχετικά με τους εντοπισμένους κινδύνους μπορεί να είναι πολύ πολύτιμες για τη διαχείριση περιστατικών και μπορεί να

συμβάλει στη μείωση των πιθανών ζημιών. Τα λεπτομερή αποτελέσματα κάθε δραστηριότητας της διαδικασίας διαχείρισης επικινδυνότητας της ασφάλειας των πληροφοριών και από τα δύο σημεία λήψης αποφάσεων σχετικά με τους κινδύνους θα πρέπει και να τεκμηριώνονται.

Χρηστικότητα

Ένα από τα βασικά πλεονεκτήματα του ISO 27005 είναι η χρηστικότητά του. Το πρότυπο έχει σχεδιαστεί ώστε να **είναι ευέλικτο και προσαρμόσιμο** και μπορεί να προσαρμοστεί ώστε να ανταποκρίνεται στις συγκεκριμένες ανάγκες και συνθήκες των επιμέρους οργανισμών. Είναι επίσης **γραμμένο σε σαφή και συνοπτική γλώσσα, καθιστώντας το εύκολο στην κατανόηση και την εφαρμογή.**

Το πρότυπο είναι οργανωμένο σε μια σειρά κατευθυντήριων γραμμών και συστάσεων και **όχι σε ένα σύνολο αυστηρών απαιτήσεων**, γεγονός που επιτρέπει στους οργανισμούς να επιλέξουν την καταλληλότερη προσέγγιση διαχείρισης επικινδυνότητας για τις συγκεκριμένες ανάγκες τους. Αυτό το καθιστά χρήσιμο πόρο για οργανισμούς όλων των μεγεθών και όλων των κλάδων.

Συνολικά, το ISO 27005 είναι ένα φιλικό προς το χρήστη πρότυπο που παρέχει μια πρακτική και αποτελεσματική και ολοκληρωμένη προσέγγιση για τη διαχείριση της επικινδυνότητας της ασφάλειας πληροφοριών κάτι που το καθιστά πλήρως χρηστικό.

Ευελιξία

Το ISO 27005 είναι ένα ευέλικτο πλαίσιο για τη διαχείριση της επικινδυνότητας της ασφάλειας πληροφοριών γιατί **μπορεί να προσαρμοστεί και να εφαρμοστεί σε οργανισμούς διαφορετικών μεγεθών και πολυπλοκότητας, καθώς και σε διαφορετικούς τομείς και κλάδους**. Παρέχει ένα γενικό πλαίσιο για τη διαχείριση της επικινδυνότητας και δεν προβλέπει συγκεκριμένα μέτρα ή τεχνολογίες που πρέπει να εφαρμοστούν. Αντ' αυτού, **παρέχει κατευθυντήριες γραμμές για τη διενέργεια αξιολόγησης επικινδυνότητας και την ανάπτυξη ενός σχεδίου αντιμετώπισης της, που μπορεί να προσαρμοστεί σε συγκεκριμένες ανάγκες οποιουδήποτε οργανισμού.**

Το πλαίσιο είναι επίσης ευέλικτο υπό την έννοια ότι **μπορεί να ενσωματωθεί με άλλα συστήματα διαχείρισης,** όπως το ISO 27001, το οποίο είναι το πρότυπο που παρέχει τις απαιτήσεις για ένα ISMS και το ISO 27002 που παρέχει τον κώδικα πρακτικής για τη διαχείριση της ασφάλειας πληροφοριών.

Η ευελιξία του πλαισίου ISO 27005 επιτρέπει επίσης στους οργανισμούς να εξελίσσουν τις διαδικασίες τους με την πάροδο του χρόνου, καθώς το περιβάλλον και τα περιουσιακά στοιχεία πληροφοριών του οργανισμού αλλάζουν. Αυτό είναι σημαντικό, διότι οι απειλές και τα τρωτά σημεία μεταβάλλονται συνεχώς και οι οργανισμοί πρέπει να είναι σε θέση να προσαρμόζουν τις διαδικασίες διαχείρισης επικινδυνότητας για την αντιμετώπιση νέων κινδύνων.

Διαχείριση περιουσιακών στοιχείων

Το ISO 27005 **περιλαμβάνει μια διαδικασία για τη διαχείριση των περιουσιακών στοιχείων** κατά τη διεργασία Αποτίμησης Επικινδυνότητας. Συγκεκριμένα στη δραστηριότητα του προσδιορισμού της επικινδυνότητας περιέχεται σχετική διαδικασία

προσδιορισμού **των περιουσιακών στοιχείων**. Η διαδικασία αυτή περιλαμβάνει τον εντοπισμό των περιουσιακών στοιχείων καθώς και τον «ιδιοκτήτη» του κάθε περιουσιακού στοιχείου , αυτόν δηλαδή που φέρει την ευθύνη και τη λογοδοσία γι' αυτό, την ταξινόμηση και την ιεράρχηση των περιουσιακών στοιχείων με βάση την αξία τους για τον οργανισμό και, στη συνέχεια, την αξιολόγηση της επικινδυνότητας που σχετίζονται με αυτά τα περιουσιακά στοιχεία. Η διαδικασία διαχείρισης περιουσιακών στοιχείων βοηθά τους οργανισμούς να κατανοήσουν την αξία των πληροφοριακών τους περιουσιακών στοιχείων και τον πιθανό αντίκτυπο ενός περιστατικού ασφάλειας στα εν λόγω περιουσιακά στοιχεία. Βοηθά επίσης τους οργανισμούς να εφαρμόσουν τα κατάλληλα μέτρα ασφαλείας για την προστασία αυτών των περιουσιακών στοιχείων και να θέσουν προτεραιότητες στην κατανομή των πόρων για την προστασία των κρίσιμων περιουσιακών στοιχείων. Το κριτήριο καλύπτεται πλήρως από το ISO 27005.

Βάση δεδομένων για απειλές

Το ISO 27005 ορίζει μια διαδικασία αξιολόγησης επικινδυνότητας που περιλαμβάνει τον εντοπισμό πιθανών απειλών για τα περιουσιακά στοιχεία πληροφοριών, καθώς και την πιθανότητα και τις πιθανές επιπτώσεις αυτών των απειλών **ως μέρος της διαδικασίας αξιολόγησης της επικινδυνότητας**.
Το πρότυπο παρέχει επίσης καθοδήγηση σχετικά με τον τρόπο διεξαγωγής μιας ανάλυσης απειλών, η οποία περιλαμβάνει τον εντοπισμό, την ανάλυση και την τεκμηρίωση των συγκεκριμένων απειλών που αντιμετωπίζει ένας οργανισμός. Το αποτέλεσμα αυτής της διαδικασίας είναι ένας πίνακας ή μια καταγραφή των απειλών που μπορεί να χρησιμοποιηθεί για την ενημέρωση της διαδικασίας αξιολόγησης της επικινδυνότητας και την επιλογή των κατάλληλων μέτρων.
Το παράρτημα C του προτύπου ISO/IEC 27005 παρέχει έναν κατάλογο παραδειγμάτων τυπικών απειλών που μπορεί να αντιμετωπίσουν οι οργανισμοί κατά τη διαχείριση της επικινδυνότητας της ασφάλειας πληροφοριών. Τα παραδείγματα αυτά προορίζονται να είναι ενδεικτικά και όχι εξαντλητικά και ομαδοποιούνται σε κατηγορίες απειλών όπως φυσικές, περιβαλλοντικές, τεχνικές, λειτουργικές κλπ.
Θεωρούμε ότι το κριτήριο καλύπτεται πλήρως.

Βάση δεδομένων για ευπάθειες

Το ISO 27005 ορίζει μια διαδικασία εκτίμησης επικινδυνότητας που **περιλαμβάνει τον εντοπισμό των πιθανών ευπαθειών των περιουσιακών στοιχείων πληροφοριών, καθώς και την πιθανότητα και τις πιθανές επιπτώσεις αυτών των ευπαθειών.** Το πρότυπο παρέχει καθοδήγηση σχετικά με τον τρόπο διεξαγωγής μιας ανάλυσης των ευπαθειών, η οποία περιλαμβάνει τον εντοπισμό, την ανάλυση και την τεκμηρίωση των συγκεκριμένων ευπαθειών που αντιμετωπίζει ένας οργανισμός. Το αποτέλεσμα αυτής της διαδικασίας είναι ένας κατάλογος ευπαθειών σε σχέση με τα περιουσιακά στοιχεία, τις απειλές και τους μέτρα που λαμβάνονται, καθώς και ένας κατάλογος ευπαθειών που δεν σχετίζονται με καμία αναγνωρισμένη απειλή και είναι προς επανεξέταση. Το ISO 27005 παρέχει στο παράρτημα D μία λίστα με παραδείγματα ευπαθειών και μεθόδων αξιολόγησης των ευπαθειών. Το ISO 27005 καλύπτει πλήρως το κριτήριο αυτό.

Βάση δεδομένων για μέτρα ασφαλείας

Το ISO 27005 ως μέρος της διαδικασίας αξιολόγησης της επικινδυνότητας περιλαμβάνει τον εντοπισμό/προσδιορισμό των μέτρων που υπάρχουν ή πρόκειται να υλοποιηθούν, για την προστασία των περιουσιακών στοιχείων, την προστασία από απειλές και τη διασφάλιση της επιχειρησιακής συνέχειας, καθώς και την αξιολόγηση της αποτελεσματικότητάς τους. Το αποτέλεσμα αυτής της διαδικασίας είναι ένας κατάλογος των υφιστάμενων μέτρων που μπορεί να χρησιμοποιηθεί για την ενημέρωση της διαδικασίας εκτίμησης της επικινδυνότητας και την επιλογή των πρόσθετων μέτρων που πρέπει να εφαρμοστούν.
Το ISO 27005 περιλαμβάνει ορισμένες συστάσεις για τα μέτρα και τα αντίμετρα διαχείρισης επικινδυνότητας, αλλά δεν παρέχει έναν ολοκληρωμένο κατάλογο. Ωστόσο, το πρότυπο παραπέμπει στο ISO 27002 ως πηγή μέτρων για την ασφάλεια των πληροφοριών. Το ISO 27005 δεν καλύπτει το συγκεκριμένο κριτήριο.

Πλοήγηση σε περιστατικά

Το ISO 27005 **δεν περιλαμβάνει συγκεκριμένη διαδικασία πλοήγησης σε περιστατικά όπως αυτό έχει οριστεί στην παρούσα μελέτη**. Παρέχει ένα πλαίσιο για τη διαχείριση της επικινδυνότητας που περιλαμβάνει καθοδήγηση σχετικά με τη διαχείριση περιστατικών ασφαλείας, αλλά δεν περιλαμβάνει λεπτομερή διαδικασία για την αντιμετώπιση περιστατικών και τη διαχείριση περιστατικών .
Κατά τη δραστηριότητα «Προσδιορισμού των συνεπειών» που ανήκει στη διεργασία «Προσδιορισμός της επικινδυνότητας» η οποία ανήκει στο στάδιο «Αποτίμησης της επικινδυνότητας» προσδιορίζονται η ζημιά και οι συνέπειες που μπορεί να προκληθούν από ένα σενάριο περιστατικού. Εκεί, προσδιορίζεται ότι «ένα σενάριο περιστατικού» είναι η περιγραφή μιας απειλής που εκμεταλλεύεται μια συγκεκριμένη ευπάθεια
ή σύνολο ευπαθειών σε ένα περιστατικό ασφάλειας πληροφοριών». Η έξοδος αυτής της δραστηριότητας είναι μία λίστα σεναρίων περιστατικών με τις συνέπειές τους που σχετίζονται με περιουσιακά στοιχεία και επιχειρησιακές διαδικασίες.
Το ISO 27005 τονίζει ότι η πλοήγηση σε περιστατικά πρέπει να συνάδει με τη διαδικασία διαχείρισης της επικινδυνότητας του οργανισμού και να ενσωματώνεται στο συνολικό σύστημα διαχείρισης ασφάλειας του οργανισμού κάτι που μας παραπέμπει στο ISO/IEC 27035. Θεωρούμε ότι το κριτήριο καλύπτεται μερικώς , υπάρχει εντοπισμός των περιστατικών και παράγεται μία λίστα.

Έλεγχος επιχειρηματικών διαδικασιών

Το ISO 27005 δεν προδιαγράφει συγκεκριμένα μέτρα ελέγχου των επιχειρηματικών διαδικασιών και δεν αποτελεί από μόνο του έλεγχο επιχειρηματικής διαδικασίας . Το πλαίσιο μπορεί να εφαρμοστεί σε όλους τους τύπους διαδικασιών, συμπεριλαμβανομένων των επιχειρηματικών διαδικασιών, ώστε να διασφαλιστεί ότι σχεδιάζονται και υλοποιούνται με τρόπο που ελαχιστοποιεί τον κίνδυνο βλάβης των περιουσιακών στοιχείων πληροφοριών του οργανισμού. Ωστόσο, δεν παρέχει συγκεκριμένο έλεγχο της ίδιας της επιχειρηματικής διαδικασίας αλλά μπορεί να χρησιμοποιηθεί για τη συμπληρωματική ή επιπρόσθετη εφαρμογή των υφιστάμενων επιχειρηματικών διαδικασιών και ελέγχων ενός οργανισμού. Θεωρούμε ότι το κριτήριο καλύπτεται μερικώς.

Αναφορές και αναλύσεις

Το ISO 27005 συμπεριλαμβάνει την υποβολή εκθέσεων/αναφορών και την ανάλυση ως βασικό στοιχείο της διαδικασίας διαχείρισης επικινδυνότητας. Ορίζει ότι ένας οργανισμός που καθιερώνει, εφαρμόζει, διατηρεί και βελτιώνει συνεχώς ένα σύστημα διαχείρισης της επικινδυνότητας **θα πρέπει να περιλαμβάνει ως μέρος της συνολικής διαδικασίας, την τακτική αναφορά και ανάλυση της επικινδυνότητας και της αποτελεσματικότητας των μέτρων που έχουν τεθεί σε εφαρμογή για τον μετριασμό τους**. Η διαδικασία αυτή περιλαμβάνει επιπλέον **την κοινοποίηση των πληροφοριών αυτών στη διοίκηση, στους υπεύθυνος λήψης αποφάσεων και γενικά στους αρμόδιους ενδιαφερόμενους φορείς.** Οι πληροφορίες αυτές μπορούν να χρησιμοποιηθούν για την ενημέρωση της λήψης αποφάσεων, τον εντοπισμό τομέων προς βελτίωση και τη διασφάλιση της αποτελεσματικότητας των διαδικασιών διαχείρισης κινδύνων του οργανισμού. Βάσει των παραπάνω το κριτήριο καλύπτεται πλήρως από το ISO 27005.

Επίπεδο τεχνικότητας

Το πλαίσιο ISO 27005 έχει σχεδιαστεί ώστε να είναι προσβάσιμο σε ένα ευρύ φάσμα χρηστών και να χρησιμοποιείται από οργανισμούς όλων των μεγεθών και τύπων και σε όλους τους τομείς και δεν απαιτεί υψηλό επίπεδο τεχνικών γνώσεων.
Για την εφαρμογή του πλαισίου όμως, οι οργανισμοί θα πρέπει να έχουν γνώση των δικών τους επιχειρηματικών διαδικασιών και των περιουσιακών στοιχείων πληροφοριών, καθώς και κατανόηση των τύπων κινδύνων που μπορούν να τα επηρεάσουν.
Το πρότυπο αυτό αποσκοπεί επίσης στο να βοηθήσει την εταιρεία να δημιουργήσει ένα ISMS . Ένα ISMS συνεπάγεται την καθιέρωση διαδικασιών και πολιτικών για την ασφάλεια στον κυβερνοχώρο, ενώ ταυτόχρονα βελτιώνει συνεχώς τη διαχείριση της επικινδυνότητας και λαμβάνει υπόψη τους ανθρώπινους και τεχνικούς παράγοντες κατά τη διαδικασία αυτή. Αν και το πλαίσιο, όπως αναφέραμε, δεν απαιτεί υψηλό επίπεδο τεχνικών γνώσεων, ενδέχεται να απαιτεί τη συμβολή τεχνικών εμπειρογνωμόνων σε ορισμένους τομείς, όπως η αξιολόγηση απειλών, η ανάλυση ευπαθειών και η αντιμετώπιση της επικινδυνότητας. Επιπλέον, η εφαρμογή του πλαισίου ενδέχεται να απαιτεί τεχνική εμπειρογνωμοσύνη σε τομείς όπως τα μέτρα ασφαλείας και η διαχείριση της ασφάλειας. Απαιτείται γενικά η εκπαίδευση των εργαζομένων, προκειμένου να τους βοηθήσει να αναπτύξουν τις δεξιότητες για την εκτέλεση αποτελεσματικών διαδικασιών διαχείρισης της επικινδυνότητας για την ασφάλεια των πληροφοριών. Τα άτομα που εκπαιδεύονται στο ISO 27005 είναι θεωρητικά σε θέση να εντοπίζουν, να αναλύουν, να μετρούν και να αντιμετωπίζουν την επικινδυνότητα. Συνολικά απαιτείται μέτρια τεχνικότητα.

Υποστήριξη και πόροι

Υπάρχει σχετική επάρκεια όσον αφορά το υποστηρικτικό υλικό και τους πόρους σχετικά με το ISO 27005 . Το ίδιο το πρότυπο **παρέχει μια λεπτομερή περιγραφή της διαδικασίας διαχείρισης επικινδυνότητας της ασφάλειας των πληροφοριών,** συμπεριλαμβανομένων κατευθυντήριων γραμμών για την έναρξη, την εφαρμογή, τη διατήρηση και τη βελτίωση ενός συστήματος διαχείρισης της ασφάλειας των πληροφοριών. **Παρέχει επίσης λεπτομερή περιγραφή των βημάτων που αφορούν τον εντοπισμό και την αξιολόγηση της**

επικινδυνότητας, την ανάπτυξη και την εφαρμογή μέτρων, καθώς και την παρακολούθηση και την επανεξέταση της αποτελεσματικότητας του ISMS.
Επιπλέον, **πολλοί οργανισμοί και εταιρείες συμβούλων έχουν αναπτύξει οδηγίες και εργαλειοθήκες για να βοηθήσουν τους οργανισμούς να εφαρμόσουν το πλαίσιο ISO 27005.** Αυτοί οι πόροι μπορούν να παρέχουν βήμα προς βήμα καθοδήγηση σχετικά με τον τρόπο εφαρμογής του πλαισίου, καθώς και πρότυπα και άλλα εργαλεία που βοηθούν τους οργανισμούς να διαχειριστούν τη διαδικασία.
Οι οργανισμοί μπορούν να λάβουν επίσης εκπαίδευση και πιστοποίηση στο πλαίσιο του ISO 27005. Τα προγράμματα αυτά μπορούν να παρέχουν εις βάθος γνώση και κατανόηση του προτύπου, καθώς και πρακτική εμπειρία στην εφαρμογή του πλαισίου. Θεωρούμε ότι το ISO 27005 καλύπτει πλήρως το κριτήριο.

Πληρότητα

Το πρότυπο ISO 27005 είναι ένα ολοκληρωμένο πρότυπο για τη διαχείριση της επικινδυνότητας της ασφάλειας των πληροφοριών, το οποίο περιλαμβάνει βήματα για τον εντοπισμό, την αξιολόγηση και τον μετριασμό της επικινδυνότητας, καθώς και μια διαδικασία για συνεχή παρακολούθηση και επανεξέταση. Παρέχει επίσης κατευθυντήριες γραμμές για την προσαρμογή της προσέγγισης διαχείρισης της επικινδυνότητας στις συγκεκριμένες ανάγκες και στόχους του οργανισμού. Επιπλέον, καλύπτει ένα ευρύ φάσμα τομέων κινδύνου και παρέχει ένα ευέλικτο πλαίσιο που μπορεί να προσαρμοστεί σε διαφορετικά μεγέθη, τύπους και τομείς οργανισμών. Σύμφωνα με τα προαναφερόμενα μπορεί να ειπωθεί ότι το ISO 27005 είναι ένα ολοκληρωμένο πρότυπο για τη διαχείριση της επικινδυνότητας της ασφάλειας πληροφοριών και **μπορεί να θεωρηθεί πλήρες για τον συγκεκριμένο τομέα.**
Σημειώνεται εδώ ότι το ISO 27005 είναι ένα πλαίσιο και όχι μια μεθοδολογία, που χρησιμεύει ως οδηγός για τη διαχείριση της επικινδυνότητας .

Χρόνος/Διάρκεια

Η χρονική πτυχή της εφαρμογής του ISO 27005 ποικίλλει ανάλογα με το μέγεθος και την πολυπλοκότητα του οργανισμού, καθώς και με την τρέχουσα κατάσταση των πρακτικών ασφάλειας πληροφοριών που ήδη εφαρμόζει. Για τον εντοπισμό των σχετικών τομέων επικινδυνότητας θα χρειαστεί μια **αποτίμηση/αξιολόγηση, η οποία μπορεί να διαρκέσει από μερικές εβδομάδες έως μερικούς μήνες**. Στη συνέχεια**, η εφαρμογή των μέτρων και η διαδικασία παρακολούθησης χρειάζονται επίσης χρόνο** γιατί η εφαρμογή του ISO 27005 είναι **μια συνεχής διαδικασία και όχι ένα εφάπαξ γεγονός**. Οι οργανισμοί προβλέπεται να διεξάγουν τακτικές αξιολογήσεις και να επικαιροποιούν τις διαδικασίες διαχείρισης επικινδυνότητας, εφόσον απαιτείται. Το πλαίσιο συνιστά επίσης την επανεξέταση και επικαιροποίηση της διαδικασίας διαχείρισης επικινδυνότητας τουλάχιστον ετησίως.
Πρόκειται για μια διαδικασία που απαιτεί χρόνο και προσπάθεια, αλλά μπορεί να παρέχει μια σταθερή βάση για την αποτελεσματική διαχείριση της επικινδυνότητας της ασφάλειας πληροφοριών με την πάροδο του χρόνου.
Συνολικά θα λέγαμε ότι το κριτήριο του χρόνου καλύπτεται εν μέρει.

Οικονομικό κόστος

Είναι σύνηθες τα πρότυπα ISO να πωλούνται από τον Διεθνή Οργανισμό Τυποποίησης (ISO) ή από τους εξουσιοδοτημένους διανομείς του, οπότε υπάρχει κάποιο κόστος για την απόκτηση του προτύπου.

Το κόστος που σχετίζεται με την εφαρμογή και τη χρήση του πλαισίου ISO 27005 ποικίλλει ανάλογα με τον εκάστοτε οργανισμό και τα τρέχοντα μέτρα ασφαλείας του και περιλαμβάνει :

- Κόστος κατάρτισης των εργαζομένων και της διοίκησης σχετικά με το πλαίσιο ISO 27005 και τις απαιτήσεις του.
- Αμοιβές συμβούλων για έναν διαπιστευμένο φορέα πιστοποίησης ISO 27005 για τη διενέργεια αξιολόγησης και την παροχή καθοδήγησης σχετικά με τη συμμόρφωση
- Κόστος που σχετίζεται με την αντιμετώπιση τυχόν κενών στα τρέχοντα μέτρα ασφαλείας για την ικανοποίηση των απαιτήσεων του πλαισίου ISO 27005.
- Συνεχές κόστος για τη διατήρηση της συμμόρφωσης με το πλαίσιο, όπως οι τακτικές αξιολογήσεις και η επικαιροποίηση των ελέγχων ασφαλείας

Το κόστος συμμόρφωσης με το πλαίσιο ISO 27005 μπορεί να μειωθεί εάν ο οργανισμός διαθέτει ήδη ένα καθιερωμένο ISMS ή εάν ο οργανισμός έχει μια ώριμη στάση ασφαλείας. Σε αυτές τις περιπτώσεις, ο οργανισμός μπορεί να χρειαστεί να κάνει μόνο ελάχιστες αλλαγές για να ανταποκριθεί στις απαιτήσεις του προτύπου.

Το ISO 27005 δεν καλύπτει το κριτήριο του κόστους εφ’ όσον υπάρχει επιβεβλημένο κόστος όχι μόνο για την απόκτησή του αλλά και την εφαρμογή του και τη διατήρηση του.

5) EU ITSRM² – IT Security Risk Management Methodology

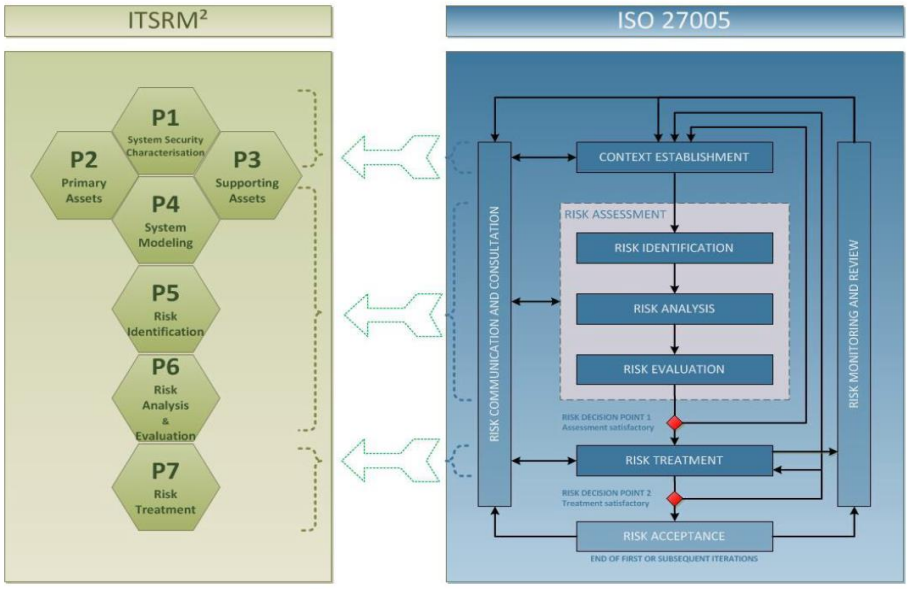
Ιστορικό

Η EU ITSRM², IT Security Risk Management Methodology, είναι μια μεθοδολογία που παρέχεται από τη από τον Οργανισμό της Ευρωπαϊκής Ένωσης για την ασφάλεια στον κυβερνοχώρο (ENISA), ως μέρος ενός συνόλου προτύπων για την ασφάλεια των πληροφοριών. Η μεθοδολογία δημοσιεύθηκε για πρώτη φορά το 2004 και έκτοτε έχει επικαιροποιηθεί αρκετές φορές. Έχει σχεδιαστεί ώστε να είναι ολοκληρωμένη και επεκτάσιμη, ώστε να μπορεί να χρησιμοποιηθεί από διαφορετικούς οργανισμούς ανάλογα με το μέγεθος, τον τύπο της επιχείρησής τους και τις απαιτήσεις ασφαλείας.

Εικόνα 6: Οι φάσεις της μεθοδολογίας EU ITSRM

Επισκόπηση

Η μεθοδολογία περιλαμβάνει φάσεις και βήματα που αντιστοιχίζονται στο ISO 27005, συμπεριλαμβανομένων των εξής: Καθορισμός πλαισίου (Context Establishment), αξιολόγηση επικινδυνότητας (Risk assessment) και αντιμετώπιση επικινδυνότητας (Risk Treatment). Οι αντιστοιχία των φάσεων και των βημάτων του EU ITSRM² με το ISO 27005 φαίνονται στην εικόνα 7.



Εικόνα 7: Αντιστοίχιση ITSRM2 σε ISO 27005

Η ITSRM² παρέχει πρακτικές κατευθυντήριες γραμμές για την εφαρμογή των διαδικασιών, όπως:

- λεπτομερή φόρμουλα για την αξιολόγηση του επιπέδου επικινδυνότητας και του επιπέδου του υπολειπόμενου κινδύνου,
- ενεργά καθήκοντα και μέθοδοι για κάθε υποδιαδικασία διαχείρισης επικινδυνότητας για την επίτευξη των αντίστοιχων αποτελεσμάτων, κυρίως την οικοδόμηση και την αξιολόγηση των διαφόρων συνιστωσών της επικινδυνότητας
- κλίμακες που πρέπει να χρησιμοποιούνται σε ολόκληρη την εταιρεία, με στόχο την επίτευξη συγκρίσιμων αποτελεσμάτων,
- κατάλογοι για τη διευκόλυνση των διαδικασιών.

Ο εντοπισμός της επικινδυνότητας χωρίζεται σε τέσσερις επιμέρους διαδικασίες:

- Προσδιορισμός των πρωταρχικών περιουσιακών στοιχείων,
- προσδιορισμός των υποστηρικτικών περιουσιακών στοιχείων,
- μοντελοποίηση του συστήματος,
- προσδιορισμός της επικινδυνότητας με την εκτέλεση ανάλυσης απειλών βάσει του μοντέλου.

Η ανάλυση και αξιολόγηση της επικινδυνότητας υπολογίζουν τα επίπεδα του υπολειπόμενου κινδύνου, τα ιεραρχούν και προβαίνουν σε αποφάσεις σχετικά με τη αντιμετώπιση ή την αποδοχή για τη διαχείρισή τους.
Ο προσδιορισμός της επικινδυνότητας βασίζεται σε σενάρια κινδύνου που προκύπτουν από το συνδυασμό περιουσιακών στοιχείων, απαιτήσεις ασφάλειας, των απειλών και τα υποστηρικτικά περιουσιακά στοιχεία και τα υφιστάμενα μέτρα.
Για την εκτίμηση του επιπέδου επικινδυνότητας , η μεθοδολογία συνδυάζει την αξία του περιουσιακού στοιχείου, την πιθανότητα ενός συμβάντος, τη συχνότητά του και την πόσο εύκολα μπορεί να υλοποιηθεί, την ελκυστικότητα του περιουσιακού στοιχείου, τη δύναμη και το ενδιαφέρον των αντιπάλων και την ισχύ των υφιστάμενων μέτρων.

Η μεθοδολογία χρησιμοποιεί καταλόγους για τύπους περιορισμών, τύπους περιουσιακών στοιχείων, τύπους αντιπάλων, απειλών και μέτρων ασφαλείας.

Χρηστικότητα

Η μεθοδολογία ITSRM^2 **θεωρείται εύχρηστη** λόγω των σαφών οδηγιών και κατευθυντήριων γραμμών της για τον εντοπισμό, την αξιολόγηση και τον μετριασμό της επικινδυνότητας της ασφάλειας των πληροφοριών.
Διαθέτει επίσης ένα φιλικό προς το χρήστη περιβάλλον για την τεκμηρίωση και την υποβολή εκθέσεων σχετικά με τη διαδικασία διαχείρισης της επικινδυνότητας και ενσωματώνεται εύκολα στις υφιστάμενες διαδικασίες και τα συστήματα του οργανισμού, καθιστώντας το φιλικό προς το χρήστη και εύκολο στην παρακολούθησή του, χωρίς να απαιτείται εκτεταμένη εκπαίδευση ή εμπειρογνωμοσύνη.
Η μεθοδολογία ITSRM βασίζεται στους κανονισμούς και τις κατευθυντήριες γραμμές της ΕΕ για την ασφάλεια των πληροφοριών, γεγονός που το καθιστά ιδιαίτερα χρήσιμο για τους οργανισμούς που δραστηριοποιούνται εντός της ΕΕ. Επίσης η ITSRM^2 αναπτύσσεται και συντηρείται από τον Οργανισμό της Ευρωπαϊκής Ένωσης για την ασφάλεια στον κυβερνοχώρο , ο οποίος επικαιροποιεί τη μεθοδολογία με βάση τις αλλαγές στην τεχνολογία, τα τοπία απειλών και τους κανονισμούς.

Ευελιξία

Η μεθοδολογία **ITSRM^2 είναι ευέλικτη** με διάφορους τρόπους:

- Μπορεί να χρησιμοποιηθεί για την αξιολόγηση της ασφάλειας ενός ευρέος φάσματος συστημάτων και δικτύων πληροφορικής, συμπεριλαμβανομένων διαφορετικών τύπων λειτουργικών συστημάτων, εφαρμογών και διαμορφώσεων δικτύου.
- Παρέχει μια ευέλικτη, σπονδυλωτή διαδικασία αξιολόγησης που επιτρέπει στους οργανισμούς να εστιάζουν σε συγκεκριμένους τομείς που τους απασχολούν και να προσαρμόζουν την αξιολόγηση στις συγκεκριμένες ανάγκες τους.
- Επιτρέπει στους οργανισμούς να ενσωματώσουν τη διαδικασία αξιολόγησης επικινδυνότητας με άλλες διαδικασίες διαχείρισης της ασφάλειας, όπως η αντιμετώπιση περιστατικών και η διαχείριση της συμμόρφωσης.
- Δεν είναι κανονιστική και επιτρέπει στους οργανισμούς να προσαρμόζουν τη μεθοδολογία στις συγκεκριμένες ανάγκες τους.
- Επιτρέπει την ενσωμάτωση διαφορετικών προτύπων, κανονισμών και βέλτιστων πρακτικών.

Συνοπτικά, η ITSRM^2 είναι ένα ευέλικτο πλαίσιο για τη διενέργεια εκτιμήσεων επικινδυνότητας των συστημάτων και δικτύων πληροφορικής.

Διαχείριση περιουσιακών στοιχείων

Στο πλαίσιο της μεθοδολογίας EU ITSRM , **η διαχείριση περιουσιακών στοιχείων είναι μια βασική και συστηματική διαδικασία που επικεντρώνεται στην αποτελεσματική και αποδοτική διαχείριση των φυσικών και λογικών περιουσιακών στοιχείων που υποστηρίζουν την παροχή υπηρεσιών πληροφορικής**. Αυτό μπορεί να περιλαμβάνει υλικό,

λογισμικό και άλλα περιουσιακά στοιχεία που σχετίζονται με την τεχνολογία πληροφοριών, όπως κέντρα δεδομένων, δίκτυα και υποδομές.
Κατά διαδικασίες P2 (Πρωτογενή περιουσιακά στοιχεία) και P3 (Υποστηρικτικά περιουσιακά στοιχεία) έχουμε τη συστηματική καταγραφή και χαρακτηρισμό των περιουσιακών στοιχείων.
Ο στόχος της διαδικασίας P2 ανάλυσης του πρωτεύοντος περιουσιακού στοιχείου είναι να εντοπίσει και να περιγράψει τα δεδομένα και τις λειτουργίες που περιλαμβάνει το σύστημα, να αξιολογηθεί η επιχειρησιακή τους αξία και να εντοπίσει και να αξιολογήσει τους πιθανούς αντιπάλους.
Ως αποτέλεσμα αυτής της διαδικασίας προκύπτει ο Κατάλογος Πρωτεύοντων Περιουσιακών Στοχείων ο οποίος περιλαμβάνει τον προσδιορισμό και την περιγραφή των δεδομένων που διαχειρίζονται και των λειτουργιών που παρέχονται από το σύστημα(-στόχο). Ελάχιστο περιεχόμενο που απαιτείται για τον κατάλογο των πρωτευόντων περιουσιακών στοιχείων:

- **PA ID:** αναγνωριστικό του πρωτεύοντος περιουσιακού στοιχείου
- **Όνομα:** το όνομα που χρησιμοποιείται στο πλαίσιο του ΕC για τον προσδιορισμό του πρωτεύοντος περιουσιακού στοιχείου.
- **Τύπος:** Προσδιορισμός αν το πρωτεύον περιουσιακό στοιχείο είναι σύνολο δεδομένων ή λειτουργία
- **Περιγραφή**: Σύντομη περιγραφή των κύριων χαρακτηριστικών του πρωτεύοντος περιουσιακού στοιχείου
- **Ιδιοκτήτης:** Προσδιορισμός του προσώπου (όνομα, επώνυμο και στοιχεία επικοινωνίας) ή της οντότητας (Μονάδα, Διεύθυνση ή Γενική Διεύθυνση) ιδιοκτήτη του πρωτεύοντος περιουσιακού στοιχείου
- **Διάσταση ασφαλείας:** χαρακτηριστικό ασφαλείας που επηρεάζεται από τον αντίκτυπο (εμπιστευτικότητα, ακεραιότητα ή διαθεσιμότητα) σε σχέση με το πρωτεύον περιουσιακό στοιχείο
- **Αξία του περιουσιακού στοιχείου:** αξιολόγηση της αξίας του περιουσιακού στοιχείου σε σχέση με το επίπεδο επιχειρηματικού αντίκτυπου σε περίπτωση απώλειας της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας
- **Ελκυστικότητα περιουσιακού στοιχείου:** ο μέγιστος συνδυασμός ΙΣΧΥΟΣ και ΕΝΔΙΑΦΕΡΟΝΤΟΣ για έναν πιθανό αντίπαλο, για δεδομένο πρωτεύον περιουσιακό στοιχείο και δεδομένη διάσταση ασφάλειας.

Ο στόχος της διαδικασίας P3 είναι να προσδιορίσει και να περιγράψει τα υποστηρικτικά περιουσιακά στοιχεία που χρησιμοποιούνται για την επεξεργασία των πρωτευόντων περιουσιακών στοιχείων ως μέρος του συστήματος-στόχου. Η διαδικασία αυτή χρησιμοποιεί τον κατάλογο με τους τύπους υποστηρικτικών περιουσιακών στοιχείων που παρέχεται από τη μεθοδολογία στο παράρτημα C.3 και παράγει έναν κατάλογος των υποστηρικτικών περιουσιακών στοιχείων του συστήματος-στόχου, με τους αντίστοιχους τύπους και ιδιοκτήτες.
Συνολικά, μπορούμε να πούμε ότι η μεθοδολογία ITSRM^2 χρησιμοποιεί πλήρεις διαδικασίες για τη διαχείριση των περιουσιακών στοιχείων.

Βάση δεδομένων για απειλές

Η μεθοδολογία χρησιμοποιεί καταλόγους για τύπους περιορισμών, τύπους περιουσιακών στοιχείων, τύπους αντιπάλων, απειλών και μέτρα ασφαλείας.
Οι κατάλογοι παρέχονται για να καθοδηγήσουν τον διαχειριστή επικινδυνότητας της ασφάλειας των πληροφοριακών συστημάτων ,κατά την εκτέλεση των καθηκόντων που προβλέπονται σε κάθε διαδικασία.
Είναι δομημένοι σε επίπεδα ώστε να επιτρέπουν την επιλογή γενικών ή συγκεκριμένων στοιχείων και τη δυνατότητα περαιτέρω εξειδίκευσης των πληροφοριών που προσδιορίζουν τα στοιχεία που απαιτούνται σε κάθε διαδικασία.
Συγκεκριμένα στο παράρτημα C.4 η μεθοδολογία EU ITSRM^2 παρέχει μία εκτεταμένη λίστα απειλών, η οποία περιέχει το όνομα της απειλής και ένα αναγνωριστικό, τη διάσταση της ασφάλειας (Confidentiality, Integrity, Availability) που επηρεάζει η κάθε απειλή και το αν η απειλή είναι ηθελημένη ή όχι. Δεν μπορούμε να πούμε ότι παρέχει κάποια βάση δεδομένων για απειλές όπως έχει οριστεί στην παρούσα μελέτη, διότι δεν περιλαμβάνει διαδικασίες διαχείρισης των απειλών, όμως καλύπτει το κριτήριο μερικώς εφ' όσον παρέχει επαρκείς πληροφορίες για απειλές, που συνεισφέρουν στη διαδικασία.

Βάση δεδομένων για ευπάθειες

Η μεθοδολογία EU ITSRM^2 **δεν περιλαμβάνει συγκεκριμένο κατάλογο ευπαθειών,** καθώς η μεθοδολογία επικεντρώνεται στον εντοπισμό και την αξιολόγηση της επικινδυνότητας για συγκεκριμένα συστήματα και τις υποδομές ενός οργανισμού. Αντ' αυτού, η μεθοδολογία ITSRM περιλαμβάνει συνήθως τον εντοπισμό πιθανών απειλών και στη συνέχεια, την αξιολόγηση της πιθανότητας και του αντίκτυπου αυτών των απειλών στα συστήματα και τα δεδομένα του οργανισμού. Οι πληροφορίες αυτές χρησιμοποιούνται στη συνέχεια για την ιεράρχηση και την εφαρμογή μέτρων μετριασμού της επικινδυνότητας. Δεν καλύπτεται το κριτήριο.

Βάση δεδομένων με μέτρα ασφάλειας

Η μεθοδολογία EU ITSRM^2 παρέχει επαρκή κάλυψη των μέτρων ασφαλείας.
Κατά τη διαδικασία P1 "Χαρακτηρισμός της ασφάλειας του συστήματος" η οποία συγκεντρώνει αρχικές πληροφορίες σχετικά με το σύστημα-στόχο και το πλαίσιό του, οι οποίες είναι απαραίτητες ή χρήσιμες για να προχωρήσει περαιτέρω η διαχείριση της επικινδυνότητας, **έχουμε τον εντοπισμό των υποχρεωτικών μέτρων ασφαλείας** που επιβάλλονται από τους περιορισμούς του συστήματος.
Από αυτή τη διαδικασία παράγεται το «Μητρώο μέτρων ασφαλείας» που περιλαμβάνει τα μέτρα ασφαλείας που έχουν επιλεγεί για τη διαχείριση της επικινδυνότητας με συνιστώμενο ελάχιστο περιεχόμενο:

- **ID Μέτρου Ασφάλειας**: Ταυτότητα του Μέτρου Ασφάλειας.
- **Supporting Asset ID:** ταυτοποίηση του υποστηρικτικού περιουσιακού στοιχείου στο οποίο το Μέτρο ασφάλειας πρέπει να εφαρμοστεί (εάν είναι ήδη γνωστό).
- **Σημαία (M):** προσδιορίζει ότι η υλοποίηση του μέτρου ασφαλείας επιβάλλεται από κάποιον περιορισμό σχετικό με την ασφάλεια.

Ταυτόχρονα η μεθοδολογία στο παράρτημα C.5 παρέχει τον «Κατάλογο μέτρων ασφαλείας» με προτεινόμενα ή ενδεικτικά μέτρα ασφαλείας τα οποία παρουσιάζονται με

ομαδοποιημένο τρόπο , περιλαμβάνοντας επίσης ποιο από τα αγαθά μεταξύ των CIA προστατεύει.

Πλοήγηση σε περιστατικά

Η μεθοδολογία ITSM² **δεν διαθέτει συγκεκριμένη διαδικασία για την πλοήγηση σε συμβάντα.**
Ωστόσο, μέσω των διαδικασιών εξέτασης σεναρίων απειλών και σεναρίων επικινδυνότητας καλύπτει κατά κάποιο τρόπο το χειρισμό και την επίλυση συμβάντων ασφαλείας, συμπεριλαμβανομένου του εντοπισμού της αιτίας, της αξιολόγησης των επιπτώσεων και της εφαρμογής των κατάλληλων μέτρων αποκατάστασης. Το κριτήριο θεωρούμε ότι καλύπτεται μερικώς.

Έλεγχος επιχειρηματικών διαδικασιών

Η μεθοδολογία ITSRM παρέχει μια διαδικασία για τη διαχείριση της επικινδυνότητας της ασφάλειας των πληροφοριών όπως έχουμε ήδη αναφέρει και **δεν ασχολείται ειδικά με τον έλεγχο των επιχειρηματικών διαδικασιών**. Το επίκεντρο της μεθοδολογίας είναι η προστασία των πληροφοριών και των πληροφοριακών συστημάτων από απειλές, ευπάθειες μέσω της εφαρμογής κατάλληλων μέτρων μετριασμού της επικινδυνότητας. Ωστόσο, η μεθοδολογία μπορεί να παρέχει κάποια καθοδήγηση σχετικά με τον τρόπο ενσωμάτωσης της διαχείρισης της επικινδυνότητας της ασφάλειας των πληροφοριών στο γενικό πλαίσιο διαχείρισης επιχειρηματικών διαδικασιών και τον τρόπο ευθυγράμμισης των στόχων ασφάλειας πληροφοριών με τους στόχους της επιχείρησης μέσω της εφαρμογής της. Δεν θεωρείται ότι το κριτήριο καλύπτεται.

Αναφορές και αναλύσεις

Η μεθοδολογία ITSRM **περιλαμβάνει μια διαδικασία υποβολής αναφορών και αναλύσεων ως μέρος του κύκλου αξιολόγησης και διαχείρισης της επικινδυνότητας και συγκεκριμένα μέσω της διαδικασίας αναφοράς και επικοινωνίας των αποτελεσμάτων της κάθε διαδικασίας που ολοκληρώνεται στα πλαίσια της μεθοδολογίας.**
Η διαδικασία περιλαμβάνει την τεκμηρίωση και την ανάλυση των αποτελεσμάτων των αξιολογήσεων επικινδυνότητας και τη χρήση αυτών των πληροφοριών για την ενημέρωση των αποφάσεων σχετικά με τον μετριασμό και την παρακολούθηση της επικινδυνότητας. Η διαδικασία αυτή συμβάλλει στη διασφάλιση της αποτελεσματικής διαχείρισης και του ελέγχου της επικινδυνότητας με την πάροδο του χρόνου.
Η επικοινωνία της επικινδυνότητας είναι επίσης μια διαδικασία η οποία περιλαμβάνει την υποβολή εκθέσεων και αναφορών. Συγκεκριμένα, οι διαδρομές επικοινωνίας και διαμοιρασμού πληροφοριών σχετικά με την επικινδυνότητα , μεταξύ των υπεύθυνων λήψης αποφάσεων και άλλων ενδιαφερόμενων μερών , αφορούν την υποβολή εκθέσεων και αναλύσεων σχετικά με τα προφίλ της επικινδυνότητας, με την περιγραφή των μέτρων ασφαλείας και τον τρόπο μετριασμού της επικινδυνότητας. Το κριτήριο καλύπτεται πλήρως από τη μεθοδολογία ITSRM.

Επίπεδο Τεχνικότητας

Η μεθοδολογία ITSRM **δεν απαιτεί υψηλό επίπεδο τεχνικών γνώσεων, αλλά ένα ορισμένο επίπεδο τεχνικής κατανόησης μπορεί να είναι απαραίτητο για την πλήρη εφαρμογή της** και τον αποτελεσματικό εντοπισμό και μετριασμό της επικινδυνότητας της ασφάλειας των πληροφοριών. Το επίπεδο των απαιτούμενων τεχνικών γνώσεων εξαρτάται από το μέγεθος και την πολυπλοκότητα του οργανισμού και των πληροφοριακών συστημάτων του.
Για παράδειγμα, τα άτομα που εμπλέκονται στην εφαρμογή της μεθοδολογίας μπορεί να χρειάζεται να έχουν μια βασική κατανόηση των κοινών κινδύνων ασφάλειας των πληροφοριών και των μέτρων μετριασμού, όπως εκείνων που σχετίζονται με την ασφάλεια του δικτύου, τις ευπάθειες του λογισμικού ή την προστασία της ιδιωτικής ζωής των δεδομένων. Επιπλέον, μπορεί να απαιτείται βαθύτερο επίπεδο τεχνικών γνώσεων για συγκεκριμένες πτυχές της μεθοδολογίας, όπως η διενέργεια τεχνικών αξιολογήσεων επικινδυνότητας ή η επιλογή και εφαρμογή τεχνικών μέτρων μετριασμού της επικινδυνότητας.
Συνοπτικά, η μεθοδολογία EU ITSRM δεν εστιάζει σε τεχνικές λεπτομέρειες ούτε απαιτεί βαθιές τεχνικές γνώσεις ωστόσο, ένα ορισμένο επίπεδο τεχνικής κατανόησης είναι επωφελές για την αποτελεσματική εφαρμογή της κάτι που κατατάσσει το επίπεδο τεχνικότητας στο μέτριο.

Υποστήριξη και πόροι

Η μεθοδολογία ITSRM περιλαμβάνει υποστηρικτικό υλικό και πόρους για να βοηθήσει τους χρήστες να κατανοήσουν και να χρησιμοποιήσουν σωστά τη μεθοδολογία.
Ο ENISA παίζει εδώ ένα βασικό ρόλο στην προώθηση της υιοθέτησης και εφαρμογής της μεθοδολογίας ITSRM και παρέχει υποστήριξη και μια σειρά από πόρους σχετικά με τη μεθοδολογία. Αυτό περιλαμβάνει καθοδήγηση σχετικά με τη μεθοδολογία, δραστηριότητες κατάρτισης και ανάπτυξης ικανοτήτων, βέλτιστες πρακτικές, εργαλεία και υποδείγματα και άλλους πόρους που θα βοηθήσουν τους οργανισμούς να εφαρμόσουν τη μεθοδολογία και να διαχειριστούν την επικινδυνότητα για την ασφάλεια των πληροφοριών. Ο ENISA συνεργάζεται επίσης με άλλους ενδιαφερόμενους φορείς, όπως τα κράτη μέλη της ΕΕ, οργανώσεις του κλάδου και ακαδημαϊκά ιδρύματα, για την προώθηση της υιοθέτησης και της εφαρμογής της μεθοδολογίας ITSRM και για την ανάπτυξη πρόσθετων πόρων και υποστήριξης, ανάλογα με τις ανάγκες. Το κριτήριο θεωρείται ότι καλύπτεται πλήρως.

Πληρότητα

Στο πλαίσιο της διαχείρισης επικινδυνότητας της ασφάλειας πληροφοριών, η μεθοδολογία ITSRM καλύπτει όλους τους σχετικούς τομείς κινδύνου.
«Η μεθοδολογία παρέχει μια ολοκληρωμένη και συστηματική προσέγγιση για τη διαχείριση της επικινδυνότητας της ασφάλειας πληροφοριών και έχει σχεδιαστεί ώστε να είναι ευέλικτη και προσαρμόσιμη στις ειδικές ανάγκες των διαφόρων οργανισμών και των πληροφοριακών συστημάτων τους», σύμφωνα με τον επίσημο δικτυακό τρόπο της Ευρωπαϊκής Επιτροπής (EC).
Το φάσμα της επικινδυνότητας της ασφάλειας των πληροφοριών που καλύπτει η μεθοδολογία είναι αρκετά ευρύ. Το φάσμα συμπεριλαμβάνει τους κινδύνους που

σχετίζονται με την ασφάλεια δικτύων, τις ευπάθειες λογισμικού, την προστασία της ιδιωτικής ζωής των δεδομένων, τον έλεγχο πρόσβασης και τη φυσική ασφάλεια. Λαμβάνει υπόψη το πλήρες φάσμα των απειλών για την ασφάλεια των πληροφοριών, όπως οι επιθέσεις στον κυβερνοχώρο, οι φυσικές καταστροφές και το ανθρώπινο λάθος, και παρέχει οδηγίες για τον εντοπισμό, την αξιολόγηση και τη διαχείριση αυτών των κινδύνων. Επιπλέον, η μεθοδολογία ITSRM της ΕΕ παρέχει καθοδήγηση σχετικά με τον τρόπο ενσωμάτωσης της διαχείρισης επικινδυνότητας για την ασφάλεια των πληροφοριών στο συνολικό πλαίσιο διαχείρισης επικινδυνότητας ενός οργανισμού.
Ωστόσο, όπως και άλλες μεθοδολογίες, δεν μπορεί να καλύψει όλους τους πιθανούς κινδύνους που μπορεί να αντιμετωπίσει ένας οργανισμός και θα πρέπει να χρησιμοποιείται ως οδηγός και να συμπληρώνεται με άλλα σχετικά πρότυπα (πχ NIST , ISO 27000) και βέλτιστες πρακτικές, ώστε να διασφαλίζεται μια ολοκληρωμένη προσέγγιση διαχείρισης επικινδυνότητας. Η πληρότητα της μεθοδολογίας θεωρείται επαρκής.

Χρόνος/Διάρκεια

Η ακριβής διάρκεια της εφαρμογής της μεθοδολογίας ITSRM εξαρτάται από διάφορους παράγοντες, όπως το μέγεθος και η πολυπλοκότητα του οργανισμού και των συστημάτων πληροφορικής του, οι διαθέσιμοι πόροι για την εφαρμογή και το επίπεδο των υφιστάμενων διαδικασιών διαχείρισης της επικινδυνότητας.
Ωστόσο, η μεθοδολογία έχει σχεδιαστεί ώστε να είναι όσο το δυνατόν πιο αποδοτική ως προς το χρόνο. Με τη χρήση προτύπων και άλλων εργαλείων που παρέχονται με τη μεθοδολογία, οι οργανισμοί μπορούν να απλοποιήσουν τη διαδικασία υλοποίησης και να ελαχιστοποιήσουν τον απαιτούμενο χρόνο.
Σε γενικές γραμμές, η εφαρμογή της μεθοδολογίας EU ITSRM είναι πιθανό να διαρκέσει αρκετές εβδομάδες ή μήνες. Οι οργανισμοί θα πρέπει επίσης να προγραμματίσουν συνεχείς δραστηριότητες διαχείρισης της επικινδυνότητας, όπως τακτικές αξιολογήσεις επικινδυνότητας, για να διασφαλίσουν ότι οι κίνδυνοι για την ασφάλεια των πληροφοριών τους διαχειρίζονται αποτελεσματικά με την πάροδο του χρόνου. Το κριτήριο του χρόνου θεωρούμε ότι καλύπτεται πλήρως.

Οικονομικό Κόστος

Παρόλο που η πρόσβαση και η χρήση της μεθοδολογίας ITSRM για τη διαχείριση της επικινδυνότητας της ασφάλειας των πληροφοριών είναι δωρεάν, ενδέχεται να προκύψει οικονομικό κόστος που συνδέεται με την εφαρμογή και τη χρήση της.
Η εφαρμογή της μεθοδολογίας EU ITSRM πιθανώς να απαιτήσει τη διάθεση εσωτερικών πόρων, όπως ο χρόνος του προσωπικού, για τη διενέργεια αξιολογήσεων , την ανάπτυξη σχεδίων διαχείρισης της επικινδυνότητας και την εφαρμογή μέτρων μετριασμού της. Ενδέχεται επίσης να υπάρξουν δαπάνες που σχετίζονται με την προμήθεια εργαλείων και συστημάτων για την υποστήριξη της εφαρμογής της μεθοδολογίας, όπως λογισμικό ή υλικό ασφαλείας.
Επιπλέον, οι οργανισμοί ενδέχεται να χρειαστεί να προσλάβουν εξωτερικούς συμβούλους ή εμπειρογνώμονες για την παροχή πρόσθετης υποστήριξης και καθοδήγησης κατά την εφαρμογή της μεθοδολογίας. Το κόστος αυτό μπορεί να ποικίλλει σε μεγάλο βαθμό ανάλογα με το μέγεθος και την πολυπλοκότητα του οργανισμού και των συστημάτων του,

καθώς και το επίπεδο των υφιστάμενων διαδικασιών διαχείρισης κινδύνων. Το κόστος θεωρείται μέτριο.

6) Microsoft Security Assessment Tool v.4

Ιστορικό

Το Microsoft Security Assessment Tool (MSAT) ,(στην έκδοση 4.0 πλέον) , είναι μια εφαρμογή αξιολόγησης επικινδυνότητας που αναπτύχθηκε από τη Microsoft ώστε να βοηθήσει τους οργανισμούς να αξιολογήσουν την κατάσταση ασφαλείας τους, να εντοπίσουν τις ευπάθειες και τις απειλές και να δώσουν προτεραιότητα στις βελτιώσεις ασφαλείας.
Το Microsoft Security Assessment Tool 4.0 είναι η αναθεωρημένη έκδοση του αρχικού Microsoft Security Risk Self-Assessment Tool (MSRSAT) που κυκλοφόρησε το 2004 και του Microsoft Security Assessment Tool 2.0 που κυκλοφόρησε το 2006.

Επισκόπηση

Το εργαλείο χρησιμοποιεί μια ολιστική προσέγγιση για τη μέτρηση της κατάστασης ασφαλείας ενός οργανισμού, καλύπτοντας θέματα που αφορούν ανθρώπους, διαδικασίες και τεχνολογία. Το MSAT αποτελείται από περισσότερες από 200 ερωτήσεις και τα ευρήματα συνδυάζονται με κανονιστικές οδηγίες και συνιστώμενες ενέργειες μετριασμού, συμπεριλαμβανομένων συνδέσμων προς περισσότερες πληροφορίες για πρόσθετη καθοδήγηση του κλάδου.
Η διεπαφή χρήστη του εργαλείου MSAT φαίνεται στην εικόνα (8).

Εικόνα 8: Microsoft Assessment Tool interface

Υπάρχουν δύο αξιολογήσεις που καθορίζουν το εργαλείο αξιολόγησης ασφάλειας της Microsoft:

- Αξιολόγηση προφίλ επιχειρηματικού κινδύνου
- Αξιολόγηση της άμυνας σε βάθος (UPDATED)

Οι ερωτήσεις που προσδιορίζονται στο κομμάτι της έρευνας του εργαλείου και οι σχετικές απαντήσεις προέρχονται από κοινά αποδεκτές βέλτιστες πρακτικές γύρω από την ασφάλεια, τόσο γενικές όσο και ειδικές. Οι ερωτήσεις και οι συστάσεις που προσφέρει το εργαλείο βασίζονται σε πρότυπα όπως το ISO 17799 και το NIST-800.x, καθώς και σε

συστάσεις και κανονιστικές οδηγίες από το Trustworthy Computing Group της Microsoft και πρόσθετους πόρους ασφάλειας που εκτιμώνται στον κλάδο.
Μετά την ολοκλήρωση της Αξιολόγησης, παρέχεται πρόσβαση σε μια λεπτομερή έκθεση των αποτελεσμάτων. Εκεί μπορεί ένας οργανισμός να συγκρίνει τα αποτελέσματά του με εκείνα των συναδέλφων του (ανάλογα με τον κλάδο και το μέγεθος της εταιρείας), με την προϋπόθεση ότι τα αποτελέσματά του θα μεταφορτωθούν ανώνυμα στον ασφαλή Web server MSAT.
Το εργαλείο παρέχει λεπτομερή ανάλυση της κατάστασης της ασφαλείας ενός οργανισμού, συμπεριλαμβανομένης της αξιολόγησης των περιουσιακών στοιχείων, του δικτύου και των εφαρμογών του. Οι πληροφορίες αυτές μπορούν να χρησιμοποιηθούν για την ιεράρχηση των βελτιώσεων της ασφάλειας, ώστε οι οργανισμοί να εστιάζουν τις προσπάθειές τους εκεί που χρειάζονται περισσότερο.
Το MSAT παρέχει επίσης μια σειρά λειτουργιών για να βοηθήσει τους οργανισμούς να διαχειριστούν και να μετριάσουν την επικινδυνότητα. Για παράδειγμα, το εργαλείο παρέχει λεπτομερείς συστάσεις για ενέργειες αποκατάστασης και μετριασμού, οι οποίες μπορούν να βοηθήσουν τους οργανισμούς να αντιμετωπίσουν γρήγορα τα ζητήματα ασφάλειας και να μειώσουν τον κίνδυνο.

Χρηστικότητα

Το εργαλείο αξιολόγησης ασφάλειας της Microsoft θεωρείται γενικά φιλικό προς το χρήστη και εύκολο στη χρήση καθιστώντας το έναν προσιτό τρόπο για οργανισμούς όλων των μεγεθών να βελτιώσουν τη θέση της ασφαλείας τους. Ωστόσο, η ευχρηστία και η φιλικότητα του εργαλείου μπορεί να ποικίλλει ανάλογα με την τεχνική επάρκεια του χρήστη και την εξοικείωσή του με τις διαδικασίες αξιολόγησης της ασφάλειας. Το εργαλείο έχει σχεδιαστεί για να είναι απλό και διαισθητικό, αλλά μπορεί να απαιτεί κάποιες τεχνικές γνώσεις για την πλήρη αξιοποίηση των χαρακτηριστικών του.
Όσον αφορά τη συντήρηση και την ενημέρωση, η Microsoft κυκλοφορεί τακτικά ενημερώσεις για το εργαλείο, προκειμένου να αντιμετωπίσει τις ανησυχίες σχετικά με την ασφάλεια και να βελτιώσει τη λειτουργικότητά του. Η διαδικασία ενημέρωσης του εργαλείου είναι συνήθως απλή, αλλά μπορεί να απαιτεί κάποια τεχνική γνώση για τη σωστή εφαρμογή. Το εργαλείο έχει σχεδιαστεί για να είναι φιλικό προς το χρήστη και εύκολο στη χρήση, καθιστώντας το έναν προσιτό τρόπο για οργανισμούς όλων των μεγεθών να βελτιώσουν τη θέση ασφαλείας τους, όμως λόγω των ιδιαιτεροτήτων των διαδικασιών που περιλαμβάνει του θεωρούμε ότι έχει μέτρια χρηστικότητα.

Ευελιξία

Το MSAT είναι ευέλικτο με διάφορους τρόπους:

- Μπορεί να χρησιμοποιηθεί για την αξιολόγηση της ασφάλειας ενός ευρέος φάσματος συστημάτων και δικτύων που βασίζονται στη Microsoft, συμπεριλαμβανομένων των περιβαλλόντων Windows και Office.
- Παρέχει μια ευέλικτη, σπονδυλωτή διαδικασία αξιολόγησης που επιτρέπει στους οργανισμούς να επικεντρωθούν σε συγκεκριμένους προβληματικούς τομείς και να προσαρμόσουν την αξιολόγηση στις ιδιαίτερες ανάγκες τους.

- Επιτρέπει στους οργανισμούς να ενσωματώσουν τη διαδικασία αξιολόγησης επικινδυνότητα με άλλες διαδικασίες διαχείρισης ασφάλειας, όπως η αντιμετώπιση περιστατικών και η διαχείριση συμμόρφωσης.
- Δεν είναι κανονιστικό και επιτρέπει στους οργανισμούς να προσαρμόζουν τη μεθοδολογία στις συγκεκριμένες ανάγκες τους.
- Επιτρέπει στους οργανισμούς να εντοπίζουν και να αξιολογούν τους κινδύνους για τα πληροφοριακά τους συστήματα και να αναπτύσσουν κατάλληλες στρατηγικές διαχείρισης κινδύνων.

Διαχείριση περιουσιακών στοιχείων

Το MSAT δεν διαθέτει συγκεκριμένη διαδικασία για τη διαχείριση περιουσιακών στοιχείων.
Ωστόσο, το MSAT παρέχει οδηγίες για τη διαχείριση των περιουσιακών στοιχείων και την προστασία τους από απειλές και ευπάθειες. Συνιστά στους οργανισμούς να προσδιορίζουν και να ιεραρχούν τα πιο κρίσιμα περιουσιακά στοιχεία τους και να λαμβάνουν μέτρα για την προστασία αυτών των περιουσιακών στοιχείων μέσω της χρήσης μέτρων ασφαλείας, διαδικασιών δημιουργίας αντιγράφων ασφαλείας και ανάκτησης και σχεδίων αντιμετώπισης περιστατικών καθώς και να επανεξετάζουν και να επικαιροποιούν τακτικά το σχέδιο διαχείρισης περιουσιακών στοιχείων για να διασφαλίζουν ότι είναι αποτελεσματικό και ότι όλα τα περιουσιακά στοιχεία προστατεύονται σωστά. Το κριτήριο δεν καλύπτεται από το MSAT.

Βάση δεδομένων για απειλές

Το Εργαλείο αξιολόγησης ασφάλειας της Microsoft , δεν περιλαμβάνει κατάλογο ή βάση δεδομένων απειλών. Το MSAT παρέχει ένα σύνολο δοκιμών, σεναρίων και βέλτιστων πρακτικών για την αξιολόγηση της κατάστασης ασφαλείας ενός οργανισμού, αλλά δεν παρέχει έναν ολοκληρωμένο κατάλογο με πιθανές απειλές ούτε προβλέπει κάποια διαδικασία εντοπισμού και καταγραφής τους. Το κριτήριο δεν καλύπτεται καθόλου.

Βάση δεδομένων για ευπάθειες

Το MSAT δεν περιλαμβάνει κάποια λίστα ή βάση δεδομένων για ευπάθειες . Αντ' αυτού το εργαλείο χρησιμοποιεί τυποποιημένα εργαλεία της βιομηχανίας για τη σάρωση ευπαθειών και ρυθμίσεων που ανιχνεύουν γνωστές ευπάθειες και λανθασμένες ρυθμίσεις ασφαλείας. Το εργαλείο μπορεί να χρησιμοποιηθεί για τον εντοπισμό πιθανών ευπαθειών και την παροχή συστάσεων για τον τρόπο αντιμετώπισης αυτών των ευπαθειών. Θεωρούμε ότι καλύπτει μερικώς το κριτήριο. Το κριτήριο δεν καλύπτεται.

Βάση δεδομένων για μέτρα ασφαλείας

Το MSAT παρέχει ένα σύνολο βέλτιστων πρακτικών και εφαρμόσιμων συστάσεων για τη βελτίωση της κατάστασης ασφαλείας ενός οργανισμού, **συμπεριλαμβανομένου ενός καταλόγου μέτρων και αντιμέτρων** που μπορούν να εφαρμοστούν για τον μετριασμό της επικινδυνότητας της ασφαλείας. Οι συστάσεις του εργαλείου βασίζονται σε βιομηχανικά πρότυπα και κατευθυντήριες γραμμές και έχουν σχεδιαστεί για να βοηθήσουν τους οργανισμούς να εντοπίσουν τομείς προς βελτίωση και να λάβουν μέτρα για τη βελτίωση της

κατάστασης ασφαλείας τους. Ο κατάλογος των μέτρων και των αντιμέτρων που παρέχει το MSAT μπορεί να χρησιμεύσει ως σημείο εκκίνησης για τους οργανισμούς που επιθυμούν να βελτιώσουν τη θέση ασφαλείας τους. Θεωρούμε ότι το κριτήριο καλύπτεται πλήρως.

Πλοήγηση σε περιστατικά

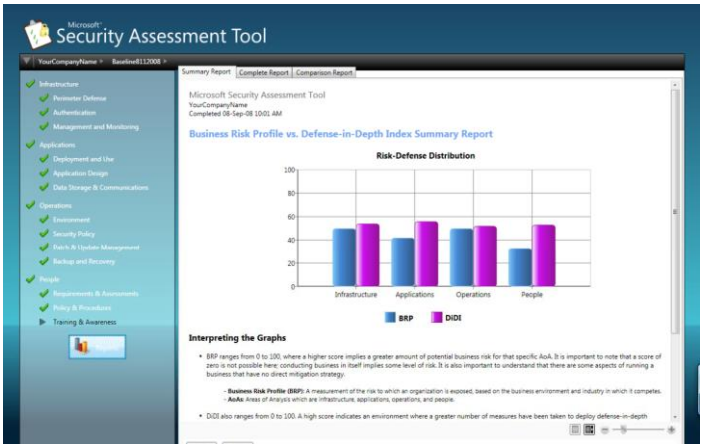
Το εργαλείο δεν διαθέτει συγκεκριμένη διαδικασία για την πλοήγηση σε συμβάντα. Ωστόσο, το MSAT παρέχει οδηγίες σχετικά με την αντιμετώπιση και τη διαχείριση περιστατικών. Συνιστά στους οργανισμούς να διαθέτουν ένα καλά καθορισμένο σχέδιο αντιμετώπισης περιστατικών και να δοκιμάζουν και να εξασκούν τακτικά τις διαδικασίες αντιμετώπισης περιστατικών, ώστε να διασφαλίζουν ότι είναι προετοιμασμένοι να ανταποκρίνονται αποτελεσματικά σε περιστατικά ασφαλείας.
Το MSAT συνιστά επίσης στους οργανισμούς να διαθέτουν ειδική ομάδα αντιμετώπισης περιστατικών και να έχουν διαδικασίες για τον εντοπισμό, την ταξινόμηση και την αντιμετώπιση περιστατικών ασφαλείας. Συμβουλεύει επίσης τους οργανισμούς να διεξάγουν ανασκοπήσεις μετά το συμβάν για να εντοπίσουν τυχόν περιοχές για βελτίωση στις διαδικασίες τους για την αντιμετώπιση συμβάντων.
Για βοήθεια στην αντιμετώπιση περιστατικών, οι οργανισμοί μπορεί να εξετάσουν το ενδεχόμενο χρήσης άλλων εργαλείων ή υπηρεσιών, όπως η πλατφόρμα Microsoft Defender Advanced Threat Protection (ATP) ή το κέντρο ασφαλείας του Microsoft 365.
Το κριτήριο θεωρούμε ότι καλύπτεται μερικώς.

Έλεγχος επιχειρηματικών διαδικασιών

Το MSAT δεν περιλαμβάνει έλεγχο επιχειρηματικών διαδικασιών. Ο έλεγχος επιχειρηματικών διαδικασιών αναφέρεται στις διαδικασίες, τις πολιτικές και τις πρακτικές που εφαρμόζει ένας οργανισμός για να διασφαλίσει ότι οι επιχειρηματικές διαδικασίες του είναι αποδοτικές, αποτελεσματικές και συμμορφώνονται με τους σχετικούς κανονισμούς και πρότυπα. Παρόλο που η ασφάλεια αποτελεί κρίσιμη πτυχή κάθε επιχειρηματικής διαδικασίας, το MSAT επικεντρώνεται κυρίως στην αξιολόγηση της κατάστασης ασφαλείας ενός οργανισμού και στην παροχή αξιοποιήσιμων συστάσεων για τη βελτίωσή της. Οι οργανισμοί που επιθυμούν να εφαρμόσουν ελέγχους επιχειρηματικών διαδικασιών θα χρειαστεί να εξετάσουν το ενδεχόμενο χρήσης άλλων εργαλείων ή υπηρεσιών που έχουν σχεδιαστεί ειδικά για το σκοπό αυτό. Το κριτήριο δεν καλύπτεται καθόλου από το MSAT.

Αναφορές και αναλύσεις

Το MSAT περιλαμβάνει δυνατότητες αναφοράς και ανάλυσης. Παρέχει αξιοποιήσιμες συστάσεις για τον μετριασμό της επικινδυνότητας της ασφαλείας και περιλαμβάνει επίσης δυνατότητες αναφοράς και ανάλυσης που βοηθούν τους οργανισμούς να παρακολουθούν την πρόοδό τους και να αξιολογούν την αποτελεσματικότητα των μέτρων ασφαλείας τους. Οι λειτουργίες αναφοράς και ανάλυσης του MSAT επιτρέπουν στους οργανισμούς να εντοπίζουν τάσεις και μοτίβα στην κατάσταση της ασφαλείας τους και να λαμβάνουν τεκμηριωμένες αποφάσεις σχετικά με το πού πρέπει να εστιάσουν τις προσπάθειές τους για τη βελτίωση της. Θεωρούμε ότι το MSAT καλύπτει πλήρως το κριτήριο.



Εικόνα 9: MSAT Ανάλυση

Επίπεδο τεχνικότητας

Το MSAT είναι φιλικό προς το χρήστη, παρέχει ένα περιβάλλον εργασίας που βασίζεται σε οδηγό και έχει σχεδιαστεί για να εκτελείται από επαγγελματίες ασφαλείας με μικρή ή καθόλου τεχνική εμπειρία. **Αν και δεν απαιτεί υψηλό επίπεδο τεχνικών γνώσεων για τη χρήση του, συνιστάται το άτομο που χρησιμοποιεί το εργαλείο να έχει κάποια κατανόηση των εννοιών και της ορολογίας της ασφάλειας για την αποτελεσματική χρήση του.** Επιπλέον, το εργαλείο παράγει αναφορές που απαιτούν κάποια ερμηνεία και ενέργειες παρακολούθησης, οι οποίες ενδέχεται να απαιτούν πιο προχωρημένες τεχνικές γνώσεις. Συνολικά το επίπεδο τεχνικότητας θεωρείται μέτριο.

Υποστήριξη και πόροι

Το MSAT περιλαμβάνει υλικό υποστήριξης και πόρους και περιλαμβάνει τα ακόλουθα υποστηρικτικά υλικά και πόρους :

- Οδηγό χρήσης που παρέχει μια επισκόπηση του εργαλείου, συμπεριλαμβανομένων οδηγιών για την εγκατάσταση και τη χρήση του.
- Μια βάση γνώσεων με άρθρα που καλύπτει διάφορα θέματα σχετικά με το εργαλείο, όπως τον τρόπο ερμηνείας των αποτελεσμάτων και τον τρόπο αποκατάστασης των εντοπισμένων ευπαθειών.
- Ένα φόρουμ κοινότητας όπου οι χρήστες μπορούν να υποβάλλουν ερωτήσεις, να μοιράζονται εμπειρίες και βέλτιστες πρακτικές και να λαμβάνουν βοήθεια από άλλους χρήστες.
- Επιπλέον, η Microsoft παρέχει οδηγίες ασφαλείας, βέλτιστες πρακτικές και συστάσεις, για να βοηθήσει τους οργανισμούς να ασφαλίσουν το περιβάλλον τους.

Συνολικά, το MSAT παρέχει ένα ολοκληρωμένο σύνολο πόρων και υποστήριξης για να βοηθήσει τους χρήστες να κατανοήσουν και να χρησιμοποιήσουν αποτελεσματικά το εργαλείο, οπότε το κριτήριο καλύπτεται πλήρως.

Πληρότητα

Το MSAT μπορεί να βοηθήσει τους οργανισμούς να εντοπίσουν πιθανούς κινδύνους και ευπάθειες σε τομείς όπως η υποδομή δικτύου, τα λειτουργικά συστήματα, οι εφαρμογές

και τα δεδομένα. Καλύπτει τομείς όπως η διαχείριση ρυθμίσεων ασφαλείας, η διαχείριση βασικών γραμμών ασφαλείας και η υποβολή εκθέσεων αξιολόγησης ασφαλείας.
Ωστόσο, το MSAT δεν είναι ένα ολοκληρωμένο εργαλείο για τη διαχείριση της επικινδυνότητας της ασφάλειας των πληροφοριών , επικεντρώνεται κυρίως σε συστήματα και περιβάλλοντα που βασίζονται στη Microsoft και ενδέχεται να μην καλύπτει όλους τους σχετικούς τομείς επικινδυνότητας για έναν οργανισμό. Συνιστάται η χρήση του MSAT ως ένα από τα εργαλεία για την αξιολόγηση της κατάστασης ασφαλείας ενός οργανισμού και η συμπλήρωσή του με άλλα σχετικά πρότυπα και βέλτιστες πρακτικές, ώστε να διασφαλίζεται μια ολοκληρωμένη προσέγγιση διαχείρισης επικινδυνότητας. Το κριτήριο θεωρούμε ότι δεν καλύπτεται καθόλου από το MSAT.

Χρόνος/Διάρκεια

Το MSAT έχει σχεδιαστεί για να αξιολογεί τις αδυναμίες στο περιβάλλον ασφαλείας ενός οργανισμού. Η αξιολόγηση μπορεί να γίνει είτε από τους ίδιους τους οργανισμούς είτε να διευκολυνθεί από έναν πιστοποιημένο συνεργάτη της Microsoft. Η αξιολόγηση της ασφάλειας βασίζεται σε μια σειρά ερωτήσεων σχετικά με διάφορα θέματα ασφάλειας. **Η συνεδρία ερωτήσεων αναμένεται να διαρκέσει κάπου 60-90 λεπτά.** Με την ολοκλήρωση της αξιολόγησης, οι πελάτες λαμβάνουν μια ολοκληρωμένη έκθεση που περιέχει συστάσεις ειδικά για τα επιχειρηματικά τους ζητήματα, με βάση τις απαντήσεις που έδωσαν κατά τη διάρκεια της αξιολόγησης. Θεωρείται χρονικά αποδοτικό για τη χρήση που προορίζεται.

Οικονομικό κόστος

Το MSAT **είναι ένα δωρεάν εργαλείο**, όμως το κόστος που σχετίζεται με την υλοποίηση και τη χρήση του εργαλείου αξιολόγησης ασφάλειας της Microsoft ποικίλλει ανάλογα με τον εκάστοτε οργανισμό και τις ανάγκες του.
Ορισμένα πιθανά κόστη που πρέπει να ληφθούν υπόψη περιλαμβάνουν:

- Κόστος αδειοδότησης για το Microsoft Security Assessment Tool, το οποίο αποτελεί μέρος του συνόλου εργαλείων Microsoft Security Compliance Manager (SCM).
- Κόστος κατάρτισης για τους υπαλλήλους και τη διοίκηση σχετικά με τον τρόπο χρήσης του εργαλείου.
- Αμοιβές συμβούλων για έναν διαπιστευμένο συνεργάτη της Microsoft για τη διενέργεια αξιολόγησης και την παροχή καθοδήγησης σχετικά με τη συμμόρφωση.
- Ορισμένοι οργανισμοί ενδέχεται να χρειαστεί να αγοράσουν πρόσθετα εργαλεία, υλικό ή υπηρεσίες για να ανταποκριθούν στις απαιτήσεις του εργαλείου.
- Συνεχές κόστος για τη διατήρηση της συμμόρφωσης με το πλαίσιο, όπως οι τακτικές αξιολογήσεις και η ενημέρωση των ελέγχων ασφαλείας.

Συνολικά το οικονομικό κόστος θεωρείται μέτριο, οπότε το κριτήριο καλύπτεται εν μέρει.

7) NIST, National Institute of Standards and Technology Special Publication 800-30

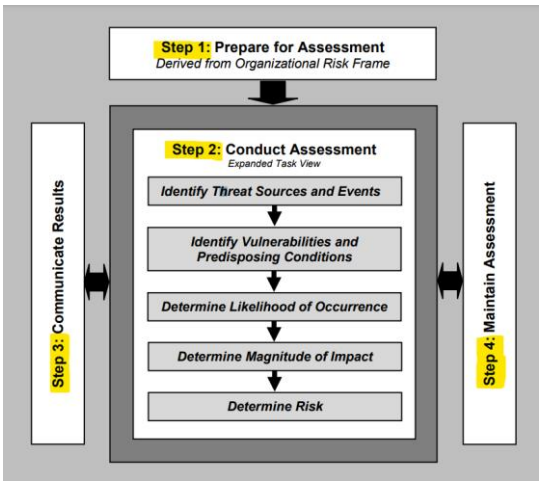
Ιστορικό

Το NIST SP 800-30, "Οδηγός διαχείρισης επικινδυνότητας για πληροφοριακά συστήματα", δημοσιεύθηκε για πρώτη φορά το 2006 από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST). Επικαιροποιήθηκε το 2010 για να ενσωματώσει τα σχόλια και τις νέες οδηγίες της κοινότητας διαχείρισης επικινδυνότητας. Στη συνέχεια, η δημοσίευση αναθεωρήθηκε το 2012 για να αντικατοπτρίζει τις αλλαγές στην τεχνολογία και τις νέες πρακτικές διαχείρισης επικινδυνότητας. Η πιο πρόσφατη αναθεώρηση, NIST SP 800-30 Rev. 1, κυκλοφόρησε το 2018 και παρέχει επικαιροποιημένη καθοδήγηση σχετικά με τη διαδικασία διαχείρισης επικινδυνότητας. (Το NIST SP 800-30 Rev. 1 περιλαμβάνει επίσης νέες πληροφορίες σχετικά με την υπολογιστική νέφους, τις κινητές συσκευές και το Διαδίκτυο των πραγμάτων (IoT). Η δημοσίευση παραμένει μια ευρέως χρησιμοποιούμενη πηγή για τους οργανισμούς που επιδιώκουν να διασφαλίσουν την ασφάλεια των πληροφοριακών τους συστημάτων.)

Επισκόπηση

Το NIST SP 800-30 παρέχει τα θεμέλια για την ανάπτυξη ενός αποτελεσματικού προγράμματος διαχείρισης επικινδυνότητας, περιλαμβάνοντας τόσο τους ορισμούς όσο και τις πρακτικές οδηγίες που είναι απαραίτητες για την αξιολόγηση και τον μετριασμό της επικινδυνότητας που εντοπίζεται στα πληροφοριακά συστήματα ενός οργανισμού.
Η διαδικασία αξιολόγησης επικινδυνότητας σύμφωνα με το NIST SP 800-30 αποτελείται από τέσσερα βήματα:

(i) προετοιμασία για την αξιολόγηση
(ii) διεξαγωγή της αξιολόγησης,
(iii) κοινοποίηση των αποτελεσμάτων της αξιολόγησης
(iv) διατήρηση της αξιολόγησης.



Εικόνα 10: Η διαδικασία αξιολόγησης επικινδυνότητας βάσει του NIST SP 800-30

Κάθε βήμα διαιρείται σε ένα σύνολο εργασιών.

(i) Η προετοιμασία για την αξιολόγηση της επικινδυνότητας περιλαμβάνει τις ακόλουθες εργασίες:

a) Προσδιορισμός του σκοπού της αξιολόγησης,
b) Προσδιορισμός του πεδίου εφαρμογής της αξιολόγησης,
c) Προσδιορισμός των παραδοχών και των περιορισμών που σχετίζονται με την αξιολόγηση,
d) Προσδιορισμός των πηγών πληροφοριών που θα χρησιμοποιηθούν ως εισροές στην αξιολόγηση
e) Προσδιορισμός του μοντέλου κινδύνου και των αναλυτικών προσεγγίσεων (δηλαδή των προσεγγίσεων αξιολόγησης και ανάλυσης) που θα χρησιμοποιηθούν κατά την αξιολόγηση.

(ii) Η διεξαγωγή της αξιολόγησης, περιλαμβάνει τις ακόλουθες ειδικές εργασίες:

a) Προσδιορισμός των πηγών απειλών που αφορούν τους οργανισμούς,
b) Προσδιορισμός των συμβάντων απειλής που θα μπορούσαν να παραχθούν από αυτές τις πηγές,
c) Προσδιορισμός των ευπαθειών εντός των οργανισμών που θα μπορούσαν να αξιοποιηθούν από τις πηγές απειλών μέσω συγκεκριμένων γεγονότων απειλής
d) Προσδιορισμός της πιθανότητας οι αναγνωρισμένες πηγές απειλών να προκαλέσουν συγκεκριμένα συμβάντα απειλών και την πιθανότητα τα γεγονότα απειλής να είναι επιτυχή.
e) Προσδιορισμός των δυσμενών επιπτώσεων στις οργανωτικές λειτουργίες και τα περιουσιακά στοιχεία, τα άτομα, άλλους οργανισμούς που προκύπτουν από την εκμετάλλευση των τρωτών σημείων από τις απειλές. (μέσω συγκεκριμένων απειλητικών γεγονότων)
f) Προσδιορισμός της επικινδυνότητας της ασφάλειας πληροφοριών ως συνδυασμός της πιθανότητας εκμετάλλευσης από απειλές των ευπαθειών και του αντίκτυπου αυτής της εκμετάλλευσης.

(iii) Η επικοινωνία και η ανταλλαγή πληροφοριών περιλαμβάνει τις ακόλουθες συγκεκριμένες εργασίες:

a) Κοινοποίηση των αποτελεσμάτων της εκτίμησης κινδύνου- και
b) Ανταλλαγή πληροφοριών που αναπτύχθηκαν κατά την εκτέλεση της αξιολόγησης επικινδυνότητας, για την υποστήριξη άλλες δραστηριότητες διαχείρισης της επικινδυνότητας.

(iv) Η διατήρηση των αξιολογήσεων της επικινδυνότητας περιλαμβάνει τις ακόλουθες ειδικές εργασίες:

a) Παρακολούθηση των παραγόντων επικινδυνότητας που προσδιορίζονται στις αξιολογήσεις επικινδυνότητας σε συνεχή βάση και κατανόηση των επακόλουθων αλλαγών στους εν λόγω παράγοντες- και
b) Επικαιροποίηση των συστατικών στοιχείων των αξιολογήσεων επικινδυνότητας που αντικατοπτρίζουν τις δραστηριότητες παρακολούθησης που διεξάγονται από τους οργανισμούς.

Χρηστικότητα

Το NIST SP 800-30 **είναι ένα τεχνικό έγγραφο που έχει σχεδιαστεί για επαγγελματίες της ασφάλειας πληροφοριών και όχι γενικούς χρήστες.**
Γενικά δεν είναι ένα χρηστικό πλαίσιο, με την έννοια ότι αποτελεί ένα έτοιμο προς χρήση εργαλείο για τη διενέργεια αξιολογήσεων κινδύνου. Παρέχει καθοδήγηση και μια διαδικασία για τη διενέργεια αξιολογήσεων επικινδυνότητας, συμπεριλαμβανομένων πληροφοριών σχετικά με το τι πρέπει να ληφθεί υπόψη και τα βήματα που πρέπει να γίνουν κατά τη διαδικασία αξιολόγησης, αλλά εξακολουθεί να **απαιτεί από τον χρήστη να έχει γνώσεις σχετικά με τις πρακτικές ασφάλειας πληροφοριών και την ικανότητα να ερμηνεύει και να εφαρμόζει την παρεχόμενη καθοδήγηση.**
Όσον αφορά τη συντηρησιμότητα και την ενημέρωση, το έγγραφο επικαιροποιείται από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας περιοδικά, ανάλογα με τις ανάγκες, ώστε να αντικατοπτρίζει τις αλλαγές στην τεχνολογία, τα περιβάλλοντα απειλών και τις βέλτιστες πρακτικές.
Συνολικά η χρηστικότητά του περιορίζεται από το ότι δεν είναι φιλικό προς τον χρήστη, εύκολο στην παρακολούθηση και απαιτεί εκτεταμένη εκπαίδευση ή εμπειρογνωμοσύνη για την εκτέλεσή του, παρέχει όμως εκτεταμένη καθοδήγηση, οπότε θεωρούμε ότι το κριτήριο καλύπτεται εν μέρει από το NIST SP 800-30

Ευελιξία

Το NIST SP 800-30 είναι ευέλικτο, δεδομένου ότι μπορεί να προσαρμοστεί στις συγκεκριμένες ανάγκες ενός οργανισμού και στις διαδικασίες διαχείρισης κινδύνων που εφαρμόζει. Ο οδηγός παρέχει ένα γενικό πλαίσιο για τη διαχείριση κινδύνων, αλλά δεν προδιαγράφει ένα συγκεκριμένο σύνολο εργαλείων ή τεχνολογιών που πρέπει να χρησιμοποιηθούν. Ο οδηγός παρέχει καθοδήγηση σχετικά με τον τρόπο διεξαγωγής αξιολογήσεων κινδύνου, αλλά επιτρέπει επίσης στους οργανισμούς να επιλέξουν το επίπεδο τυπικότητας και αυστηρότητας που είναι κατάλληλο για τις συγκεκριμένες ανάγκες και τους στόχους τους.
Ο οδηγός επιτρέπει επίσης στους οργανισμούς να προσαρμόσουν τη διαδικασία αξιολόγησης στο συγκεκριμένο περιβάλλον τους, για παράδειγμα, επιτρέπει στους οργανισμούς να επιλέξουν ποιες συγκεκριμένες περιοχές του περιβάλλοντος θα αξιολογήσουν και επιτρέπει στους οργανισμούς να αποκλείσουν ορισμένες περιοχές του περιβάλλοντος από την αξιολόγηση. Παρέχει επίσης καθοδήγηση σχετικά με τον τρόπο ενσωμάτωσης της διαδικασίας αξιολόγησης κινδύνων στη συνολική στρατηγική διαχείρισης κινδύνων ενός οργανισμού. Συνολικά θεωρείται ένα αρκετά ευέλικτο πλαίσιο.

Διαχείριση περιουσιακών στοιχείων

Το NIST SP 800-30 δεν περιλαμβάνει συγκεκριμένη διαδικασία για τη διαχείριση περιουσιακών στοιχείων. Αντ' αυτού, παρέχει καθοδήγηση σχετικά με τον τρόπο χρήσης των αρχών διαχείρισης επικινδυνότητας για τον εντοπισμό και τη διαχείριση των κινδύνων που συνδέονται με τη χρήση των περιουσιακών στοιχείων των πληροφοριακών συστημάτων.

Παρέχει μία σχετική καθοδήγηση για τον εντοπισμό και την καταγραφή των περιουσιακών στοιχείων, καθώς και για την αξιολόγηση της αξίας και της κρισιμότητάς τους για τον οργανισμό. Οι πληροφορίες αυτές χρησιμοποιούνται στη συνέχεια για την ιεράρχηση των προσπαθειών μετριασμού της επικινδυνότητας και την ανάπτυξη στρατηγικών για την προστασία των περιουσιακών στοιχείων. Συνολικά θεωρούμε ότι το NIST SP 800-30 καλύπτει εν μέρει το εν λόγω κριτήριο.

Βάση δεδομένων για απειλές

Το NIST SP 800-30 παρέχει έναν εκτεταμένο κατάλογο πηγών και κατηγοριών απειλών που μπορούν να χρησιμοποιηθούν ως σημείο εκκίνησης για τον εντοπισμό πιθανών απειλών σε συστήματα πληροφοριών. Ο κατάλογος περιλαμβάνει κατηγορίες όπως φυσικές καταστροφές, ανθρώπινα λάθη και κακόβουλες επιθέσεις, μεταξύ άλλων.
Το έγγραφο περιγράφει τη διαδικασία εντοπισμού πιθανών πηγών απειλών για ένα σύστημα πληροφοριών, οι οποίες μπορεί να περιλαμβάνουν εσωτερικές και εξωτερικές απειλές, καθώς και φυσικές και ανθρωπογενείς απειλές.
Εναπόκειται στον οργανισμό που διεξάγει την αξιολόγηση κινδύνου να συγκεντρώσει πληροφορίες σχετικά με τις πιθανές απειλές που αφορούν ειδικά το περιβάλλον του και να καταρτίσει έναν κατάλογο απειλών, που θα εξετάσει στο πλαίσιο της διαδικασίας αξιολόγησης επικινδυνότητας.
Επιπλέον, οι οργανισμοί θα πρέπει να λαμβάνουν υπόψη τους εξωτερικές πηγές, όπως τροφοδοσίες πληροφοριών για απειλές, κοινότητες ανταλλαγής απειλών στον κυβερνοχώρο και εκθέσεις από ομάδες αντιμετώπισης περιστατικών, για να συμπληρώσουν τη διαδικασία αξιολόγησης κινδύνου και να κατανοήσουν τους τύπους απειλών που αντιμετωπίζει ο οργανισμός και ο κλάδος του. Θεωρούμε ότι το κριτήριο καλύπτεται μερικώς.

Βάση δεδομένων για ευπάθειες

Το NIST SP 800-30 παρέχει καθοδήγηση για τη διενέργεια αξιολογήσεων επικινδυνότητας των πληροφοριακών συστημάτων, η οποία περιλαμβάνει τον εντοπισμό ευπαθειών ως μέρος της διαδικασίας αξιολόγησης. Περιγράφει ένα πλαίσιο διαχείρισης κινδύνου (RMF) το οποίο με τη σειρά του περιγράφει τον τρόπο με τον οποίο οι οργανισμοί πρέπει να εντοπίζουν τις ευπάθειες, να αξιολογούν την επικινδυνότητα που συνδέεται με την ευπάθεια, να αναπτύσσουν τα κατάλληλα μέτρα ασφαλείας και να τα εφαρμόζουν.
Παρέχει πίνακα με ένα σύνολο υποδειγματικών εισόδων για την εργασία του εντοπισμού ευπαθειών , ένα πίνακα με μια υποδειγματική κλίμακα αξιολόγησης για την αξιολόγηση της σοβαρότητας των εντοπισμένων ευπαθειών, και ένα πίνακα υπόδειγμα για τη σύνοψη/τεκμηρίωση των αποτελεσμάτων του εντοπισμού ευπαθειών.
Οι οργανισμοί είναι υπεύθυνοι για τη διενέργεια των δικών τους αξιολογήσεων επικινδυνότητας και τον εντοπισμό τυχόν ευπαθειών που αφορούν ειδικά τα συστήματα και τα περιβάλλοντά τους. Μπορούν να χρησιμοποιούν διάφορες πηγές, όπως συμβουλές ασφαλείας, δελτία ασφαλείας των προμηθευτών και άλλες σχετικές δημοσιεύσεις του κλάδου, για να εντοπίζουν και να ενημερώνονται για τις τελευταίες απειλές και ευπάθειες.

Συνολικά το NIST SP 800-30 δεν περιλαμβάνει ούτε παρέχει κατάλογο ή βάση δεδομένων ευπαθειών του συστήματος, παρέχει όμως τις κατάλληλες διαδικασίες για τον εντοπισμό την αξιολόγηση και την καταγραφή τους κάτι που θεωρητικά καλύπτει εν μέρει το κριτήριο.

Βάση δεδομένων για μέτρα ασφαλείας

Η ειδική έκδοση 800-30 του NIST δεν περιλαμβάνει κατάλογο μέτρων ασφαλείας ή αντιμέτρων. Παρέχει καθοδήγηση για τον τρόπο διενέργειας αξιολόγησης επικινδυνότητας συμπεριλαμβανομένου του τρόπου εντοπισμού και αξιολόγησης της επικινδυνότητας της ασφάλειας πληροφοριών και του τρόπου προσδιορισμού της κατάλληλης αντιμετώπισης της και όχι για συγκεκριμένα μέτρα ασφαλείας ή αντίμετρα. Για έναν ολοκληρωμένο κατάλογο ελέγχων ασφαλείας και αντιμέτρων, θα πρέπει κάποιος να ανατρέξει στο NIST SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations". Το κριτήριο δεν καλύπτεται καθόλου από το NIST SP 800-30.

Πλοήγηση σε περιστατικά

Το NIST SP 800-δεν περιγράφει κάποια συγκεκριμένη διαδικασία για την πλοήγηση σε περιστατικά. Η συγκεκριμένη δημοσίευση επικεντρώνεται στη διαδικασία διενέργειας αξιολογήσεων επικινδυνότητας όπως έχουμε ήδη αναφέρει και δεν παρέχει συγκεκριμένες διαδικασίες για τη διαχείριση του εντοπισμού, της αντιμετώπισης και της επίλυσης περιστατικών ασφαλείας σε έναν οργανισμό. Για έναν ολοκληρωμένο οδηγό σχετικά με τις διαδικασίες χειρισμού περιστατικών, σημείο αναφοράς είναι το NIST SP 800-61 Rev. 2, "Computer Security Incident Handling Guide".

Έλεγχος επιχειρηματικών διαδικασιών

Το NIST SP 800-30 δεν προβλέπει ούτε περιγράφει έλεγχο επιχειρηματικών διαδικασιών. Καλύπτει θέματα όπως η διαδικασία διαχείρισης επικινδυνότητας, οι πρακτικές αξιολόγησης επικινδυνότητας και οι απαιτήσεις υποβολής εκθέσεων. Δεν ασχολείται με τον έλεγχο επιχειρηματικών διαδικασιών. Για οδηγίες σχετικά με τη διενέργεια ελέγχων επιχειρησιακών διαδικασιών και την παρακολούθηση της ασφάλειας και του απορρήτου των πληροφοριακών συστημάτων, θα πρέπει να ανατρέξουμε στο NIST SP 800-53 Revision 5, "Security and Privacy Controls for Federal Information Systems and Organizations", Έλεγχοι ασφάλειας και απορρήτου για ομοσπονδιακά πληροφοριακά συστήματα και οργανισμούς. Το κριτήριο δεν καλύπτεται καθόλου.

Αναφορές και αναλύσεις

Το NIST SP 800-30 απαιτεί από τους οργανισμούς να τεκμηριώνουν και να υποβάλλουν εκθέσεις σχετικά με τις δραστηριότητες διαχείρισης της επικινδυνότητας, συμπεριλαμβανομένων των αποτελεσμάτων των αξιολογήσεων επικινδυνότητας. Το NIST SP 800-30 επικεντρώνεται στη διαδικασία διαχείρισης επικινδυνότητας και στις πρακτικές εκτίμησης επικινδυνότητας, συμπεριλαμβανομένης της τεκμηρίωσης και της αναφοράς των εκτιμήσεων επικινδυνότητας. Η οδηγία απαιτεί από τους οργανισμούς να παρέχουν πληροφορίες σχετικά με τους κινδύνους, τις ευπάθειες και τα αντίμετρα που εφαρμόζονται και να χρησιμοποιούν αυτές τις πληροφορίες για την υποστήριξη της λήψης αποφάσεων

και την κατανόηση της κατάστασης κινδύνου του οργανισμού. Οι εκθέσεις αξιολόγησης επικινδυνότητας που παράγονται στο πλαίσιο της διαδικασίας διαχείρισης επικινδυνότητας NIST SP 800-30 μπορούν να χρησιμοποιηθούν για την υποστήριξη δραστηριοτήτων αναφοράς και ανάλυσης και για τον εντοπισμό των τομέων όπου ο οργανισμός είναι πιο ευάλωτος και όπου απαιτούνται πρόσθετα μέτρα. Σύμφωνα με τα παραπάνω το κριτήριο θεωρείται ότι καλύπτεται πλήρως.

Επίπεδο τεχνικότητας

Το NIST SP 800-30 προορίζεται για χρήση από επαγγελματίες της ασφάλειας πληροφοριών και διαχειριστές συστημάτων πληροφορικής.
Θεωρείται ένα σχετικά λεπτομερές και τεχνικό έγγραφο και απαιτεί ένα ορισμένο επίπεδο τεχνικών γνώσεων για την κατανόηση και την αποτελεσματική εφαρμογή του.
Περιλαμβάνει επίσης μια σειρά από βήμα προς βήμα διαδικασίες για τη διενέργεια μιας αξιολόγησης κινδύνου, η οποία μπορεί να είναι αρκετά λεπτομερής και τεχνική.
Πρόκειται για έγγραφο καθοδήγησης και όχι για κανονισμό και το επίπεδο εφαρμογής των συστάσεων του εγγράφου μπορεί να ποικίλλει ανάλογα με τις ανάγκες, τους πόρους και την εμπειρογνωμοσύνη του οργανισμού όσον αφορά τη διαχείριση της επικινδυνότητας. Είναι σημαντικό να σημειωθεί ότι το NIST 800-30 δεν προορίζεται να είναι μια λύση που ταιριάζει σε όλους και οι οργανισμοί θα πρέπει να το προσαρμόσουν στις συγκεκριμένες ανάγκες τους. Το επίπεδο τεχνικότητας θεωρείται υψηλό.

Υποστήριξη και πόροι

Το SP 800-30 περιλαμβάνει τα ακόλουθα υποστηρικτικά υλικά και πόρους:

- Μια λεπτομερή διαδικασία βήμα προς βήμα για τη διεξαγωγή μιας αξιολόγησης της επικινδυνότητας, συμπεριλαμβανομένης της καθοδήγησης σχετικά με τον τρόπο εντοπισμού και ιεράρχησης των κινδύνων, τον τρόπο ανάλυσης και αξιολόγησής τους και τον τρόπο κοινοποίησης των αποτελεσμάτων στους σχετικούς ενδιαφερόμενους.
- Υποδείγματα και παραδείγματα εγγράφων αξιολόγησης κινδύνων, όπως εκθέσεις και σχέδια αξιολόγησης επικινδυνότητας, τα οποία μπορούν να χρησιμοποιηθούν ως σημείο εκκίνησης για τη διενέργεια αξιολόγησης κινδύνων.
- Γλωσσάριο βασικών όρων και ορισμών που χρησιμοποιούνται στον οδηγό, για να βοηθηθούν οι χρήστες να κατανοήσουν τη γλώσσα και τις έννοιες που χρησιμοποιούνται στον οδηγό.
- Πρόσθετες δημοσιεύσεις του NIST στις οποίες παραπέμπει ο οδηγός, οι οποίες παρέχουν πρόσθετες οδηγίες και πληροφορίες για συγκεκριμένα θέματα που σχετίζονται με την αξιολόγηση κινδύνου.

Τα περισσότερα από αυτά μπορούν να βρεθούν στο δικτυακό τόπο του NIST.
Το κριτήριο θεωρούμε ότι καλύπτεται πλήρως.

Πληρότητα

Το NIST SP 800-30 δεν καλύπτει όλους τους σχετικούς τομείς της επικινδυνότητας στο πλαίσιο της ασφάλειας των πληροφοριών, όπως ο σχεδιασμός της επιχειρησιακής

συνέχειας, η κανονιστική συμμόρφωση ή η φυσική ασφάλεια, οι οποίοι αποτελούν επίσης σημαντικούς τομείς της διαχείρισης επικινδυνότητας.
Η δημοσίευση προορίζεται να αποτελέσει σημείο εκκίνησης για τους οργανισμούς για τη δημιουργία ενός προγράμματος διαχείρισης επικινδυνότητας και να παρέχει καθοδήγηση σχετικά με κοινές πρακτικές διαχείρισης της. Οι οργανισμοί θα πρέπει επίσης να εξετάζουν πρόσθετες πηγές πληροφοριών και καθοδήγησης, όπως είναι οι κανονισμοί και τα πρότυπα που αφορούν συγκεκριμένο κλάδο, για να διασφαλίσουν ότι αντιμετωπίζουν πλήρως όλους τους σχετικούς τομείς επικινδυνότητας για το συγκεκριμένο περιβάλλον τους. (Συνιστάται η χρήση του NIST SP 800-30 ως οδηγού και η συμπλήρωσή του με άλλα σχετικά πρότυπα και βέλτιστες πρακτικές για να διασφαλιστεί μια ολοκληρωμένη προσέγγιση διαχείρισης κινδύνων.) Επιπλέον, οι οργανισμοί θα πρέπει να επανεξετάζουν και να επικαιροποιούν τακτικά το πρόγραμμα διαχείρισης επικινδυνότητας ώστε να διασφαλίζουν ότι παραμένει αποτελεσματικό και σχετικό με τις μεταβαλλόμενες ανάγκες και το περιβάλλον κινδύνων.
Το κριτήριο θεωρούμε ότι καλύπτεται εν μέρει από το NIST SP 800-30.

Χρόνος/Διάρκεια

Ο χρόνος που απαιτείται για την εφαρμογή του NIST SP 800-30 εξαρτάται από διάφορους παράγοντες, όπως το μέγεθος και η πολυπλοκότητα του οργανισμού, οι διαθέσιμοι πόροι και η κατάσταση του τρέχοντος προγράμματος διαχείρισης επικινδυνότητας του οργανισμού**. Η εφαρμογή ενός ολοκληρωμένου προγράμματος, μπορεί να διαρκέσει από μερικούς μήνες έως ένα έτος ή και περισσότερο, ανάλογα με τον οργανισμό.**
Σύμφωνα με τον ιστότοπο του NIST, δεν είναι δυνατόν να δοθεί ακριβές χρονοδιάγραμμα για την εφαρμογή, αλλά εκτιμάται ότι **οι περισσότεροι οργανισμοί θα πρέπει να είναι σε θέση να ολοκληρώσουν την εφαρμογή εντός 12 μηνών.**
Συνολικά θεωρείται σχετικά χρονοβόρο , οπότε το κριτήριο θεωρούμε ότι δεν καλύπτεται.

Οικονομικό κόστος

Η Ειδική Δημοσίευση 800-30 του Εθνικού Ινστιτούτου Προτύπων και Τεχνολογίας (NIST) "Οδηγός διαχείρισης κινδύνων για συστήματα τεχνολογίας πληροφοριών" είναι ένα δωρεάν έγγραφο που διατίθεται για λήψη από τον δικτυακό τόπο του NIST.
Ορισμένες πιθανές δαπάνες που πρέπει να ληφθούν υπόψη περιλαμβάνουν:

- Κόστος κατάρτισης των εργαζομένων και της διοίκησης σχετικά με το NIST SP 800-30 και τις απαιτήσεις του
- Αμοιβές συμβούλων για έναν διαπιστευμένο φορέα αξιολόγησης NIST SP 800-30 για τη διενέργεια αξιολόγησης και την παροχή καθοδήγησης σχετικά με τη συμμόρφωση
- Κόστος που σχετίζεται με την αντιμετώπιση τυχόν κενών στα τρέχοντα μέτρα ασφαλείας για την ικανοποίηση των απαιτήσεων του NIST SP 800-30.
- Συνεχές κόστος για τη διατήρηση της συμμόρφωσης με το πλαίσιο, όπως οι τακτικές αξιολογήσεις και η ενημέρωση των ελέγχων ασφαλείας

Το επίπεδο του κόστους θεωρείται μέτριο, διότι οι δαπάνες που σχετίζονται με το πλαίσιο είναι προαιρετικές, οπότε θεωρούμε το κριτήριο ότι καλύπτεται εν μέρει.

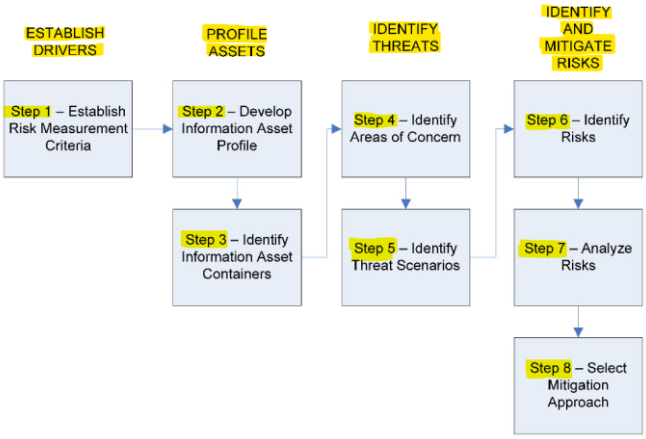
8) OCTAVE Allegro

Ιστορικό

Η μεθοδολογία OCTAVE Allegro, που δημοσιεύθηκε το 2007, αποτελεί την επόμενη γενιά της μεθόδου OCTAVE® - Operationally Critical Threat, Asset, and Vulnerability Evaluation- που δημιουργήθηκε από την Ομάδα Αντιμετώπισης Εκτάκτων Αναγκών για Υπολογιστές (CERT) του Ινστιτούτου Τεχνολογίας Λογισμικού, του τμήματος του Πανεπιστημίου Carnegie Mellon (ΗΠΑ).
Μαζί με τους προκατόχους της, OCTAVE και OCTAVE-S, η OCTAVE Allegro αποτελεί μια οικογένεια αξιολογήσεων OCTAVE. Όπως και οι OCTAVE και OCTAVE-S, η OCTAVE Allegro επικεντρώνεται στην τοποθέτηση της αξιολόγησης της επικινδυνότητας στο κατάλληλο οργανωτικό πλαίσιο, αλλά προσφέρει μια εναλλακτική προσέγγιση που στοχεύει ειδικά στα περιουσιακά στοιχεία πληροφοριών και την ανθεκτικότητά τους.

Επισκόπηση

Η OCTAVE Allegro έχει σχεδιαστεί για να επιτρέπει την ευρεία αξιολόγηση του περιβάλλοντος λειτουργικής επικινδυνότητας ενός οργανισμού, με στόχο την παραγωγή ισχυρών αποτελεσμάτων χωρίς να απαιτούνται εκτεταμένες γνώσεις αξιολόγησης επικινδυνότητας. Διαφέρει από τα προηγούμενα OCTAVE (OCTAVE και OCTAVE-S) γιατί εστιάζει κυρίως στα περιουσιακά στοιχεία πληροφοριών στο πλαίσιο του τρόπου χρήσης τους, του τόπου αποθήκευσης, μεταφοράς και επεξεργασίας τους και του τρόπου με τον οποίο εκτίθενται σε απειλές, ευπάθειες και διαταραχές.
Η προσέγγιση OCTAVE Allegro αποτελείται από οκτώ βήματα που οργανώνονται σε τέσσερις φάσεις, όπως απεικονίζεται στην εικόνα 5.



Εικόνα 11: Τα οκτώ βήματα και οι τέσσερις φάσεις της μεθοδολογίας Octave Allegro

Φάση 1 → Καθορισμός οδηγών - Η περιοχή αυτή περιλαμβάνει μόνο το πρώτο βήμα μέσω του οποίου ο οργανισμός αναπτύσσει **κριτήρια μέτρησης επικινδυνότητας** που συνάδουν με τους οργανωτικούς οδηγούς. Αυτοί οι οδηγοί θα χρησιμοποιηθούν για την αξιολόγηση των επιπτώσεων της επικινδυνότητας στην αποστολή και τους στόχους του οργανισμού.

Φάση 2 → Προφίλ περιουσιακών στοιχείων - Η περιοχή αυτή περιλαμβάνει τα βήματα 2 και 3, μέσω των οποίων δημιουργούνται τα **προφίλ των περιουσιακών στοιχείων πληροφοριών**. Αφού προσδιοριστούν και δημιουργηθούν τα προφίλ, **προσδιορίζονται τα «δοχεία» των περιουσιακών στοιχείων** και αποτυπώνεται το προφίλ για κάθε περιουσιακό στοιχείο. Ένα προφίλ αντιπροσωπεύει ένα πληροφοριακό περιουσιακό στοιχείο που περιγράφει τα μοναδικά χαρακτηριστικά, τις ιδιότητες, τα χαρακτηριστικά και την αξία του. (Ως δοχεία θεωρούνται οι τοποθεσίες όπου το περιουσιακό στοιχείο αποθηκεύεται, μεταφέρεται ή επεξεργάζεται).
Φάση 3 → Προσδιορισμός απειλών - Ο τομέας αυτός περιλαμβάνει τα βήματα 4 και 5, όπου **οι απειλές για τα περιουσιακά στοιχεία πληροφοριών προσδιορίζονται και τεκμηριώνονται** μέσω μιας δομημένης διαδικασίας. Σε αυτή την κατηγορία, οι προβληματικές περιοχές παρουσιάζουν σενάρια πραγματικού κόσμου που μπορούν να συμβούν σε οργανισμούς, και εντοπίζονται σενάρια απειλών που περιέχουν πρόσθετες απειλές.
Φάση 4 → Προσδιορισμός και μετριασμός της επικινδυνότητας - Αυτό είναι το τελευταίο στάδιο της αξιολόγησης της επικινδυνότητας. Σε αυτή την κατηγορία **εντοπίζονται και αναλύονται οι επικινδυνότητες** με βάση τις πληροφορίες για τις απειλές και **αναπτύσσονται στρατηγικές μετριασμού** για την αντιμετώπιση τους. Σε αυτό το στάδιο θα αναλυθούν και θα μετριαστούν οι απειλές που εντοπίστηκαν στην προηγούμενη κατηγορία.

Χρηστικότητα

Η μεθοδολογία OCTAVE Allegro θεωρείται ότι είναι εύχρηστη στο πλαίσιο της διαχείρισης επικινδυνότητας της ασφάλειας των πληροφοριών. Είναι γνωστή για τις σαφείς οδηγίες, τις κατευθυντήριες γραμμές και τη φιλική προς το χρήστη διεπαφή για την τεκμηρίωση και την υποβολή εκθέσεων σχετικά με τη διαδικασία διαχείρισης επικινδυνότητας. Μπορεί επίσης να ενσωματωθεί εύκολα στις υπάρχουσες διαδικασίες και συστήματα ενός οργανισμού, καθιστώντας την ένα προσιτό και πρακτικό εργαλείο για τη διαχείριση της επικινδυνότητας της ασφάλειας πληροφοριών. Προσφέρει χαρακτηριστικά όπως διαχείριση έργων και εργασιών, διαχείριση πόρων, διακυβέρνηση, συνεργασία και ανάλυση. Είναι σχεδιασμένο για χρήση σε μεγάλους οργανισμούς και γενικά θεωρείται **ότι είναι μια χρηστική μεθοδολογία.**

Ευελιξία

Η μεθοδολογία OCTAVE Allegro θεωρείται ευέλικτη. Παρέχει ένα ευέλικτο πλαίσιο που μπορεί να προσαρμοστεί ώστε να ανταποκρίνεται στις συγκεκριμένες ανάγκες και απαιτήσεις ενός οργανισμού. Η μεθοδολογία μπορεί να προσαρμοστεί ώστε να αντικατοπτρίζει τις πολιτικές και τους στόχους διαχείρισης επικινδυνότητας ενός οργανισμού, καθώς και την τρέχουσα κατάσταση επικινδυνότητας και το επίπεδο ωριμότητάς του.
Η ευελιξία του OCTAVE Allegro επιτρέπει επίσης στους οργανισμούς να αναβαθμίζουν και να βελτιώνουν συνεχώς τις διαδικασίες διαχείρισης επικινδυνότητας με την πάροδο του χρόνου, καθώς αναδύονται νέοι κίνδυνοι και αλλάζει η στάση τους. Αυτό διασφαλίζει ότι η μεθοδολογία παραμένει σχετική και αποτελεσματική στην προστασία του οργανισμού από τις εξελισσόμενες απειλές ασφάλειας.

Επιπλέον, το OCTAVE Allegro μπορεί να χρησιμοποιηθεί σε διάφορους κλάδους, καθιστώντας το ένα ευέλικτο εργαλείο που μπορεί να εφαρμοστεί σε διαφορετικά πλαίσια και καταστάσεις. Σύμφωνα με τα παραπάνω το κριτήριο καλύπτεται πλήρως.

Διαχείριση περιουσιακών στοιχείων

Η μέθοδος OCTAVE Allegro διαχειρίζεται πλήρως τα περιουσιακά στοιχεία ενός οργανισμού δίνοντας μεγαλύτερη έμφαση στα περιουσιακά στοιχεία των πληροφοριών. Όλα τα άλλα περιουσιακά στοιχεία που είναι σημαντικά για τον οργανισμό προσδιορίζονται και αξιολογούνται στο πλαίσιο των περιουσιακών στοιχείων πληροφοριών με τα οποία συνδέονται. Με τον τρόπο αυτό εξαλείφεται η πιθανή σύγχυση σχετικά με το πεδίο εφαρμογής και μειώνεται η πιθανότητα να πραγματοποιηθεί εκτεταμένη συλλογή και ανάλυση δεδομένων για περιουσιακά στοιχεία που αργότερα διαπιστώνονται να είναι ανεπαρκώς καθορισμένα, εκτός του πεδίου εφαρμογής της αξιολόγησης, ή να χρειάζονται περαιτέρω ανάλυση.
Στο βήμα 2 ξεκινά τη διαδικασία δημιουργίας ενός προφίλ για τα εν λόγω περιουσιακά στοιχεία. Ένα προφίλ είναι μια αναπαράσταση ενός πληροφοριακού περιουσιακού στοιχείου που περιγράφει τα μοναδικά χαρακτηριστικά, τις ιδιότητες, τα χαρακτηριστικά και την αξία του. Η διαδικασία δημιουργίας προφίλ της μεθοδολογίας διασφαλίζει ότι ένα περιουσιακό στοιχείο περιγράφεται με σαφήνεια και συνέπεια, ότι υπάρχει ένας σαφής ορισμός των ορίων του περιουσιακού στοιχείου και ότι οι απαιτήσεις ασφαλείας για το περιουσιακού στοιχείου είναι επαρκώς καθορισμένες. Το προφίλ για κάθε περιουσιακό στοιχείο αποτυπώνεται σε ένα ενιαίο φύλλο εργασίας το οποίο αποτελεί τη βάση για τον προσδιορισμό των απειλών και της επικινδυνότητας στα επόμενα βήματα. Αυτό το κριτήριο καλύπτεται πλήρως από το OCTAVE Allegro.

Βάση δεδομένων για απειλές

Η μεθοδολογία δεν παρέχει κάποιον προκαθορισμένο κατάλογο ή μια βάση δεδομένων για τις απειλές, αντίθετα επικεντρώνεται στον εντοπισμό πιθανών απειλών μέσω μιας συστηματικής και ενδελεχούς ανάλυσης των πληροφοριακών συστημάτων ενός οργανισμού, καθώς και του περιβάλλοντος και των λειτουργιών του.
Το OCTAVE Allegro χρησιμοποιεί ερωτηματολόγια σεναρίων απειλών για να βοηθήσει τους χρήστες να εντοπίσουν τις απειλές που σχετίζονται με ένα περιουσιακό στοιχείο πληροφοριών. Αυτά τα ερωτηματολόγια βασίζονται στα δέντρα απειλών που περιλαμβάνονται στη μέθοδο OCTAVE και έτσι εξασφαλίζουν μια ευρεία εξέταση των πιθανών απειλών.
Τα ερωτηματολόγια είναι σχεδιασμένα γύρω από την έννοια του «δοχείου» για να εστιάζουν τους χρήστες στις απειλές που αφορούν ένα περιουσιακό στοιχείο πληροφοριών όταν αυτό αποθηκεύεται, μεταφέρεται ή επεξεργάζεται σε ένα συγκεκριμένο περιέκτη. Αυτό απλοποιεί τη δομή του ερωτηματολογίου και μειώνει το συνολικό χρόνο που απαιτείται για την καταγραφή μιας αξιόπιστης συλλογής πιθανών απειλών.
Το κριτήριο θωρούμε ότι καλύπτεται μερικώς.

Βάση δεδομένων για ευπάθειες

Η μεθοδολογία δεν διαθέτει λίστα ή βάση δεδομένων για ευπάθειες. Σύμφωνα με την τεκμηρίωση της μεθοδολογίας η χρήση και η εκτέλεση εργαλείων εντοπισμού ευπαθειών, καθώς και η ανάλυση των αποτελεσμάτων αυτών των εργαλείων, είναι απαιτητικές και δυσκίνητες εργασίες ακόμη και για οργανισμούς που εκτελούν αυτές τις εργασίες σε μια σε τακτική βάση.
Σύμφωνα με το OCTAVE Allegro μόνο μέσω της ανάλυσης των πιθανών αποτελεσμάτων και των επιπτώσεων μπορούν οι ευπάθειες να θεωρηθούν κίνδυνοι που πρέπει να αντιμετωπιστούν. **Η απαίτηση για την εκτέλεση εργαλείων εντοπισμού ευπαθειών για την ολοκλήρωση της τεχνολογικής θεώρησης της επικινδυνότητας εξαλείφεται στο OCTAVE Allegro και γι' αυτό δεν παρέχεται ούτε παράγεται κάποια λίστα με ευπάθειες.** Ωστόσο, εάν ένας οργανισμός διαθέτει μια κεντρική διαδικασία στον εντοπισμό ευπαθειών με βάση εργαλεία, μπορεί εύκολα να ενσωματωθεί σε διάφορες διαδικασίες του OCTAVE Allegro για να παρέχει μια πιο ισχυρή διατύπωση της επικινδυνότητας.
Το OCTAVE Allergro δεν καλύπτει αυτό το κριτήριο.

Βάση δεδομένων για μέτρα ασφαλείας

Η μεθοδολογία OCTAVE δεν περιλαμβάνει συγκεκριμένο κατάλογο ή διαδικασία που να περιλαμβάνει βάση δεδομένων για μέτρα ασφαλείας ή αντίμετρα.
Ωστόσο, ως μέρος της μεθοδολογίας της το OCTAVE Allegro παρέχει διάφορα πρότυπα και παραδείγματα που μπορούν να χρησιμοποιηθούν για την τεκμηρίωση της διαδικασίας αξιολόγησης και τον προσδιορισμό των σχετικών μέτρων ασφάλειας πληροφοριών.
Επιπλέον, ο οργανισμός μπορεί να χρησιμοποιήσει εξωτερικούς πόρους, όπως πρότυπα όπως τα NIST, ISO και COBIT για πιθανά μέτρα ασφαλείας και αντίμετρα.
Συνολικά θεωρούμε ότι δεν καλύπτεται αυτό το κριτήριο.

Πλοήγηση σε περιστατικά

Δεν διαθέτει συγκεκριμένη διαδικασία για την πλοήγηση σε περιστατικά, ούτε παρέχει οδηγίες για την αντιμετώπιση και τη διαχείριση περιστατικών.
Σύμφωνα με τη μέθοδο OCTAVE Allegro, οι οργανισμοί θα πρέπει να διαθέτουν ένα καλά καθορισμένο σχέδιο αντιμετώπισης περιστατικών και να δοκιμάζουν και να εξασκούνται τακτικά στις διαδικασίες αντιμετώπισης περιστατικών, ώστε να διασφαλίζουν ότι είναι προετοιμασμένοι να ανταποκρίνονται αποτελεσματικά σε περιστατικά ασφαλείας. Η μέθοδος συνιστά επίσης να διαθέτουν οι οργανισμοί μια ειδική ομάδα αντιμετώπισης περιστατικών και να διαθέτουν διαδικασίες για τον εντοπισμό, την ταξινόμηση και την αντιμετώπιση περιστατικών ασφαλείας.
Συνολικά δεν καλύπτεται αυτό το κριτήριο.

Έλεγχος επιχειρηματικών διαδικασιών

Το OCTAVE Allegro έχει σχεδιαστεί για να ενσωματωθεί στο συνολικό πρόγραμμα διαχείρισης κινδύνων ενός οργανισμού και μπορεί να χρησιμοποιηθεί για την υποστήριξη του ελέγχου των επιχειρηματικών διαδικασιών μέσω του εντοπισμού και του μετριασμού της επικινδυνότητας ασφάλειας πληροφοριών.

Η μεθοδολογία OCTAVE μπορεί να χρησιμοποιηθεί για την αξιολόγηση της ασφάλειας των συστημάτων πληροφορικής, των υποδομών και των δεδομένων που υποστηρίζουν τις επιχειρηματικές διαδικασίες του οργανισμού και μπορεί να βοηθήσει τον οργανισμό να κατανοήσει πώς οι κίνδυνοι ασφάλειας μπορούν να επηρεάσουν την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των κρίσιμων επιχειρηματικών διαδικασιών. Έτσι, μπορεί να χρησιμοποιηθεί ως εργαλείο για τον εντοπισμό ευπαθειών στην επιχειρησιακή διαδικασία και την ανάπτυξη αντιμέτρων για την ελαχιστοποίηση του κινδύνου, τα οποία μπορούν να θεωρηθούν ως μια μορφή ελέγχου της επιχειρησιακής διαδικασίας.
Συνολικά, το κριτήριο καλύπτεται πλήρως.

Αναφορές και αναλύσεις

Το πλαίσιο OCTAVE Allegro παρέχει δυνατότητες αναφοράς και ανάλυσης. Επιτρέπει στους οργανισμούς να δημιουργούν αναφορές που παρέχουν πληροφορίες σχετικά με την αποτελεσματικότητα των μέτρων ασφάλειας των πληροφοριών τους, να παρακολουθούν την πρόοδο και να παρέχουν επίσης τα απαραίτητα έγγραφα για σκοπούς συμμόρφωσης και κανονιστικούς σκοπούς. Το πλαίσιο περιλαμβάνει από οδηγίες, φύλλα εργασίας και ερωτηματολόγια, που μπορούν να χρησιμοποιήσουν οι οργανισμοί για να καθοδηγήσουν τις αξιολογήσεις επικινδυνότητας και να τεκμηριώσουν τα αποτελέσματά τους. Το κριτήριο καλύπτεται πλήρως.

Επίπεδο τεχνικότητας

Η μεθοδολογία OCTAVE Allegro **έχει σχεδιαστεί για χρήση από μη τεχνικό προσωπικό και δεν απαιτεί υψηλό επίπεδο τεχνικών γνώσεων** και είναι κατάλληλο για χρήση από άτομα που θέλουν να εκτελέσουν αξιολόγηση κινδύνου χωρίς εκτεταμένη οργανωτική συμμετοχή, εμπειρογνωμοσύνη ή συνεισφορά. Η μεθοδολογία εστιάζει στην οργανωτική διαδικασία και δομή για τη διαχείριση της επικινδυνότητας της ασφάλειας πληροφοριών και όχι σε συγκεκριμένες τεχνικές λεπτομέρειες. **Ωστόσο, η εμπλοκή τεχνικών εμπειρογνωμόνων μπορεί να είναι απαραίτητη** σε ορισμένα στάδια της διαδικασίας, όπως η διενέργεια εκτιμήσεων επικινδυνότητας , η αξιολόγηση των μέτρων ασφαλείας ή η αντιμετώπιση περιστατικών. Συνολικά το επίπεδο τεχνικότητας που απαιτεί η μεθοδολογία θεωρείται μέτριο , οπότε θεωρούμε ότι το κριτήριο καλύπτεται μερικώς.

Υποστήριξη και πόροι

Η μεθοδολογία OCTAVE Allegro περιλαμβάνει υποστηρικτικό υλικό και πόρους που βοηθούν τους χρήστες να κατανοήσουν και να χρησιμοποιήσουν σωστά το πλαίσιο
Το υποστηρικτικό υλικό για τη μεθοδολογία OCTAVE Allegro περιλαμβάνει:

- Οδηγίες χρήσης και εγχειρίδια: Λεπτομερείς οδηγίες και επεξηγήσεις των διαφόρων βημάτων που εμπλέκονται στη διαδικασία OCTAVE Allegro, καθώς και πρακτικές οδηγίες για την αποτελεσματική χρήση του πλαισίου.

- Πρότυπα: Προκατασκευασμένα έντυπα, φύλλα εργασίας και λίστες ελέγχου που μπορούν να χρησιμοποιηθούν για την τεκμηρίωση διαφόρων πτυχών της μεθοδολογίας, όπως οι αξιολογήσεις επικινδυνότητας, τα μέτρα ασφαλείας και οι απαντήσεις σε περιστατικά.

- Εργαλειοθήκες: Σύνολα εργαλείων και πόρων που μπορούν να χρησιμοποιηθούν για την αυτοματοποίηση ορισμένων τμημάτων της διαδικασίας OCTAVE Allegro, όπως η αξιολόγηση κινδύνων και η επιλογή μέτρων.

- Εκπαιδευτικό υλικό: Διαφάνειες, παρουσιάσεις και άλλοι εκπαιδευτικοί πόροι που μπορούν να χρησιμοποιηθούν για την παροχή εκπαίδευσης σχετικά με τη μεθοδολογία OCTAVE Allegro, συμπεριλαμβανομένων των βασικών εννοιών, των διαδικασιών και των βέλτιστων πρακτικών της.

- Μελέτες περιπτώσεων και παραδείγματα: Παραδείγματα από τον πραγματικό κόσμο για το πώς η μεθοδολογία OCTAVE Allegro έχει εφαρμοστεί σε διάφορους οργανισμούς, αναδεικνύοντας τις προκλήσεις, τις επιτυχίες και τα διδάγματα που αποκομίστηκαν.

Συνολικά, θεωρούμε ότι το κριτήριο καλύπτεται πλήρως.

Πληρότητα

Το επίπεδο πληρότητας της μεθοδολογίας OCTAVE Allegro θεωρείται υψηλό. Πρόκειται για ένα ολοκληρωμένο πλαίσιο που καλύπτει όλους τους σχετικούς τομείς κινδύνου στη διαχείριση της επικινδυνότητας της ασφάλειας των πληροφοριών, παρέχοντας μια συστηματική και δομημένη προσέγγιση για τον εντοπισμό, την αξιολόγηση, την ιεράρχηση και τη διαχείριση της επικινδυνότητας της ασφάλειας των πληροφοριών.
Η μεθοδολογία είναι καθιερωμένη και χρησιμοποιείται από οργανισμούς σε όλο τον κόσμο εδώ και πολλά χρόνια. Η αποτελεσματικότητά της όσον αφορά τη βοήθεια που παρέχει στους οργανισμούς για τη διαχείριση της επικινδυνότητας της ασφάλειας των πληροφοριών έχει αποδειχθεί μέσω της επιτυχημένης εφαρμογής και χρήσης της.

Χρόνος/Διάρκεια

Η χρονική αποτελεσματικότητα της μεθοδολογίας εξαρτάται από διάφορους παράγοντες, όπως το μέγεθος του οργανισμού, ο αριθμός των περιουσιακών στοιχείων που πρέπει να αξιολογηθούν, το επίπεδο λεπτομέρειας που απαιτείται και οι διαθέσιμοι πόροι για τη διεξαγωγή της αξιολόγησης. Κατά μέσο όρο, η εφαρμογή του OCTAVE ALLEGRO μπορεί να διαρκέσει **από μερικές εβδομάδες έως αρκετούς μήνες** για να ολοκληρωθεί. Ωστόσο, η ακριβής διάρκεια εξαρτάται από τις συγκεκριμένες ανάγκες και τους στόχους του οργανισμού, καθώς και από το επίπεδο εμπειρίας των ατόμων που διεξάγουν την αξιολόγηση. Σύμφωνα με τα παραπάνω θεωρούμε ότι το κριτήριο καλύπτεται πλήρως.

Οικονομικό κόστος

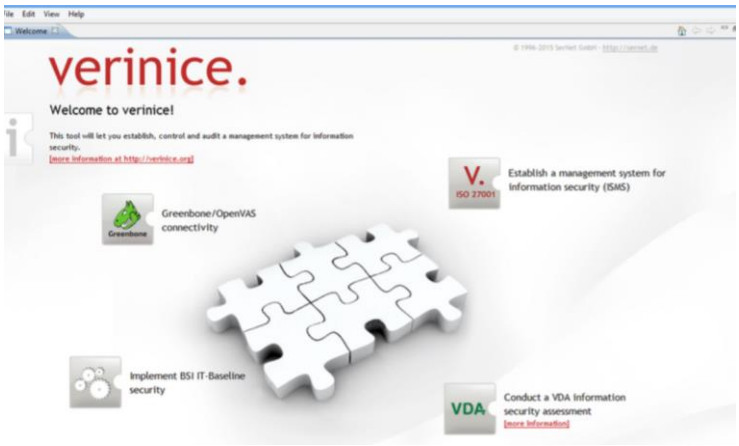
Η μεθοδολογία OCTAVE Allegro δεν είναι δωρεάν. Πρόκειται για ένα εμπορικό προϊόν που αναπτύχθηκε από το τμήμα CERT του Ινστιτούτου Τεχνολογίας Λογισμικού (SEI) του Πανεπιστημίου Carnegie Mellon.
Οι οργανισμοί που ενδιαφέρονται να χρησιμοποιήσουν τη μεθοδολογία πρέπει να αγοράσουν μια άδεια χρήσης και να παρακολουθήσουν μια εκπαιδευτική συνεδρία για να μάθουν πώς να χρησιμοποιούν τη μεθοδολογία. Επιπλέον θα πρέπει να αγοράσουν την

εργαλειοθήκη OCTAVE Allegro και να πληρώσουν για την υποστήριξη της μεθοδολογίας προκειμένου να τη χρησιμοποιήσουν. Το κόστος για την εργαλειοθήκη και την υποστήριξη μπορεί να ποικίλλει ανάλογα με τις ανάγκες του οργανισμού και το μέγεθος της αξιολόγησης . Συνολικά το οικονομικό κόστος που σχετίζεται με τη χρήση και την εφαρμογής του OCTAVE Allegro θεωρείται υψηλό, οπότε το κριτήριο δεν καλύπτεται καθόλου.

9) Verinice - Risk Management Tool

Ιστορικό

Το εργαλείο διαχείρισης επικινδυνότητας Verinice είναι ένα γερμανικό προϊόν λογισμικού που είναι διαθέσιμο για χρήση από το 2009. Το εργαλείο αναπτύχθηκε από το Γερμανικό Ομοσπονδιακό Γραφείο Ασφάλειας Πληροφοριών (BSI) και έχει σχεδιαστεί για να υποστηρίζει τους οργανισμούς στη διαχείριση της επικινδυνότητας της ασφάλειας πληροφοριών. Το Verinice έχει επικαιροποιηθεί και βελτιωθεί με την πάροδο των ετών, ώστε να ανταποκρίνεται στις εξελισσόμενες ανάγκες των οργανισμών. Η διεπαφή χρήστη του εργαλείου Verinice φαίνεται στην εικόνα 12.



Εικόνα 12: Το user interface του Verinice

Επισκόπηση

Το Verinice είναι ένα ευρέως αναγνωρισμένο εργαλείο διαχείρισης κινδύνων ανοικτού κώδικα που χρησιμοποιείται για τη διακυβέρνηση και τη συμμόρφωση της πληροφορικής. Πρόκειται για ένα εργαλείο ISMS που μπορεί να χρησιμοποιηθεί για την εκτέλεση μιας πλήρους ανάλυσης της επικινδυνότητας των περιουσιακών στοιχείων πληροφοριών, τον εντοπισμό και τη διαχείριση της επικινδυνότητας που σχετίζονται με την προστασία των δεδομένων, την ασφάλεια συστημάτων πληροφορικής και τη συμμόρφωση με κανονισμούς όπως ο GDPR και το ISO 27001.

Συνοπτικά οι λειτουργίες που παρέχει είναι :

Αξιολόγηση κινδύνου (Risk Assessment) : Το Verinice επιτρέπει την εκτέλεση μίας πλήρους ανάλυσης επικινδυνότητας των περιουσιακών στοιχείων πληροφοριών και τη δυνατότητα άντλησης περαιτέρω ενεργειών από τα αποτελέσματα.

Μητρώο περιουσιακών στοιχείων (Asset Register) : Δυνατότητα σύνδεσης των περιουσιακών στοιχείων με διαδικασίες, ιδιοκτήτες διαδικασιών και άλλα περιουσιακά στοιχεία. Το Verinice έχει τη δυνατότητα να κληρονομεί αυτόματα τις τιμές των επιχειρηματικών επιπτώσεων σε ένα δέντρο περιουσιακών στοιχείων. Πρόσθετες

λειτουργίες φιλτραρίσματος και επεξεργασίας, όπως ο μαζικός επεξεργαστής, απλοποιούν περαιτέρω την καθημερινή εργασία.

Αξιολόγηση ασφάλειας πληροφοριών (Information Security Assessment, ISA): Ερωτηματολόγια όπως το Information Security Assessment (ISA) της Γερμανικής Ένωσης Βιομηχανίας Αυτοκινήτου (VDA) προσφέρουν μια καθοδηγούμενη αυτοαξιολόγηση με βάση το ISO 27002.

Βασική γραμμή προστασίας (IT Baseline Protection) : Η verinice έχει χορηγήσει άδεια χρήσης για το Compendium IT Baseline Protection το οποίο έχει σκοπό να διασφαλίσει ένα ελάχιστο επίπεδο ασφάλειας για τα πληροφοριακά συστήματα που χρησιμοποιούνται από τις ομοσπονδιακές υπηρεσίες και να προωθήσει τη συνεπή εφαρμογή των μέτρων ασφαλείας σε ολόκληρο τον τομέα .

Έγγραφα και αρχεία (Documents and Records) : Το verinice απλοποιεί τη διαχείριση της τεκμηρίωσης ενός ISMS. Τα έγγραφα μπορούν είτε να αποθηκεύονται απευθείας σε μία βάση δεδομένων του Verinice είτε να παραπέμπουν μέσω URL σε εξωτερικές πηγές (DMS, wiki κ.λπ.).

Αναφορές (Reporting) : Παρέχεται η δυνατότητα δημιουργίας αναφορών για τους ελεγκτές, τη διοίκηση, τους ιδιοκτήτες των διαδικασιών και η σύνταξη εγγράφων αναφοράς για τη διαδικασία πιστοποίησης. Οι εκθέσεις της verinice χρησιμοποιούνται για την τεκμηρίωση καθώς και για την υποστήριξη της λήψης αποφάσεων και του σχεδιασμού. Υποδεικνύουν την κατάσταση της ασφάλειας πληροφοριών σε έναν οργανισμό με πίνακες και διαγράμματα.

Διεπαφές (Interfaces) : Η κύρια ιδέα του verinice είναι να είναι ανοιχτό. Το εργαλείο δημοσιεύεται ως λογισμικό ανοικτού κώδικα, χρησιμοποιεί ανοικτά πρότυπα και παρέχει πολλές διεπαφές. Η ενσωμάτωση του verinice με ένα ανοικτό σύστημα αξιολόγησης ευπαθειών (OpenVAS), όπως το Greenbone Security Manager (GSM), προωθεί τις σαρώσεις ευπαθειών σε μια κεντρικά ελεγχόμενη διαδικασία διαχείρισης ευπαθειών.

Έλεγχοι & Πιστοποιήσεις (Audits & Certifications) : Το verinice επιτρέπει αποτελεσματικούς και βιώσιμους ελέγχους. Τυποποιημένοι κατάλογοι, όπως το ISO 27001 ή το πλήρες περιεχόμενο των καταλόγων BSI IT Baseline Protection Catalogs, είναι έτοιμοι προς χρήση.

Χρηστικότητα

Το εργαλείο θεωρείται ευέλικτο, φιλικό προς το χρήστη και μπορεί να επεκταθεί ανάλογα με τις απαιτήσεις και τα σενάρια χρήσης, γεγονός που το καθιστά μια καλή επιλογή για οργανισμούς κάθε μεγέθους. Πρόκειται για ένα εργαλείο ISMS (Σύστημα διαχείρισης ασφάλειας πληροφοριών) ανοικτού κώδικα που μπορεί να χρησιμοποιηθεί για την εκτέλεση πλήρους ανάλυσης επικινδυνότητας των περιουσιακών στοιχείων πληροφοριών, τον εντοπισμό και τη διαχείριση κινδύνων που σχετίζονται με την προστασία των δεδομένων, την ασφάλεια πληροφοριακών συστημάτων και τη συμμόρφωση με κανονισμούς όπως ο GDPR και το ISO 27001.
Ωστόσο, πρόκειται για ένα εργαλείο ανοικτού κώδικα και η υποστήριξη και η συντήρηση εξαρτώνται από την κοινότητα που βρίσκεται πίσω από αυτό, γεγονός που μπορεί να

αποτελέσει περιορισμό για ορισμένους οργανισμούς. Επιπλέον, το εργαλείο ενδέχεται να στερείται ορισμένων χαρακτηριστικών που συνήθως συναντώνται σε εμπορικά εργαλεία, όπως οι προηγμένες δυνατότητες υποβολής εκθέσεων και η παρακολούθηση σε πραγματικό χρόνο. Συνολικά η χρηστικότητα του εργαλείου θεωρείται μέτρια.

Ευελιξία

Το Verinice είναι ένα ευέλικτο εργαλείο διαχείρισης επικινδυνότητας που μπορεί να προσαρμοστεί στις συγκεκριμένες ανάγκες ενός οργανισμού. Προσφέρει μια ποικιλία χαρακτηριστικών και δυνατοτήτων που μπορούν να διαμορφωθούν ώστε να υποστηρίζουν διαφορετικούς τύπους διαδικασιών διαχείρισης επικινδυνότητας και μπορεί να ενσωματωθεί με άλλα εργαλεία και συστήματα.
Ορισμένοι από τους τρόπους με τους οποίους το Verinice είναι ευέλικτο περιλαμβάνουν:

- Προσαρμόσιμη διαδικασία διαχείρισης επικινδυνότητας: Το εργαλείο επιτρέπει στους οργανισμούς να καθορίζουν τις δικές τους μεθοδολογίες και διαδικασίες διαχείρισης επικινδυνότητας.
- Επεκτάσιμο μοντέλο δεδομένων: Το μοντέλο δεδομένων που χρησιμοποιεί το Verinice είναι επεκτάσιμο, πράγμα που σημαίνει ότι μπορεί να προσαρμοστεί ώστε να ανταποκρίνεται στις ειδικές απαιτήσεις διαφορετικών τύπων περιουσιακών στοιχείων και επικινδυνότητας.
- Διαμορφώσιμες αναφορές και αναλύσεις: Το εργαλείο παρέχει υποστήριξη για την υποβολή εκθέσεων και την ανάλυση, η οποία μπορεί να διαμορφωθεί έτσι ώστε να ανταποκρίνεται στις ανάγκες διαφορετικών χρηστών και ενδιαφερομένων μερών.
- Εισαγωγή και εξαγωγή δεδομένων: Το Verinice επιτρέπει την εισαγωγή και εξαγωγή δεδομένων, γεγονός που επιτρέπει στους οργανισμούς να ενσωματώνουν το εργαλείο με άλλα συστήματα και να πραγματοποιούν περαιτέρω ανάλυση με τη χρήση εξωτερικών εργαλείων.
- Προσαρμόσιμοι ρόλοι και δικαιώματα χρηστών: Το Verinice επιτρέπει τη δημιουργία προσαρμοσμένων ρόλων και δικαιωμάτων χρηστών, επιτρέποντας στους οργανισμούς να ελέγχουν την πρόσβαση στο εργαλείο με βάση τους ρόλους και τις αρμοδιότητες των χρηστών.

Το κριτήριο θεωρούμε ότι καλύπτεται πλήρως.

Διαχείριση περιουσιακών στοιχείων

Το Verinice διαθέτει μια συγκεκριμένη διαδικασία για τη διαχείριση περιουσιακών στοιχείων. Συγκεκριμένα παρέχει μια ενότητα που επιτρέπει στους οργανισμούς να τεκμηριώνουν και να διαχειρίζονται τα περιουσιακά τους στοιχεία, συμπεριλαμβανομένων πληροφοριών σχετικά με τη θέση, τον ιδιοκτήτη, την αξία και την κρισιμότητα κάθε περιουσιακού στοιχείου. Επιτρέπει επίσης τη σύνδεση των περιουσιακών στοιχείων με ευπάθειες, απειλές και κινδύνους, την παρακολούθηση των περιουσιακών στοιχείων, την εκτέλεση αξιολογήσεων ευπάθειας και δοκιμών διείσδυσης και τη σύνδεση των ευπαθειών με τους κινδύνους και τα περιουσιακά στοιχεία, γεγονός που βοηθά τους οργανισμούς να ιεραρχούν τις προσπάθειες μετριασμού της επικινδυνότητας και να λαμβάνουν τεκμηριωμένες αποφάσεις σχετικά με την κατανομή των πόρων. Το Verinice καλύπτει πλήρως το κριτήριο .

Βάση δεδομένων για απειλές

Το Verinice παρέχει παραδείγματα απειλών που πρέπει να ληφθούν υπόψη, αν και μπορεί να μην αποτελεί πλήρη κατάλογο απειλών. Επιτρέπει όμως στους χρήστες να προσθέτουν απειλές και ευπάθειες από διάφορες υπάρχουσες πηγές, όπως ένας σαρωτής ευπαθειών ή ένα τεστ διείσδυσης, και να χρησιμοποιούν τα αποτελέσματα στην ανάλυση επικινδυνότητας για να εκτελούν αυτόματα μια αξιολόγηση κινδύνου για όλα τα περιουσιακά στοιχεία ενός οργανισμού. Συνολικά θεωρούμε ότι το κριτήριο δεν καλύπτεται, εφ' όσον δεν προβλέπεται συγκεκριμένη διαδικασία διαχείρισης των απειλών που μπορεί να αντιμετωπίσει ένας οργανισμός.

Βάση δεδομένων για ευπάθειες

Το Verinice δεν περιλαμβάνει μια βάση δεδομένων ευπαθειών καθεαυτή, αλλά μπορεί να ενσωματωθεί με άλλα εργαλεία και πλατφόρμες για την εισαγωγή δεδομένων ευπαθειών, όπως η Εθνική Βάση Δεδομένων Ευπαθειών (NVD) και η Common Vulnerabilities and Exposures (CVE). Συνολικά θεωρούμε ότι το κριτήριο δεν καλύπτεται.

Βάση για μέτρα ασφαλείας

Το Verinice περιλαμβάνει μια βάση δεδομένων με μέτρα ασφαλείας και αντίμετρα για τη διαχείριση της ασφάλειας των πληροφοριών. Το εργαλείο υποστηρίζει διάφορα πρότυπα και κανονισμούς, όπως το ISO 27001, το NIST 800-53 και το BSI IT-Grundschutz. Αυτά τα πρότυπα παρέχουν έναν κατάλογο μέτρων και αντιμέτρων που μπορούν να εφαρμόσουν οι οργανισμοί για την προστασία από διάφορους τύπους κινδύνων. Το Verinice επιτρέπει στους χρήστες να αντιστοιχίσουν αυτά τα μέτρα στα περιουσιακά στοιχεία του συγκεκριμένου οργανισμού και βοηθά στην αξιολόγηση της αποτελεσματικότητας των εφαρμοζόμενων μέτρων. Σύμφωνα με τα παραπάνω το Verinice καλύπτει πλήρως το κριτήριο.

Πλοήγηση σε περιστατικά

Σύμφωνα με τις πληροφορίες που διατίθενται στον δικτυακό τόπο του Verinice, το εργαλείο παρέχει μια ενότητα διαχείρισης συμβάντων και παρέχει λειτουργίες για την παρακολούθηση και τη διαχείριση συμβάντων και περιστατικών που σχετίζονται με την ασφάλεια των πληροφοριών. Αυτό περιλαμβάνει την αναφορά, την κατηγοριοποίηση, την ιεράρχηση, τον χειρισμό, την τεκμηρίωση και την αξιολόγηση των συμβάντων. Η ενότητα παρέχει επίσης τη δυνατότητα διαχείρισης περιστατικών σύμφωνα με τις σχετικές νομικές απαιτήσεις.
Επιπλέον, το εργαλείο παρέχει μια λειτουργία παρακολούθησης περιστατικών, η λειτουργία αυτή επιτρέπει στους οργανισμούς να καταγράφουν τα περιστατικά και να παρακολουθούν την πρόοδό τους καθώς τα χειρίζονται. Η λειτουργία παρακολούθησης συμβάντων επιτρέπει επίσης στους οργανισμούς να αναθέτουν συμβάντα σε συγκεκριμένα άτομα ή ομάδες για χειρισμό και να ορίζουν προθεσμίες για την επίλυση των συμβάντων. Η διαδικασία συμβάλλει στη διασφάλιση του αποτελεσματικού και αποδοτικού χειρισμού των συμβάντων και στην καταγραφή και αποθήκευση των σχετικών πληροφοριών για μελλοντική αναφορά. Συνολικά το Verinice καλύπτει πλήρως το κριτήριο.

Έλεγχος επιχειρηματικών διαδικασιών

Το Verinice είναι ένα εργαλείο διαχείρισης επικινδυνότητας που επικεντρώνεται κυρίως στη διαχείριση της ασφάλειας των πληροφοριών και περιλαμβάνει ένα σύνολο λειτουργιών που επιτρέπουν στους οργανισμούς να διαχειρίζονται την ασφάλεια των πληροφοριών σύμφωνα με τα εθνικά και διεθνή πρότυπα και κανονισμούς. Ο έλεγχος επιχειρηματικών διαδικασιών αναφέρεται συνήθως στη διαχείριση και παρακολούθηση των επιχειρηματικών διαδικασιών, ώστε να διασφαλίζεται η αποδοτική και αποτελεσματική λειτουργία τους. Αυτό περιλαμβάνει δραστηριότητες όπως η χαρτογράφηση των διαδικασιών, η βελτίωση των διαδικασιών και η μέτρηση της απόδοσης.
Ενώ το Verinice μπορεί να είναι σε θέση να υποστηρίξει ορισμένες από αυτές τις δραστηριότητες παρέχοντας ορατότητα και αναφορές σχετικά με τις διαδικασίες διαχείρισης της ασφάλειας των πληροφοριών, που μπορούν να χρησιμοποιηθούν για την υποστήριξη της συνεχούς βελτίωσης και για την απόδειξη της συμμόρφωσης με τους σχετικούς κανονισμούς και πρότυπα, **δεν έχει σχεδιαστεί πρωτίστως για αυτόν τον σκοπό**.
Σύμφωνα με τα παραπάνω θεωρούμε ότι το κριτήριο δεν καλύπτεται από το Verinice.

Αναφορές και αναλύσεις

Το Verinice παρέχει υποστήριξη για υποβολή εκθέσεων και ανάλυση. Επιτρέπει στους χρήστες να δημιουργούν προσαρμοσμένες αναφορές, να προβάλλουν στατιστικά στοιχεία και τάσεις και να αναλύουν δεδομένα για τον εντοπισμό πιθανών κινδύνων και τρωτών σημείων. Προσφέρει μια σειρά από δυνατότητες, όπως: πίνακες ελέγχου, γραφικές αναφορές, ανάλυση τάσεων και προσαρμόσιμες αναφορές. Το εργαλείο περιλαμβάνει επίσης έναν πίνακα ελέγχου που εμφανίζει βασικές πληροφορίες, όπως η κατάσταση των ανοικτών κινδύνων και η πρόοδος των δραστηριοτήτων διαχείρισης κινδύνων. Επιπλέον, το Verinice παρέχει μια διεπαφή για την εισαγωγή και εξαγωγή δεδομένων, επιτρέποντας στους χρήστες να ενσωματώσουν το εργαλείο με άλλα συστήματα και να πραγματοποιήσουν περαιτέρω ανάλυση χρησιμοποιώντας εξωτερικά εργαλεία.
Επιπλέον, το Verinice παρέχει μια διαδρομή ελέγχου (audit trail) που επιτρέπει στους χρήστες να παρακολουθούν τις αλλαγές με την πάροδο του χρόνου.
Συνολικά, το Verinice καλύπτει πλήρως το κριτήριο.

Επίπεδο τεχνικότητας

Το Verinice απαιτεί ένα ορισμένο επίπεδο τεχνικών γνώσεων για την εφαρμογή και τη συντήρησή του, καθώς είναι ένα ολοκληρωμένο εργαλείο που παρέχει υποστήριξη για τον εντοπισμό, την αξιολόγηση και τον μετριασμό της επικινδυνότητας σε έναν ολόκληρο οργανισμό.
Για την εφαρμογή του Verinice, ένας οργανισμός θα χρειαστεί συνήθως μια ομάδα ατόμων με γνώσεις στη διαχείριση κινδύνων, τη μηχανική ασφάλειας και την τεχνολογία πληροφοριών. Αυτό περιλαμβάνει άτομα με γνώση των βέλτιστων πρακτικών και προτύπων ασφαλείας, καθώς και άτομα με εμπειρία σε συγκεκριμένους τομείς, όπως η ασφάλεια δικτύου, η ανάπτυξη λογισμικού και η διαχείριση περιστατικών. Η ομάδα θα πρέπει επίσης να είναι εξοικειωμένη με τα εργαλεία και τις τεχνικές που χρησιμοποιούνται για την

εφαρμογή της μεθοδολογίας, όπως η σάρωση ευπαθειών, η μοντελοποίηση απειλών και η διαχείριση περιστατικών.
Το εργαλείο παρέχει πολλές οδηγίες και υποστήριξη για να βοηθήσει τους οργανισμούς να εφαρμόσουν τη μεθοδολογία, συμπεριλαμβανομένων προτύπων και παραδειγμάτων, ενώ μπορεί επίσης να εφαρμοστεί με τη βοήθεια μιας συμβουλευτικής υπηρεσίας. Είναι επίσης σημαντικό να σημειωθεί ότι το επίπεδο των απαιτούμενων τεχνικών γνώσεων μπορεί να διαφέρει ανάλογα με το συγκεκριμένο πακέτο και τη διαμόρφωση που επιλέγεται. Συνολικά η τεχνικότητα που απαιτεί το εργαλείο θεωρείται υψηλή, οπότε δεν καλύπτεται το κριτήριο.

Υποστήριξη και πόροι

Το Verinice περιλαμβάνει υποστηρικτικό υλικό και πόρους για να βοηθήσει τους χρήστες να κατανοήσουν και να χρησιμοποιήσουν σωστά το πλαίσιο.
Αυτοί οι πόροι περιλαμβάνουν:

- Εγχειρίδια χρήσης: Αυτά παρέχουν λεπτομερείς πληροφορίες σχετικά με τον τρόπο εγκατάστασης και διαμόρφωσης του Verinice, καθώς και οδηγίες για τη χρήση των διαφόρων χαρακτηριστικών του εργαλείου.
- Ηλεκτρονική βοήθεια: Αυτή παρέχει βοήθεια και πληροφορίες σχετικά με συγκεκριμένα χαρακτηριστικά και λειτουργίες του εργαλείου.
- Εκπαιδευτικά βίντεο: Παρέχουν βήμα προς βήμα οδηγίες για τον τρόπο χρήσης διαφόρων πτυχών του εργαλείου.
- Κοινοτικό φόρουμ: Πρόκειται για μια πλατφόρμα όπου οι χρήστες μπορούν να μοιράζονται τις εμπειρίες τους, να υποβάλλουν ερωτήσεις και να παρέχουν ανατροφοδότηση σχετικά με τη χρήση του εργαλείου.
- Η εταιρεία που βρίσκεται πίσω από το Verinice παρέχει επίσης υπηρεσίες κατάρτισης και συμβουλευτικής για τους πελάτες, ώστε να τους βοηθήσει να αξιοποιήσουν στο έπακρο το εργαλείο

Αξίζει να σημειωθεί ότι αυτοί οι πόροι μπορεί να διαφέρουν ανάλογα με την έκδοση του Verinice, όμως θεωρούμε ότι το κριτήριο καλύπτεται πλήρως.

Πληρότητα

Το εργαλείο Verinice παρέχει μια ολοκληρωμένη προσέγγιση για τη διαχείριση επικινδυνότητας και καλύπτει ένα ευρύ φάσμα τομέων επικινδυνότητας, όπως ο εντοπισμός, η αξιολόγηση, η αντιμετώπιση και η παρακολούθηση της. Προσφέρει χαρακτηριστικά όπως ανάλυση επικινδυνότητας, υποβολή εκθέσεων και οπτικοποίηση και επιτρέπει στους χρήστες να ιεραρχούν, να παρακολουθούν και να διαχειρίζονται αποτελεσματικά την επικινδυνότητα ενός οργανισμού. **Θεωρείται ένα πλήρες εργαλείο στον τομέα του,** καθώς προσφέρει μια αρκετά ολοκληρωμένη προσέγγιση για τον εντοπισμό, την αξιολόγηση και τη διαχείριση της επικινδυνότητας της ασφάλειας πληροφοριών. Επιτρέπει επίσης την ενσωμάτωση με άλλα πλαίσια, μεθοδολογίες και εργαλεία, επιτρέποντας την εισαγωγή και εξαγωγή δεδομένων, γεγονός που το καθιστά πιο ευέλικτο.

Ωστόσο, η πληρότητα της κάλυψης του εργαλείου εξαρτάται από τις συγκεκριμένες απαιτήσεις και ανάγκες κάθε οργανισμού. Είναι πιθανό ορισμένοι οργανισμοί να έχουν συγκεκριμένους τομείς επικινδυνότητας που δεν καλύπτονται από το Verinice, οπότε μπορεί να χρειαστεί να συμπληρώσουν το εργαλείο με πρόσθετους ελέγχους ή διαδικασίες για την αντιμετώπιση αυτών των κινδύνων. Παρ' όλα αυτά το Verinice καλύπτει πλήρως το κριτήριο.

Χρόνος/Διάρκεια

Η αποτελεσματικότητα και η διάρκεια της εφαρμογής του Verinice ως εργαλείου διαχείρισης επικινδυνότητας εξαρτάται από διάφορους παράγοντες, όπως το μέγεθος και η πολυπλοκότητα του οργανισμού, το εύρος της εφαρμογής και η διαθεσιμότητα των πόρων. **Σε γενικές γραμμές, η εφαρμογή του Verinice μπορεί να διαρκέσει αρκετούς μήνες, ανάλογα με τις συγκεκριμένες ανάγκες και απαιτήσεις του οργανισμού**. Κατά τη φάση της υλοποίησης, οι οργανισμοί ενδέχεται να χρειαστεί να διαθέσουν πόρους, όπως προσωπικό, χρόνο και προϋπολογισμό, για να διασφαλίσουν την επιτυχή ανάπτυξη του εργαλείου. Ωστόσο, μόλις το εργαλείο εφαρμοστεί και διαμορφωθεί, μπορεί να βοηθήσει τους οργανισμούς να εξορθολογίσουν και να αυτοματοποιήσουν τις διαδικασίες διαχείρισης κινδύνων, γεγονός που μπορεί να οδηγήσει σε εξοικονόμηση χρόνου και βελτίωση της αποδοτικότητας. Ο χρόνος που απαιτείται για την εφαρμογή του εργαλείου θεωρείται μέτριος και γι' αυτό το κριτήριο θεωρούμε ότι καλύπτεται εν μέρει.

Οικονομικό κόστος

Το Verinice δεν είναι ένα εντελώς δωρεάν εργαλείο διαχείρισης επικινδυνότητας, αλλά προσφέρει μια δωρεάν έκδοση με περιορισμένη λειτουργικότητα. Η δωρεάν έκδοση του Verinice, που ονομάζεται "Verinice Lite", προορίζεται για μικρούς οργανισμούς και μη εμπορική χρήση. Περιλαμβάνει βασικές λειτουργίες, όπως εισαγωγή και εξαγωγή δεδομένων, αναφορές και λειτουργίες διαχείρισης επικινδυνότητας. Ωστόσο, είναι περιορισμένη όσον αφορά τον αριθμό των περιουσιακών στοιχείων που μπορούν να διαχειριστούν και το επίπεδο της παρεχόμενης υποστήριξης.
Η εμπορική έκδοση του εργαλείου , VerinicePRO, παρέχει προηγμένες λειτουργίες οι οποίες προσφέρονται σε διαφορετικές επιλογές αδειοδότησης, όπως άδεια χρήσης για έναν χρήστη, άδεια χρήσης για ομάδες και άδεια χρήσης για ολόκληρη την εταιρεία , οι οποίες φυσικά εμπεριέχουν έναν οικονομικό κόστος. Συνολικά το κόστος του θεωρείται κυμαινόμενο , οπότε θεωρούμε ότι καλύπτει το κριτήριο εν μέρει.

4. Πίνακας Συγκριτικής Αξιολόγησης

Κριτήρια συγκριτικής αξιολόγησης	Πλαίσια – Μεθοδολογίες – Εργαλεία								
	COSO (IC –IF)	**FAIR Methodology**	**RiskIT Framework**	**ISO 27005 Framework**	**EU ITSRM²**	**MSAT**	**NIST SP 800-30**	**OCTAVE Allegro**	**Verinice**
Χρηστικότητα (Usability)									
Ευελιξία (Flexibility)									
Διαχείριση περιουσιακών στοιχείων (Asset management)									
Βάση δεδομένων για απειλές (Database for threats)									
Βάση δεδομένων για ευπάθεις (Database for vulnerabilities)									
Βάση δεδομένων για μέτρα ασφαλείας. (Database for controls)									
Πλοήγηση σε περιστατικά (Incident navigation)									
Έλεγχος επιχειρησιακών διαδικασιών (Business process control)									
Αναφορές και αναλύσεις (Reporting and analytics)									
Επίπεδο τεχνικότητας (Technicality)									
Υποστήριξη και πόροι (Support and resources)									
Πληρότητα (Completeness)									
Χρόνος (Time ή Duration)									
Οικονομικό κόστος (Financial Cost)									

Υπόμνημα :
Μπλε → το κριτήριο καλύπτεται πλήρως
Γκρι → το κριτήριο καλύπτεται μερικώς
Άσπρο → το κριτήριο δεν καλύπτεται

5. Ανάλυση αποτελεσμάτων συγκριτικής αξιολόγησης

Αναλύοντας τα αποτελέσματα της συγκριτικής αξιολόγησης με βάση τα κριτήρια που έχουμε θέσει, μπορούμε να αποκτήσουμε εικόνα για τα σημαντικά χαρακτηριστικά που πρέπει να περιλαμβάνονται σε ένα πλαίσιο, μια μεθοδολογία ή ένα εργαλείο για τη διαχείριση της επικινδυνότητας της ασφάλειας πληροφοριών. Μπορούμε επίσης να προσδιορίσουμε ποια χαρακτηριστικά θεωρούν οι δημιουργοί αυτών των λύσεων ως τα πιο κρίσιμα και ποια μπορεί να μην είναι πάντα παρόντα.
Τέλος, η ανάλυση θα μας δείξει ποιο πλαίσιο, μεθοδολογία ή εργαλείο προσφέρει ολοκληρωμένη κάλυψη των βασικών χαρακτηριστικών. Με αυτόν τον τρόπο, η ανάλυση συγκριτικής αξιολόγησης μπορεί να βοηθήσει τους οργανισμούς να λάβουν τεκμηριωμένες αποφάσεις σχετικά με την επιλογή εκείνου του πλαισίου, μεθοδολογίας ή εργαλείου που τους ταιριάζει καλύτερα για τη διαχείριση της επικινδυνότητας της ασφάλειας πληροφοριών.

5.1 Κάλυψη Χρηστικότητας

Η χρηστικότητα είναι ένα χαρακτηριστικό που πρέπει να αναζητήσει κάποιος που θέλει το πλαίσιο/μεθοδολογία/εργαλείο που θα χρησιμοποιήσει να είναι φιλικό και εύκολο στη χρήση και την κατανόηση, με σαφείς οδηγίες και καθοδήγηση σχετικά με τον τρόπο εφαρμογής του. Να διαχειρίζεται την επικινδυνότητα της ασφάλειας των πληροφοριών με συστηματικό και οργανωμένο τρόπο και να ενσωματώνεται εύκολα στις υφιστάμενες διαδικασίες και συστήματα του οργανισμού. Με αυτό τον τρόπο διασφαλίζεται ότι η μεθοδολογία ή το πλαίσιο ή το εργαλείο χρησιμοποιούνται πραγματικά και ότι εφαρμόζονται αποτελεσματικά, αντί να αγνοούνται ή να μην γίνονται κατανοητά.
Το κριτήριο αυτό, όπως προκύπτει και από τον πίνακα καλύπτεται από τα πλαίσια Risk IT και ISO/IEC 27005 και τις μεθοδολογίες FAIR και EU ITSRM.
Το κριτήριο καλύπτεται μερικώς από το COSO IC-IF και το NIST SP 800-30 γιατί το ένα είναι αρκετά λεπτομερές και πολύπλοκο ενώ το άλλο δεν είναι εύκολο στην παρακολούθηση και απαιτεί εκτεταμένη εκπαίδευση και εμπειρογνωμοσύνη για την εκτέλεση του.
Τα εργαλεία MSAT και Verinice δεν θεωρούνται χρηστικά γιατί θεωρούνται δύσκολα στη χρήση ή την κατανόηση, λόγω της πολυπλοκότητας των αξιολογήσεων ασφαλείας και του όγκου των πληροφοριών που παρουσιάζουν και γιατί οι χρήστες ενδέχεται να δυσκολευτούν να ενσωματώσουν αυτά τα εργαλεία στα υπάρχοντα συστήματα και τις ροές εργασίας τους, με αποτέλεσμα την έλλειψη υιοθέτησης και χρήσης τους.

5.2 Παράγοντας Ευελιξία

Η ευελιξία είναι ένα χαρακτηριστικό που δίνει την δυνατότητα σε αυτόν που θα χρησιμοποιήσει το πλαίσιο, τη μεθοδολογία ή το εργαλείο να μπορεί να το προσαρμόσει και να το τροποποιήσει ώστε να ανταποκρίνεται στις συγκεκριμένες ανάγκες και απαιτήσεις του οργανισμού. Επιπλέον δίνει τη δυνατότητα εύκολης επέκτασης ή προσαρμογής του πλαισίου, της μεθοδολογίας ή του εργαλείου καθώς ο οργανισμός αναπτύσσεται ή αλλάζει

περιβάλλον και την ικανότητα ενσωμάτωσης με τα υπάρχοντα συστήματα, διαδικασίες και τεχνολογίες εντός του οργανισμού.
Όπως προκύπτει και από το πίνακα όλα τα εργαλεία, μεθοδολογίες και εργαλεία, που εξετάζονται στην παρούσα μελέτη, διαθέτουν αυτή την ιδιότητα. Αυτό σημαίνει ότι είναι ένας σημαντικός παράγοντας υιοθέτησης ενός πλαισίου/μεθοδολογίας/εργαλείου , που οι δημιουργοί τον λαμβάνουν υπόψη τους. Τη μόνη εξαίρεση αποτελεί το FAIR Methodology και είναι απολύτως κατανοητό, μιας και είναι η μόνη μεθοδολογία η οποία ακολουθεί την ποσοτική εκτίμηση της επικινδυνότητας και αυτό την καθιστά αυστηρή , εφ' όσον ακολουθεί μαθηματικούς κανόνες και λιγότερο ευέλικτη από τα υπόλοιπα.

5.3 Διαδικασίες διαχείρισης περιουσιακών στοιχείων

Επιλέγοντας κάποιος ένα πλαίσιο/μεθοδολογία /εργαλείο που διαθέτει μια ολοκληρωμένη διαδικασία διαχείρισης περιουσιακών στοιχείων, μπορεί να προσδιορίσει και να ιεραρχήσει τα περιουσιακά του στοιχεία, να αξιολογήσει τους κινδύνους που σχετίζονται με κάθε περιουσιακό στοιχείο και να εφαρμόσει τα κατάλληλα μέτρα για τον μετριασμό αυτών των κινδύνων, γεγονός που μπορεί να συμβάλει στη μείωση της πιθανότητας περιστατικών ασφάλειας και στην ελαχιστοποίηση των επιπτώσεών τους εάν αυτά συμβούν.
Από τα αποτελέσματα του πίνακα, προκύπτει ότι η πλειονότητα των εξεταζόμενων πλαισίων, μεθοδολογιών και εργαλείων έχει φροντίσει ώστε να καλύπτεται πλήρως αυτό το χαρακτηριστικό , κάτι που το κατατάσσει στα σημαντικά χαρακτηριστικά που θα πρέπει να διαθέτει ένα πλαίσιο/μεθοδολογία/εργαλείο.
Τα FAIR Methodology , RiskIT Framework, ISO 27005 Framework, EU ITSRM2, OCTAVE Allegro και Verinice προσφέρουν πλήρως μία τέτοια διαδικασία ενώ το NIST SP 800-30 αν και δεν διαθέτει μία αποκλειστική διαδικασία παρέχει μία σχετική καθοδήγηση για τον εντοπισμό και την καταγραφή των περιουσιακών στοιχείων. Το COSO IC-IF όπως και το MSAT δεν παρέχουν αυτή τη δυνατότητα , είτε γιατί παρέχουν απλώς συστάσεις για τη διαδικασία είτε γιατί προτείνουν κάποια εξωτερική/εναλλακτική πηγή για την εκπλήρωση αυτής της διαδικασίας.

5.4 Βάση δεδομένων για απειλές.

Παρέχοντας το πλαίσιο/μεθοδολογία/εργαλείο μία βάση δεδομένων για απειλές ή μία κατάλληλη διαδικασία για τη συλλογή και αποθήκευση πληροφοριών σχετικά με πιθανές απειλές ασφάλειας, επιτρέπει στους οργανισμούς να εντοπίζουν **προληπτικά** και να ιεραρχούν τους πιθανούς κινδύνους ασφάλειας που αντιμετωπίζουν. Επιλέγοντας κάποιος ένα πλαίσιο ή μία μεθοδολογία ή ένα εργαλείο που διαθέτει αυτό το χαρακτηριστικό μπορεί να κατανοήσει καλύτερα τους τύπους επιθέσεων που συμβαίνουν και τις πιθανές επιπτώσεις τους και να αναπτύξει και εφαρμόσει πιο αποτελεσματικές στρατηγικές μετριασμού τους.
Όπως προκύπτει από τον πίνακα είναι ένα χαρακτηριστικό το οποίο δεν υιοθετείται ευρέως από τους δημιουργούς των πλαισίων/μεθοδολογιών/εργαλείων και ο λόγος είναι ότι μία διαδικασία συλλογής και καταγραφής των απειλών είναι αρκετά χρονοβόρα και απαιτεί αρκετούς πόρους για τη συντήρησή της αφού πρέπει να είναι πάντα ενημερωμένη και επικαιροποιημένη. Προτιμάται συνήθως η χρήση εξωτερικών πηγών για την πληροφόρηση σχετικά με τις απειλές.

Από τα εξεταζόμενα πλαίσια, μεθοδολογίες και εργαλεία μόνο το ISO 27005 Framework και το NIST SP 800-30 καλύπτουν πλήρως αυτό το χαρακτηριστικό.
Το COSO IC-IF, το FAIR Methodology , το EU ITSRM2 και το OCTAVE Allegro , το καλύπτουν εν μέρει, είτε γιατί περιλαμβάνουν κάποιες διαδικασίες για τον εντοπισμό και την ανάλυση πιθανών απειλών αλλά δεν έχουν έναν συστηματικό τρόπο διαχείρισής τους, είτε γιατί συμμετέχουν απλώς σε κάποιο στάδιο της διαδικασίας αξιολόγησης των απειλών.
Τα RiskIT Framework, MSAT και Verinice χρησιμοποιούν εξωτερικές πηγές για πληροφορίες σχετικά με τις απειλές.

5.5 Βάση δεδομένων για ευπάθειες

Επιλέγοντας κάποιος ένα πλαίσιο/μεθοδολογία/εργαλείο που να διαθέτει την ιδιότητα να παρέχει μια συλλογή πληροφοριών σχετικά με γνωστές ευπάθειες σε λογισμικό, υλικό και άλλα συστήματα , έχει τη δυνατότητα να αξιολογήσει με ακρίβεια τους κινδύνους που σχετίζονται με τα συστήματα του , να δράσει προληπτικά στη διαχείριση πιθανών απειλών αλλά ταυτόχρονα να λάβει εμπεριστατωμένες αποφάσεις σχετικά με τον τρόπο κατανομής των πόρων του αλλά και της όλης προσπάθειας για την ασφάλεια των πληροφοριών.
Είναι ένα χαρακτηριστικό που επίσης δεν υποστηρίζεται ευρέως από τους δημιουργούς , όπως προκύπτει και από τον πίνακα και συνήθως προτείνεται να υιοθετηθεί μία εξωτερική πηγή ή εργαλείο που θα παρέχει πληροφορίες σχετικά τις ευπάθειες το οποίο θα λειτουργήσει συνδυαστικά με το πλαίσιο, μεθοδολογία ή εργαλείο που χρησιμοποιείται.
Μόνο το ISO/IEC 27005 παρέχει μία ολοκληρωμένη διαχείρισης των πληροφοριών για τις ευπάθειες.
Το FAIR και το NIST SP 800-30 περιγράφουν απλώς διαδικασίες για τον εντοπισμό και την αξιολόγηση των ευπαθειών ενός οργανισμού κάτι που θεωρητικά καλύπτει μερικώς το κριτήριο.
Τα COSO IC-IF , RiskIT Framework, EU ITSRM2, MSAT, OCTAVE Allegro και Verinice, δεν ασχολούνται καθόλου με τον εντοπισμό και την καταγραφή των ευπαθειών ενός οργανισμού.

5.6 Βάση δεδομένων για μέτρα.

Η ύπαρξη μιας βάσης δεδομένων με μέτρα ή αντίμετρα ασφαλείας ή η ύπαρξη της διαδικασία συλλογής και αποθήκευσης πληροφοριών σχετικά με τα μέτρα ασφαλείας που εφαρμόζει ένας οργανισμός σε ένα πλαίσιο/μεθοδολογία/εργαλείο, διασφαλίζει ότι το πλαίσιο, η μεθοδολογία ή το εργαλείο που χρησιμοποιείται λαμβάνει υπόψη όλα τα σχετικά μέτρα και αντίμετρα ασφαλείας κατά την αξιολόγηση και τον μετριασμό της επικινδυνότητας. Διαθέτοντας μια βάση δεδομένων, η διαδικασία διαχείρισης επικινδυνότητας της ασφάλειας των πληροφοριών είναι πιο συστηματική, συνεπής και αποτελεσματική, μειώνοντας την πιθανότητα να λείπουν σημαντικές εκτιμήσεις για την ασφάλεια.
Το χαρακτηριστικό αυτό, σύμφωνα με τον πίνακα αξιολόγησης δεν παρέχεται από όλες τις λύσεις. Για εκείνες που δεν το συμπεριλαμβάνουν είτε επιλέγουν να δίνουν συστάσεις για την υιοθέτηση των κατάλληλων μέτρων και εναπόκειται στον οργανισμό να εφαρμόσει τα μέτρα εκείνα που είναι κατάλληλα για την δική του κατάσταση ασφάλειας, είτε προτείνουν την υιοθέτηση κάποιου άλλου πλαισίου που εξειδικεύεται στο να συλλέγει και να

καταγράφει και να αξιολογεί τα μέτρα και τα αντίμετρα που εφαρμόζονται και που είναι κατάλληλα για τον εκάστοτε οργανισμό.
Η μεθοδολογία EU ITSRM και το MSAT περιέχουν αυτό το χαρακτηριστικό παρέχοντας μία πλήρη διαδικασία τη διαχείριση των μέτρων ασφαλείας που εφαρμόζονται σε έναν οργανισμό.
Το COSO IC-IF και το FAIR παρέχουν οδηγίες για την ανάπτυξη μέτρων που ανταποκρίνονται στους συγκεκριμένους κινδύνους του οργανισμού.
Το Risk IT, το ISO/IEC 27005, το NIST SP 800-30 και το OCTAVE Allegro προτείνουν τη χρήση εξωτερικών διαδικασιών για την διαχείριση των μέτρων ασφαλείας .

5.7 Πλοήγηση σε περιστατικά.

Όταν ένα πλαίσιο/μεθοδολογία/εργαλείο διαθέτει αυτό το χαρακτηριστικό διασφαλίζει ότι τα κατάλληλα άτομα και οι πόροι κινητοποιούνται έγκαιρα και αποτελεσματικά για την αντιμετώπιση περιστατικών ασφαλείας, έτσι ώστε να ελαχιστοποιηθούν α) οι επιπτώσεις των περιστατικών στον οργανισμό, β) ο χρόνος διακοπής λειτουργίας του και γ) ο κίνδυνος παραβίασης δεδομένων και απώλειας ευαίσθητων πληροφοριών.
Σύμφωνα με τον πίνακα, αυτό το χαρακτηριστικό δεν παρέχεται ευρέως από τις λύσεις που εξετάζουμε. Οι δημιουργοί των λύσεων, επιλέγουν να αφήνουν τη διαχείριση των περιστατικών σε ειδική ομάδα αντιμετώπισης περιστατικών , λόγω α) της πολυπλοκότητας της διαδικασίας η οποία απαιτεί ενδελεχή κατανόηση των συστημάτων, των δικτύων και των δεδομένων του κάθε οργανισμού, β) του περιορισμένου πεδίου εφαρμογής του πλαισίου, της μεθοδολογίας ή του εργαλείου και γ) της επικάλυψης που μπορεί να προκληθεί με άλλες υφιστάμενες διαδικασίες ενός οργανισμού για την αντιμετώπιση συμβάντων.
Το Risk IT και το Verinice εστιάζουν σε αυτόν τον τομέα παρέχοντας παρέχει οδηγίες για τον τρόπο διαχείρισης των περιστατικών καθ' όλη τη διάρκεια του κύκλου ζωής τους, από τον εντοπισμό έως την επίλυση.
Το COSO IC-IF, το ISO 27005, το EU ITSRM[2] και το MSAT καλύπτουν εμμέσως αυτό το χαρακτηριστικό είτε μέσω διαδικασιών εξέτασης σεναρίων, είτε μέσω συστάσεων για την χρήση κατάλληλων διαδικασιών και εργαλείων για την αντιμετώπιση περιστατικών.
Τα FAIR, NIST SP 800-30 και OCTAVE Allegro επικεντρώνονται σε άλλες διαδικασίες προσδιορισμού και αξιολόγησης της επικινδυνότητας και δεν εστιάζουν καθόλου σε αυτό το κομμάτι.

5.8 Έλεγχος επιχειρηματικών διαδικασιών

Ένα πλαίσιο/μεθοδολογία/εργαλείο που συμπεριλαμβάνει ελέγχους των επιχειρηματικών διαδικασιών στις διαδικασίες του αξιολόγησης της επικινδυνότητας, παρέχει μία δομημένη και συνεπή προσέγγιση της επικινδυνότητας της ασφάλειας που μπορεί να εξασφαλίσει την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των συστημάτων, των υποδομών και των δεδομένων που υποστηρίζουν τις επιχειρηματικές διαδικασίες ενός οργανισμού.
Όπως προκύπτει και από τον πίνακα είναι ένα χαρακτηριστικό στο οποίο δεν εστιάζουν οι περισσότερες λύσεις γιατί θεωρείται γενικά ως μία ξεχωριστή και διακριτή διαδικασία σε έναν οργανισμό και η ευθύνη για τον έλεγχο των διαδικασιών μπορεί να ανήκει σε διαφορετικές ομάδες εντός ενός οργανισμού, όπως ο εσωτερικός έλεγχος ή η

συμμόρφωση και ένα πλαίσιο, μια μεθοδολογία ή ένα εργαλείο μπορεί να μην έχει την εξουσία να υπαγορεύει τον τρόπο λειτουργίας αυτών των ομάδων.
Το COSO IC-IF όπως και το OCTAVE Allegro περιλαμβάνουν πλήρης οδηγίες και σχετικά με το πώς μπορούν να χρησιμοποιηθούν για τον έλεγχο επί των επιχειρηματικών διαδικασιών.
Το Risk IT και το ISO 27005 καλύπτουν εν μέρει αυτό το χαρακτηριστικό παρέχοντας καθοδήγηση σχετικά με τον τρόπο με τον οποίο διασφαλίζεται η ενσωμάτωση των επιχειρηματικών διαδικασιών με τα συστήματα πληροφορικής, καθώς και με τον τρόπο παρακολούθησης και διαχείρισης της επικινδυνότητας που σχετίζεται με αυτές τις διαδικασίες.
Τα υπόλοιπα , δηλαδή το FAIR , το EU ITSRM2, το MSAT, το NIST SP 800-30 προτείνουν είτε τη χρήση άλλων εργαλείων ή υπηρεσιών που έχουν σχεδιαστεί ειδικά για το σκοπό αυτό είτε την ενσωμάτωση άλλων πλαισίων ή μεθοδολογιών που καλύπτουν επαρκώς αυτή τη δυνατότητα.

5.9 Υποβολή αναφορών και αναλύσεων.

Ένα πλαίσιο/μεθοδολογία/εργαλείο που διαθέτει τη δυνατότητα υποβολής αναφορών και αναλύσεων μπορεί να παρέχει στους ενδιαφερόμενους μια σαφή και συνοπτική επισκόπηση της τρέχουσας κατάστασης της ασφαλείας ενός οργανισμού, επισημαίνοντάς τις περιοχές που απαιτούν βελτίωση και βοηθά στον εντοπισμό των τάσεων, προτύπων και σχέσεων στις βασικές αιτίες των περιστατικών ασφαλείας. Απώτερος σκοπός είναι η λήψη εμπεριστατωμένων αποφάσεων σχετικά με το που πρέπει να διατεθούν οι πόροι και που να εφαρμοστούν κατάλληλα μέτρα.
Από τον πίνακα προκύπτει ότι είναι ένα χαρακτηριστικό το οποίο καλύπτεται από όλα τα πλαίσια , τις μεθοδολογίες και τα εργαλεία και άρα λαμβάνεται υπόψη από όλους τους δημιουργούς των λύσεων, γιατί ουσιαστικά είναι ο τρόπος επικοινωνίας των αποτελεσμάτων της αξιολόγησης της διαχείρισης της επικινδυνότητας προς κάθε κατεύθυνση της διοίκησης, τους υπεύθυνους λήψης αποφάσεων και κάθε ενδιαφερόμενο.
Ταυτόχρονα προσφέρει τη δυνατότητα παρακολούθησης της συμμόρφωσης του οργανισμού σύμφωνα με τις κανονιστικές απαιτήσεις, όπως αυτές επιβάλλονται από νόμους, πρότυπα του κλάδου και βέλτιστες πρακτικές, μέσω των αναφορών και αναλύσεων.

5.10 Επίπεδο τεχνικότητας

Ένα πλαίσιο , μία μεθοδολογία ή ένα εργαλείο που δεν απαιτεί υψηλό επίπεδο τεχνικότητας , μπορεί να γίνει πιο εύκολα κατανοητό και να χρησιμοποιηθεί από άτομα με λιγότερη τεχνική εμπειρία , συμβάλλοντας έτσι στην αύξηση της υιοθέτησης και εφαρμογής του, με αποτέλεσμα ένα πιο αποτελεσματικό και βιώσιμο πρόγραμμα διαχείρισης επικινδυνότητας.
Ένα ιδιαίτερα τεχνικό πλαίσιο, μεθοδολογία ή εργαλείο μπορεί α) να είναι δύσκολο να εφαρμοστεί και να υιοθετηθεί, απαιτώντας εξειδικευμένες δεξιότητες και τεχνογνωσία που μπορεί να μην είναι ευρέως διαθέσιμες σε έναν οργανισμό, β) να μην επικοινωνεί αποτελεσματικά την επιχειρηματική αξία της διαχείρισης επικινδυνότητας της ασφάλειας των πληροφοριών στους υπεύθυνους λήψης αποφάσεων και στα ενδιαφερόμενα μέρη, και γ) να δημιουργεί εμπόδια στην κατανόηση και τη συμμετοχή, καθιστώντας δύσκολο για

τους μη τεχνικούς ενδιαφερόμενους να συμβάλουν αποτελεσματικά στη διαδικασία διαχείρισης της επικινδυνότητας.
Αναπόφευκτα η χρήση οποιουδήποτε πλαισίου, μεθοδολογίας ή εργαλείου ενέχει κάποιο επίπεδο τεχνικότητας, άμεσα ή έμμεσα και αυτό αποτυπώνεται στον πίνακα, όπου όλες οι λύσεις εμφανίζονται να απαιτούν μέτριο ή υψηλό επίπεδο τεχνικότητας για την εφαρμογή τους.
Τα COSO IC-IF , RiskIT, ISO 27005 Framework , EU ITSRM^2, MSAT και OCTAVE Allegro είναι αυτά που δεν απαιτούν υψηλό επίπεδο τεχνικών γνώσεων , αλλά ενδέχεται α) να απαιτούνται κάποιες τεχνικές γνώσεις ανάλογα με τα συγκεκριμένα συστήματα και τις διαδικασίες που χρησιμοποιεί ο οργανισμός που τα εφαρμόζει και β) να απαιτείται η συμβολή τεχνικών εμπειρογνωμόνων σε ορισμένους τομείς.
Το FAIR Methodology , το NIST SP 800-30 και το Verinice θεωρούνται λύσεις υψηλών τεχνικών γνώσεων. Για παράδειγμα το FAIR βασίζεται σε μαθηματικές έννοιες και απαιτεί γνώσεις στατιστικής, πιθανοτήτων και άλλων συναφών θεμάτων ,το NIST προορίζεται για χρήση από επαγγελματίες της ασφάλειας πληροφοριών και διαχειριστές συστημάτων πληροφορικής και το Verinice χρειάζεται μια ομάδα ατόμων με γνώσεις στη διαχείριση κινδύνων, τη μηχανική ασφάλειας και την τεχνολογία πληροφοριών.

5.11 Υποστήριξη και πόροι

Ένα πλαίσιο, μία μεθοδολογία ή ένα εργαλείο που διαθέτει υποστήριξη και πόρους διευκολύνει τους χρήστες να το κατανοήσουν και να το χρησιμοποιήσουν αποτελεσματικά, ενθαρρύνει την ευρύτερη υιοθέτηση του και συνολικά οδηγεί σε καλύτερα αποτελέσματα και αποτελεσματικότερες διαδικασίες, καθώς οι χρήστες είναι σε θέση να αξιοποιήσουν πλήρως τις δυνατότητες του πλαισίου, της μεθοδολογίας ή του εργαλείου.
Θεωρείται ένα σημαντικό χαρακτηριστικό που καλύπτεται πλήρως από όλες τις μεθοδολογίες , τα πλαίσια και τα εργαλεία του πίνακα γιατί οι δημιουργοί των λύσεων φροντίζουν να παρέχουν επαρκή υποστήριξη και πόρους συμπεριλαμβανομένων οδηγιών βήμα προς βήμα, εγχειρίδια χρήσης , πρότυπα, εργαλειοθήκες και εκπαιδευτικό υλικό.
Επίσης για τα περισσότερα υπάρχει και δικτυακή κοινότητα η οποία συμμετέχει ενεργά για την αντιμετώπιση οποιονδήποτε θεμάτων προκύψουν όπως υπάρχουν και επαρκείς δικτυακοί πόροι.

5.12 Επίπεδο πληρότητας

Όταν ένα πλαίσιο/μεθοδολογία/εργαλείο διαθέτει υψηλό επίπεδο πληρότητας τότε καλύπτει όλες τις πτυχές της διαδικασίας διαχείρισης της επικινδυνότητας της ασφάλειας των πληροφοριών, δηλαδή παρέχει σαφείς και λεπτομερείς οδηγίες σχετικά με τον τρόπο εκτέλεσης κάθε βήματος της διαδικασίας διαχείρισης επικινδυνότητας , συμπεριλαμβανομένου του τρόπου εντοπισμού και αξιολόγησης της επικινδυνότητας, του τρόπου εφαρμογής αποτελεσματικών μέτρων και του τρόπου παρακολούθησης της αποτελεσματικότητας αυτών των μέτρων, είναι αρκετά ευέλικτο ώστε να προσαρμόζεται στις συγκεκριμένες ανάγκες ενός οργανισμού και στους κινδύνους που αντιμετωπίζει και ενσωματώνεται εύκολα στο συνολικό πλαίσιο διαχείρισης επικινδυνότητας τους οργανισμού.

Είναι αναμενόμενο, όπως προκύπτει από τον πίνακα, το επίπεδο πληρότητας μεταξύ των πλαισίων , μεθοδολογιών και εργαλείων να διαφοροποιείται.
Το ISACA RiskIT, το ISO/IEC 27005, το EU ITSRM^2, το OCTAVE Allegro και το Verinice διαθέτουν υψηλό επίπεδο πληρότητας γιατί καλύπτουν όλες τις πτυχές της διαχείρισης της επικινδυνότητας της ασφάλειας των πληροφοριών, από την αξιολόγηση της επικινδυνότητας έως την εφαρμογή των μέτρων ασφαλείας. συμπεριλαμβανομένης της αξιολόγησης , της αντιμετώπισης και της παρακολούθησης κινδύνων.
Το COSO IC-IF, το FAIR και το NIST SP 800-30 θεωρούνται εν μέρει πλήρεις λύσεις γιατί συνιστούν τη συμπλήρωσή τους με άλλα σχετικά πρότυπα και βέλτιστες πρακτικές για να παρέχουν μία ολοκληρωμένη προσέγγιση στη διαχείριση της επικινδυνότητας της ασφάλειας των πληροφοριών.
Το MSAT επικεντρώνεται κυρίως σε συστήματα και περιβάλλοντα που βασίζονται στη Microsoft και δεν καλύπτει όλους τους σχετικούς τομείς επικινδυνότητας για έναν οργανισμό.

5.13 Αποτελέσματα σύγκρισης χρονικής διάρκειας

Ένα πλαίσιο/μεθοδολογία/εργαλείο που μπορεί να υλοποιηθεί και να εφαρμοσθεί σε ένα εύλογα σύντομο χρονικό διάστημα βοηθά τους οργανισμούς να ελαχιστοποιούν το κόστος, να ανταποκρίνονται άμεσα στους αναδυόμενους κινδύνους και απειλές, να πληρούν έγκαιρα τις απαιτήσεις συμμόρφωσης και να διασφαλίζουν την επιχειρηματική συνέχεια.
Όπως προκύπτει και από τον πίνακα, αλλά και από την όλη μελέτη, αυτό το χαρακτηριστικό εξαρτάται άμεσα από το μέγεθος και την πολυπλοκότητα του οργανισμού και των συστημάτων πληροφορικής του, τους διαθέσιμους πόρους για την εφαρμογή του πλαισίου ή της μεθοδολογίας ή της εργαλείου και το επίπεδο των υφιστάμενων διαδικασιών διαχείρισης της επικινδυνότητας της ασφάλειας των πληροφοριών.
Παρ' όλα αυτά θέσαμε στην παρούσα μελέτη ένα χρονικό διάστημα μεταξύ εβδομάδων και μηνών να θεωρείται επαρκές για την εφαρμογή του κάθε πλαισίου, μεθοδολογίας και εργαλείου, το χρονικό διάστημα ενός χρόνου να θεωρείται λιγότερο επαρκές και οτιδήποτε ξεπερνάει αυτό το διάστημα να θεωρείται χρονοβόρο.
Όπως προκύπτει από τον πίνακα , το Risk IT, το EU ITSRM^2, MSAT και το OCTAVE Allegro καλύπτουν πλήρως αυτό το κριτήριο και μπορούν να υλοποιηθούν στο ως άνω αναφερόμενο επαρκές χρονικό διάστημα μεταξύ εβδομάδων και μηνών.
Το FAIR, το ISO 27005 και το Verinice χρειάζονται οριακά δώδεκα μήνες για την εφαρμογή τους, κάτι περισσότερο ή κάτι λιγότερο, οπότε όπως βλέπουμε καλύπτουν εν μέρει αυτό το κριτήριο.
Τέλος το COSO IC-IF και το NIST SP 800-30 ξεπερνούν το χρόνο και θεωρούνται χρονοβόρα, οπότε και δεν καλύπτουν το κριτήριο.

5.14 Οικονομικό κόστος

Όταν λέμε ότι ένα πλαίσιο, μεθοδολογία ή εργαλείο έχει ένα χαμηλό οικονομικό κόστος για τον οργανισμό που το εφαρμόζει εννοούμε ότι το κόστος απόκτησης δεν απαιτεί σημαντική επένδυση , το κόστος εφαρμογής ,συμπεριλαμβανομένου οποιουδήποτε απαιτούμενου υλικού ή λογισμικού, της εκπαίδευσης και κάθε αναγκαίας προσαρμογής, είναι επίσης χαμηλό και τέλος το κόστος συντήρησης στο οποίο συμπεριλαμβάνονται το

κόστος της συνεχούς υποστήριξης ,των αναβαθμίσεων και της συντήρησης του πλαισίου, της μεθοδολογίας ή του εργαλείου απαιτεί ελάχιστους πόρους για την ομαλή λειτουργία του.
Είναι φυσικό όπως προκύπτει και από τον πίνακα, πάντα να εμπλέκεται κάποιο οικονομικό κόστος σε σχέση με το εκάστοτε πλαίσιο/μεθοδολογία/εργαλείο που θα υιοθετηθεί από έναν οργανισμό. Ακόμα και αν παρέχονται δωρεάν, εμπεριέχουν την έννοια της οικονομικής επιβάρυνσης σε ένα από τα κόστη που έχουν αναφερθεί παραπάνω.
Το COSO IC-IF , το EU ITSRM^2, το MSAT και το NIST SP 800-30 αν και παρέχονται δωρεάν σαν έγγραφα, συμπεριλαμβάνουν κάποιες δαπάνες που θα πρέπει να ληφθούν υπόψη , από κάποιον που ενδιαφέρεται να τα υιοθετήσει , όπως το κόστος πρόσβασης στο πλαίσιο ή τη μεθοδολογία (όπου απαιτείται), η κατάρτιση των εργαζομένων, οι αμοιβές συμβούλων για έναν διαπιστευμένο φορέα αξιολόγησης , συνεχές κόστος για τη διατήρηση της συμμόρφωσης με το πλαίσιο/μεθοδολογία, οι τακτικές αξιολογήσεις και η ενημέρωση των μέτρων ασφαλείας. Το FAIR χρεώνει ετήσια συνδρομή μέλους για πρόσβαση στη μεθοδολογία, εκπαίδευση, πιστοποίηση και συνεχή υποστήριξη. Το πλαίσιο RiskIT είναι διαθέσιμο στα μέλη της ISACA ως μέρος του πακέτου συνδρομής τους. Το ISO 27005 έχει κόστος απόκτησης επιπλέον των υπολοίπων δαπανών που έχουν αναφερθεί παραπάνω. Το OCTAVE Allegro επιβαρύνεται με άδεια χρήσης και επιπλέον εκπαίδευση. Τέλος το Verinice παρέχει μία έκδοση η οποία διατίθεται δωρεάν με περιορισμένες όμως λειτουργίες και μία εμπορική έκδοση η οποία παρέχει προηγμένες λειτουργίες οι οποίες προσφέρονται σε διαφορετικές επιλογές αδειοδότησης, όπως άδεια χρήσης για έναν χρήστη, άδεια χρήσης για ομάδες και άδεια χρήσης για ολόκληρη την εταιρεία.

6. Αποτελέσματα

6.1 Σύνοψη των κυρίων ευρημάτων

Συνοψίζοντας τα ευρήματα της παρούσας μελέτης και εκπληρώνοντας και τη χρηστικότητα που θέλουμε να παρέχουμε στον αναγνώστη , παραθέτουμε μία λίστα με τα καταλληλότερα πλαίσια, μεθοδολογίες και εργαλεία που μπορούν να υιοθετηθούν από έναν οργανισμό για τη διαχείριση της επικινδυνότητας της ασφάλειας των πληροφοριών του , όπως προέκυψαν από την έως τώρα συγκριτική αξιολόγηση.

6.1.1 Το καταλληλότερο πλαίσιο

Το ISO/IEC 27005 κρίνεται το καταλληλότερο και αποτελεσματικότερο πλαίσιο που μπορεί να υιοθετηθεί από έναν οργανισμό διότι καλύπτει την πλειονότητα των κριτηρίων που θέσαμε στην παρούσα μελέτη, τόσο ποιοτικών όσο και πρακτικών. Καλύπτει πλήρως το σκοπό της διαχείρισης της επικινδυνότητας της ασφάλειας των πληροφοριών σε όλους τους τομείς και αναφέρεται σε οργανισμούς και επιχειρήσεις οποιουδήποτε μεγέθους και κλάδου.

Είναι χρηστικό, ευέλικτο, παρέχει βάσεις δεδομένων για απειλές και ευπάθειες, δεν ασχολείται με τα μέτρα ασφαλείας γιατί θεωρεί ότι χρειάζεται ξεχωριστή λύση σε αυτόν τον τομέα , παρέχει καθοδήγηση σχετικά με τη διαχείριση των περιστατικών και των επιχειρησιακών διαδικασιών, παρέχει τη δυνατότητα υποβολής αναφορών και αναλύσεων, δεν απαιτεί υψηλό επίπεδο τεχνικών γνώσεων , αν και χρειάζεται η συμβολή εμπειρογνωμόνων για τη εφαρμογή του , υποστηρίζεται ευρέως με πηγές και πόρους , θεωρείται ένα πλήρες πλαίσιο γενικά και δεν είναι χρονοβόρο, αλλά έχει ένα υψηλό κόστος υλοποίησης , εφαρμογής και παρακολούθησης.

6.1.2 Η καταλληλότερη μεθοδολογία.

Η μεθοδολογία EU ITSRM κρίνεται ως καταλληλότερη και αποτελεσματικότερη επειδή παρέχει μια δομημένη και συστηματική προσέγγιση για τη διαχείριση της επικινδυνότητας της ασφάλειας πληροφοριών , συμπεριλαμβανομένης της καθοδήγησης σχετικά με την αξιολόγηση των κινδύνων, την αντιμετώπιση των κινδύνων και τη συνεχή βελτίωση. Είναι ειδικά σχεδιασμένη για τα θεσμικά όργανα και τους οργανισμούς της Ευρωπαϊκής Ένωσης (ΕΕ).

Είναι χρηστική και ευέλικτη , παρέχει βάση δεδομένων για μέτρα ασφαλείας , ενώ καλύπτει μερικώς τη βάση δεδομένων για τις απειλές και καθόλου αυτή για τις ευπάθειες, παρέχει καθοδήγηση σχετικά με την πλοήγηση σε περιστατικά ενώ δεν επικεντρώνεται καθόλου στις επιχειρησιακές διαδικασίες , υποστηρίζει την υποβολή αναφορών και αναλύσεων ενώ απαιτεί ένα μέτριο επίπεδο τεχνικότητας , θεωρείται μία πλήρης μεθοδολογία στο πλαίσιο της διαχείρισης της επικινδυνότητας της ασφάλειας των πληροφοριών , δεν απαιτεί εκτεταμένο χρόνο για την υλοποίηση και την εφαρμογή της και το κόστος της θεωρείται μέτριο.

6.1.3 Το καταλληλότερο εργαλείο

Εκ των δύο εργαλείων που εξετάστηκαν στην παρούσα μελέτη καταλληλότερο και αποτελεσματικότερο κρίθηκε το Verinice-Risk Management Tool επειδή είναι ένα ιδιαίτερα

προσαρμόσιμο εργαλείο , επιτρέποντας στους οργανισμούς να προσαρμόζουν το εργαλείο στις συγκεκριμένες ανάγκες και απαιτήσεις τους. Περιλαμβάνει μια ισχυρή ενότητα αξιολόγησης της επικινδυνότητας που εμπεριέχει αξιολόγηση των απειλών και των ευπαθειών , αυτοματοποιημένο υπολογισμό του επιπέδου κινδύνου για κάθε περιουσιακό στοιχείο ή σύστημα και προτείνει στρατηγικές μετριασμού επικινδυνότητας περιγράφοντας τα βήματα που απαιτούνται για την αντιμετώπιση των εντοπισμένων κινδύνων. Παρέχει εκτεταμένες δυνατότητες αναφοράς και τεκμηρίωσης και μπορεί εύκολα να ενσωματωθεί με άλλα εργαλεία και συστήματα. Δεν περιλαμβάνει ελέγχους επιχειρησιακών διαδικασιών και απαιτεί ένα υψηλό επίπεδο τεχνικών γνώσεων.

Τα παραπάνω αποτελέσματα δεν ακυρώνουν την εγκυρότητα ή την αποτελεσματικότητα των υπόλοιπων πλαισίων , μεθοδολογιών και εργαλείων που εξετάστηκαν στην παρούσα μελέτη.

6.2 Κατηγοριοποίηση αποτελεσμάτων.

Τα αποτελέσματα που προέκυψαν από την συγκριτική αξιολόγηση και παρατίθενται στη συνέχεια, έρχονται να εκπληρώσουν τον επόμενο στόχο της παρούσας μελέτης , που είναι η παρουσίαση των χαρακτηριστικών και η καταλληλότητα των πλαισίων, μεθοδολογιών και εργαλείων σε σχέση με τα χαρακτηριστικά αυτά , έτσι ώστε να παρέχουν σαφή εικόνα για την καταλληλότητα τους, σύμφωνα με τις ανάγκες που θέλει να καλύψει κάποιος.

6.2.1 Ποιοτικά χαρακτηριστικά

I. Όταν αναζητάμε τη χρηστικότητα, όπως έχει ορισθεί στην παρούσα μελέτη, από ένα πλαίσιο μεθοδολογία ή εργαλείο έχουμε να επιλέξουμε μέσα από το σύνολο των λύσεων που εξετάστηκαν στην παρούσα μελέτη τα FAIR, RiskIT, ISO/IEC 27005, EU ITSRM^2 και OCTAVE Allegro. Οι λιγότερο θελκτικές σε σχέση με την χρηστικότητα είναι το COSO IC-IF, το MSAT , το NIST SP 800-30 και το Verinice.

II. Όταν αναζητάμε ένα ευέλικτο πλαίσιο, μεθοδολογία ή εργαλείο, έχουμε να επιλέξουμε μέσα από το σύνολο των εξεταζόμενων λύσεων με μόνη εξαίρεση το λιγότερο ευέλικτο που είναι το FAIR.

III. Όταν αναζητάμε μία λύση η οποία δεν απαιτεί υψηλό επίπεδο τεχνικών γνώσεων για την εφαρμογή της έχουμε να επιλέξουμε μέσα από ένα σύνολο που απαιτεί μέτριο επίπεδο τεχνικών γνώσεων και που αποτελείται από τα COSO IC-IF, Risk IT, ISO/IEC 27005 , EU ITSRM^2 , MSAT και OCTAVE Allegro. Το Fair, το NIST SP 800-0 και το Verinice απαιτούν υψηλό επίπεδο τεχνικότητας , όπως έχει ορισθεί στην παρούσα μελέτη.

IV. Όταν μας ενδιαφέρει η πληρότητα στη διαχείριση της επικινδυνότητας που παρέχει ένα πλαίσιο, μεθοδολογία ή εργαλείο , έχουμε να επιλέξουμε μεταξύ των πλαισίων Risk IT , ISO/IEC 27005 , των μεθοδολογιών EU ITSRM^2 , OCTAVE Allegro και του εργαλείου Verinice. Με το λιγότερο πλήρες να είναι το εργαλείο MSAT.

V. Όταν αναζητούμε μια σύντομη και αποτελεσματική διαδικασία αξιολόγησης κινδύνων που μπορεί να παρέχει σε έναν οργανισμό τις πληροφορίες που χρειάζεται για την αποτελεσματική διαχείριση της επικινδυνότητας της ασφάλειας των πληροφοριών, μειώνοντας παράλληλα τον χρόνο και τους πόρους που απαιτούνται για την υλοποίηση της έχουμε να επιλέξουμε μεταξύ του Risk IT, του EU ITSRM2, του MSAT και του OCTAVE Allegro ενώ θα πρέπει να αποκλείσουμε ως αρκετά χρονοβόρα το COSO IC-IF και το NIST SP 800-30.

VI. Όταν αναζητούμε μια οικονομικά αποδοτική προσέγγιση διαχείρισης επικινδυνότητας, ώστε ο οργανισμός να μπορεί να διαθέσει τους πόρους του σε άλλες σημαντικές πρωτοβουλίες και δράσεις και παράλληλα να έχουμε μεγιστοποίηση των οφελών της επένδυσής ελαχιστοποιώντας παράλληλα το κόστος τότε όλες οι προτεινόμενες λύσεις μπορούν να χρησιμοποιηθούν αποτελεσματικά γιατί τα οφέλη της αποτελεσματικής διαχείρισης επικινδυνότητας της ασφάλειας πληροφοριών μπορούν να προσφέρουν σημαντικά οφέλη για τον οργανισμό μακροπρόθεσμα. Μόνο το ISO/IEC 27005 και το OCTAVE Allegro, από τη λίστα των πλαισίων, μεθοδολογιών και εργαλείων θεωρούνται οι λιγότερο οικονομικές λύσεις.

6.2.2 Χρηστικά χαρακτηριστικά

I. Όταν κάποιος θέλει πλήρη διαχείριση των περιουσιακών στοιχείων του, στο πλαίσιο της διαχείρισης της επικινδυνότητας της ασφάλειας των πληροφοριών, θα πρέπει να επιλέξει μεταξύ των FAIR, RiskIT, ISO 27005, EU ITSRM^2 , OCTAVE Allegro και Verinice. Με το COSO IC-IF και το MSAT να μην περιλαμβάνουν καθόλου αυτό το χαρακτηριστικό.

II. Όταν κάποιος θέλει να ιεραρχήσει τις προσπάθειες μετριασμού της επικινδυνότητας βάση της πιθανότητας και του αντίκτυπου συγκεκριμένων απειλών, αναζητά μία βάση δεδομένων για τις απειλές στη λύση που θα επιλέξει. Τη δυνατότητα αυτή την παρέχουν το ISO/IEC 27005 και το NIST SP 800-30. Ενώ το Risk IT, το MSAT και το Verinice δεν καλύπτουν καθόλου αυτό το χαρακτηριστικό.

III. Όταν κάποιος θέλει να γνωρίζει πληροφορίες σχετικά με γνωστές ευπάθειες σε λογισμικό, υλικό και άλλα συστήματα, μαζί με λεπτομέρειες σχετικά με τον τρόπο με τον οποίο μπορούν να αξιοποιηθούν και τον τρόπο επιδιόρθωσης ή μετριασμού των ευπαθειών αυτών , τότε αναζητά μία βάση δεδομένων ευπαθειών στη λύση που θα επιλέξει. Τη δυνατότητα αυτή την παρέχει μόνο το ISO/IEC 27005. Το COSO IC-IF , το Risk IT, το EU ITSRM^2, το MSAT, το OCTAVE Allegro και το Verinice δεν παρέχουν καθόλου αυτή τη δυνατότητα.

IV. Όταν κάποιος θέλει να δημιουργήσει ένα ολοκληρωμένο σχέδιο ασφαλείας, το οποίο μπορεί να περιλαμβάνει πληροφορίες σχετικά με τα μέτρα που πρέπει να εφαρμοστούν, τη σειρά με την οποία πρέπει να εφαρμοστούν και τους πόρους που απαιτούνται για την εφαρμογή τους, τότε αναζητά μία βάση δεδομένων με μέτρα ασφαλείας στη λύση που θα επιλέξει. Μία τέτοια δυνατότητα παρέχουν πλήρως τα EU ITSRM^2 , MSAT και Verinice. Το Risk IT ,το ISO/IEC 27005, το NIST SP 800-30 και το OCTAVE Allegro δεν παρέχουν αυτή τη

δυνατότητα για λόγους που έχουμε αναφέρει σε προηγούμενη ενότητα της παρούσας μελέτης.

V. Όταν κάποιος επιθυμεί να ανταποκρίνεται γρήγορα και αποτελεσματικά σε παραβιάσεις της ασφάλειας, να ελαχιστοποιούνται οι ζημίες που μπορεί να προκληθούν και να αποτρέπονται παρόμοια περιστατικά από το να συμβούν στο μέλλον, τότε η λύση που θα επιλέξει θα πρέπει να διαθέτει δυνατότητα πλοήγησης σε περιστατικά. Το Risk IT και το Verinice παρέχουν πλήρως μία τέτοια δυνατότητα ενώ τα FAIR, NIST SP 800-30 και OCTAVE Allegro δεν παρέχουν καθόλου αυτή τη δυνατότητα.

VI. Όταν αναζητείται η διασφάλιση ότι οι πολιτικές και οι διαδικασίες ασφάλειας πληροφοριών ενσωματώνονται στις επιχειρηματικές διαδικασίες, ότι ακολουθούνται και με συνέπεια και ότι οι επιχειρηματικές διαδικασίες εκτελούνται σωστά, αποτελεσματικά και με ασφάλεια, τότε η λύση που θα επιλεγεί θα προβλέπει έλεγχο των επιχειρηματικών διαδικασιών. Αυτό το χαρακτηριστικό καλύπτεται από το COSO IC-IF και το OCTAVE Allegro, ενώ το FAIR, το EU ITSRM2, το MSAT, το NIST SP 800-30 και το Verinice δεν προσφέρουν καθόλου αυτή τη δυνατότητα.

VII. Όταν κάποιος επιθυμεί να έχει διαφάνεια και λογοδοσία σχετικά με την αποτελεσματικότητα του προγράμματος διαχείρισης της επικινδυνότητας, την κατανομή των πόρων του οργανισμού, να έχει μία πλήρη εικόνα για την τρέχουσα θέση της ασφάλειας των πληροφοριών στον οργανισμό , για τη συμμόρφωση με κανονιστικές απαιτήσεις, τις στρατηγικές που ακολουθούνται και τις προτεραιότητες διαχείρισης επικινδυνότητας, τότε η λύση που θα επιλέξει θα πρέπει να καλύπτει τη δυνατότητα υποβολής αναφορών και αναλύσεων. Όλα τα πλαίσια, οι μεθοδολογίες και τα εργαλεία καλύπτουν πλήρως αυτό το πολύ σημαντικό, για τη διαδικασία διαχείρισης της επικινδυνότητας των πληροφοριών, χαρακτηριστικό.

VIII. Όταν κάποιος αναζητά στο πλαίσιο, μεθοδολογία ή εργαλείο που θα επιλέξει να του παρέχει βοήθεια και τεχνική υποστήριξη τότε αναζητά μία λύση που να διαθέτει κατάλληλη υποστήριξη και πόρους: α) για την εκμάθηση και την εφαρμογή του , β) για την τυχόν εκπαίδευση που μπορεί να απαιτείται, γ) για την παροχή εγχειριδίων χρήσης και οδηγούς βήμα προς βήμα, δ) να υποστηρίζεται κατάλληλα έτσι ώστε να επιλύονται τυχόν τεχνικά ή λειτουργικά προβλήματα που μπορεί να αντιμετωπίσει κάποιος κατά τη χρήση του πλαισίου, της μεθοδολογίας ή του εργαλείου. Όλα τα πλαίσια, οι μεθοδολογίες και τα εργαλεία που εξετάστηκαν στο πλαίσιο αυτής της μελέτης υποστηρίζονται πλήρως και με κάθε τρόπο από τους δημιουργούς των λύσεων .

6.3 Περαιτέρω έρευνα

Με βάση τα ευρήματα της παρούσας μελέτης, η μελλοντική έρευνα στον τομέα της διαχείρισης της επικινδυνότητας της ασφάλειας των πληροφοριών θα μπορούσε να στοχεύσει στη διεύρυνση των κριτηρίων συγκριτικής αξιολόγησης και στη συμπερίληψη ενός ευρύτερου φάσματος πλαισίων, μεθοδολογιών και εργαλείων. Με τον τρόπο αυτό, η παρούσα έρευνα θα μπορούσε να προσφέρει μια πιο ολοκληρωμένη και σε βάθος

κατανόηση του τομέα και να συμβάλει στην παραγωγή πιο έγκυρων και ολοκληρωμένων προτάσεων για τη διαχείριση της επικινδυνότητας της ασφάλειας των πληροφοριών.
Για παράδειγμα, μία μελλοντική έρευνα θα μπορούσε να στοχεύσει :

- Στην ενσωμάτωση πρόσθετων πλαισίων, μεθοδολογιών και εργαλείων έτσι ώστε να προσφέρει μια ακόμα πιο ολοκληρωμένη κατανόηση του πεδίου
- Στην ανάπτυξη νέων κριτηρίων συγκριτικής αξιολόγησης ώστε να συμβάλει στη βελτίωση της τρέχουσας προσέγγισης της διαχείρισης επικινδυνότητας και στον εντοπισμό τομέων προς βελτίωση.
- **Στη μελέτη της επίδρασης των διαφόρων οργανωτικών παραγόντων , όπως το μέγεθος, ο κλάδος και η κουλτούρα**, στην υιοθέτηση και την εφαρμογή κατάλληλων πρακτικών διαχείρισης επικινδυνότητας της ασφάλειας των πληροφοριών, ώστε να διασφαλίζεται η αποτελεσματικότητα των στρατηγικών διαχείρισης της.
- Στην αξιολόγηση της αποτελεσματικότητας των πρακτικών διαχείρισης επικινδυνότητας σε σενάρια του πραγματικού κόσμου ώστε να παραχθούν πολύτιμες πληροφορίες για το πώς αυτά μπορούν να εφαρμοστούν αποτελεσματικά στον πραγματικό κόσμο.

Συμπεράσματα

Η διαχείριση της επικινδυνότητας της ασφάλειας πληροφοριών είναι ένα κρίσιμο ζήτημα για τους οργανισμούς ανεξαρτήτου μεγέθους ή κλάδου, καθώς η αυξανόμενη εξάρτηση από την τεχνολογία και η διασυνδεδεμένη φύση των πληροφοριακών συστημάτων έχουν καταστήσει τους κινδύνους ασφάλειας πληροφοριών πιο πολύπλοκους και δύσκολα διαχειρίσιμους. Σε αυτό το πλαίσιο, είναι σημαντικό για τους οργανισμούς να έχουν πρόσβαση σε αποτελεσματικά πλαίσια, μεθοδολογίες και εργαλεία για τη διαχείριση της επικινδυνότητας, προκειμένου να μετριάσουν τις πιθανές επιπτώσεις των απειλών στον κυβερνοχώρο και να προστατεύσουν τις ευαίσθητες πληροφορίες και τα περιουσιακά τους στοιχεία.

Η παρούσα μελέτη ανέδειξε την ιδιαίτερη φύση των λύσεων που παρέχονται προς υιοθέτηση από τους οργανισμούς.

Με την παρούσα μελέτη διαπιστώσαμε ότι καμία ενιαία μεθοδολογία, πλαίσιο ή εργαλείο δεν μπορεί να απευθύνεται σε όλους τους οργανισμούς, γιατί οι διάφοροι οργανισμοί και κλάδοι έχουν διαφορετικές απαιτήσεις και περιορισμούς. Ορισμένες μεθοδολογίες επικεντρώνονται στην αξιολόγηση και την ανάλυση επικινδυνότητας, ενώ άλλες επικεντρώνονται στον μετριασμό και την αντιμετώπιση των επικινδυνότητας. Ορισμένες είναι ολοκληρωμένες, καλύπτοντας όλα τα στάδια της διαδικασίας διαχείρισης κινδύνου ασφάλειας πληροφοριών, ενώ άλλες είναι πιο εξειδικευμένες, εστιάζοντας σε μια συγκεκριμένη πτυχή της διαδικασίας.

Για την παρούσα μελέτη χρησιμοποιήθηκε ένα συνδυασμός ποιοτικών και χρηστικών κριτηρίων αξιολόγησης, προκειμένου να παραχθεί μια εμπεριστατωμένη και διαφοροποιημένη κατανόηση των δυνατών και αδύναμων σημείων κάθε προσέγγισης. Η συγκριτική αξιολόγηση που πραγματοποιήθηκε , μπορεί να χρησιμοποιηθεί για την ενημέρωση της επιλογής πλαισίων, μεθοδολογιών και εργαλείων για τη διαχείριση της επικινδυνότητας της ασφάλειας πληροφοριών, με βάση συγκεκριμένες οργανωτικές ανάγκες και στόχους.

Αξιολογώντας ένα πλαίσιο, μια μεθοδολογία ή ένα εργαλείο βάσει αυτών των κριτηρίων συγκριτικής αξιολόγησης, οι οργανισμοί μπορούν να καθορίσουν αν είναι κατάλληλο για τις ανάγκες τους όσον αφορά τη διαχείριση επικινδυνότητας της ασφάλειας πληροφοριών. Εάν ένα πλαίσιο, μια μεθοδολογία ή ένα εργαλείο πληροί τα περισσότερα από τα χαρακτηριστικά που ορίζονται στην παρούσα μελέτη, μπορεί να θεωρηθεί βέλτιστη πρακτική για τη διαχείριση κινδύνων ασφάλειας πληροφοριών.

Αναφορές

1. Committee of Sponsoring Organizations of the Treadway Commission , (September 2012), *COSO - Internal Control—Integrated Framework,* https://ce.jalisco.gob.mx/sites/ce.jalisco.gob.mx/files/coso_mejoras_al_control_interno.pdf

2. Risk & Compliance Jounal by Deloitte, (Jan, 27, 2016), *COSO - guided Cybersecurity: Risk Assessment*, https://deloitte.wsj.com/articles/coso-guided-cybersecurity-risk-assessment-1453870942

3. Risk & Compliance Jounal by Deloitte, (Jan. 6, 2016), *Using the COSO Framework to Mitigate Cyber Risks, https://deloitte.wsj.com/articles/using-the-coso-framework-to-mitigate-cyber-risks-1452056499*

4. Deloitte, Mary E. Galligan | Sandy Herrygers | Kelly Rau,(November 2019), *COSO – Deloitte Managing Cyber Risk in a Digital Age*, https://www.coso.org/Shared%20Documents/COSO-Deloitte-Managing-Cyber-Risk-in-a-Digital-Age.pdf

5. Christophe Veltsos, (December 11, 2017), *Understanding the COSO 2017 Enterprise Risk Management Framework, Part 1: An Introduction,* https://securityintelligence.com/understanding-the-coso-2017-enterprise-risk-management-framework-part-1-an-introduction/

6. Protiviti KnowledgeLeader, (Mar 12, 2020*), Five Components of the COSO Framework You Need to Know,* https://info.knowledgeleader.com/bid/161685/What-Are-the-Five-Components-of-the-COSO-Framework

7. Society of Corporate Compliance and Ethics & Health Care Compliance Association (SCCE & HCCA), (November 2020), Compliance Risk Management : Applying the COSO ERM framework, https://www.coso.org/Shared%20Documents/Compliance-Risk-Management-Applying-the-COSO-ERM-Framework.pdf

8. Ann Snook, (November 21st, 2019), *COSO Framework: What it is and How to Use it, https://www.i-sight.com/resources/coso-framework-what-it-is-and-how-to-use-it/*

9. Graham L., (2015) *Internal Control Audit and Compliance: Documentation and Testing Under the New COSO Framework*, https://doi.org/10.1002/9781119029540

10. Uwadiae O. Financial Reporting -Deloitte (2015), *COSO - An Approach to Internal Control Framework*, https://www2.deloitte.com/za/en/nigeria/pages/audit/articles/financial-reporting/coso-an-approach-to-internal-control-framework.html

11. Bill Dixon Nebraska CERT Conference (2009), *Understanding the FAIR Risk Assessment*, https://www.certconf.org/presentations/2009/files/TA-2.pdf

12. Jack Freund | Jack Jones (2015), *Measuring and Managing Information Risk : A FAIR Approach*, https://dl.acm.org/doi/pdf/10.5555/2769769

13. https://www.fairinstitute.org/what-is-fair

14. ANAÏS ETIENNE (2021), *Cyber risk quantification : understanding the FAIR methodology*, https://www.riskinsight-wavestone.com/en/2020/10/cyber-risk-quantification-understanding-the-fair-methodology/

15. ISACA (2009), *The RiskIT Framework*, https://www.hci-itil.com/ITIL_v3/docs/RiskIT_FW_30June2010_Research.pdf

16. Anestis Demopoulos (April 2012), *Assessing & Managing IT Risks: Using ISACA's Cobit & Risk IT Frameworks*, https://infocomsecurity.gr/ppts_2012/demopoulos_isaca.pdf

17. ISACA (June 25, 2020), *ISACA's Risk IT Framework Offers a Structured Methodology for Enterprises to Manage Information and Technology Risk*, https://www.isaca.org/why-isaca/about-us/newsroom/press-releases/2020/isacas-risk-it-framework-offers-a-structured-methodology

18. Kaitlyn Archibald (FEBRUARY 4, 2021), *5 IT Risk Management Frameworks to Consider for Your Program*, https://www.onetrust.com/blog/5-it-risk-management-frameworks-to-consider-for-your-program/

19. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) (2022), *ISO 27005*, https://www.itgovernance.co.uk/iso27005

20. Steven Ross , (Feb, 2010), *Applying the ISO 27005 risk management standard*, https://www.techtarget.com/searchsecurity/tip/Applying-the-ISO-27005-risk-management-standard

21. Pia Bogush (Feb 14,2022), ISO 27005 in 6 Steps: A Quick Overview of ISO 27005 for Business Users, https://www.businesstechweekly.com/legal-and-compliance/iso27001-certification/iso-27005/

22. ENISA (Dec 2022), *Interoperable EU Risk Management Framework,* https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-framework

23. ENISA (Jan 13,2022), Compendium of Risk Management Frameworks with Potential Interoperability, https://www.enisa.europa.eu/publications/compendium-of-risk-management-frameworks

24. SecurityScorecard (May 25,2018), *IT Security Risk Assessment Methodology: Quantitative vs Qualitative Approaches*, https://securityscorecard.com/blog/it-security-risk-assessment-methodology/

25. Saluja, U., & Idris, D. N. B. (2015). Statistics Based Information Security Risk Management Methodology., International Journal of Computer Science and Network

26. Spears, J. L., & Barki, H. (2010). *User participation in information systems security risk management. MIS Quarterly: Management Information Systems*, 34(SPEC. ISSUE 3), 503–522. https://doi.org/10.2307/25750689

27. Mayer, N., Aubert, J., Grandry, E., Feltus, C., Goettelmann, E., & Wieringa, R. (2019). *An integrated conceptual model for information system security risk management supported by enterprise architecture management. Software and Systems Modeling*, https://doi.org/10.1007/s10270-018-0661-x

28. Bergström, E., Lundgren, M., & Ericson, Å. (2019). *Revisiting information security risk management challenges: a practice perspective. Information and Computer Security*, https://doi.org/10.1108/ICS-09-2018-0106

29. Stroie, E. R., & Rusu, A. C. (2011). *Security Risk Management - Approaches and Methodology. Informatica Economica*, https://core.ac.uk/download/pdf/6612749.pdf

30. Fatima, M., Abbas, H., Yaqoob, T., & Ahmad, Z. (2021). FOIST - Framework for Operating System Testing by Integrating Standards and Tools. https://doi.org/10.1109/ComTech52583.2021.9616680

31. Zubair Alexander, (Dec 9, 2005), *Microsoft Security Assessment Tool: Can It Make Your Organization More Secure?* https://www.informit.com/articles/article.aspx?p=431710&seqNum=6

32. Turgut, Y. (2016). *A Comparative Analysis of University Information Systems within the Scope of the A Comparative Analysis of University Information Systems within the Scope of the Information Security Risks*. http://www.tem-journal.com/content/52/TemJournalMay2016_180_191.pdf

33. Kuzminykh, I | Ghita, B.| Sokolov, V.| Bakhshi, T. (2021), *Information Security Risk Assessment.* https://www.researchgate.net/publication/353436973_Information_Security_Risk_Assessment

34. https://www.microsoft.com/en-us/security/business/threat-protection/security-operations-assessment?activetab=solution-wizard%3aprimaryr2

35. Microsoft (Jan 27,2023), *Threat and vulnerability management overview*, https://learn.microsoft.com/en-us/compliance/assurance/assurance-vulnerability-management.

36. Microsoft (2023), *The Microsoft Security Assessment Tool*, https://www.microsoft.com/en-us/download/details.aspx?id=12273

37. ISACA (Jan 1, 2010), Performing a Security Risk Assessment, https://www.isaca.org/resources/isaca-journal/past-issues/2010/performing-a-security-risk-assessment

38. NIST, (Sep 2012.) Special Publication 800-30 Revision 1 - Guide for Conducting Risk Assessments. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf

39. Supriyadi, Y., & Hardani, C. W. (2018). Information system risk scenario using COBIT 5 for risk and NIST SP 800-30 Rev. 1 a case study. In Proceedings - 2018 3rd International Conference on Information Technology, Information Systems and Electrical Engineering, ICITISEE 2018 (pp. 287–291). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ICITISEE.2018.872103

40. Caralli, R. a R. a. C., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). Introducing OCTAVE Allegro : Improving the Information Security Risk Assessment Process, https://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf

41. Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). The OCTAVE Allegro Guidebook. https://www.scribd.com/document/344795891/OCTAVE-Allegro-Method-v1-0-doc#

42. Corland G. Keating (2014), Validating the OCTAVE Allegro Information Systems Risk Assessment Methodology: A Case Study , https://nsuworks.nova.edu/cgi/viewcontent.cgi?article=1191&context=gscis_etd

43. Caralli, Richard | Stevens, James F. | Young, Lisa R.| Wilson, William R. (2018): Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. https://doi.org/10.1184/R1/6574790.v1

44. Hom, J., Anong, B., Rii, K. B., Choi, L. K., & Zelina, K. (2020). The Octave Allegro Method in Risk Management Assessment of Educational Institutions. https://doi.org/10.34306/att.v2i2.103

45. Prajanti, A. D., & Ramli, K. (2019). A Proposed Framework for Ranking Critical Information Assets in Information Security Risk Assessment Using the OCTAVE Allegro Method with Decision Support System Methods https://doi.org/10.1109/ITC-CSCC.2019.8793421

46. Cyrill Brunchwiler (Apr 9, 2013), Lean Risk Assessment based on OCTAVE Allegro, https://blog.compass-security.com/2013/04/lean-risk-assessment-based-on-octave-allegro/

47. Alberts, C., & Dorofee, A. (2009). *OCTAVE Threat Profiles. ISACA Journal*, https://search.proquest.com/docview/891463174

48. European Commission, About Verinice - the ISMS tool, https://joinup.ec.europa.eu/collection/ict-security/solution/verinice-isms-tool/about

49. Yildirim, E. Y. (2017). The Importance of Risk Management in Information Security. International Journal of Advances in Electronics and Computer Science, 4(1), 18–21. http://iraj.in

50. Fenz, S., Heurix, J., Neubauer, T., & Pechstein, F. (2014). Current challenges in information security risk management. https://doi.org/10.1108/IMCS-07-2013-0053

51. Zarei, J., & Sadoughi, F. (2016). Information security risk management for computerized health information systems in hospitals: A case study of Iran. https://doi.org/10.2147/RMHP.S99908

52. Fenz, S., Heurix, J., Neubauer, T., & Pechstein, F. (2014). *Current challenges in information security risk management. Information Management and Computer Security,*. https://doi.org/10.1108/IMCS-07-2013-0053

ΠΙΝΑΚΑΣ ΟΡΩΝ

Ελληνικά	Αγγλικά
Σύστημα διαχείρισης της ασφάλειας των πληροφοριών	Information Security Management System
Πλαίσιο	Framework
Μεθοδολογία	Methodology
Εργαλείο	Tool
Χρηστικότητα	Usability
Ευελιξία	Ευελιξία
Διαχείριση περιουσιακών στοιχείων	Asset management
Βάση δεδομένων για απειλές	Database for threats
Βάση δεδομένων για ευπάθειες	Database for vulnerabilities
Βάση δεδομένων για μέτρα ασφαλείας	Database for controls
Πλοήγηση σε περιστατικά	Incident navigation
Έλεγχος επιχειρησιακών διαδικασιών	Business process control
Αναφορές και αναλύσεις	Reporting and analytics
Επίπεδο τεχνικότητας	Technicality
Υποστήριξη και πόροι	Support and resources
Πληρότητα	Completeness
Χρόνος/Διάρκεια	Time /Duration
Οικονομικό κόστος	Financial Cost
Συχνότητα συμβάντων απώλειας	Lost Event Frequency
Πληροφορική	Information Technology
Διακυβέρνηση επικινδυνότητας	Risk Governance
Εκτίμηση επικινδυνότητας	Risk Evaluation
Απόκριση στην επικινδυνότητα	Risk Response
Προσδιορισμός επικινδυνότητας	Risk Identification
Καθορισμός πλαισίου	Context Establishment
Αξιολόγηση επικινδυνότητας	Risk assessment
Αντιμετώπιση επικινδυνότητας	Risk Treatment
Ευρωπαϊκή Επιτροπή	European Commission
Μητρώο περιουσιακών στοιχείων	Asset Register
Βασική γραμμή προστασίας	IT Baseline Protection
Έγγραφα και αρχεία	Documents and Records
Αναφορές	Reporting
Διεπαφές	Interfaces
Έλεγχοι & Πιστοποιήσεις	Audits & Certifications

Αγγλικά	Ελληνικά
Information Security Management System	Σύστημα διαχείρισης της ασφάλειας πληροφοριών
Framework	Πλαίσιο
Methodology	Μεθοδολογία
Tool	Εργαλείο
Usability	Χρηστικότητα
Flexibility	Ευελιξία
Asset management	Διαχείριση περιουσιακών στοιχείων
Database for threats	Βάση δεδομένων για απειλές
Database for vulnerabilities	Βάση δεδομένων για ευπάθειες
Database for controls	Βάση δεδομένων για μέτρα ασφαλείας
Incident navigation	Πλοήγηση σε περιστατικά
Business process control	Έλεγχος επιχειρησιακών διαδικασιών
Reporting and analytics	Αναφορές και αναλύσεις
Technicality	Επίπεδο τεχνικότητας
Support and resources	Υποστήριξη και πόροι
Completeness	Πληρότητα
Time /Duration	Χρόνος/Διάρκεια
Financial Cost	Οικονομικό κόστος
Lost Event Frequency	Συχνότητα συμβάντων απώλειας
Information Technology	Πληροφορική
Risk Governance	Διακυβέρνηση επικινδυνότητας
Risk Evaluation	Εκτίμηση επικινδυνότητας
Risk Response	Απόκριση στην επικινδυνότητα
Risk Identification	Προσδιορισμός επικινδυνότητας
Context Establishment	Καθορισμός πλαισίου
Risk assessment	Αξιολόγηση επικινδυνότητας
Risk Treatment	Αντιμετώπιση επικινδυνότητας
European Commission	Ευρωπαϊκή Επιτροπή
Internal Control - Integrated Framework	Εσωτερικός έλεγχος - Ενοποιημένο πλαίσιο
Security Assessment Tool	Εργαλείο αξιολόγησης ασφάλειας
Special Publication	Ειδική έκδοση
Risk Management Tool	Εργαλείο διαχείρισης κινδύνων
Enterprise Risk Management framework	Πλαίσιο διαχείρισης επιχειρηματικού κινδύνου
Cybersecurity Framework	Πλαίσιο κυβερνοασφάλειας
Factor Analysis of Information Risk	Ανάλυση παραγόντων πληροφοριακού κινδύνου
Analysis Body of Knowledge	Σώμα γνώσεων ανάλυσης
Information Systems Audit and Control Association	Ένωση Επιθεώρησης και Ελέγχου Πληροφοριακών Συστημάτων
Acquire and Implement	Απόκτηση και υλοποίηση
National Vulnerability Database	Εθνική βάση δεδομένων ευπαθειών
Common Vulnerabilities and Exposures	Κοινές ευπάθειες και εκθέσεις
Open Web Application Security Project	Ανοικτό έργο ασφάλειας εφαρμογών ιστού
Cloud computing	Υπολογιστικό νέφος
Risk Decision Point	Σημείο απόφασης επικινδυνότητας
Confidentiality, Integrity, Availability	Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα
Supporting Asset	Υποστηρικτικό περιουσιακό στοιχείο
Advanced Threat Protection	Προηγμένη προστασία από απειλές
Security Compliance Manager	Διαχειριστής συμμόρφωσης ασφάλειας
Security and Privacy Controls for Federal Information Systems and Organizations	Έλεγχοι ασφάλειας και απορρήτου για ομοσπονδιακά συστήματα και οργανισμούς πληροφοριών
Computer Security Incident Handling Guide	Οδηγός χειρισμού περιστατικών ασφάλειας υπολογιστών
Operationally Critical Threat, Asset, and Vulnerability Evaluation	Αξιολόγηση επιχειρησιακά κρίσιμων απειλών, περιουσιακών στοιχείων και ευπαθειών

Τέλος