ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ
UNIVERSITY OF WEST ATTICA

Σχολή Μηχανικών
Τμήμα Μηχανικών Πληροφορικής και Υπολογιστών
Πρόγραμμα Μεταπτυχιακών Σπουδών: ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

Διπλωματική Εργασία

RISK MANAGEMENT PROCESS

ISO/IEC 27005 & NIST SP 800-30 rev.1

Φοιτήτρια: Αγγελίδου Μαρία
AM:cscyb2002

Επιβλέπων Καθηγητής:

Στέφανος Γκρίτζαλης

Αιγάλεω, Μάϊος 2023

ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ
UNIVERSITY OF WEST ATTICA

Σχολή Μηχανικών
Τμήμα Μηχανικών Πληροφορικής και Υπολογιστών
Πρόγραμμα Μεταπτυχιακών Σπουδών: ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

RISK MANAGEMENT PROCESS

ISO/IEC 27005 & NIST SP. 800-30 rev.1

Μέλη εξεταστικής επιτροπής συμπεριλαμβανομένου και του Εισηγητή

Η μεταπτυχιακή διπλωματική εργασία εξετάσθηκε επιτυχώς από την κάτωθι εξεταστική Επιτροπή:

Α/Α	ΟΝΟΜΑ-ΕΠΩΝΥΜΟ	ΥΠΟΓΡΑΦΗ
1	**Δρ. Παναγιώτης Γιαννακόπουλος**	Panagiotis Giannakopoulos Digitally signed by Panagiotis Giannakopoulos Date: 2023.08.23 16:02:42 +03'00'
2	**Δρ. Στέφανος Γκρίτζαλης**	STEFANOS GKRITZALIS 25/08/2023 14:53
3	**Δρ. Κωνσταντίνος Μαυρομμάτης**	Konstantinos Mavrommatis Digitally signed by Konstantinos Mavrommatis Date: 2023.08.24 15:51:01 +03'00'

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

Η κάτωθι υπογεγραμμένη **ΑΓΓΕΛΙΔΟΥ ΜΑΡΙΑ** του **Αντωνίου,** με αριθμό μητρώου **cscyb2002** φοιτήτρια του Προγράμματος Μεταπτυχιακών Σπουδών της Κυβερνοασφά-λειας του **ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ** της σχολής ΜΗΧΑΝΙΚΩΝ του Τμήματος **ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ**,

δηλώνω υπεύθυνα 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, ανα-φέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδο-τικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδε-χομένως χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από μένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο, του Ιδρύματος όσο και δικής μου.

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

Επιθυμώ την απαγόρευση πρόσβασης στο πλήρες κείμενο της εργασίας μου, μέχρι την βαθμολόγηση της και έγκριση του επιβλέποντος καθη-γητή.»

Η ΔΗΛΟΥΣΑ
ΑΓΓΕΛΙΔΟΥ ΜΑΡΙΑ του **ΑΝΤΩΝΙΟΥ**

(Υπογραφή φοιτητή)

Ευχαριστίες

Με την ολοκλήρωση της μεταπτυχιακής διπλωματικής μου εργασίας, θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες σε όλους όσους συνέβαλλαν στην εκπόνησή της.

Ευχαριστώ θερμά τον επιβλέπων καθηγητή μου, κύριο Στέφανο Γκρίτζαλη, για την εμπιστοσύνη που μου έδειξε εξ' αρχής, αναθέτοντάς μου το συγκεκριμένο θέμα, την επιστημονική του καθοδήγηση και τη συμπαράστασή του. Επίσης, θα ήθελα να ευχαριστήσω τον υπεύθυνο καθηγητή μου κύριο Παναγιώτη Γιαννακόπουλο για την επιμονή του, το αμείωτο ενδιαφέρον του και τη συνεχή του υποστήριξη που έδειξε από την αρχή μέχρι το τέλος.

Τέλος, θα ήθελα να εκφράσω την ευγνωμοσύνη μου στη οικογένειά μου και τον σύντροφό μου για όλη τη στήριξη, τη συμπαράσταση και την κατανόησή τους καθ' όλη τη διάρκεια των σπουδών μου.

Αιγάλεω, 2023
Αγγελίδου Μαρία

RISK MANAGEMENT PROCESS

ISO/IEC 27005 & NIST SP 800-30 rev.1

Περίληψη

Στον σύγχρονο κόσμο μας και με γνώμονα την τεχνολογία, οι παραβιάσεις δεδομένων και οι επιθέσεις στον κυβερνοχώρο παραμένουν σημαντική απειλή για τους οργανισμούς. Συχνά για αυτό ευθύνεται η έλλειψη επίγνωσης των κινδύνων. Η προστασία της ασφάλειας των πληροφοριών μιας εταιρείας είτε πρόκειται για εμπορικά ευαίσθητες πληροφορίες, είτε για προσωπικά στοιχεία των πελατών δεν ήταν ποτέ περισσότερο στο επίκεντρο.

Η αξιολόγηση των κινδύνων ασφαλείας είναι ένα από τα βασικά στάδια της διαδικασίας διαχείρισης κινδύνων. Πάνω απ' όλα, αναφέρεται στον εντοπισμό των κινδύνων, την εκτίμηση των επιπτώσεων στους οργανισμούς και τον προσδιορισμό των πηγών. Οι οργανισμοί χρησιμοποιούν την αξιολόγηση κινδύνων για να προσδιορίσουν την έκταση των πιθανών απειλών, των τρωτών σημείων και των κινδύνων που σχετίζονται με ένα σύστημα τεχνολογίας πληροφοριών. Εξαιτίας αυτού, είναι δυνατός ο σχεδιασμός κατάλληλων μέτρων μετριασμού. Σίγουρα, η συνεχής βελτίωση του σχεδίου διαχείρισης κινδύνων αποτελεί επένδυση για την προστασία της φήμης, των χρημάτων και του χρόνου του οργανισμού.

Στην παρούσα εργασία θα παρουσιαστούν οι αρχές και οι διαδικασίες, βάσει των οποίων μπορεί να υλοποιηθεί αποτελεσματικά και αποδοτικά, η διαχείριση επικινδυνότητας ασφάλειας πληροφοριών, όπως αυτές περιγράφονται στο πρότυπο ISO 27005 καθώς και στην ειδική έκδοση του NIST 800-30 revision 1. Επιπλέον, θα παρουσιαστούν κάποιες μέθοδοι και εργαλεία διαχείρισης κινδύνου.

1. Εισαγωγικά στοιχεία

1.1 Γενικά

Μια συστηματική προσέγγιση στη διαχείριση επικινδυνότητας ασφάλειας πληροφοριών (Information Security Risk Management) είναι απαραίτητη για τον προσδιορισμό των οργανωτικών αναγκών σχετικά με τις απαιτήσεις ασφάλειας πληροφοριών αλλά και για τη δημιουργία ενός αποτελεσματικού Σύστηματος Διοίκησης Ασφάλειας Πληροφοριών (ISMS). Αυτή η προσέγγιση θα πρέπει να είναι κατάλληλη για το περιβάλλον του Οργανισμού και ειδικότερα, θα πρέπει να ευθυγραμμίζεται με τη συνολική διαχείριση επιχειρηματικού κινδύνου.

Η διαχείριση επικινδυνότητας ασφάλειας πληροφοριών πρέπει να αποτελεί αναπόσπαστο μέρος όλων των δραστηριοτήτων διαχείρισης ασφάλειας πληροφοριών και να εφαρμόζεται κατά την διάρκεια όλου του κύκλου ζωής ενός ISMS όντας μια συνεχής διαδικασία. Η διαδικασία αυτή πρέπει να καθορίσει το εξωτερικό και το εσωτερικό πλαίσιο αξιολόγησης των κινδύνων και να τους εντοπίσει, χρησιμοποιώντας παράλληλα ένα σχέδιο αντιμετώπισης τους, για την εφαρμογή των συστάσεων και των αποφάσεων. Η διαχείριση επικινδυνότητας αναλύει τι μπορεί να συμβεί και ποιες είναι οι πιθανές συνέπειες, πριν αποφασιστεί τι πρέπει να γίνει και πότε για να μειωθεί ο κίνδυνος σε αποδεκτό επίπεδο.

Περιεχόμενα

1.2 Συντομεύσεις - Ακρωνύμια

Information Security Management System	ISMS
Advanced Persistent Threat	APT
Business Continuity Plan	BCP
Business Impact Analysis	BIA
Committee on National Security Systems	CNSS
Continuity of Operations	COOP
Department of Defense	DoD
Department of Homeland Security	DHS
Director of National Intelligence	DNI
Enterprise Architecture	EA
Federal Information Processing Standards	FIPS
CAPEC	Common Attack Pattern Enumeration and Classification
Risk Management Framework	RMF
Federal Information Security Management Act	FISMA
Industrial Control System	ICS
International Electrotechnical Commission	IEC
International Organization for Standardization	ISO
Information Technology	IT
Joint Task Force	JTF
National Institute of Standards and Technology	NIST
Not Releasable to Foreign Nationals	NOFORN
Office of the Director of National Intelligence	ODNI
Office of Management and Budget	OMB
Risk Assessment Report	RAR
Security Content Automation Protocol	SCAP
Special Publication	SP
Tactic Technique Procedure	TTP
United States Code	U.S.C.
System Development Life Cycle	SDLC
Software as a Service	SaaS

2. ISO/IEC 27005

Το πρότυπο ISO/IEC 27005 είναι ένα διεθνές πρότυπο, το οποίο ανήκει στη σειρά προτύπων ISO/IEC 27000 και παρέχει οδηγίες για τη διαχείριση κινδύνου ασφάλειας πληροφοριών σε έναν οργανισμό. Ωστόσο, αυτό το έγγραφο δεν παρέχει καμία συγκεκριμένη μέθοδο για τη διαχείριση κινδύνου ασφάλειας πληροφοριών. Εναπόκειται στον οργανισμό να καθορίσει την προσέγγισή του στη διαχείριση κινδύνου, ανάλογα για παράδειγμα με το πεδίο εφαρμογής ενός συστήματος διαχείρισης ασφάλειας πληροφοριών (ISMS), το πλαίσιο διαχείρισης κινδύνου ή τον κλάδο της βιομηχανίας. Ορισμένες υπάρχουσες μεθοδολογίες μπορούν να χρησιμοποιηθούν στο πλαίσιο που περιγράφεται σε αυτό το έγγραφο για την υλοποίηση των απαιτήσεων ενός ISMS. Αυτό το έγγραφο βασίζεται στη μέθοδο αναγνώρισης κινδύνου περιουσιακών στοιχείων, απειλών και ευπάθειας που δεν απαιτείται πλέον από το ISO/IEC 27001. Υπάρχουν ορισμένες άλλες προσεγγίσεις που μπορούν να χρησιμοποιηθούν.

Αυτό το έγγραφο δεν περιέχει άμεσες οδηγίες για την εφαρμογή των απαιτήσεων ISMS που δίνονται στο ISO/IEC 27001.

Αυτό το έγγραφο μπορεί να εφαρμοστεί σε όλους τους οργανισμούς, ανεξαρτήτως το μέγεθος που σκοπό έχουν να διαχειριστούν απειλές που μπορεί να θέσουν σε κίνδυνο την ασφάλεια πληροφοριών.

2.1. Διοίκηση της επικινδυνότητας (risk management)

Διοίκηση επικινδυνότητας είναι μια μεθοδολογία η οποία περιλαμβάνει δύο βασικά ερωτήματα:

α) Πόσο μεγάλο είναι το πρόβλημα (risk assessment).
β) Πώς θα αντιμετωπίσουμε το πρόβλημα (risk treatment).

Συμπερασματικά, πρώτα αποτιμούμε την επικινδυνότητα και μετά την αντιμετωπίζουμε. Η μεθοδολογία της διοίκησης επικινδυνότητας υλοποιείται με την υιοθέτηση κάποιας μεθόδου (software tool). Μετά την αποτίμηση της επικινδυνότητας σε έναν Οργανισμό, για την αντιμετώπισή της απαιτείται η σύνταξη ενός σχεδίου ασφαλείας (security plan). Προϋπόθεση για να ακολουθήσει το σχέδιο ασφάλειας, είναι η οριοθέτηση του πληροφοριακού συστήματος στο οποίο θα υλοποιηθεί η διοίκηση επικινδυνότητας για να εξακριβωθεί αν ολόκληρο το πληροφοριακό σύστημα [1]θα αναλυθεί ή κάποια επιμέρους τμήματά του. Το Σχέδιο ασφάλειας θα περιλαμβάνει:

- Καθορισμό πολιτικής ασφάλειας (security policy), πρόκειται για ένα κείμενο γενικού χαρακτήρα, υψηλού επιπέδου αφαίρεσης που δείχνει κατευθυντήριες οδηγίες.
- Επιλογή Αντιμέτρων – Μέτρων ασφαλείας – Μέτρων προστασίας (countermeasures, controls, safeguards), τα οποία μπορούν να βρεθούν στο ISO 27002 και πρόκειται για τεχνικά, διοικητικά, φυσικά και αντίμετρα που σχετίζονται με τον ανθρώπινο παράγοντα.
- Εφαρμογή (roadmaps) και παρακολούθηση Σχεδίου ασφαλείας.

Η επικινδυνότητα ορίζεται ως το γινόμενο της πιθανότητας να συμβεί μια απειλή επί την επίπτωση των συνεπειών που θα έχει στον Οργανισμό όταν συμβεί. Η επικινδυνότητα δεν μπορεί να μηδενιστεί. Συμπερασματικά, στόχος είναι η απομένουσα επικινδυνότητα (residual risk) να περιοριστεί σε ¨ανεκτά¨ επίπεδα.

2.1.1 Τρόποι διοίκησης της επικινδυνότητας

Παρακάτω παρατίθενται μερικοί τρόποι τους οποίους αν ακολουθήσουμε με την σειρά που εμφανίζονται και συνδυάζοντάς τους κατάλληλα, θα επιτύχουμε αποτελεσματική διοίκηση της επικινδυνότητας.

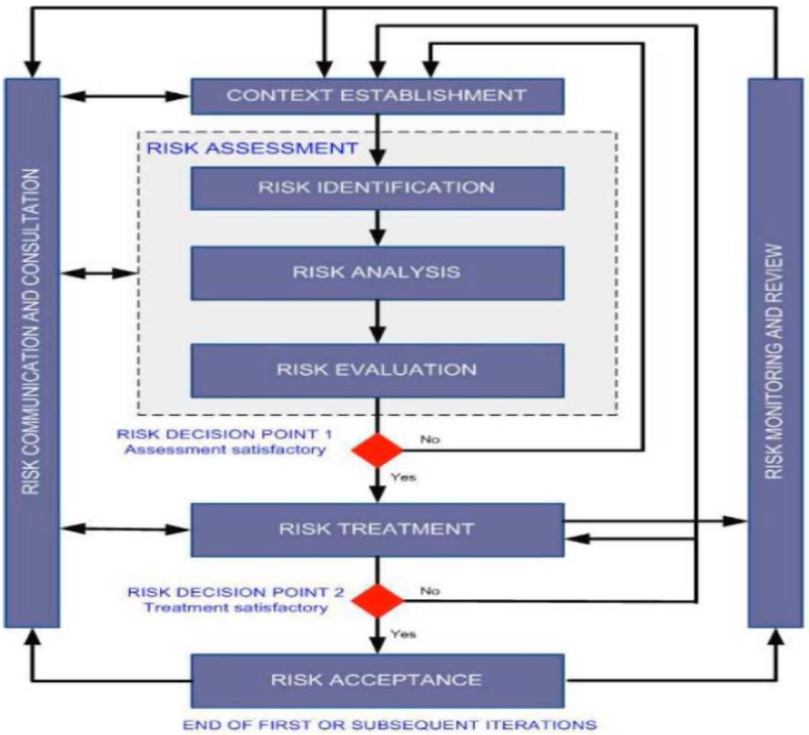
- μείωση πιθανότητας εκδήλωσης απειλών,

[1] Ένα πληροφοριακό σύστημα είναι ένα διακριτό σύνολο πόρων πληροφοριών που οργανώνονται για τη συλλογή, επεξεργασία, συντήρηση, χρήση, κοινή χρήση, διάδοση ή διάθεση πληροφοριών.

- μείωση των ευπαθειών,
- περιορισμός επιπτώσεων,
- ανάκαμψη,
- μεταβίβαση της επικινδυνότητας,
- αποδοχή της επικινδυνότητας.

2.2. Διαχείριση Επικινδυνότητας Ασφάλειας Πληροφοριών (Information Security Risk Management)

Στο παρακάτω σχήμα απεικονίζεται η διαδικασία που ακολουθείται για τη διαχείριση της επικινδυνότητας της ασφάλειας πληροφοριών σε έναν Οργανισμό.



Εικόνα 1: Διαχείριση επικινδυνότητας

Πιο αναλυτικά η διαδικασία υλοποιείται στα εξής στάδια:

- Καθορισμός περιεχομένου (Context establishment)
- Αποτίμηση επικινδυνότητας (Risk assessment)
  - Αναγνώριση επικινδυνότητας (Risk identification)
  - Ανάλυση επικινδυνότητας (Risk analysis)
  - Αξιολόγηση επικινδυνότητας (Risk evaluation)
- Αντιμετώπιση επικινδυνότητας (Risk treatment)
- Αποδοχή επικινδυνότητας (Risk acceptance)
- Επικοινωνία και συμβουλευτική (Risk communication and consultation)
- Παρακολούθηση και αναθεώρηση επικινδυνότητας (Risk monitoring and review)

Αξίζει να αναφερθεί ότι τα στάδια της διαχείρισης και αντιμετώπισης της επικινδυνότητας είναι πιθανόν να επαναληφθούν. Η επανάληψη βοηθάει στη μείωση του κινδύνου τόσο ώστε να είναι σε ανεκτά επίπεδα

για τον Οργανισμό. Ανάλογα με το εύρος και τους στόχους της διαχείρισης κινδύνου, μπορούν να εφαρμοστούν διαφορετικές προσεγγίσεις. Η προσέγγιση μπορεί επίσης να είναι διαφορετική για κάθε επανάληψη.

Θα πρέπει να αναπτυχθεί ή επιλεγεί κατάλληλη προσέγγιση διαχείρισης επικινδυνότητας που να καλύπτει επαρκώς βασικά κριτήρια. Τέτοια κριτήρια είναι: Αξιολόγησης κινδύνου, επιπτώσεων του κινδύνου και αποδοχής του κινδύνου.

Επιπλέον, ο Οργανισμός θα πρέπει να εκτιμήσει αν θα χρειαστούν επιπλέον πόροι:

- Για την αξιολόγηση κινδύνου και τη δημιουργία σχεδίου αντιμετώπισης του.
- Να ορίσει και να υλοποιήσει διαδικασίες και πολιτικές, συμπεριλαμβανομένων και των ελέγχων που έχουν επιλεγεί.
- Παρακολούθηση ελέγχων.
- Παρακολούθηση της διαδικασίας διαχείρισης κινδύνου της ασφάλειας της πληροφορίας.

Σε όλα τα στάδια της διαδικασίας ορίζονται:

- Είσοδος: οποιαδήποτε σχετική πληροφορία για την υλοποίηση της δραστηριότητας.
- Δράση: περιγραφή της δραστηριότητας
- Καθοδήγηση υλοποίησης: καθοδήγηση ως προς την υλοποίηση της δραστηριότητας. Μπορεί η καθοδήγηση να μην είναι εφικτό να εφαρμοστεί σε όλες τις περιπτώσεις.
- Έξοδος: οτιδήποτε προκύπτει ως αποτέλεσμα της δραστηριότητας .

2.3 Καθορισμός περιεχομένου (Context establishment)

- Είσοδος: Οποιαδήποτε πληροφορία θα μας βοηθήσει για να κατανοήσουμε το πλαίσιο στο οποίο θα υλοποιηθεί η διαχείριση επικινδυνότητας ασφάλειας πληροφοριών (νόμοι, κανονισμοί, συνεργάτες, διαχείριση προσωπικών δεδομένων κ.λπ.)
- Δράση: ακριβής προσδιορισμός του πλαισίου, εσωτερικού και εξωτερικού, μέσα στο οποίο θα υλοποιηθεί η διαχείριση επικινδυνότητας ασφάλειας πληροφοριών που περιλαμβάνει:
  - Τα κριτήρια βάση των οποίων θα υλοποιηθεί.
  - Τον ορισμό του περιεχομένου και των ορίων που θα υλοποιηθεί.
  - Τον ορισμό των ρόλων και των αρμοδιοτήτων που εμπλέκονται σε αυτή.
- Έξοδος: τα κριτήρια βάση των οποίων θα υλοποιηθεί η διαχείριση επικινδυνότητας ασφάλειας πληροφοριών, ο σκοπός και οι περιορισμοί/όρια εντός των οποίων θα υλοποιηθεί και οι ρόλοι και αρμοδιότητες των εμπλεκομένων σε αυτή τη διαδικασία.

Το στάδιο αυτό αποτελεί τη βάση πάνω στην οποία θα στηριχτεί η διαδικασία διαχείρισης επικινδυνότητας της ασφάλειας πληροφοριών. Πιο αναλυτικά:

- Κατανόηση του Οργανισμού: Μελέτη όλων εκείνων των στοιχείων που καθορίζουν τον Οργανισμό ως οντότητα. Με λίγα λόγια, τον σκοπό του Οργανισμού, τις δραστηριότητές του, την αποστολή και τις αξίες του. Σκοπός του Οργανισμού μπορεί να οριστεί ως ο λόγος για τον οποίο υπάρχει. Οι δραστηριότητες μιας επιχείρησης ορίζονται από τις τεχνικές και την τεχνογνωσία των ανθρώπων της και της δίνει τη δυνατότητα να φέρει εις πέρας την αποστολή της. Ένας Οργανισμός επιτυγχάνει τον σκοπό του εκπληρώνοντας την αποστολή του. Η αποστολή του αναφέρεται στα προϊόντα και στις υπηρεσίες της εταιρείας καθώς και στον τρόπο που σχετίζονται με τους πελάτες ή/και τους χρήστες. Τέλος, οι αξίες είναι οι βασικές αρχές ενός Οργανισμού. Μπορούν για παράδειγμα να συμπεριληφθούν σε κώδικα δεοντολογίας.
- Σκοπός της διαδικασία διαχείρισης κινδύνου: Για παράδειγμα αυτός μπορεί να είναι ο σκοπός ανάπτυξης ενός ISMS (Information Security Management System) ή η συμμόρφωση με νομικές απαιτήσεις.
- Ορισμός του εύρους και των ορίων της διαδικασίας διαχείρισης κινδύνου: Το πεδίο εφαρμογής μπορεί να αναφέρεται σε ολόκληρο τον Οργανισμό ή σε ένα πεδίο του Οργανισμού. Αυτό εξαρτάται από τις ανάγκες του κάθε Οργανισμού και είναι σημαντικό να καθοριστεί με σαφήνεια το πεδίο εφαρμογής ώστε να λαμβάνονται υπόψη όλα τα σχετικά περιουσιακά στοιχεία εντός του πεδίου για την αξιολόγηση κινδύνου.
- Περιορισμοί: Για κάθε Οργανισμό υπάρχουν περιορισμοί που επηρεάζουν τον προσανατολισμό της ασφάλειας πληροφοριών. Ορισμένοι περιορισμοί μπορεί να προέρχονται από τον Οργανισμό και έτσι

η επιχείρηση να έχει τον έλεγχό τους. Από την άλλη, υπάρχουν κι εξωτερικοί περιορισμοί. Όπως δημοσιονομικοί περιορισμοί, μη προσιτό κόστος, διαθεσιμότητα προσωπικού, επίγνωση ασφαλείας και επίπεδο ευθύνης του προσωπικού. Το σημαντικό είναι όλοι αυτοί οι περιορισμοί να ληφθούν υπόψη κατά τον καθορισμό πλαισίου του Οργανισμού επειδή η επιρροή τους μπορεί να είναι αξιόλογη.

Στη συνέχεια, θα πρέπει να γίνει ορισμός των βασικών κριτηρίων για τη διαχείριση επικινδυνότητας ασφάλειας πληροφοριών. Τα κριτήρια αυτά είναι:

- Κριτήρια αξιολόγησης επικινδυνότητας (Risk evaluation criteria): Αναπτύσσονται για να αξιολογήσουν την επικινδυνότητα της ασφάλειας των πληροφοριών ενός Οργανισμού. Για την αξιολόγηση αυτή λαμβάνονται υπόψη:

- Η στρατηγική αξία της επιχειρησιακής διαδικασίας πληροφοριών,
- η κρισιμότητα των αγαθών που σχετίζονται με την πληροφορία,

- η σημασία που έχει για τη λειτουργία του Οργανισμού η διαθεσιμότητα, η εμπιστευτικότητα και η ακεραιότητα της πληροφορίας,
- οι προσδοκίες και οι αντιλήψεις των εμπλεκόμενων μερών καθώς και οι πιθανές αρνητικές επιπτώσεις στη φήμη του Οργανισμού.

- Κριτήρια επίπτωσης (Impact criteria): Πρέπει να καθοριστούν με γνώμονα το εύρος της βλάβης και του κόστους σε έναν Οργανισμό όταν θα λάβει χώρα ένα συμβάν. Πρέπει να ληφθούν υπόψη:
    - Το επίπεδο ταξινόμησης του αγαθού που επηρεάζεται,
    - οι παραβιάσεις στην ασφάλεια πληροφορίας σχετικές με απώλεια διαθεσιμότητας, εμπιστευτικότητας και ακεραιότητας,
    - οι λειτουργίες (εσωτερικές ή που αφορούν τρίτα μέρη) που έχουν υποστεί βλάβη,
    - απώλεια επιχειρηματικής και οικονομικής αξίας,
    - η διαταραχή όσον αφορά στην ολοκλήρωση σχεδίων και επίτευξη προθεσμιών,
    - η βλάβη στη φήμη.

- Κριτήρια αποδοχής της επικινδυνότητας (Risk acceptance criteria): Τα κριτήρια αποδοχής της επικινδυνότητας συχνά βασίζονται στις πολιτικές του Οργανισμού, τους στόχους και τις απαιτήσεις των εμπλεκόμενων μερών. Στον καθορισμό τους συνυπολογίζονται επιχειρησιακά κριτήρια, οι λειτουργίες του Οργανισμού, η τρέχουσα τεχνολογία καθώς και παράγοντες κοινωνικοί, ανθρωπιστικοί και οικονομικοί. Είναι σημαντικό να αναφερθεί ότι τα κριτήρια αποδοχής της επικινδυνότητας είναι δυνατόν να διαφέρουν ανάλογα με τη διάρκεια της επικινδυνότητας. Πιο συγκεκριμένα τα κριτήρια μπορεί να:

    - περιλαμβάνουν πολλαπλά όρια με στόχο ένα επιθυμητό επίπεδο επικινδυνότητας αλλά στην περίπτωση αυτή, οι διαχειριστές (senior managers) θα έχουν τη δυνατότητα, κάτω από συγκεκριμένες συνθήκες, να αποδεχτούν επικινδυνότητα πάνω από αυτά τα όρια
    - αποτελούν το κλάσμα του υπολογιζόμενου κέρδους προς το υπολογιζόμενο ρίσκο
    - εφαρμόζονται για αυτά, διαφορετικά κριτήρια αποδοχής ανάλογα με την τάξη της επικινδυνότητας
    - περιέχουν απαιτήσεις για μελλοντική αντιμετώπιση δηλαδή η επικινδυνότητα γίνεται προσωρινά αποδεκτή με την προϋπόθεση ότι θα αντιμετωπιστεί σε ένα αποδεκτό επίπεδο, σε προκαθορισμένο χρόνο.

Τέλος, στο στάδιο αυτό ορίζεται η οργανωτική δομή, με τους απαραίτητους ρόλους και αρμοδιότητες, που απαιτούνται για να υλοποιηθεί η διαδικασία διαχείρισης επικινδυνότητας ασφάλειας πληροφοριών. Η δομή θα πρέπει να έχει την έγκριση της ανώτερης διοίκησης. Προκειμένου να υλοποιηθεί μία αποτελεσματική δομή, πρέπει να ληφθούν υπόψη τα ακόλουθα:

- η διαδικασία που θα οριστεί θα πρέπει να είναι η κατάλληλη για τον συγκεκριμένο Οργανισμό
- να γίνει αναγνώριση και ανάλυση των ενδιαφερομένων
- οι ρόλοι και οι αρμοδιότητες σε σχέση με τη διαδικασία θα πρέπει να είναι σαφώς καθορισμένοι είτε αυτό αφορά το εσωτερικό του Οργανισμού είτε αυτό αφορά εξωτερικούς συνεργάτες.

- θα πρέπει να δημιουργηθούν οι απαραίτητες σχέσεις / η απαραίτητη επικοινωνία, τόσο μεταξύ του Οργανισμού και των ενδιαφερομένων όσο και στο εσωτερικό του Οργανισμού (π.χ. με την ανώτερη διοίκηση)
- να καθοριστεί η διαδικασία κλιμάκωσης των αποφάσεων

Είναι σημαντικό να ανατεθούν και να κοινοποιηθούν οι ευθύνες και οι αρχές για τη διαδικασία διαχείρισης κινδύνου. Θα πρέπει να είναι σαφείς και να γίνονται κατανοητές από τα άτομα που εμπλέκονται σε αυτή τη διαδικασία ή που επηρεάζονται από τα αποτελέσματα αυτής της διαδικασίας.

2.4 Αποτίμηση επικινδυνότητας (Risk assessment)

Σε αυτό το στάδιο στόχος είναι η αναγνώριση των κινδύνων, η ποσοτικοποίηση ή ποιοτική περιγραφή τους και η προτεραιοποίησή τους (πιθανόν μετά από επαναληπτική διαδικασία).

- Είσοδος: τα κριτήρια βάση των οποίων θα υλοποιηθεί η διαχείριση επικινδυνότητας ασφάλειας πληροφοριών, ο σκοπός και οι περιορισμοί εντός των οποίων θα υλοποιηθεί και οι ρόλοι και οι αρμοδιότητες των εμπλεκόμενων μερών.
- Δράση: αναγνώριση όλων των κινδύνων, ποσοτικοποίηση ή ποιοτική περιγραφή τους και η προτεραιοποίησή τους βάση των κριτηρίων αξιολόγησης επικινδυνότητας και των στόχων του Οργανισμού.
- Έξοδος: κατάλογος των κινδύνων όπως έχουν εκτιμηθεί και προτεραιοποιηθεί βάση των κριτηρίων αξιολόγησης επικινδυνότητας.

Σύμφωνα με το πρότυπο καθοδήγησης, κίνδυνος είναι ο συνδυασμός των επιπτώσεων που θα προκαλέσει ένα ανεπιθύμητο συμβάν καθώς και η πιθανότητα να συμβεί. Στο στάδιο αυτό, αφού ποσοτικοποιηθούν και προσδιοριστούν ποιοτικά οι κίνδυνοι, οι διαχειριστές του Οργανισμού, τους προτεραιοποιούν σύμφωνα με τη σοβαρότητα που εκτιμούν ότι έχουν οι κίνδυνοι και λαμβάνοντας υπόψη πιθανώς και άλλα κριτήρια που έχουν τεθεί από τον Οργανισμό.

Μια λεπτομερής αξιολόγηση κινδύνου θα πρέπει να αναγνωρίζει τα αγαθά, να ποσοτικοποιεί την αξία τους για τον οργανισμό, να εντοπίζει υπάρχουσες ή πιθανές απειλές και τρωτά σημεία, να εξετάζει τυχόν ελέγχους που ενδέχεται να έχουν επίδραση στους κινδύνους που έχουν εντοπιστεί, να προσδιορίσει τις πιθανές συνέπειες και, τέλος, θα πρέπει να ιεραρχήσει τους κινδύνους με βάση ορισμένα κριτήρια που έχουν καθοριστεί εκ των προτέρων. Ωστόσο, οι Οργανισμοί, μπορούν να επιλέξουν διαφορετικές προσεγγίσεις για την αξιολόγηση κινδύνου ασφάλειας πληροφοριών, ανάλογα με τους στόχους τους, το ημερολόγιο της διαδικασίας διαχείρισης κινδύνου και ίσως άλλους παράγοντες.

Να σημειωθεί ότι, η αποτίμηση της επικινδυνότητας συχνά επαναλαμβάνεται τουλάχιστον δύο (2) φορές. Την πρώτη φορά, λαμβάνει χώρα μία υψηλότερου επιπέδου εκτίμηση ενώ στη δεύτερη επανάληψη γίνεται μια, πιο σε βάθος εκτίμηση των κινδύνων. Στις περιπτώσεις που η αρχική εκτίμηση, προσέφερε ανεπαρκή στοιχεία για να αξιολογηθούν οι κίνδυνοι (π.χ δεν λάβαμε υπόψη όλη τη νομοθεσία), διεξάγεται μια πιο λεπτομερή ανάλυση χρησιμοποιώντας πιθανών και άλλη προσέγγιση ή μέθοδο.

Η αποτίμηση επικινδυνότητας υλοποιείται σε τρία (3) στάδια.

2.4.1 Αναγνώριση επικινδυνότητας (Risk identification)

Ο στόχος της αναγνώρισης επικινδυνότητας είναι να προσδιοριστεί τι μπορεί να συμβεί το οποίο μπορεί να οδηγήσει σε απώλεια καθώς και να διερευνηθεί ο τρόπος, η αιτία και το που μπορεί να συμβεί. Οι κίνδυνοι που λαμβάνονται υπόψη δεν είναι απαραίτητο να είναι υπό τον έλεγχο του Οργανισμού, ούτε η πηγή τους να βρίσκεται σε αυτόν.

Η αναγνώριση επικινδυνότητας υλοποιείται με τα παρακάτω βήματα.

2.4.1.1 Αναγνώριση αγαθών

- Είσοδος: ο σκοπός και τα όρια για την αποτίμηση επικινδυνότητας, ένας κατάλογος με στοιχεία (όπως τους ιδιοκτήτες, η τοποθεσία, οι λειτουργίες κτλ.) που αφορούν τον Οργανισμό
- Δράση: αναγνώριση όλων των αγαθών που βρίσκονται μέσα στον σκοπό
- Έξοδος: κατάλογος των αγαθών για τα οποία πρέπει να γίνει η διαχείριση κινδύνου και κατάλογος των διεργασιών που σχετίζονται με αυτά τα αγαθά.

Σύμφωνα με το πρότυπο καθοδήγησης, ως αγαθό ορίζεται οτιδήποτε έχει αξία για το Οργανισμό και χρήζει προστασίας. Κρίνεται λοιπόν αναγκαίο να αναγνωριστεί ότι ένα πληροφοριακό σύστημα δεν αποτελείται μόνο από λογισμικό και εξοπλισμό.

Η αναγνώριση αγαθών μπορεί να εκτελεστεί κάτω από ένα συγκεκριμένο επίπεδο λεπτομέρειας το οποίο θα παρέχει επαρκείς πληροφορίες για την αξιολόγηση επικινδυνότητας. Το επίπεδο λεπτομέρειες επηρεάζει την ποσότητα πληροφορίας που θα συλλεχθεί κατά τη διάρκεια της αξιολόγησης κινδύνου. Το επίπεδο λεπτομέρειας μπορεί να βελτιωθεί περαιτέρω στις επόμενες επαναλήψεις της αξιολόγησης επικινδυνότητας.

Κατά τη διάρκεια αναγνώρισης αγαθών, θα πρέπει να εντοπιστεί ο ιδιοκτήτης του κάθε αγαθού ο οποίος θα είναι υπεύθυνος και υπόλογος γι' αυτό. Ο ιδιοκτήτης ενός αγαθού είναι συνήθως το άτομο που μπορεί να υποδείξει την αξία που έχει το αγαθό για τον Οργανισμό και κατ' επέκταση είναι υπεύθυνος για την παραγωγή, την ανάπτυξη, την συντήρηση και την ασφαλή χρήση του στον Οργανισμό.

2.4.1.2 Αναγνώριση απειλών

- Είσοδος: Πληροφορίες απειλών που προήλθαν από την ανασκόπηση συμβάντων, από ιδιοκτήτες αγαθών, από χρήστες αγαθών και άλλες πηγές συμπεριλαμβανομένων εξωτερικών καταλόγων απειλών.
- Δράση: Αναγνώριση των απειλών και των πηγών τους
- Έξοδος: Κατάλογος των απειλών συμπεριλαμβανομένων των τύπων τους και των πηγών τους.

Σύμφωνα με την καθοδήγηση υλοποίησης που προτείνει το πρότυπο, μια απειλή μπορεί να προκαλέσει ζημιά σε αγαθά όπως πληροφορίες, διεργασίες, συστήματα και κατ' επέκταση στον Οργανισμό. Οι απειλές μπορεί να είναι φυσικής ή ανθρώπινης προέλευσης και διακρίνονται σε τυχαίες ή σκόπιμες. Οι απειλές πρέπει να εντοπίζονται και να αναγνωρίζονται είτε προέρχονται από το εσωτερικό του Οργανισμού είτε από εξωτερικούς παράγοντες. Οι απειλές θα πρέπει να αναγνωρίζονται με βάση το είδος τους (μη εξουσιοδοτημένες πράξεις, φυσικές καταστροφές, τεχνικές βλάβες κ.λπ.).

Στην περίπτωση που οι απειλές επηρεάζουν πάνω από ένα αγαθό, θα πρέπει να συνυπολογιστεί η πιθανότητα να υφίστανται διαφορετικές επιπτώσεις ανάλογα με το αγαθό που επηρεάζεται σε κάθε περίπτωση. Η πιθανότητα να συμβεί μια απειλή προσδιορίζεται από συλλογή πληροφοριών από διάφορες πηγές όπως οι ιδιοκτήτες αγαθών, οι χρήστες, οι ειδικοί της ασφάλειας πληροφοριών και της φυσικής ασφάλειας, το νομικό τμήμα και γενικότερα ότι σχετίζεται με τον Οργανισμό συμπεριλαμβανομένων και των περιβαλλοντολογικών παραγόντων και των ασφαλιστικών εταιρειών.

Κρίνεται επίσης σημαντικό να ληφθεί υπόψη η εμπειρία που προέρχεται από περιστατικά που έχουν συμβεί από παλαιότερες εκτιμήσεις απειλών. Θεωρείται καλή πρακτική να ληφθούν υπόψη κατάλογοι απειλών όπως αυτοί έχουν καταρτιστεί από διάφορους φορείς (βιομηχανία, κυβερνητικοί φορείς, νομικές αρχές, ασφαλιστικές εταιρείες, κ.λπ.).

2.4.1.3 Αναγνώριση των υπαρχόντων μέτρων

- Είσοδος: τεκμηριωμένα μέτρα, σχέδια υλοποίησης αντιμετώπισης της επικινδυνότητας.
- Δράση: αναγνώριση υπαρχόντων και υπό σχεδίαση μέτρων.
- Έξοδος: κατάλογος όλων των μέτρων, υπαρχόντων και σχεδιαζόμενων, τρόπος υλοποίησης του καθενός και κατάσταση χρήσης τους.

Η αναγνώριση υπαρχόντων μέτρων θα πρέπει να γίνεται με σκοπό την αποφυγή περιττού φόρτου εργασίας ή περιττού κόστους. Κατά τη διάρκεια της αναγνώρισης των υπαρχόντων μέτρων, θα πρέπει να διεξάγεται έλεγχος για να εξασφαλιστεί η αποτελεσματικότητα των μέτρων αυτών βασισμένη κυρίως στις εκθέσεις ελέγχου του ISMS, έτσι ώστε να αποφευχθεί η δημιουργία νέων ευπαθειών. Στην περίπτωση όπου κάποιο μέτρο δεν αποδίδει στο βαθμό που απαιτείται υπάρχει πιθανότητα να οδηγήσει σε νέες ευπάθειες. Σε τέτοιες περιπτώσεις είναι πιθανόν να πρέπει να γίνει ενίσχυση με νέα μέτρα ή ακόμα και αντικατάσταση με πιο αποτελεσματικά μέτρα.

Για να αναγνωριστούν τα υπάρχοντα μέτρα κι αυτά που σχεδιάζονται θα πρέπει:

- Αναθεωρηθούν αρχεία που περιλαμβάνουν πληροφορίες σχετικά με τα μέτρα. Αν υπάρχει σωστή καταγραφή, θα υπάρχουν όλα τα μέτρα, υπάρχοντα και σχεδιαζόμενα και η κατάσταση υλοποίησής τους
- να γίνει έλεγχος με τους υπεύθυνους για την ασφάλεια της πληροφορίας και τους χρήστες για να διασαφηνιστεί ποια μέτρα έχουν υλοποιηθεί

- να διεξαχθεί επιτόπιος έλεγχος των φυσικών μέτρων σε σύγκριση με αυτά που θα έπρεπε να είχαν υλοποιηθεί. Αυτά τα μέτρα που ήδη έχουν υλοποιηθεί θα πρέπει να εξεταστούν ως προς την ορθότητα και αποτελεσματικότητά τους
- να ελεγχθούν τα αποτελέσματα των επιθεωρήσεων.

2.4.1.4 Αναγνώριση ευπαθειών

- Είσοδος: κατάλογος με όλες τις γνωστές απειλές, λίστα με τα αγαθά και τα υπάρχοντα μέτρα
- Δράση: αναγνώριση ευπαθειών που μπορούν να εκμεταλλευτούν από τις απειλές και να προκαλέσουν ζημιά στα αγαθά και γενικότερα στον Οργανισμό
- Έξοδος: κατάλογος με τις ευπάθειες που έχουν συσχετιστεί με τα αγαθά, τις απειλές και τα μέτρα καθώς επίσης και κατάλογος με τις ευπάθειες που δεν έχουν συσχετιστεί ακόμα με απειλές για έλεγχο.

Σύμφωνα με την καθοδήγηση υλοποίησης που προτείνει το πρότυπο οι ευπάθειες μπορεί να σχετίζονται με τον Οργανισμό, το προσωπικό, τις διεργασίες και τις λειτουργίες, το φυσικό περιβάλλον, τις ρυθμίσεις των παραμέτρων του πληροφοριακού συστήματος, το λειτουργικό και τον εξοπλισμό, τυχόν εξαρτήσεις από τρίτα μέρη κτλ. Μια ευπάθεια που δεν σχετίζεται με μια απειλή μπορεί να μην χρειάζεται να αντιμετωπιστεί με κάποιο μέτρου, ωστόσο πρέπει να αναγνωριστεί και να παρακολουθείται για αλλαγές. Αξίζει να σημειωθεί ότι ευπάθεια μπορεί να προκαλέσει και ένα μέτρο που δεν λειτουργεί αποτελεσματικά. Η αποτελεσματικότητα ενός μέτρου κρίνεται από το περιβάλλον στο οποίο λειτουργεί αυτό. Τέλος πρέπει να σημειωθεί ότι στην περίπτωση της ευπάθειας που σχετίζεται με αγαθό μπορεί αυτή να μην προκύπτει από την κύρια λειτουργία του αγαθού ή από τον λόγο για τον οποίο κατασκευάστηκε.

2.4.1.5 Αναγνώριση συνεπειών

- Είσοδος: κατάλογος αγαθών, κατάλογος με επιχειρησιακές διεργασίες και κατάλογος με απειλές και ευπάθειες σε αντιστοιχία με αγαθά όπου αυτό είναι εφικτό.
- Δράση: αναγνώριση των συνεπειών που υπάρχουν στα αγαθά από την απώλεια της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας.
- Έξοδος: κατάλογος με σενάρια συμβάντων και τις συνέπειες που έχουν αυτά στα αγαθά και στις επιχειρησιακές διεργασίες.

Σύμφωνα με την καθοδήγηση υλοποίησης που προτείνει το πρότυπο, μια συνέπεια μπορεί να είναι η απώλεια της αποτελεσματικότητας, η δημιουργία δυσμενών συνθηκών λειτουργίας, η απώλεια της φήμης.

Αυτή η δραστηριότητα αναγνωρίζει τη ζημιά ή τις συνέπειες στον Οργανισμό που μπορεί να προκληθούν από ένα σενάριο συμβάντος. Σ' ένα σενάριο συμβάντος περιγράφεται ο τρόπος όπου μια απειλή εκμεταλλεύεται κάποια ευπάθεια. Παράλληλα, πρέπει να ληφθούν υπόψη τα κριτήρια επίπτωσης όπως αυτά καθορίστηκαν στο στάδιο "Καθορισμός Περιεχομένου". Οι συνέπειες μπορούν να αφορούν παραπάνω από ένα αγαθά και διακρίνονται σε προσωρινές ή μόνιμες (όπως είναι στην περίπτωση καταστροφής ενός αγαθού).

Για να καθοριστούν οι συνέπειες στα σενάρια συμβάντων πρέπει να ληφθούν υπόψη οι εξής παράγοντες:

- ο χρόνος που απαιτήθηκε για την έρευνα και για την επιδιόρθωση,
- ο χρόνος εργασίας που χάθηκε,
- οι ευκαιρίες που χάθηκαν,
- η υγεία και η ασφάλεια,
- το οικονομικό κόστος για την επιδιόρθωση,
- η φήμη και η υπόληψη.

2.4.2 Ανάλυση επικινδυνότητας (Risk analysis)

Η ανάλυση επικινδυνότητας πραγματοποιείται σε διαφορετικό βαθμό λεπτομέρειας ανάλογα με την κρισιμότητα των αγαθών, το εύρος των γνωστών ευπαθειών και τα συμβάντα που έχουν προηγηθεί και αφορούν τον Οργανισμό. Η ανάλυση επικινδυνότητας μπορεί να είναι είτε ποιοτική είτε ποσοτική είτε να είναι συνδυασμός και των δύο.

Με την ποιοτική ανάλυση αποκτούμε αρχικά μια γενική εικόνα για το επίπεδο κινδύνου και προσδιορίζουμε τους σημαντικότερους κινδύνους. Αργότερα, στην περίπτωση που απαιτείται μια πιο λεπτομερή ανάλυση μπορούμε να προχωρήσουμε σε ποσοτική ανάλυση καθώς συνήθως είναι πιο απαιτητικό και ακριβό να εκτελέσει κανείς ποσοτική ανάλυση.

Ακολουθούν λεπτομέρειες για τις δύο μεθόδους:

- *α) Ποιοτική ανάλυση*

Για την υλοποίηση της, χρησιμοποιούμε μία κλίμακα ποιοτικών χαρακτηριστικών για να περιγράψουμε το μέγεθος των πιθανών συνεπειών (μικρό, μεσαίο, μεγάλο) και την πιθανότητα που έχουν αυτές οι συνέπειες να συμβούν. Το πλεονέκτημα της μεθοδολογίας αυτής είναι ότι είναι κατανοητή από όλο το εμπλεκόμενο προσωπικό ενώ το μειονέκτημα της είναι ότι η επιλογή της κλίμακας γίνεται με υποκειμενικά κριτήρια. Η κλίμακα αυτή μπορεί να προσαρμοστεί για να ταιριάζει σε διαφορετικές συνθήκες. Η ποιοτική ανάλυση κινδύνου μπορεί να χρησιμοποιηθεί:

- ως μια αρχική δραστηριότητα ελέγχου με σκοπό την αναγνώριση των κινδύνων που απαιτούν πιο λεπτομερή έλεγχο,
- όπου αυτού του είδους η ανάλυση είναι κατάλληλη για την ανάληψη αποφάσεων,
- όπου τα αριθμητικά δεδομένα ή οι πηγές είναι μη επαρκή για ποσοτική ανάλυση.

Η ποιοτική ανάλυση θα πρέπει να χρησιμοποιεί τεκμηριωμένες πληροφορίες και δεδομένα όποτ αυτό είναι εφικτό.

- *β) Ποσοτική ανάλυση*

Η ποσοτική ανάλυση χρησιμοποιεί ως κλίμακα αριθμητικές τιμές τόσο για την αναγνώριση των συνεπειών όσο και για την πιθανότητα να συμβούν, χρησιμοποιώντας δεδομένα από πολλές πηγές. Η ποιότητα της ανάλυσης εξαρτάται από την ακρίβεια και την πληρότητα των αριθμητικών δεδομένων καθώς επίσης και την εγκυρότητα των μοντέλων που χρησιμοποιούνται. Το πλεονέκτημα της ποσοτικής ανάλυση κινδύνου είναι ότι, στις περισσότερες περιπτώσεις χρησιμοποιεί δεδομένα από συμβάντα που έχουν προηγηθεί δίνοντας έτσι το προβάδισμα ότι μπορεί να συσχετιστεί άμεσα με την ασφάλεια πληροφοριών που αφορούν τον Οργανισμό. Ένα μειονέκτημα είναι η έλλειψη τέτοιων δεδομένων που αφορούν νέους κινδύνους και ευπάθειες. Επίσης, η ποσοτική ανάλυση μπορεί να συμβεί όταν πραγματικά, ελεγχόμενα δεδομένα δεν είναι διαθέσιμα και έτσι μπορεί να δημιουργηθεί η ψευδαίσθηση αξίας και ακρίβειας της αξιολόγησης του κινδύνου.

2.4.2.1 Εκτίμηση Συνεπειών

- Είσοδος: κατάλογος των σχετικών σεναρίων συμβάντων, που συμπεριλαμβάνουν απειλές, ευπάθειες, αγαθά που επηρεάζονται, συνέπειες στα αγαθά και στις επιχειρησιακές διεργασίες.
- Δράση: εκτίμηση της επιχειρησιακής επίπτωσης στον Οργανισμό, από συμβάν το οποίο είναι πιθανόν να υπάρξει ή έχει υπάρξει, λαμβάνοντας υπόψη παραβίαση η οποία σχετίζεται με απώλεια της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των αγαθών.
- Έξοδος: κατάλογος των συνεπειών από ένα σενάριο συμβάντος, όπως αυτές έχουν εκτιμηθεί, σε συνάρτηση με τα αγαθά και τα κριτήρια επίπτωσης.

Σύμφωνα με τη καθοδήγηση υλοποίησης που προτείνει το πρότυπο, η έννοια της επιχειρησιακής επίπτωσης χρησιμοποιείται για να μετρήσει συνέπειες. Η αξία της επιχειρησιακής επίπτωσης μπορεί να εκφραστεί είτε σε ποιοτική, είτε σε ποσοτική μορφή με σκοπό την παροχή πληροφοριών για μια πιο αποτελεσματική διαδικασία ανάληψης αποφάσεων.

Η εκτίμηση των αγαθών, ξεκινάει με την ταξινόμηση τους, ανάλογα με την κρισιμότητα τους (πόσο σημαντικά είναι για την υλοποίηση των διεργασιών του Οργανισμού) ενώ για να πραγματοποιηθεί λαμβάνονται υπόψη παράγοντες όπως:

- το κόστος που θα απαιτηθεί για την αντικατάσταση του αγαθού
- οι συνέπειες από την απώλεια του

Η αξιολόγηση των αγαθών γίνεται μέσω ανάλυσης επιχειρησιακής επίπτωσης (Business Impact Analysis – BIA).

Οι συνέπειες μπορούν να καθοριστούν είτε ομαδοποιώντας τα αποτελέσματα ενός συμβάντος ή ενός συνόλου συμβάντων είτε εξάγοντας συμπεράσματα από πειραματικές μελέτες ή δεδομένα του παρελθόντος.

Εκφράζονται με βάση χρηματικά, τεχνικά ή άλλα κριτήρια που έχουν να κάνουν είτε με τον άνθρωπο είτε με τον Οργανισμό. Για την μέτρηση των συνεπειών σε χρόνο και χρήμα πρέπει να χρησιμοποιείται ίδια προσέγγιση όπως και στη μέτρηση της πιθανότητας των απειλών και των ευπαθειών.

2.4.2.2 Εκτίμηση Πιθανότητας συμβάντων

- Είσοδος: κατάλογος των σχετικών σεναρίων συμβάντων, που συμπεριλαμβάνουν απειλές, αγαθά που επηρεάζονται, εκμεταλλευόμενες ευπάθειες και συνέπειες στα αγαθά και στις επιχειρησιακές διεργασίες. Επίσης καταλόγους όλων των μέτρων, υπαρχόντων και σχεδιαζόμενων, της αποτελεσματικότητας τους, του τρόπου υλοποίησης τους και της κατάστασης χρήσης τους.
- Δράση: εκτίμηση της πιθανότητας των σεναρίων συμβάντων
- Έξοδος: η πιθανότητα των σεναρίων συμβάντων (ποιοτική ή ποσοτική)

Σύμφωνα με τη καθοδήγηση υλοποίησης που προτείνει το πρότυπο, αφού προσδιοριστούν τα σενάρια συμβάντων είναι απαραίτητο να γίνει αξιολόγηση της πιθανότητας για κάθε σενάριο και μια επίπτωση χρησιμοποιώντας ποσοτικές ή ποιοτικές τεχνικές ανάλυσης. Στο διάστημα αυτό θα πρέπει να λαμβάνεται υπόψη πόσο συχνά συμβαίνουν οι απειλές και πόσο εύκολα μπορούν να εκμεταλλευτούν οι ευπάθειες. Για να προσδιοριστούν αυτοί οι παράγοντες θα πρέπει να συλλεχθούν στοιχεία που αφορούν τα παρακάτω:

- στατιστικά σχετικά με την πιθανότητα των απειλών,
- κίνητρα και ικανότητες που έχουν οι επιτιθέμενοι σε μια επίθεση που συμβαίνει ηθελημένα αλλά και το τι θεωρούν ελκυστικό κατά διαστήματα για τις επιθέσεις τους,
- στις περιπτώσεις που η απειλή συμβαίνει τυχαία: γεωγραφικούς και περιβαλλοντολογικούς παράγοντες που μπορούν να προκαλέσουν ανθρώπινα λάθη ή δυσλειτουργία του εξοπλισμού
- ευπάθειες,
- υπάρχοντα μέτρα αντιμετώπισης τους καθώς και πόσο αποτελεσματικά μπορούν να μειωθούν.

Ανάλογα με το πόσο ακριβής θέλουμε να είμαστε στην εκτίμηση μας, είναι δυνατόν να αντιμετωπίσουμε κάποια αγαθά σαν ένα σύνολο ενώ σε άλλες περιπτώσεις να ¨σπάσουμε ¨ τα αγαθά στα συστατικά τους μέρη και να συσχετίσουμε το σενάριο με αυτά.

2.4.2.3 Επίπεδο προσδιορισμού επικινδυνότητας

- Είσοδος: κατάλογος των σεναρίων συμβάντων, με τις συνέπειες τους που σχετίζονται με τα αγαθά, τις επιχειρησιακές διεργασίες και την πιθανότητα αυτές να συμβούν
- Δράση: προσδιορισμός του επιπέδου επικινδυνότητας για όλα τα σενάρια συμβάντων
- Έξοδος: κατάλογος κινδύνων με τιμή που δείχνει το επίπεδο τους.

Σύμφωνα με τη καθοδήγηση υλοποίησης που προτείνει το πρότυπο, το επίπεδο του κινδύνου είναι συνδυασμός της πιθανότητας να λάβει χώρα ένα σενάριο συμβάντος και των συνεπειών του.

2.4.3 Αξιολόγηση επικινδυνότητας (Risk evaluation)

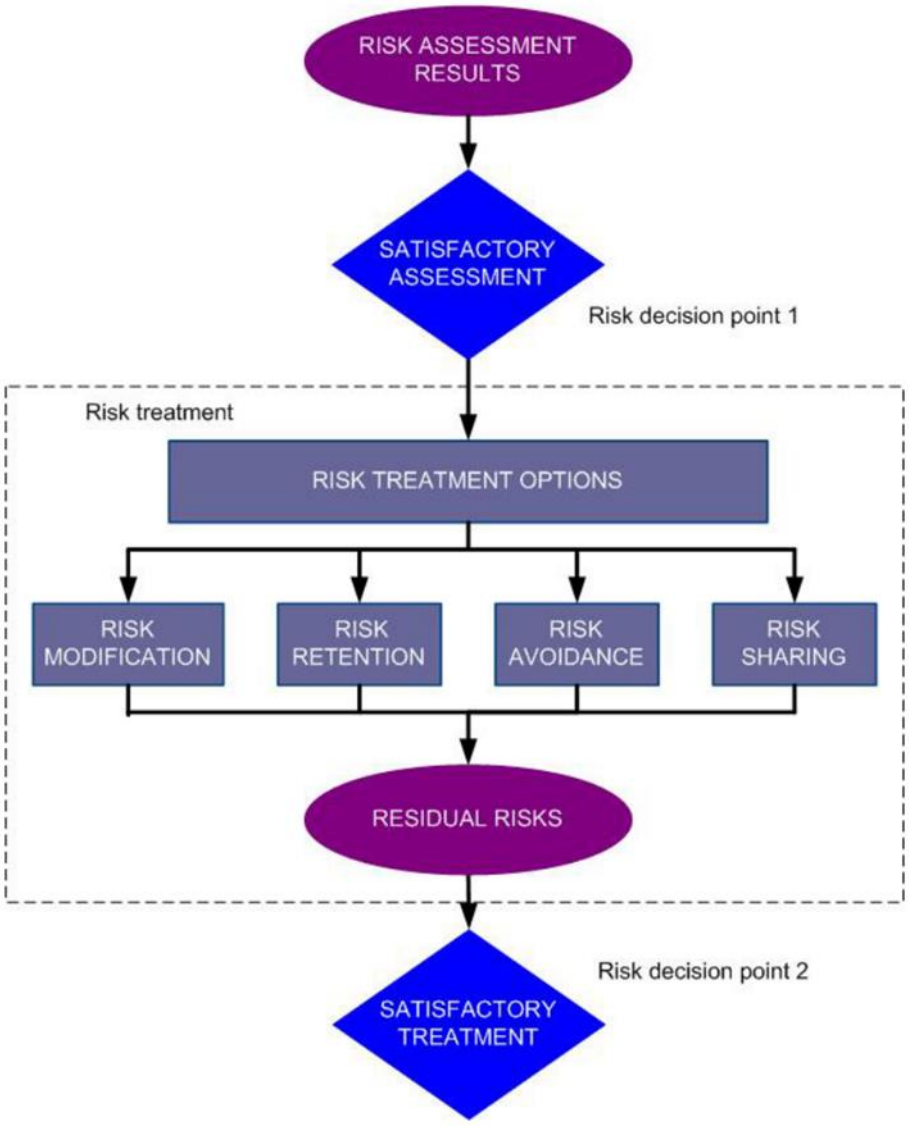
- Είσοδος: κατάλογος κινδύνων με τιμή που δείχνει το επίπεδο τους.
- Δράση: σύγκριση των επιπέδων των κινδύνων σε σχέση με τα κριτήρια αξιολόγησης επικινδυνότητας και κριτήρια αποδοχής της επικινδυνότητας
- Έξοδος: κατάλογος των κινδύνων οι οποίοι έχουν μπει σε σειρά προτεραιότητας,σύμφωνα με τα κριτήρια αξιολόγησης επικινδυνότητας και τα σενάρια συμβάντων που έχουν οδηγήσει σε αυτούς τους κινδύνους.

Σύμφωνα με τη καθοδήγηση υλοποίησης που προτείνει το πρότυπο, προκειμένου να πραγματοποιηθεί η αξιολόγηση επικινδυνότητας, ο Οργανισμός πρέπει να συγκρίνει τους υπολογιζόμενους κινδύνους με τα κριτήρια αξιολόγησης επικινδυνότητας όπως αυτά καθορίστηκαν στο στάδιο ¨Καθορισμός Περιεχομένου¨. Οι αποφάσεις που θα ληφθούν σε αυτό το στάδιο σχετίζονται με το αποδεκτό επίπεδο επικινδυνότητας αλλά θα πρέπει να συνυπολογιστούν και άλλοι παράγοντες όπως η πιθανότητα και ο βαθμός εμπιστοσύνης όσον αφορά την αναγνώριση επικινδυνότητας και την ανάλυση.

2.5 Αντιμετώπιση επικινδυνότητας (Risk treatment)

- Είσοδος: κατάλογος των κινδύνων οι οποίοι έχουν πρωτεραιοποιηθεί σύμφωνα με τα κριτήρια αξιολόγησης επικινδυνότητας και τα σενάρια συμβάντων που έχουν οδηγήσει σε αυτούς τους κινδύνους
- Δράση: επιλογή των μέτρων που αποσκοπούν στη μείωση, διατήρηση, αποφυγή ή διαμοιρασμό των κινδύνων και δημιουργία σχεδίου αντιμετώπισης επικινδυνότητας
- Έξοδος: σχέδιο αντιμετώπισης επικινδυνότητας και απομένουσα επικινδυνότητα ανάλογα με την απόφαση αποδοχής από τη διοίκηση του Οργανισμού.

Σύμφωνα με την καθοδήγηση υλοποίησης που προτείνει το πρότυπο και όπως παρουσιάζεται στο Σχ.2 υπάρχουν τέσσερις (4) επιλογές στο στάδιο αυτό: α) τροποποίηση επικινδυνότητας, β) διατήρηση επικινδυνότητας, γ) αποφυγή επικινδυνότητας και δ) διαμοιρασμός επικινδυνότητας.



Εικόνα 2.3: Αντιμετώπιση κινδύνου

Οι επιλογές αντιμετώπισης της επικινδυνότητας θα πρέπει να βασίζονται στα αποτελέσματα της αποτίμησης επικινδυνότητας, στο αναμενόμενο κόστος υλοποίησης αυτών των επιλογών καθώς και στα οφέλη που μπορεί να αποφέρει κάθε μία επιλογή αντιμετώπισης. Επίσης, θεωρείται σημαντικό να λαμβάνεται υπόψη ο τρόπος με τον οποίο τα εμπλεκόμενα μέρη αντιλαμβάνονται την απειλή και τον κίνδυνο καθώς και κατάλληλους τρόπους για να επικοινωνηθούν οι επιλογές αντιμετώπισης.

Το μεγαλύτερο ρίσκο για όλους τους Οργανισμούς είναι η αποτυχία να συμμορφωθούν με τις οδηγίες και τους κανόνες και έτσι κρίνεται απαραίτητο να υλοποιηθούν τρόποι αντιμετώπισης για να περιοριστεί όσον το δυνατόν περισσότερο αυτή η πιθανότητα. Όλοι οι περιορισμοί που αναγνωρίστηκαν στο αρχικό στάδιο ¨Καθορισμός Περιεχομένου¨, θα πρέπει να λαμβάνονται υπόψη κατά τη διάρκεια της αντιμετώπισης του κινδύνου.

Εφόσον το σχέδιο αντιμετώπισης της επικινδυνότητας έχει αποφασιστεί, η διαδικασία συνεχίζεται με τον καθορισμό της εναπομένουσας επικινδυνότητας (residual risk). Στο στάδιο αυτό περιέχεται η επανάληψη του σταδίου ¨Αποτίμηση της επικινδυνότητας¨ και αναθεώρηση όπου τυχόν χρειάζεται. Αν η εναπομένουσα επικινδυνότητα δεν πληροί τα κριτήρια αποδοχής της επικινδυνότητας, τότε είναι πιθανόν να απαιτηθεί επανάληψη του σταδίου αντιμετώπιση της επικινδυνότητας.

2.5.1 Τροποποίηση επικινδυνότητας (risk modification):

- Δράση: διαχείριση του επιπέδου του κινδύνου εφαρμόζοντας, αφαιρώντας ή τροποποιώντας μέτρα έτσι ώστε η εναπομένουσα επικινδυνότητα να είναι αποδεκτή.

Σύμφωνα με την καθοδήγηση υλοποίησης που προτείνει το πρότυπο, κατάλληλα και αιτιολογημένα μέτρα πρέπει να λαμβάνονται, βάση των απαιτήσεων που έχουν αναγνωριστεί κατά την αποτίμηση και αντιμετώπιση της επικινδυνότητας. Επίσης, θα πρέπει να λαμβάνονται υπόψη το κόστος και το χρονικό πλαίσιο για την υλοποίηση των μέτρων καθώς και άλλοι παράγοντες όπως τεχνικοί, περιβαλλοντολογικοί ή πολιτισμικοί. Αξίζει να αναφερθεί ότι η λήψη κατάλληλων μέτρων που αφορούν την ασφάλεια πληροφορίας συχνά οδηγεί σε μείωση του κόστους κτήσης ενός συστήματος.

Γενικότερα, τα μέτρα μπορούν να προσφέρουν ένα ή περισσότερα από τα ακόλουθα είδη προστασίας: διόρθωση, εξάλειψη, πρόληψη, μείωση της επίπτωσης, αποτροπή, ανίχνευση, ανάκαμψη, παρακολούθηση και επίγνωση. Είναι σημαντικό να αξιολογηθεί το κόστος κτήσης, υλοποίησης, διαχείρισης, λειτουργίας, ελέγχου και διατήρησης των μέτρων σε σχέση με την αξία των αγαθών που αυτά προστατεύουν. Το ISO/IEC 27002 προσφέρει λεπτομερείς πληροφορίες για τα μέτρα.

Αξίζει να αναφερθεί ότι υπάρχουν πολλοί περιορισμοί που μπορεί να επηρεάσουν την επιλογή των κατάλληλων μέτρων. Τεχνικοί περιορισμοί όπως η επίδοση, οι απαιτήσεις, η συμβατότητα, μπορεί να εμποδίσουν τη χρήση συγκεκριμένων μέτρων ή να προκαλέσουν ανθρώπινο λάθος.

Επιπλέον, είναι απαραίτητο, να λαμβάνονται υπόψη οι περιορισμοί που μπορούν να επηρεάσουν, τόσο την επιλογή όσο και την υλοποίηση των μέτρων. Τέτοιοι περιορισμοί είναι: χρονικοί, οικονομικοί, τεχνικοί, λειτουργικοί, κουλτούρας, ηθικοί, ευκολίας χρήσης, προσωπικού και τέλος περιορισμοί που αφορούν την ενσωμάτωση νέων και υπαρχόντων μέτρων.

Προκειμένου να ληφθούν τα κατάλληλα για τον Οργανισμό μέτρα, οι διαχειριστές θα πρέπει να επιλέξουν μία λύση που να είναι σύμφωνη με τις απαιτήσεις απόδοσης που έχει θέσει ο Οργανισμός, ενώ ταυτόχρονα θα εξασφαλίζει ασφάλεια πληροφορίας σε ικανοποιητικό βαθμό. Το αποτέλεσμα θα είναι ένας κατάλογος με πιθανά μέτρα που θα συμπεριλαμβάνει το κόστος τους, το όφελος τους και την προτεραιότητα υλοποίησης τους.

2.5.2 Διατήρηση επικινδυνότητας (risk retention)

- Δράση: απόφαση για την διατήρηση του κινδύνου χωρίς να ληφθεί κάποιο μέτρο και η οποία θα πρέπει να βασίζεται στην αξιολόγηση επικινδυνότητας.

Σύμφωνα με την καθοδήγηση υλοποίησης που προτείνει το πρότυπο, αν το επίπεδο του κινδύνου βρίσκεται σύμφωνο με τα κριτήρια αποδοχής της επικινδυνότητας, δεν υπάρχει κανένας λόγος για λήψη μέτρων και ο κίνδυνος παραμένει ως έχει.

2.5.3 Αποφυγή επικινδυνότητας (risk avoidance)

- Δράση: αποφυγή της δραστηριότητας ή της συνθήκης βάση της οποίας δημιουργείται ο κίνδυνος

Σύμφωνα με την καθοδήγηση υλοποίησης που προτείνει το πρότυπο, όταν ο κίνδυνος που έχει αναγνωριστεί θεωρείται πολύ υψηλός, ή όταν το κόστος της υλοποίησης της αντιμετώπισης επικινδυνότητας για αυτόν υπερβαίνει τα οφέλη, θα πρέπει ο κίνδυνος να αποφευχθεί. Αυτό υλοποιείται είτε με την απόσυρση του Οργανισμού από μια δραστηριότητα ή σύνολο δραστηριοτήτων που σχεδιάζονται ή υπάρχουν ήδη είτε αλλάζοντας τις συνθήκες κάτω από τις οποίες λειτουργεί η δραστηριότητα / οι δραστηριότητες.

2.5.4 Διαμοιρασμός επικινδυνότητας (risk sharing)

- Δράση: διαμοιρασμός της επικινδυνότητας με συμβαλλόμενο μέρος που έχει την ικανότητα να αντιμετωπίσει αποτελεσματικά τον συγκεκριμένο κίνδυνο με βάση την αξιολόγηση επικινδυνότητας

Σύμφωνα με την καθοδήγηση υλοποίησης που προτείνει το πρότυπο, ο διαμοιρασμός της επικινδυνότητας πραγματοποιείται μεταξύ του Οργανισμού και εξωτερικού συμβαλλόμενου. Από την διαδικασία αυτή είναι πιθανόν να προκύψουν νέοι κίνδυνοι ή να μεταβληθούν κίνδυνοι που ήδη υπάρχουν και έχουν αναγνωριστεί. Αυτό έχει σαν αποτέλεσμα σε κάποιες περιπτώσεις να είναι απαραίτητη και περεταίρω διαδικασία αντιμετώπισης επικινδυνότητας. Σημειώνεται ότι κατά τη διαδικασία του διαμοιρασμού της επικινδυνότητας, διαμοιράζεται η διαχείριση του κινδύνου αλλά όχι η ευθύνη για την επίπτωση. Η ευθύνη για την επίπτωση βαραίνει τον Οργανισμό.

2.6 Αποδοχή επικινδυνότητας (Risk acceptance)

- Είσοδος: σχέδιο αντιμετώπισης επικινδυνότητας και αποτίμηση απομένουσας επικινδυνότητας ανάλογα με την απόφαση αποδοχής των διαχειριστών του Οργανισμού
- Δράση: καταγραφή της απόφασης αποδοχής της επικινδυνότητας και των αρμοδιοτήτων που σχετίζονται με αυτή
- Έξοδος: κατάλογος με κινδύνους που έχουν γίνει αποδεκτοί από τον Οργανισμό ο οποίος συμπεριλαμβάνει τεκμηρίωση για αυτούς που δεν συμμορφώνονται με τα κριτήρια αποδοχής της επικινδυνότητας που έχει θέσει ο Οργανισμός.

Σύμφωνα με την καθοδήγηση υλοποίησης που προτείνει το πρότυπο, τα σχέδια αντιμετώπισης επικινδυνότητας πρέπει να περιγράφουν πως οι κίνδυνοι που εκτιμήθηκαν συμμορφώνονται με τα κριτήρια αποδοχής της επικινδυνότητας. Είναι σημαντικό για τους διαχειριστές που είναι υπεύθυνοι, να εξετάσουν και να εγκρίνουν τα σχέδια αντιμετώπισης επικινδυνότητας και την απομένουσα επικινδυνότητα και να καταγράψουν όλες τις συνθήκες που σχετίζονται με την έγκριση τους.

Σε κάποιες περιπτώσεις η εναπομένουσα επικινδυνότητα δεν συμμορφώνεται με τα κριτήρια αποδοχής της επικινδυνότητας, είτε γιατί είναι περίπλοκα ή ανεπαρκή, είτε γιατί δεν λαμβάνουν υπόψη κάποιες ισχύουσες περιστάσεις. Σε αυτές τις περιπτώσεις οι υπεύθυνοι λήψης των αποφάσεων, μπορούν να αποδεχτούν κινδύνους που δεν συμμορφώνονται με τα κριτήρια, αιτιολογώντας γιατί οδηγήθηκαν σε αυτή την απόφαση.

2.7 Επικοινωνία και συμβουλευτική (Risk communication and consultation)

- Είσοδος: όλες οι πληροφορίες σχετικά με τους κινδύνους που προέκυψαν από τη διαχείριση επικινδυνότητας
- Δράση: ανταλλαγή και/ή διαμοιρασμός της πληροφορίας όσον αφορά την επικινδυνότητα μεταξύ αυτών που παίρνουν τις αποφάσεις και των ενδιαφερομένων.
- Έξοδος: συνεχόμενη κατανόηση της διαδικασίας διαχείρισης επικινδυνότητας ασφάλειας πληροφοριών του Οργανισμού και των αποτελεσμάτων της.

Σύμφωνα με την καθοδήγηση υλοποίησης που προτείνει το πρότυπο, στο στάδιο αυτό πραγματοποιείται ανταλλαγή και/ή διαμοιρασμός της πληροφορίας όσον αφορά την επικινδυνότητα μεταξύ αυτών που παίρνουν τις αποφάσεις και των ενδιαφερομένων. Η πληροφορία περιλαμβάνει μεταξύ άλλων στοιχεία που αφορούν την ύπαρξη, τη φύση, τον τύπο, την πιθανότητα, την σοβαρότητα, την αντιμετώπιση και την αποδοχή των κινδύνων.

Η αποτελεσματική επικοινωνία μεταξύ των ενδιαφερομένων είναι πολύ σημαντική και μπορεί να επηρεάσει σε μεγάλο βαθμό τις αποφάσεις που θα ληφθούν. Η επικοινωνία εξασφαλίζει ότι αυτοί που είναι υπεύθυνοι για την υλοποίηση της διαχείρισης επικινδυνότητας και αυτοί που έχουν έννομο συμφέρον κατανοούν τη βάση για τις αποφάσεις που λήφθηκαν και τους λόγους για τους οποίους έγιναν συγκεκριμένες ενέργειες και αυτή είναι μια διαδικασία αμφίδρομη.

Διαφορετικοί ενδιαφερόμενοι έχουν πολύ συχνά διαφορετική αντίληψη σχετικά με τους κινδύνους και τα οφέλη και αυτό θα πρέπει να αναγνωριστεί, καταγραφεί και επεξηγηθεί σαφώς. Τα αναμενόμενα αποτελέσματα από μία σωστή διαδικασία επικοινωνίας είναι να:

- διασφαλίσει το αποτέλεσμα της διαχείρισης επικινδυνότητας του Οργανισμού
- συλλέξει πληροφορίες για την επικινδυνότητα
- διαμοιράσει τα αποτελέσματα της αποτίμησης επικινδυνότητας και να παρουσιάσει το σχέδιο αντιμετώπισης επικινδυνότητας
- αποφύγει ή να μειώσει την ύπαρξη και τη συνέπεια παραβίασης ασφάλειας πληροφοριών λόγω της αμοιβαίας κατανόησης μεταξύ αυτών που παίρνουν τις αποφάσεις και των ενδιαφερομένων
- υποστηρίξει τη λήψη αποφάσεων
- παρέχει γνώση για την ασφάλεια πληροφοριών
- συντονίσει με συμβαλλόμενους και να σχεδιάσει απόκριση τέτοια που να μειώνει τις συνέπειες ενός συμβάντος
- αποδώσει σε αυτούς που παίρνουν τις αποφάσεις και στους ενδιαφερόμενους μια αίσθηση ευθύνης σχετικά με τους κινδύνους
- βελτιώσει την επίγνωση

Κάθε Οργανισμός θα πρέπει να αναπτύξει σχέδιο επικοινωνίας όχι μόνο για τις καθιερωμένες λειτουργίες αλλά και για έκτακτες περιστάσεις έτσι ώστε η επικοινωνία να διεξάγεται συνεχόμενα. Για τον συντονισμό της επικοινωνίας μεταξύ των εμπλεκομένων, θεωρούνται καλές πρακτικές, να σχηματιστεί μία επιτροπή όπου να διεξάγεται συνεχείς διάλογος σχετικά με τα θέματα που αφορούν τη διαχείριση επικινδυνότητας και να υπάρχει στενή συνεργασία με τη αρμόδια μονάδα επικοινωνίας ή δημοσίων σχέσεων του Οργανισμού, ειδικά για τις περιπτώσεις που απαιτείται διαχείριση επικοινωνίας λόγω σοβαρού συμβάντος.

2.8. Παρακολούθηση και αναθεώρηση επικινδυνότητας (Risk monitoring and review)

2.8.1 Παρακολούθηση και αναθεώρηση των παραγόντων επικινδυνότητας

- Είσοδος: όλες οι πληροφορίες σχετικά με τους κινδύνους που προέκυψαν από τη διαχείριση επικινδυνότητας
- Δράση: παρακολούθηση και αναθεώρηση των κινδύνων και των παραγόντων τους προκειμένου να αναγνωριστούν εγκαίρως, όποιες αλλαγές αφορούν το περιεχόμενο του Οργανισμού και να διατηρείται η πλήρη εικόνα όσον αφορά τους κινδύνους.
- Έξοδος: συνεχής συμμόρφωση της διαχείρισης επικινδυνότητας με τους επιχειρησιακούς στόχους του Οργανισμού και τα κριτήρια αποδοχής επικινδυνότητας.

Σύμφωνα με την καθοδήγηση υλοποίησης που προτείνει το πρότυπο, οι κίνδυνοι δεν είναι στατικοί. Οι απειλές, οι ευπάθειες, η πιθανότητα, ή οι συνέπειες μπορεί να αλλάξουν ριζικά χωρίς προειδοποίηση. Γι' αυτό και η συνεχής παρακολούθηση θεωρείται σημαντική για να εντοπίζει εγκαίρως τυχόν αλλαγές. Σε αυτήν την παρακολούθηση των αλλαγών μπορούν να βοηθήσουν εξωτερικές υπηρεσίες οι οποίες παρέχουν πληροφορίες σχετικά με νέες απειλές ή ευπάθειες. Ο Οργανισμός θα πρέπει να εξασφαλίζει ότι τα παρακάτω παρακολουθούνται διαρκώς:

- τα νέα αγαθά που αποτελούν πλέον μέρος του σκοπού της διαχείρισης επικινδυνότητας
- τις απαραίτητες αλλαγές στην αξία των αγαθών λόγω π.χ. αλλαγής στις επιχειρησιακές προδιαγραφές
- τις νέες απειλές εντός ή εκτός του Οργανισμού που δεν έχουν ακόμα αποτιμηθεί
- την πιθανότητα, νέες ή αυξημένες ευπάθειες, να επιτρέψουν σε απειλές να τις εκμεταλλευτούν
- τις αναγνωρισμένες ευπάθειες, ώστε να προσδιοριστούν αυτές που πλέον εκτίθενται σε νέες ή διαφοροποιημένες απειλές
- τις αυξανόμενες συνέπειες, των απειλών, ευπαθειών και κινδύνων που έχουν εκτιμηθεί και συνολικά καταλήγουν σε ένα μη αποδεκτό επίπεδο επικινδυνότητας
- τα συμβάντα που σχετίζονται με την ασφάλεια πληροφοριών

Νέες απειλές, ευπάθειες ή αλλαγές στην πιθανότητα και τις συνέπειες, μπορεί να αυξήσουν κινδύνους που προηγουμένως είχαν εκτιμηθεί ως χαμηλού επιπέδου. Για το λόγο αυτό, θα πρέπει να οι κίνδυνοι που είναι χαμηλοί και έχουν γίνει αποδεκτοί να επιθεωρούνται τόσο ξεχωριστά όσο και σαν σύνολο προκειμένου να εκτιμηθεί η πιθανή συνολική επίπτωση τους. Στην περίπτωση που από αυτό τον έλεγχο, προκύψουν

διαφοροποιήσεις στο επίπεδο των κινδύνων και αυτό δεν είναι πλέον αποδεκτό, η διαχείριση τους πραγματοποιείται όπως αναφέρεται στη παρ. 2.3.

Επίσης είναι πιθανόν να συμβούν, αλλαγές σε παράγοντες που επηρεάζουν την πιθανότητα και τις συνέπειες των απειλών ή/και την καταλληλόλητα και το κόστος τον τρόπων αντιμετώπισης τους, καθώς και μεγάλες αλλαγές που επηρεάζουν τον Οργανισμό. Η παρακολούθηση της επικινδυνότητας θα πρέπει να επαναλαμβάνεται τακτικά αλλά και μετά από μεγάλες αλλαγές.

2.8.2 Παρακολούθηση, αναθεώρηση και βελτίωση της διαχείρισης επικινδυνότητας

- Είσοδος: όλες οι πληροφορίες σχετικά με τους κινδύνους που προέκυψαν από τη διαχείριση επικινδυνότητας
- Δράση: συνεχή παρακολούθηση, αναθεώρηση και βελτίωση της διαδικασίας διαχείρισης επικινδυνότητας ασφάλειας πληροφοριών, όπου και όπως απαιτείται.
- Έξοδος: συνεχής συμμόρφωση της διαχείρισης επικινδυνότητας με τους επιχειρησιακούς στόχους του Οργανισμού και δημιουργία ενημερωμένης έκδοσης της όπου απαιτείται.

Σύμφωνα με την καθοδήγηση υλοποίησης που προτείνει το πρότυπο, η παρακολούθηση και η αναθεώρηση είναι απαραίτητη έτσι ώστε να εξασφαλιστεί ότι το περιεχόμενο, το αποτέλεσμα της αποτίμησης επικινδυνότητας και της αντιμετώπισης επικινδυνότητας καθώς και όλα τα πλάνα διαχείρισης, παραμένουν σύμφωνα και κατάλληλα με τις περιστάσεις. Οποιαδήποτε βελτίωση πραγματοποιηθεί σχετικά με τη διαδικασία διαχείρισης επικινδυνότητας ασφάλειας πληροφοριών πρέπει να γνωστοποιείται στους υπεύθυνους διαχειριστές έτσι ώστε να εξασφαλιστεί ότι δεν θα παραλειφθούν σημαντικά στοιχεία που θα επηρεάσουν την αποτελεσματικότητα της διαδικασίας.

Επίσης ο Οργανισμός θα πρέπει να εξασφαλίζει ότι τα κριτήρια που έχουν τεθεί για να υλοποιηθεί η διαδικασία εξακολουθούν να είναι σύμφωνα με τους στόχους, τη στρατηγική και την πολιτική του καθώς και ότι το επιχειρησιακό περιεχόμενο λαμβάνεται επαρκώς υπόψη κατά τη διάρκεια της διαδικασίας.

Η παρακολούθηση διαχείρισης επικινδυνότητας είναι δυνατόν να καταλήξει σε μεταβολές ή προσθήκες όσον αφορά την προσέγγιση, τη μεθοδολογία και τα εργαλεία που χρησιμοποιήθηκαν. Το εύρος και το είδος των μεταβολών αυτών εξαρτάται από:

- τις αλλαγές που αναγνωρίστηκαν
- τις επαναλήψεις στην αποτίμηση επικινδυνότητας
- τον στόχο της διαχείρισης επικινδυνότητας ασφάλειας πληροφοριών
- το αντικείμενο της διαχείρισης επικινδυνότητας ασφάλειας πληροφοριών

3. NIST Special Publication 800-30 Revision 1

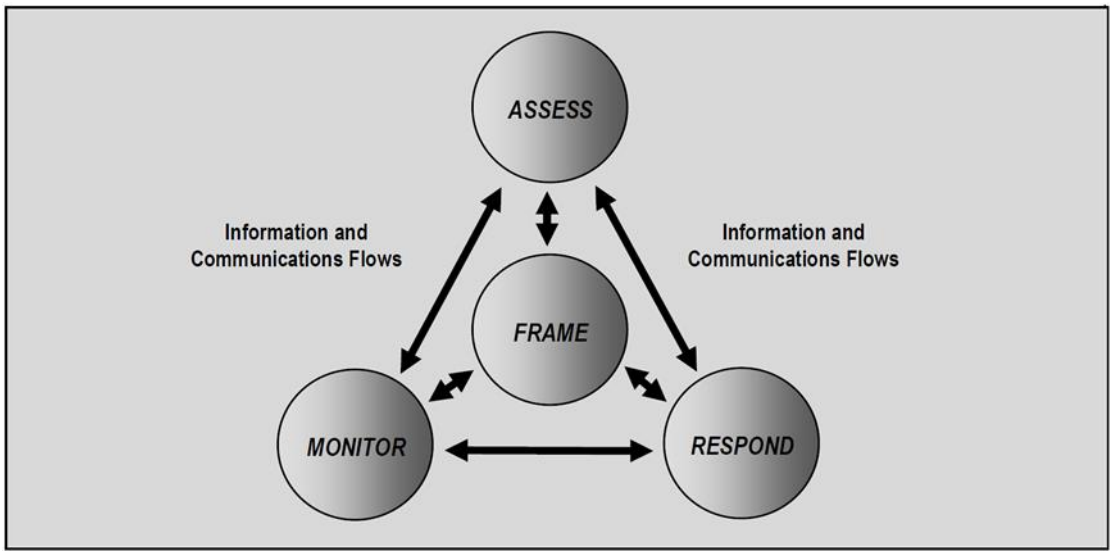
3.1 Σκοπός και εφαρμογή

Σκοπός της ειδικής έκδοσης 800-30 είναι να παρέχει οδηγίες για τη διεξαγωγή εκτιμήσεων κινδύνου ομοσπονδιακών πληροφοριακών συστημάτων και οργανισμών ενισχύοντας τις οδηγίες που παρέχονται από την έκδοση NIST 800-39[2]. Οι αξιολογήσεις κινδύνου μπορούν να πραγματοποιηθούν και στα τρία ιεραρχικά επίπεδα ενός οργανισμού και αποτελούν τμήμα της διαχείρισης κινδύνου (risk management). Παρέχεται στα ανώτερα στελέχη η πληροφορία που χρειάζονται για να εκτιμήσουν μια κατάσταση και να λάβουν σωστές αποφάσεις για την αντιμετώπιση των κινδύνων. Πιο συγκεκριμένα, αυτό το έγγραφο προσφέρει οδηγίες για την εκτέλεση κάθε βήματος της διαδικασίας αξιολόγησης κινδύνου καθώς και το πώς οι αξιολογήσεις κινδύνου και άλλες διαδικασίες διαχείρισης κινδύνου σε έναν οργανισμό αλληλοσυμπληρώνονται. Επιπλέον, η ειδική έκδοση 800-30 παρέχει οδηγίες στους οργανισμούς σχετικά με τον εντοπισμό συγκεκριμένων παραγόντων κινδύνου, που πρέπει να παρακολουθούνται σε συνεχή βάση με σκοπό οι οργανισμοί να μπορούν να προσδιορίζουν, εάν οι κίνδυνοι αυτοί έχουν αυξηθεί σε μη ανεκτά επίπεδα για τον οργανισμό και πρέπει να ληφθούν διαφορετικοί τρόποι δράσης.

[2] Η Ειδική δημοσίευση 800-39 αντικαθιστά την Ειδική δημοσίευση 800-30 ως την κύρια πηγή καθοδήγησης σχετικά με τη διαχείριση κινδύνου ασφάλειας πληροφοριών.

3.2 Διαδικασία διαχείρισης κινδύνου (risk management process)

Η αξιολόγηση κινδύνου αποτελεί βασικό συστατικό μιας ολιστικής διαδικασίας διαχείρισης κινδύνου σε επίπεδο οργανισμού, όπως ορίζεται στο NIST SP 800-39: *Διαχείριση κινδύνου ασφάλειας πληροφοριών: Οργανισμός, αποστολή και προβολή του πληροφοριακού συστήματος*. Η διαδικασία διαχείρισης κινδύνου περιλαμβάνει: i) τον κίνδυνο πλαισίου, ii) αξιολόγηση του κινδύνου, iii) αντιμετώπιση του κινδύνου iv) και παρακολούθηση του κινδύνου. Η εικόνα 1 παρακάτω δείχνει τα τέσσερα βήματα της διαδικασίας διαχείρισης κινδύνου καθώς επίσης και τις ροές πληροφοριών και επικοινωνιών που απαιτούνται για να λειτουργήσει αποτελεσματικά η διεργασία.



Εικόνα 3.2:Η αξιολόγηση κινδύνου κατά τη διαδικασία διαχείρισης κινδύνου.

Το πρώτο στοιχείο της διαχείρισης κινδύνου εξετάζει τον τρόπο με τον οποίο οι οργανισμοί *πλαισιώνουν* τον κίνδυνο ή δημιουργούν ένα πλαίσιο κινδύνου, περιγράφοντας το περιβάλλον στο οποίο λαμβάνονται οι αποφάσεις που βασίζονται στον κίνδυνο.

Το δεύτερο στοιχείο της διαχείρισης κινδύνου εξετάζει τον τρόπο με τον οποίο οι οργανισμοί αξιολογούν τον κίνδυνο μέσα στο πλαίσιο του οργανωτικού κινδύνου. Σκοπός της αξιολόγησης κινδύνου είναι να αναγνωρίσει: i) απειλές προς τον οργανισμό (π.χ. διαδικασίες, αγαθά, άνθρωποι) ή απειλές προερχόμενες από άλλους οργανισμούς με στόχο άλλους οργανισμούς ή το Έθνος, ii) εσωτερικές ή εξωτερικές ευπάθειες για τον οργανισμό, iii) τη βλάβη (δηλαδή, δυσμενείς επιπτώσεις) που μπορεί να προκύψουν δεδομένης της πιθανότητας απειλών που εκμεταλλεύονται τις ευπάθειες και iv) την πιθανότητα αύτη η βλάβη να προκύψει. Το τελικό αποτέλεσμα θα αφορά τον προσδιορισμό του κινδύνου (συνήθως πρόκειται για μια συνάρτηση του βαθμού της βλάβης και της πιθανότητας να προκύψει αυτή η βλάβη).

Η τρίτη συνιστώσα της διαχείρισης κινδύνου εξετάζει τον τρόπο με τον οποίο οι οργανισμοί ανταποκρίνονται στον κίνδυνο από τη στιγμή που αυτός ο κίνδυνος προσδιοριστεί με βάση τα αποτελέσματα μιας αξιολόγησης κινδύνου. Ο σκοπός της συνιστώσας απόκρισης κινδύνου είναι να παρέχει μια συνεπή, σε όλο τον οργανισμό ανταπόκριση στον κίνδυνο σύμφωνα με το πλαίσιο οργανωτικού κινδύνου με: (i) ανάπτυξη εναλλακτικών τρόπων δράσης για την αντιμετώπιση του κινδύνου, ii) αξιολόγηση των εναλλακτικών τρόπων δράσης, iii) τον καθορισμό κατάλληλων τρόπων δράσης σύμφωνα με την ανοχή οργανωτικού κινδύνου, και (iv) την εφαρμογή ανταποκρίσεων κινδύνου βάσει επιλεγμένων τρόπων δράσης.

Το τέταρτο στοιχείο της διαχείρισης κινδύνου εξετάζει τον τρόπο με τον οποίο οι οργανισμοί παρακολουθούν τον κίνδυνο με την πάροδο του χρόνου. Ο σκοπός της συνιστώσας παρακολούθησης κινδύνου είναι: (i) να προσδιορίσει τη διαρκή αποτελεσματικότητα των ανταποκρίσεων στον κίνδυνο (σύμφωνα με το πλαίσιο οργανωτικού κινδύνου), (ii) να προσδιορίζει τις αλλαγές που επηρεάζουν τον κίνδυνο στα συστήματα πληροφοριών του οργανισμού και στα περιβάλλοντα στα οποία λειτουργούν τα συστήματα, και (iii) να επαληθεύει ότι εφαρμόζονται οι προγραμματισμένες ανταποκρίσεις κινδύνου και ότι οι απαιτήσεις ασφάλειας

πληροφοριών προκύπτουν και ανιχνεύονται σε οργανωτικές αποστολές/επιχειρηματικές λειτουργίες, και ότι η ομοσπονδιακή νομοθεσία, οι οδηγίες, οι κανονισμοί, οι πολιτικές, τα πρότυπα και οι οδηγίες πληρούνται.

3.3 Αξιολόγηση κινδύνου

Όπως αναφέρθηκε και παραπάνω, αυτή η έκδοση επικεντρώνεται στην αξιολόγηση του κινδύνου ως σημαντικό μέρος της διαχείρισης του κινδύνου. Η διαχείριση του κινδύνου δεν είναι μια διαδικασία που αναπτύσσεται μια φορά και προσφέρει μόνιμη και συνεχής ενημέρωση στους ειδικούς που αναλαμβάνουν να πάρουν μια απόφαση σχετική με την αντιμετώπιση του κινδύνου. Αντιθέτως, η αξιολόγηση κινδύνου είναι μια διαδικασία που θα πρέπει να επαναλαμβάνεται σε τακτά χρονικά διαστήματα και καθ' όλη τη διάρκεια ζωής της ανάπτυξης ενός πληροφοριακού συστήματος καθώς επίσης και να εφαρμόζεται κατά μήκος όλων των ιεραρχικών επιπέδων της διαχείρισης κινδύνου ενός οργανισμού.

Οι εκτιμήσεις κινδύνου αντιμετωπίζουν τις πιθανές αρνητικές επιπτώσεις σε οργανωτικές λειτουργίες και περιουσιακά στοιχεία, άτομα, άλλους οργανισμούς, και τα οικονομικά συμφέροντα και τα συμφέροντα εθνικής ασφάλειας των Ηνωμένων Πολιτειών, που απορρέουν από τη λειτουργία και τη χρήση των πληροφοριακών συστημάτων και των πληροφοριών που επεξεργάζονται, αποθηκεύονται και μεταδίδονται από αυτά τα συστήματα. Οι οργανισμοί διενεργούν αξιολογήσεις κινδύνου για να προσδιορίσουν τους κινδύνους που είναι κοινοί για τις βασικές αποστολές/επιχειρηματικές λειτουργίες, τις αποστολές/επιχειρηματικές διαδικασίες, τα τμήματα αποστολής/επιχειρήσεων, την κοινή υποδομή/υπηρεσίες υποστήριξης ή τα συστήματα πληροφοριών. Οι αξιολογήσεις κινδύνου μπορούν να υποστηρίξουν μια μεγάλη ποικιλία αποφάσεων και δραστηριοτήτων που βασίζονται στον κίνδυνο από στελέχη του οργανισμού και στα τρία επίπεδα της ιεραρχίας διαχείρισης κινδύνου, συμπεριλαμβανομένων, ενδεικτικά, των εξής:

• Ανάπτυξη αρχιτεκτονικής ασφάλειας πληροφοριών

• Καθορισμός απαιτήσεων διασύνδεσης για συστήματα πληροφοριών (συμπεριλαμβανομένων συστημάτων που υποστηρίζουν διαδικασίες αποστολής/επιχειρήσεων και κοινές υποδομές/υπηρεσίες υποστήριξης).

• Σχεδιασμός λύσεων ασφαλείας για συστήματα πληροφοριών και περιβάλλοντα λειτουργίας, συμπεριλαμβανομένης της επιλογής ελέγχων ασφαλείας, προϊόντων τεχνολογίας πληροφοριών, προμηθευτών/αλυσίδας εφοδιασμού και εργολάβων.

• Εξουσιοδότηση (ή άρνηση εξουσιοδότησης) για τη λειτουργία συστημάτων πληροφοριών ή για τη χρήση ελέγχων ασφαλείας που κληρονομήθηκαν από αυτά τα συστήματα.

• Τροποποίηση αποστολών/επιχειρηματικών λειτουργιών ή/και αποστολών/επιχειρηματικών διαδικασιών μόνιμα ή για συγκεκριμένο χρονικό πλαίσιο (π.χ., έως ότου αντιμετωπιστεί μια απειλή ή ευπάθεια που ανακαλύφθηκε πρόσφατα, έως ότου αντικατασταθεί ένας αντισταθμιστικός έλεγχος).

• Εφαρμογή λύσεων ασφαλείας (π.χ. εάν συγκεκριμένα προϊόντα τεχνολογίας πληροφοριών ή διαμορφώσεις για αυτά τα προϊόντα πληρούν τις καθιερωμένες απαιτήσεις).

• Λειτουργία και συντήρηση λύσεων ασφαλείας (π.χ. στρατηγικές και προγράμματα συνεχούς παρακολούθησης, συνεχείς εξουσιοδοτήσεις).

Επειδή οι οργανωτικές αποστολές και οι λειτουργίες της επιχείρησης καθώς επίσης οι επιχειρηματικές διαδικασίες, τα πληροφοριακά συστήματα, οι απειλές, και τα περιβάλλοντα λειτουργίας τείνουν να αλλάζουν με την πάροδο του χρόνου, η εγκυρότητα και η χρησιμότητα των εκτιμήσεων κινδύνου περιορίζεται χρονικά.

3.3.1 Μοντέλα κινδύνου

Τα μοντέλα κινδύνου προσδιορίζουν τους παράγοντες κινδύνου που πρέπει να εκτιμηθούν καθώς και τη σχέση μεταξύ αυτών των παραγόντων. Οι παράγοντες κινδύνου είναι χαρακτηριστικά που χρησιμοποιούμε ως εισόδους στα μοντέλα κινδύνου με σκοπό να καθορίσουμε το επίπεδο του ρίσκου στην εκτίμηση του κινδύνου. Επίσης, οι παράγοντες κινδύνου χρησιμοποιούνται εκτεταμένα και στις επικοινωνίες που σχετίζονται με τον κίνδυνο για να επισημάνουν τι επηρεάζει έντονα τα επίπεδα κινδύνου σε συγκεκριμένες καταστάσεις, περιστάσεις ή περιβάλλοντα. Οι συνήθεις παράγοντες κινδύνου περιλαμβάνουν: την απειλή, την ευπάθεια, την πιθανότητα, την επίπτωση και την προδιαθεσική κατάσταση. Οι παράγοντες κινδύνου μπορούν να αναλυθούν σε πιο λεπτομερή χαρακτηριστικά (για παράδειγμα, οι απειλές να αναλυθούν σε πηγές απειλών και σε συμβάντα απειλών). Αυτοί οι ορισμοί είναι σημαντικό για τον οργανισμό να τεκμηριώνονται πριν την διεξαγωγή της αξιολόγησης του κινδύνου, καθώς οι αξιολογήσεις βασίζονται σε καλώς-καθορισμένα χαρακτηριστικά

απειλών, ευπαθειών, επιπτώσεων, πιθανοτήτων και άλλων παραγόντων κινδύνου με σκοπό τον αποτελεσματικό προσδιορισμό του κινδύνου.

Απειλές

Όταν αναφερόμαστε στον όρο απειλή, εννοούμε οποιαδήποτε περίσταση ή συμβάν που μπορεί να επηρεάσει αρνητικά της λειτουργίες ενός οργανισμού, τα περιουσιακά αγαθά, τα άτομα, άλλους οργανισμούς ή ακόμα και το Έθνος μέσω ενός πληροφοριακού συστήματος. Αυτό μπορεί να επιτευχθεί είτε μέσω της μη εξουσιοδοτημένης πρόσβασης, καταστροφής, αποκάλυψης, τροποποίησης πληροφοριών και/ή άρνηση εξυπηρέτησης. Ένα συμβάν απειλής προκαλείται από μια πηγή απειλής. Ως *πηγή απειλής* χαρακτηρίζεται: i) η πρόθεση και η μέθοδος που στοχεύουν στην εκμετάλλευση μιας ευπάθειας, ή ii) μια κατάσταση και η μέθοδος που μπορεί να εκμεταλλευτούν μια ευπάθεια μη εσκεμμένα. Γενικότερα, οι τύποι απειλών που προέρχονται από πηγές περιλαμβάνουν: i) εχθρικές επιθέσεις στον κυβερνοχώρο ή φυσικές επιθέσεις, ii) ανθρώπινα λάθη παράλειψης ή εκτέλεσης, iii) δομικές αστοχίες πόρων που ελέγχονται από τον οργανισμό (υλικό, λογισμικό), iv) φυσικές και ανθρωπογενείς καταστροφές, ατυχήματα και αποτυχίες πέρα από τον έλεγχο του οργανισμού. Πολλαπλές πηγές απειλών μπορούν να ξεκινήσουν ή να προκαλέσουν το ίδιο συμβάν απειλής—για παράδειγμα, ένας διακομιστής μπορεί να αποσυνδεθεί από επίθεση άρνησης υπηρεσίας, σκόπιμη ενέργεια από έναν κακόβουλο διαχειριστή συστήματος, ένα διαχειριστικό σφάλμα, ένα σφάλμα υλικού, ή διακοπή ρεύματος.

Τα μοντέλα κινδύνου διαφέρουν ως προς τον βαθμό λεπτομέρειας και πολυπλοκότητας με τον οποίο αναγνωρίζονται τα συμβάντα απειλών. Όταν τα συμβάντα απειλών αναγνωριστούν, τότε σενάρια απειλών μπορούν να μοντελοποιηθούν, αναπτυχθούν και αναλυθούν. Τα συμβάντα απειλών που αφορούν είτε τις κυβερνοεπιθέσεις είτε τις φυσικές επιθέσεις χαρακτηρίζονται από τακτικές (tactics), τεχνικές (techniques) και διαδικασίες (procedures) (TTPs) που χρησιμοποιούν οι επιτιθέμενοι. Η κατανόηση των συμβάντων απειλών που βασίζονται σε αντιπάλους δίνει στους οργανισμούς πληροφορίες για τις δυνατότητες που σχετίζονται με ορισμένες πηγές απειλών. Επιπλέον, γνωρίζοντας περισσότερα σχετικά με το ποιος εκτελεί τις επιθέσεις δίνει στους οργανισμούς βαθύτερη κατανόηση του τι επιθυμούν να κερδίσουν οι αντίπαλοι από τις επιθέσεις.

Ευπάθειες και προδιαθεσικές καταστάσεις

Μια ευπάθεια είναι μια αδυναμία ενός συστήματος πληροφοριών, των διαδικασιών ασφάλειας συστήματος, των εσωτερικών ελέγχων ή της εφαρμογής που θα μπορούσε να εκμεταλλευτεί μια πηγή απειλής. Οι περισσότερες ευπάθειες πληροφοριακών συστημάτων σχετίζονται με αντίμετρα που είτε δεν έχουν εφαρμοστεί (ακουσίως ή εκουσίως), είτε εφαρμόστηκαν με λάθος τρόπο και παρουσιάζουν ακόμα αδυναμίες. Ωστόσο, είναι σημαντικό να αφήσουμε χώρο και για την πιθανότητα των αναδυόμενων ευπαθειών οι οποίες μπορεί να προκύψουν φυσικά με την πάροδο του χρόνου καθώς οι λειτουργίες του οργανισμού εξελίσσονται, τα περιβάλλοντα αλλάζουν, νέες τεχνολογίες αυξάνονται και νέες απειλές εμφανίζονται. Στο πλαίσιο αυτών των αλλαγών, τα αντίμετρα μπορεί να θεωρούνται ανεπαρκή και μπορεί να χρειάζονται επαναξιολόγηση της αποτελεσματικότητάς τους. Η τάση για την πιθανή μείωση της αποτελεσματικότητας των αντιμέτρων με την πάροδο του χρόνου, ενισχύει την ανάγκη για τη διατήρηση των αξιολογήσεων κινδύνου καθ' όλη τη διάρκεια ανάπτυξης ενός πληροφοριακού συστήματος καθώς επίσης και για τις συνεχείς παρακολουθήσεις των συστημάτων με σκοπό τη συνεχή επίγνωσης της κατάστασης ασφαλείας που έχει ένας οργανισμός.

Οι ευπάθειες δεν εντοπίζονται μόνο στα πληροφοριακά συστήματα. Ευπάθειες μπορεί να βρεθούν στις οργανωτικές δομές (π.χ. έλλειψη αποτελεσματικών στρατηγικών διαχείρισης κινδύνου, κακή επικοινωνία μεταξύ των τμημάτων του οργανισμού), στις εξωτερικές σχέσεις (π.χ. πάροχοι τηλεπικοινωνιών, τεχνολογίες πληροφοριών) καθώς επίσης και στις αρχιτεκτονικές ασφάλειας πληροφοριών.

Οι κίνδυνοι είναι γενικότερα μια σειρά συμβάντων από απειλές, καθένα από τα οποία εκμεταλλεύεται ένα ή περισσότερα τρωτά σημεία. Οι οργανισμοί ορίζουν *σενάρια απειλών* για να περιγράψουν πώς αυτά τα συμβάντα απειλών που προκαλούνται από μια πηγή απειλής μπορούν να συμβάλλουν θετικά ή να προκαλέσουν βλάβη. Η ανάπτυξη τέτοιων σεναρίων είναι χρήσιμη από αναλυτικής πλευράς, καθώς ορισμένα ευπαθή σημεία ενδέχεται να μην εκτεθούν ως προς εκμετάλλευση εκτός και αν εκμεταλλευτούν άλλα τρωτά σημεία πρώτα. Επομένως, η ανάλυση που μας δείχνει τον τρόπο με τον οποίο ένα σύνολο τρωτών σημείων θα μπορούσε να εκμεταλλευτεί από ένα ή περισσότερα συμβάντα απειλής, είναι πιο χρήσιμη από την ανάλυση μεμονωμένων ευπαθειών. Επιπλέον, ένα σενάριο απειλής αφηγείται μια ιστορία και ως εκ τούτου είναι κατάλληλο να χρησιμοποιηθεί κατά την επικοινωνία του κινδύνου μεταξύ των τμημάτων του οργανισμού καθώς και για την ανάλυση.

Εκτός από τις ευπάθειες όπως περιγράψαμε παραπάνω, οι οργανισμοί λαμβάνουν υπόψη και τις προδιαθεσικές καταστάσεις. Με τον όρο *προδιαθεσική κατάσταση* εννοούμε την συνθήκη που υπάρχει σε έναν οργανισμό, στην αποστολή ή σε μια επιχειρησιακή λειτουργία, στο πληροφοριακό σύστημα, ή στο περιβάλλον λειτουργίας, η οποία μπορεί να επηρεάσει (αρνητικά ή θετικά) την πιθανότητα να προκύψει ένα συμβάν απειλής, και αυτό με τη σειρά του να έχει αρνητική επίπτωση στις οργανωτικές λειτουργίες, στα περιουσιακά αγαθά, τους ανθρώπους, άλλους οργανισμούς ή και το Έθνος. Προδιαθεσική κατάσταση είναι για παράδειγμα η τοποθεσία μιας εγκατάστασης σε σεισμογενή περιοχή (αυξάνοντας την πιθανότητα έκθεσης σε σεισμούς) ή ένα αυτόνομο πληροφοριακό σύστημα χωρίς σύνδεση στο διαδίκτυο (μειώνοντας την πιθανότητα έκθεση σε κυβερνοεπίθεση). Οι ευπάθειες που προκύπτουν από προδιαθεσικές καταστάσεις και δεν μπορούν να διορθωθούν εύκολα, συνήθως περιλαμβάνουν κενά σε σχέδια έκτακτης ανάγκης, χρήση απαρχαιωμένων τεχνολογιών ή αδυναμίες/ελλείψεις σε μηχανισμούς δημιουργίας αντιγράφων ασφαλείας συστήματος πληροφοριών. Σε όλες αυτές τις περιπτώσεις, αυτοί οι τύποι ευπαθειών δημιουργούν μια προδιάθεση για συμβάντα απειλών που θα έχουν αρνητικές επιπτώσεις στους οργανισμούς. Οι ευπάθειες (συμπεριλαμβανομένων εκείνων που αποδίδονται σε συνθήκες προδιάθεσης) αποτελούν μέρος της συνολικής θέσης ασφάλειας των συστημάτων πληροφοριών και του περιβάλλοντος λειτουργίας του οργανισμού που μπορεί να επηρεάσει την πιθανότητα εμφάνισης ενός γεγονότος απειλής.

Πιθανότητα

Η *πιθανότητα εμφάνισης* είναι ένας σταθμισμένος παράγοντας κινδύνου που βασίζεται σε ανάλυση της πιθανότητας ότι μια δεδομένη απειλή είναι ικανή να εκμεταλλευτεί μια δεδομένη ευπάθεια. Ο παράγοντας κινδύνου πιθανότητας συνδυάζει μια εκτίμηση της πιθανότητας να ξεκινήσει το συμβάν απειλής με μια εκτίμηση της πιθανότητας επίδρασης που θα έχει (δηλαδή, την πιθανότητα το γεγονός απειλής να οδηγήσει σε δυσμενείς επιπτώσεις). Για τις απειλές που προέρχονται από τους επιτιθέμενους, μια εκτίμηση της πιθανότητας εμφάνισης ενός συμβάντος συνήθως βασίζεται στα εξής: i) *κίνητρο* του επιτιθέμενου, ii) *ικανότητα* του επιτιθέμενου, iii) και *στόχο* του επιτιθέμενου. Για τις απειλές που δεν προέρχονται από τους επιτιθέμενους, η πιθανότητα εμφάνισης ενός γεγονότος απειλής, υπολογίζεται με βάση ιστορικά στοιχεία, εμπειρικά δεδομένα, ή άλλους παράγοντες. Η πιθανότητα ένα συμβάν απειλής να ξεκινήσει ή να συμβεί εκτιμάται μέσα σε συγκεκριμένο χρονικό πλαίσιο (π.χ. τους επόμενους έξι μήνες, τον επόμενο χρόνο, ή την περίοδο όταν ολοκληρωθεί μια συγκεκριμένη ενέργεια). Αν ένα συμβάν απειλής είναι σχεδόν σίγουρο ότι θα εμφανιστεί σε ένα συγκεκριμένο χρονικό πλαίσιο, τότε η αξιολόγηση κινδύνου μπορεί να λάβει υπόψη την εκτιμώμενη συχνότητα του συμβάντος. Η πιθανότητα εμφάνισης μιας απειλής μπορεί να βασιστεί και στην κατάσταση που βρίσκεται ο οργανισμός (συμπεριλαμβανομένων, για παράδειγμα, της βασικής αποστολής, της εταιρικής αρχιτεκτονικής, της αρχιτεκτονικής ασφάλειας πληροφοριών, των συστημάτων πληροφοριών και των περιβαλλόντων στα οποία λειτουργούν αυτά τα συστήματα). Επιπλέον, λαμβάνονται υπόψη οι προδιαθεσικές καταστάσεις που αναφέραμε παραπάνω καθώς και η παρουσία και υλοποίηση αποτελεσματικών μέτρων ασφαλείας που έχουν ως σκοπό την προστασία από μη εξουσιοδοτημένη συμπεριφορά, τον εντοπισμό και περιορισμό βλαβών, και τη διατήρηση και επανάκτηση των επιχειρησιακών λειτουργιών. Η πιθανότητα της επίπτωσης αντιμετωπίζει την πιθανότητα το γεγονός απειλής να οδηγήσει σε δυσμενή επίπτωση, ανεξάρτητα από το μέγεθος της βλάβης που τυχόν αναμένεται να προκύψει.

Οι οργανισμοί συνήθως χρησιμοποιούν μια διαδικασία τριών βημάτων για να καθορίσουν τη συνολική πιθανότητα των γεγονότων απειλών. Πρώτον, οι οργανισμοί αξιολογούν την πιθανότητα να ξεκινήσουν γεγονότα απειλής (για συμβάντα απειλής από επιτιθέμενο) ή να συμβούν. Δεύτερον, οι οργανισμοί αξιολογούν την πιθανότητα ότι τα γεγονότα απειλής μόλις ξεκινήσουν ή συμβούν, θα οδηγήσουν σε δυσμενείς επιπτώσεις ή ζημιά σε οργανωτικές λειτουργίες και περιουσιακά στοιχεία, άτομα, άλλους οργανισμούς ή και το Έθνος. Τέλος, οι οργανισμοί αξιολογούν τη συνολική πιθανότητα ως συνδυασμό πιθανότητας έναρξης/εμφάνισης αυτής της απειλής και πιθανότητας να οδηγήσει σε δυσμενείς επιπτώσεις.

Ένα ζεύγος απειλής-ευπάθειας μπορεί να είναι ανεπιθύμητο κατά την αξιολόγηση της πιθανότητας σε επίπεδο λειτουργίας της επιχείρησης και σε πολλές περιπτώσεις μπορεί να είναι προβληματικό ακόμη και σε επίπεδο συστήματος πληροφοριών λόγω τον δυνητικά μεγάλο αριθμό απειλών και ευπαθειών. Αυτή η προσέγγιση συνήθως στρέφεται προς στον εντοπισμό γεγονότων και τρωτών σημείων απειλής, αντί να επιτρέπει στους οργανισμούς να κάνουν αποτελεσματική χρήση των πληροφοριών που σχετίζονται με απειλές ή/και να εντοπίζουν απειλές σε επίπεδο λεπτομέρειας που έχει νόημα. Ανάλογα με το επίπεδο λεπτομέρειας στις προδιαγραφές απειλής, ένα δεδομένο συμβάν απειλής θα μπορούσε να εκμεταλλευτεί πολλαπλά τρωτά σημεία. Κατά την αξιολόγηση των πιθανοτήτων, οι οργανισμοί εξετάζουν τις ευπάθειες που θα μπορούσαν να εκμεταλλευτούν

τα γεγονότα απειλών και επίσης την ευαισθησία της επιχειρηματικής λειτουργίας σε γεγονότα για τα οποία δεν υπάρχουν έλεγχοι ασφαλείας ή βιώσιμες εφαρμογές ελέγχων ασφαλείας (π.χ. λόγω λειτουργικών εξαρτήσεων, ιδιαίτερα εξωτερικών εξαρτήσεων). Σε ορισμένες περιπτώσεις, ο πιο αποτελεσματικός τρόπος για να μειωθεί ο επιχειρηματικός κίνδυνος που αποδίδεται στον κίνδυνο ασφάλειας πληροφοριών είναι ο επανασχεδιασμός των διαδικασιών αποστολής/επιχειρήσεων, ώστε να υπάρχουν βιώσιμες λύσεις όταν τα συστήματα πληροφοριών διακυβεύονται. Η χρήση της έννοιας των σεναρίων απειλών που περιγράφονται παραπάνω, μπορεί να βοηθήσει τους οργανισμούς να ξεπεράσουν ορισμένους από τους περιορισμούς των ζευγών απειλής-ευπάθειας.

Επίπτωση

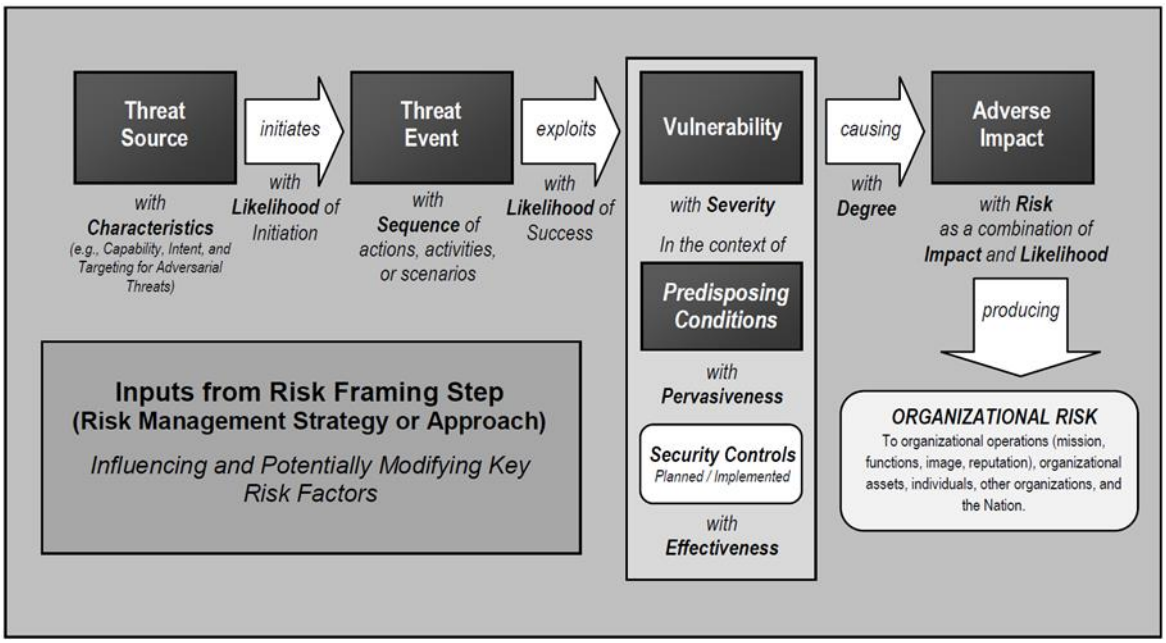
Το μέγεθος της επίπτωσης που προέρχεται από ένα συμβάν απειλής εξαρτάται από το μέγεθος της βλάβης που μπορεί να προκύψει από τις συνέπειες της μη εξουσιοδοτημένης αποκάλυψης πληροφοριών, της μη εξουσιοδοτημένης τροποποίησης πληροφοριών, της μη εξουσιοδοτημένης καταστροφής ή απώλειας πληροφοριών ή διαθεσιμότητας του συστήματος πληροφοριών. Τέτοια ζημιά μπορεί να υποστεί οποιοσδήποτε έχει έννομο συμφέρον για τις λειτουργίες, τα περιουσιακά στοιχεία ή τα άτομα του οργανισμού, συμπεριλαμβανομένων άλλων οργανισμών σε συνεργασία με τον οργανισμό ή το Έθνος. Οι οργανισμοί διευκρινίζουν: (i) τη διαδικασία που χρησιμοποιείται για τη διενέργεια προσδιορισμών επιπτώσεων, (ii) παραδοχές που σχετίζονται με προσδιορισμούς επιπτώσεων, (iii) πηγές και μέθοδοι για τη λήψη πληροφοριών για τον αντίκτυπο, και (iv) το σκεπτικό για τα συμπεράσματα που συνάγονται σχετικά με τους προσδιορισμούς επιπτώσεων.

Οι οργανισμοί μπορούν να ορίσουν ρητά πώς οι καθορισμένες προτεραιότητες και αξίες καθοδηγούν τον εντοπισμό περιουσιακών στοιχείων υψηλής αξίας και τις πιθανές δυσμενείς επιπτώσεις στα ενδιαφερόμενα μέρη του οργανισμού. Εάν αυτές οι πληροφορίες δεν έχουν καθοριστεί, οι προτεραιότητες και οι αξίες που σχετίζονται με τον προσδιορισμό των στόχων των πηγών απειλών και των σχετικών οργανωτικών επιπτώσεων μπορούν συνήθως να προκύψουν από στρατηγικό σχεδιασμό και πολιτικές. Για παράδειγμα, τα επίπεδα κατηγοριοποίησης ασφαλείας υποδεικνύουν τις οργανωτικές επιπτώσεις της έκθεσης διαφορετικών τύπων πληροφοριών. Οι αξιολογήσεις επιπτώσεων απορρήτου και τα επίπεδα κρισιμότητας (όταν ορίζονται ως μέρος του σχεδιασμού έκτακτης ανάγκης ή της επιχειρησιακής ανάλυσης επιπτώσεων) υποδεικνύουν τις αρνητικές επιπτώσεις της καταστροφής, της διαφθοράς ή της απώλειας ευθύνης για τους πόρους πληροφοριών στους οργανισμούς.

Τα στρατηγικά σχέδια και πολιτικές επιβεβαιώνουν ή υπονοούν επίσης τις σχετικές προτεραιότητες της άμεσης ή βραχυπρόθεσμης ολοκλήρωσης της επιχειρηματικής λειτουργίας και της μακροπρόθεσμης οργανωτικής βιωσιμότητας (που μπορεί να υπονομευθεί από την απώλεια φήμης ή από κυρώσεις που προκύπτουν από την παραβίαση ευαίσθητων πληροφοριών). Οι οργανισμοί μπορούν επίσης να εξετάσουν το εύρος των επιπτώσεων των απειλών, συμπεριλαμβανομένου του σχετικού μεγέθους του συνόλου των πόρων που επηρεάζονται, όταν κάνουν τους τελικούς προσδιορισμούς του αντίκτυπου. Οι παραδοχές ανοχής κινδύνου μπορεί να αναφέρουν ότι τα γεγονότα απειλών με αντίκτυπο κάτω από μια συγκεκριμένη τιμή δεν δικαιολογούν περαιτέρω ανάλυση.

Ρίσκο

Η εικόνα 3.3.1 δείχνει ένα παράδειγμα από ένα μοντέλο κινδύνου συμπεριλαμβανομένου και τους βασικούς παράγοντες κινδύνου που αναφέρθηκαν παραπάνω καθώς και τη σχέση μεταξύ των παραγόντων. Κάθε παράγοντας κινδύνου χρησιμοποιείται στη διαδικασία εκτίμησης κινδύνου στο κεφάλαιο 3.



Εικόνα 3.3.1: Γενικό μοντέλο κινδύνου με βασικούς παράγοντες κινδύνου.

Όπως έχουμε ήδη αναφέρει, ρίσκο είναι η πιθανότητα εμφάνισης ενός συμβάντος απειλής και η πιθανή αρνητική επίπτωση που μπορεί να προκύψει. Αυτός ο ορισμός περιλαμβάνει πολλούς τύπους δυσμενών επιπτώσεων σε όλα τα επίπεδα στην ιεραρχία διαχείρισης κινδύνου (risk management tiers[3]) που περιγράφεται στην ειδική δημοσίευση 800-39 (ζημιά στην εικόνα ή στη φήμη της επιχείρησης ή οικονομική ζημιά στο πρώτο επίπεδο ιεραρχίας, ανικανότητα διεξαγωγής επιχειρηματικής λειτουργίας στο δεύτερο επίπεδο ιεραρχίας ή ακόμη και οι πόροι που ξοδεύονται για την αντιμετώπιση ενός περιστατικού ασφαλείας στο τρίτο επίπεδο ιεραρχίας). Εξηγεί επίσης τις σχέσεις μεταξύ των επιπτώσεων (απώλεια τρέχουσας ή μελλοντικής επιχειρησιακής αποτελεσματικότητας λόγω απώλειας του απορρήτου των δεδομένων· απώλεια εμπιστοσύνης σε κρίσιμες πληροφορίες λόγω απώλειας δεδομένων ή ακεραιότητας συστήματος· ή μη διαθεσιμότητα ή υποβάθμιση πληροφοριών ή πληροφοριακών συστημάτων). Αυτός ο ευρύς ορισμός επιτρέπει επίσης να αναπαρασταθεί ο κίνδυνος ως ενιαία τιμή ή ως συνδυασμός τιμών όπου διαφορετικοί τύποι επιπτώσεων αξιολογούνται χωριστά. Για σκοπούς επικοινωνίας κινδύνου, ο κίνδυνος γενικά ομαδοποιείται σύμφωνα με τους τύπους των δυσμενών επιπτώσεων (και πιθανώς τα χρονικά πλαίσια μέσα στα οποία είναι πιθανό να υπάρξουν αυτές οι επιπτώσεις).

Συνάθροιση κινδύνου

Οι οργανισμοί μπορούν να χρησιμοποιήσουν τη *συνάθροιση* κινδύνων για να συνδυάσουν αρκετούς διακριτούς ή κινδύνους κατώτερου επιπέδου σε ένα γενικότερο ή υψηλότερου-επιπέδου κίνδυνο. Οι οργανισμοί μπορούν επίσης να χρησιμοποιούν συνάθροιση κινδύνων για να διαχειριστούν αποτελεσματικά το εύρος και την κλίμακα των αξιολογήσεων κινδύνου που περιλαμβάνουν πολλαπλά συστήματα πληροφοριών και πολλαπλές επιχειρησιακές διαδικασίες με καθορισμένες σχέσεις και εξαρτήσεις μεταξύ αυτών των συστημάτων και διαδικασιών. Η συνάθροιση κινδύνων, που διεξάγεται κυρίως στις βαθμίδες ιεραρχίας 1 και 2 και περιστασιακά στη βαθμίδα 3, αξιολογεί τον συνολικό κίνδυνο για τις οργανωτικές λειτουργίες, τα περιουσιακά στοιχεία και τα άτομα δεδομένου του συνόλου των διακριτών κινδύνων. Γενικά, για διακριτούς κινδύνους (π.χ. τον κίνδυνο που σχετίζεται με ένα ενιαίο σύστημα πληροφοριών που υποστηρίζει μια καλά καθορισμένη επιχειρησιακή διαδικασία), ο αντίκτυπος στη χειρότερη περίπτωση καθορίζει ένα ανώτερο όριο για το συνολικό κίνδυνο για τις οργανωτικές λειτουργίες, τα περιουσιακά στοιχεία και τα άτομα. Ένα ζήτημα για τη συνάθροιση κινδύνων είναι ότι αυτό το ανώτερο όριο κινδύνου ενδέχεται να μην ισχύει. Για παράδειγμα, μπορεί να είναι επωφελές για τους οργανισμούς να αξιολογούν τον κίνδυνο σε επίπεδο οργανισμού όταν πολλαπλοί κίνδυνοι

[3] Το NIST Special Publication 800-39 παρέχει καθοδήγηση για τα τρία επίπεδα της ιεραρχίας διαχείρισης κινδύνου, συμπεριλαμβανομένων των Tier 1 (οργάνωση), Tier 2 (αποστολή/επιχειρησιακή διαδικασία) και Tier 3 (σύστημα πληροφοριών).

υλοποιούνται ταυτόχρονα ή όταν ο ίδιος κίνδυνος υλοποιείται επανειλημμένα σε μια χρονική περίοδο. Σε τέτοιες περιπτώσεις, υπάρχει η πιθανότητα ότι το ποσό του συνολικού κινδύνου που υφίσταται είναι πέρα από την ικανότητα κινδύνου του οργανισμού, και επομένως ο συνολικός αντίκτυπος στις οργανωτικές λειτουργίες και τα περιουσιακά στοιχεία υπερβαίνει αυτό που είχε αρχικά εκτιμηθεί για κάθε συγκεκριμένο κίνδυνο.

Κατά τη συνάθροιση του κινδύνου, οι οργανισμοί εξετάζουν τη σχέση μεταξύ διαφόρων διακριτών κινδύνων. Για παράδειγμα, μπορεί να υπάρχει σχέση αιτίου-αποτελέσματος κατά το οποίο εάν πραγματοποιηθεί ένας κίνδυνος, ένας άλλος κίνδυνος είναι περισσότερο ή λιγότερο πιθανό να πραγματοποιηθεί. Εάν υπάρχει άμεση ή αντίστροφη σχέση μεταξύ διακριτών κινδύνων, τότε οι κίνδυνοι μπορούν να συσχετιστούν (με ποιοτική ή με ποσοτική έννοια) είτε με θετικό είτε με αρνητικό τρόπο. Η σύζευξη ή η συσχέτιση κινδύνου (δηλαδή, η εύρεση σχέσεων μεταξύ των κινδύνων που αυξάνουν ή μειώνουν την πιθανότητα υλοποίησης οποιουδήποτε συγκεκριμένου κινδύνου) μπορεί να γίνει στις βαθμίδες 1, 2 ή 3.

Αβεβαιότητα

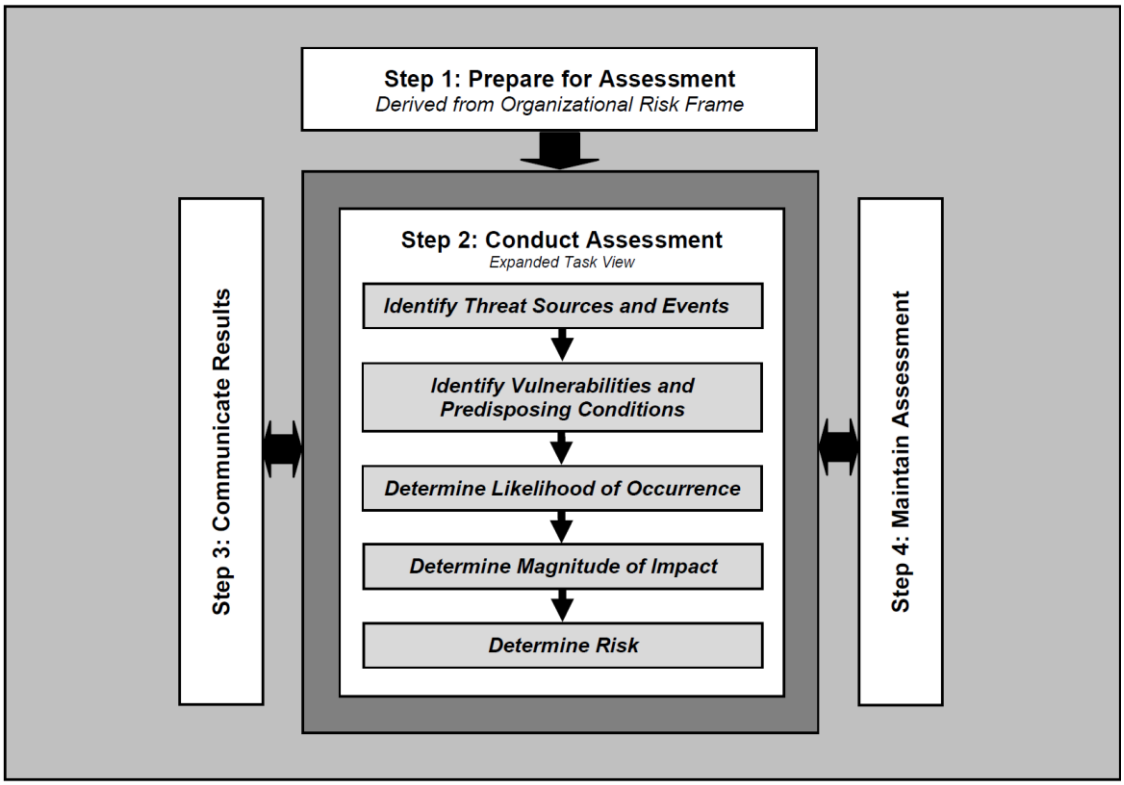
Η *αβεβαιότητα* είναι εγγενής στην αξιολόγηση του κινδύνου, λόγω παραμέτρων όπως: (i) περιορισμοί στον βαθμό στον οποίο το μέλλον θα μοιάζει με το παρελθόν, (ii) ατελής ή ελλιπής γνώση της απειλής (π.χ. χαρακτηριστικά των αντιπάλων, συμπεριλαμβανομένων τακτικών, τεχνικών και διαδικασιών), (iii) μη ανακαλυφθέντα τρωτά σημεία σε τεχνολογίες ή προϊόντα, και (iv) μη αναγνωρισμένες εξαρτήσεις, οι οποίες μπορούν να οδηγήσουν σε απρόβλεπτες επιπτώσεις. Η αβεβαιότητα σχετικά με την αξία συγκεκριμένων παραγόντων κινδύνου μπορεί επίσης να οφείλεται στο βήμα στο RMF[4] (Risk Management Framework) ή στη φάση του κύκλου ζωής ανάπτυξης του συστήματος κατά την οποία πραγματοποιείται η αξιολόγηση κινδύνου. Για παράδειγμα, στις πρώιμες φάσεις του κύκλου ζωής ανάπτυξης του συστήματος, η παρουσία και η αποτελεσματικότητα των ελέγχων ασφαλείας μπορεί να είναι άγνωστες, ενώ σε μεταγενέστερες φάσεις του κύκλου ζωής, το κόστος της αξιολόγησης της αποτελεσματικότητας του ελέγχου μπορεί να υπερτερεί των οφελών όσον αφορά τη λήψη αποφάσεων με πληρέστερη επίγνωση. Τέλος, η αβεβαιότητα μπορεί να οφείλεται σε ελλιπή γνώση των κινδύνων που σχετίζονται με άλλα συστήματα πληροφοριών, επιχειρηματικές διαδικασίες, υπηρεσίες, κοινές υποδομές ή/και οργανισμούς. Ο βαθμός αβεβαιότητας στα αποτελέσματα αξιολόγησης κινδύνου, λόγω αυτών των διαφορετικών λόγων, μπορεί να κοινοποιηθεί με τη μορφή των αποτελεσμάτων (π.χ., εκφράζοντας τα αποτελέσματα ποιοτικά, παρέχοντας σειρές τιμών αντί για μεμονωμένες τιμές για εντοπισμένους κινδύνους ή χρησιμοποιώντας οπτικές αναπαραστάσεις ασαφών περιοχών παρά σημείων).

4. Διαδικασία εκτίμησης κινδύνου με βάση το NIST SP 800-30

Διεξαγωγή εκτιμήσεων κινδύνου μέσα στους οργανισμούς

Αυτό το κεφάλαιο περιγράφει τη διαδικασία αξιολόγησης του κινδύνου ασφάλειας πληροφοριών, συμπεριλαμβανομένων: i) μια επισκόπηση υψηλού επιπέδου της διαδικασίας αξιολόγησης κινδύνου, ii) τις δραστηριότητες που είναι απαραίτητες για την προετοιμασία εκτιμήσεων κινδύνου, iii) τις δραστηριότητες που είναι απαραίτητες για τη διεξαγωγή αποτελεσματικών αξιολογήσεων κινδύνου, iv) τις δραστηριότητες που είναι απαραίτητες για την κοινοποίηση των αποτελεσμάτων της αξιολόγησης κινδύνου και την ανταλλαγή πληροφοριών σχετικά με τον κίνδυνο, και v) τις δραστηριότητες που είναι απαραίτητες για τη διατήρηση των αποτελεσμάτων των αξιολογήσεων κινδύνου σε συνεχή βάση. Η διαδικασία αξιολόγησης κινδύνου αποτελείται από τέσσερα βήματα: i) *προετοιμασία* για την αξιολόγηση, ii) *διεξαγωγή* της αξιολόγησης, iii) *κοινοποίηση* των αποτελεσμάτων της αξιολόγησης, και iv) *διατήρηση* της αξιολόγησης. Κάθε βήμα χωρίζεται σε ένα σύνολο εργασιών. Για κάθε εργασία, η συμπληρωματική καθοδήγηση παρέχει πρόσθετες πληροφορίες για οργανισμούς που διενεργούν αξιολογήσεις κινδύνου. Οι πίνακες κινδύνου και οι υποδειγματικές κλίμακες αξιολόγησης παρατίθενται στα παραρτήματα. Η παρακάτω εικόνα απεικονίζει τα βασικά βήματα στη διαδικασία αξιολόγησης κινδύνου και επισημαίνει τις συγκεκριμένες εργασίες για τη διεξαγωγή της αξιολόγησης.

[4] Το Πλαίσιο Διαχείρισης Κινδύνων περιγράφεται στην Ειδική Έκδοση 800-37 του NIST.



Εικόνα 3: Διαδικασία εκτίμησης κινδύνου.

4.1 Προετοιμασία για την εκτίμηση κινδύνου

Το πρώτο βήμα στη διαδικασία αξιολόγησης κινδύνου είναι η προετοιμασία για την αξιολόγηση. Ο στόχος αυτού του βήματος είναι να δημιουργήσει ένα πλαίσιο για την αξιολόγηση κινδύνου. Αυτό το πλαίσιο καθορίζεται και ενημερώνεται από τα αποτελέσματα από το βήμα πλαισίωσης κινδύνου της διαδικασίας διαχείρισης κινδύνου. Το πλαίσιο κινδύνου προσδιορίζει, για παράδειγμα, οργανωτικές πληροφορίες σχετικά με τις πολιτικές και τις απαιτήσεις για τη διεξαγωγή αξιολογήσεων κινδύνου, τις συγκεκριμένες μεθοδολογίες αξιολόγησης που πρέπει να χρησιμοποιηθούν, τις διαδικασίες επιλογής παραγόντων κινδύνου που πρέπει να ληφθούν υπόψη, το εύρος των αξιολογήσεων, την αυστηρότητα των αναλύσεων, τον βαθμό τυπικότητας και τις απαιτήσεις που διευκολύνουν συνεπείς και επαναλαμβανόμενους προσδιορισμούς κινδύνου σε ολόκληρο τον οργανισμό. Οι οργανισμοί χρησιμοποιούν τη στρατηγική διαχείρισης κινδύνου στο βαθμό που είναι εφικτό για να λάβουν πληροφορίες για να προετοιμαστούν για την αξιολόγηση κινδύνου. Η προετοιμασία για μια αξιολόγηση κινδύνου περιλαμβάνει τις ακόλουθες εργασίες:

- Προσδιορισμός του σκοπού της αξιολόγησης,
- προσδιορισμός του εύρους της αξιολόγησης,
- προσδιορισμός των παραδοχών και των περιορισμών που σχετίζονται με την αξιολόγηση,
- προσδιορισμός των πηγών πληροφοριών που θα χρησιμοποιηθούν ως εισροές στην αξιολόγηση, και
- προσδιορισμός του μοντέλου κινδύνου και αναλυτικές προσεγγίσεις που θα χρησιμοποιηθούν κατά την αξιολόγηση.

Βήμα 1: Προετοιμασία για την αξιολόγηση

Προσδιορισμός του σκοπού

Δράση 1-1: Προσδιορισμός του σκοπού της αξιολόγησης κινδύνου όσον αφορά τις πληροφορίες που προορίζεται να παράγει η αξιολόγηση και τις αποφάσεις που προορίζεται να υποστηρίξει η αξιολόγηση.

Συμπληρωματική καθοδήγηση: Ο σκοπός της αξιολόγησης κινδύνου αναφέρεται ρητά με επαρκή λεπτομέρεια ώστε να διασφαλίζεται ότι η αξιολόγηση παράγει τις κατάλληλες πληροφορίες και υποστηρίζει τις επιδιωκόμενες αποφάσεις. Οι οργανισμοί μπορούν να παρέχουν καθοδήγηση σχετικά με τον τρόπο συλλογής και παρουσίασης των πληροφοριών που παράγονται κατά την αξιολόγηση κινδύνου (π.χ. χρησιμοποιώντας ένα καθορισμένο οργανωτικό πρότυπο). Το Παράρτημα Κ παρέχει ένα υποδειγματικό πρότυπο για μια έκθεση αξιολόγησης κινδύνου ή το προτιμώμενο όχημα για επικοινωνία κινδύνου. Στο επίπεδο τρία της ιεραρχίας, οι αξιολογήσεις κινδύνου υποστηρίζουν: i) αποφάσεις που σχετίζονται με την εξουσιοδότηση σε όλο τον κύκλο ζωής του συστήματος, ii) την αμοιβαιότητα, ιδίως για την επαναχρησιμοποίηση των πληροφοριών αξιολόγησης, iii) δραστηριότητες διαχείρισης κινδύνου στο επίπεδο δύο, και iv) δραστηριότητες διαχείρισης προγραμματισμού σε όλο τον κύκλο ζωής του συστήματος. Στο επίπεδο δύο, οι αξιολογήσεις κινδύνου επιτρέπουν στους οργανισμούς να: i) κατανοήσουν τις εξαρτήσεις και τους τρόπους με τους οποίους οι κίνδυνοι γίνονται δεκτοί, απορρίπτονται, μοιράζονται, μεταφέρονται ή μετριάζονται μεταξύ των πληροφοριακών συστημάτων που υποστηρίζουν τις οργανωτικές επιχειρηματικές διαδικασίες, ii) υποστηρίξουν αρχιτεκτονικές και επιχειρησιακές αποφάσεις για απαντήσεις οργανωτικών κινδύνων (π.χ. μείωση των εξαρτήσεων, περιορίζοντας τη συνδεσιμότητα, ενίσχυση ή εστίαση στην παρακολούθηση και ενίσχυση της ανθεκτικότητας του συστήματος), iii) να προσδιοριστούν οι τάσεις, έτσι ώστε να μπορούν να καθοριστούν οι προληπτικές στρατηγικές αντιμετώπισης κινδύνου και τα μαθήματα δράσης για επιχειρηματικές διαδικασίες, και iv) υποστηρίζουν την αμοιβαιότητα, ιδίως για να επιτρέψει την ανταλλαγή πληροφοριών. Στο επίπεδο ένα, οι αξιολογήσεις κινδύνου: i) υποστηρίζουν το στέλεχος κινδύνου, και ii) χρησιμεύουν ως βασική εισροή στη στρατηγική διαχείρισης κινδύνου. Εκτός από αυτούς τους κοινούς σκοπούς, οι αξιολογήσεις κινδύνου ενδέχεται να έχουν πολύ συγκεκριμένο σκοπό, να απαντήσουν σε μια συγκεκριμένη ερώτηση (π.χ. ποιες είναι οι επιπτώσεις κινδύνου μιας πρόσφατα ανακαλυφθέντας ευπάθειας ή κατηγορίας ευπαθειών επιτρέποντας μια νέα συνδεσιμότητα, την εξωτερική ανάθεση μιας συγκεκριμένης λειτουργίας ή την υιοθέτηση μιας νέας τεχνολογίας;). Τα αποτελέσματα αξιολόγησης κινδύνου από όλες τις βαθμίδες μπορούν να χρησιμοποιηθούν από οργανισμούς για την ενημέρωση της διαδικασίας απόκτησης πληροφοριών, βοηθώντας να διασφαλιστούν οι απαιτήσεις ασφάλειας πληροφοριών.

Ο σκοπός της αξιολόγησης κινδύνου επηρεάζεται από το εάν η αξιολόγηση είναι: (i) αρχική εκτίμηση, ή (ii) μια επαναξιολόγηση που αρχικοποιείται από τα βήματα παρακολούθησης του κινδύνου στη διαδικασία διαχείρισης κινδύνου. Για τις αρχικές εκτιμήσεις, ο σκοπός μπορεί να περιλαμβάνει, για παράδειγμα: (i) τη δημιουργία βασικής εκτίμησης του κινδύνου, ή ii) τον εντοπισμό απειλών και τρωτών σημείων, επιπτώσεων σε οργανωτικές λειτουργίες και περιουσιακά στοιχεία, άτομα, άλλους οργανισμούς και το Έθνος και άλλους παράγοντες κινδύνου που πρέπει να παρακολουθούνται με την πάροδο του χρόνου ως μέρος της παρακολούθησης κινδύνου. Για μια επαναξιολόγηση που ξεκινά από το βήμα αντιμετώπισης κινδύνου, ο σκοπός μπορεί να περιλαμβάνει, για παράδειγμα, την παροχή μιας συγκριτικής ανάλυσης εναλλακτικών αντιμετωπίσεων κινδύνου ή την απάντηση σε μια συγκεκριμένη ερώτηση. Εναλλακτικά, για μια επαναξιολόγηση που ξεκινά από το βήμα παρακολούθησης κινδύνων, ο σκοπός μπορεί να περιλαμβάνει, για παράδειγμα, την ενημέρωση της εκτίμησης κινδύνου με βάση: i) συνεχείς προσδιορισμούς της αποτελεσματικότητας των ελέγχων ασφαλείας σε οργανωτικά συστήματα πληροφοριών ή περιβάλλοντα λειτουργίας, ii) αλλαγές σε συστήματα πληροφοριών ή περιβάλλοντα λειτουργίας (π.χ. αλλαγές σε υλικό, υλικολογισμικό, λογισμικό, αλλαγές σε ειδικά για το σύστημα, υβριδικά ή κοινά στοιχεία ελέγχου, αλλαγές σε διαδικασίες επιχειρήσεων, κοινές υποδομές και υπηρεσίες υποστήριξης, απειλές, ευπάθειες , ή εγκαταστάσεις), και iii) αποτελέσματα από δραστηριότητες επαλήθευσης συμμόρφωσης. Οι επαναξιολογήσεις μπορούν επίσης να ξεκινήσουν από οργανισμούς λόγω συμβάντων που έχουν συμβεί (π.χ. επιθέσεις στον κυβερνοχώρο που διακυβεύουν οργανωτικές πληροφορίες ή συστήματα πληροφοριών).

Προσδιορισμός του εύρους

Δράση 1-2: Προσδιορισμός του εύρους της αξιολόγησης κινδύνου όσον αφορά την οργανωτική εφαρμογή, το υποστηριζόμενο χρονικό πλαίσιο και αρχιτεκτονικά/τεχνολογικά ζητήματα.

Συμπληρωματική καθοδήγηση: Το εύρος της αξιολόγησης κινδύνου καθορίζει τι θα ληφθεί υπόψη στην αξιολόγηση. Το εύρος της αξιολόγησης κινδύνου επηρεάζει το εύρος των διαθέσιμων πληροφοριών για τη λήψη αποφάσεων βάσει κινδύνου και καθορίζεται από τον υπεύθυνο του οργανισμού που ζητά την αξιολόγηση και τη στρατηγική διαχείρισης κινδύνου. Ο καθορισμός του πεδίου εφαρμογής της αξιολόγησης κινδύνου βοηθά τους οργανισμούς να προσδιορίσουν: i) ποια επίπεδα εξετάζονται στην αξιολόγηση, ii) ποια μέρη των οργανισμών επηρεάζονται από την αξιολόγηση και πώς επηρεάζονται, (iii) ποιες αποφάσεις υποστηρίζουν τα αποτελέσματα της αξιολόγησης, iv) πόσο καιρό είναι σχετικά τα αποτελέσματα της αξιολόγησης, και v) τι

επηρεάζει την ανάγκη επικαιροποίησης της αξιολόγησης. Ο καθορισμός του πεδίου εφαρμογής της αξιολόγησης κινδύνου βοηθά στον προσδιορισμό της μορφής και του περιεχομένου της έκθεσης αξιολόγησης κινδύνου, καθώς και των πληροφοριών που πρέπει να κοινοποιηθούν ως αποτέλεσμα της διεξαγωγής της αξιολόγησης. Στο επίπεδο τρία, το εύρος μιας αξιολόγησης κινδύνου μπορεί να εξαρτάται από το όριο εξουσιοδότησης για το σύστημα πληροφοριών. Το Παράρτημα Κ παρέχει ένα παράδειγμα του τύπου πληροφοριών που μπορεί να περιλαμβάνονται σε μια έκθεση αξιολόγησης κινδύνου ή το προτιμώμενο όχημα για την επικοινωνία κινδύνου.

Οργανωτική εφαρμογή

Η οργανωτική εφαρμογή περιγράφει ποια τμήματα του οργανισμού ή των υπό-οργανισμών επηρεάζονται από την αξιολόγηση κινδύνου και τις αποφάσεις που βασίζονται στον κίνδυνο που προκύπτουν από την αξιολόγηση (συμπεριλαμβανομένων των τμημάτων του οργανισμού ή των υπό-οργανισμών που είναι υπεύθυνοι για την υλοποίηση των δραστηριοτήτων και των καθηκόντων που σχετίζονται με τις αποφάσεις). Για παράδειγμα, η αξιολόγηση κινδύνου μπορεί να δώσει πληροφορίες σχετικά με τα συστήματα πληροφοριών που υποστηρίζουν μια συγκεκριμένη οργανωτική επιχειρηματική λειτουργία ή διαδικασία. Αυτό μπορεί να περιλαμβάνει αποφάσεις σχετικά με την επιλογή, την προσαρμογή ή τη συμπλήρωση ελέγχων ασφαλείας για συγκεκριμένα συστήματα πληροφοριών ή την επιλογή κοινών ελέγχων. Εναλλακτικά, η αξιολόγηση κινδύνου μπορεί να λαμβάνει αποφάσεις σχετικά με ένα σύνολο στενά συνδεδεμένων επιχειρηματικών λειτουργιών ή επιχειρηματικών διαδικασιών. Το εύρος της αξιολόγησης κινδύνου μπορεί να περιλαμβάνει όχι μόνο τις επιχειρηματικές λειτουργίες, τις διαδικασίες επιχειρήσεων, την κοινή υποδομή ή τις κοινές υπηρεσίες από τις οποίες εξαρτάται επί του παρόντος ο οργανισμός, αλλά και εκείνες που μπορεί να χρησιμοποιήσει ο οργανισμός υπό συγκεκριμένες συνθήκες λειτουργίας.

Χρονικό πλαίσιο αποτελεσματικότητας

Οι οργανισμοί καθορίζουν πόσο καιρό μπορούν να χρησιμοποιηθούν τα αποτελέσματα συγκεκριμένων αξιολογήσεων κινδύνου για τη νόμιμη ενημέρωση των αποφάσεων που βασίζονται στον κίνδυνο. Το χρονικό πλαίσιο συνήθως σχετίζεται με το σκοπό της αξιολόγησης. Για παράδειγμα, μια αξιολόγηση κινδύνου για την ενημέρωση των αποφάσεων που σχετίζονται με την πολιτική του επιπέδου ένα της ιεραρχίας πρέπει να είναι σχετική για εκτεταμένη χρονική περίοδο, καθώς η διαδικασία διακυβέρνησης για αλλαγές πολιτικής μπορεί να είναι χρονοβόρα σε πολλούς οργανισμούς. Μια αξιολόγηση κινδύνου που διενεργείται για την ενημέρωση μιας απόφασης επιπέδου τρία σχετικά με τη χρήση αντισταθμιστικού ελέγχου ασφαλείας για ένα σύστημα πληροφοριών μπορεί να είναι σχετική μόνο μέχρι την επόμενη κυκλοφορία του προϊόντος τεχνολογίας πληροφοριών που παρέχει την απαιτούμενη ικανότητα ασφάλειας. Οι οργανισμοί καθορίζουν την ωφέλιμη ζωή των αποτελεσμάτων αξιολόγησης κινδύνου και υπό ποιες συνθήκες τα τρέχοντα αποτελέσματα αξιολόγησης καθίστανται αναποτελεσματικά ή όχι. Η παρακολούθηση κινδύνων μπορεί να χρησιμοποιηθεί για να βοηθήσει στον προσδιορισμό της αποτελεσματικότητας των χρονικών πλαισίων για τις εκτιμήσεις κινδύνου. Εκτός από τα αποτελέσματα της αξιολόγησης κινδύνου, οι οργανισμοί λαμβάνουν επίσης υπόψη την επικαιρότητα (δηλαδή, την καθυστέρηση ή την ηλικία) όλων των τύπων πληροφοριών/δεδομένων που χρησιμοποιούνται για την αξιολόγηση του κινδύνου. Αυτό προκαλεί ιδιαίτερη ανησυχία για την επαναχρησιμοποίηση πληροφοριών και την αξιολόγηση της εγκυρότητας των αποτελεσμάτων της αξιολόγησης.

Αρχιτεκτονικές/τεχνολογικές εκτιμήσεις

Οι οργανισμοί χρησιμοποιούν αρχιτεκτονικές και τεχνολογικές εκτιμήσεις για να διευκρινίσουν το πεδίο εφαρμογής της αξιολόγησης κινδύνου. Για παράδειγμα, στο επίπεδο τρία, το πεδίο εφαρμογής της εκτίμησης κινδύνου μπορεί να είναι ένα οργανωτικό σύστημα πληροφόρησης στο περιβάλλον λειτουργίας του. Αυτό συνεπάγεται την τοποθέτηση του συστήματος πληροφοριών στο αρχιτεκτονικό του πλαίσιο, έτσι ώστε να λαμβάνονται υπόψη τα τρωτά σημεία σε κληρονομικούς ελέγχους. Εναλλακτικά, το πεδίο εφαρμογής της αξιολόγησης μπορεί να περιοριστεί αποκλειστικά στο σύστημα πληροφοριών, χωρίς να λαμβάνονται υπόψη οι κληρονομικοί έλεγχοι των τρωτών σημείων. Στο επίπεδο δύο, το πεδίο εφαρμογής της αξιολόγησης κινδύνου μπορεί να οριστεί με όρους αρχιτεκτονικής αποστολής/επιχειρηματικού τμήματος (π.χ., συμπεριλαμβανομένων όλων των συστημάτων, υπηρεσιών και υποδομών που υποστηρίζουν μια συγκεκριμένη αποστολή/λειτουργία). Για μια στοχευμένη εκτίμηση κινδύνου σε οποιαδήποτε βαθμίδα, η συγκεκριμένη ερώτηση που πρέπει να απαντηθεί μπορεί να περιορίσει το πεδίο εφαρμογής σε μια συγκεκριμένη τεχνολογία.

Προσδιορισμός των παραδοχών και των περιορισμών

Δράση 1-3: Προσδιορισμός των συγκεκριμένων υποθέσεων και περιορισμών βάσει των οποίων διεξάγεται η εκτίμηση κινδύνου.

Συμπληρωματική καθοδήγηση: Όσον αφορά το βήμα πλαισίωσης κινδύνου στη διαδικασία διαχείρισης κινδύνου, οι οργανισμοί καθιστούν ρητά τις συγκεκριμένες υποθέσεις, τους περιορισμούς, την ανοχή κινδύνου και τις προτεραιότητες/συμβιβασμούς που χρησιμοποιούνται στους οργανισμούς για τη λήψη επενδυτικών και επιχειρησιακών αποφάσεων. Αυτές οι πληροφορίες καθοδηγούν και ενημερώνουν τις αξιολογήσεις οργανωτικών κινδύνων. Όταν μια στρατηγική οργανωτικής διαχείρισης κινδύνου δεν μπορεί να αναφερθεί, οι αξιολογήσεις κινδύνου προσδιορίζουν και καταγράφουν υποθέσεις και περιορισμούς. Οι υποθέσεις και οι περιορισμοί που εντοπίστηκαν από τους οργανισμούς κατά τη διάρκεια του βήματος πλαισίωσης κινδύνου και συμπεριλήφθηκαν ως μέρος της στρατηγικής διαχείρισης κινδύνου δεν πρέπει να επαναληφθούν σε κάθε ατομική εκτίμηση κινδύνου. Κάνοντας ρητά υποθέσεις και περιορισμούς, υπάρχει μεγαλύτερη σαφήνεια στο μοντέλο κινδύνου που επιλέχθηκε για την αξιολόγηση κινδύνου, την αυξημένη αναπαραγωγιμότητα/επαναληψιμότητα των αποτελεσμάτων αξιολόγησης και την αυξημένη ευκαιρία για αμοιβαιότητα μεταξύ των οργανισμών. Οι οργανισμοί εντοπίζουν υποθέσεις σε βασικούς τομείς που σχετίζονται με την αξιολόγηση κινδύνου, όπως, για παράδειγμα: i) πηγές απειλής, ii) γεγονότα απειλής, iii) τρωτά σημεία και προδιαγραφές, iv) πιθανές επιπτώσεις, v) προσεγγίσεις αξιολόγησης και ανάλυσης, και vi) ποιες αποστολές/επιχειρηματικές λειτουργίες είναι πρωταρχικές. Οι οργανισμοί προσδιορίζουν επίσης περιορισμούς σε βασικούς τομείς που σχετίζονται με την αξιολόγηση κινδύνου, όπως, για παράδειγμα: i) διαθέσιμοι πόροι για την αξιολόγηση, ii) τις δεξιότητες και την τεχνογνωσία που απαιτούνται για την αξιολόγηση, και iii) επιχειρησιακές εκτιμήσεις σχετικά με τις δραστηριότητες επιχειρηματικών διαδικασιών. Για παράδειγμα, οι οργανωτικές υποθέσεις σχετικά με τον τρόπο αξιολόγησης των απειλών και των επιπτώσεων μπορεί να κυμαίνονται από τη χρήση των προβολών της χειρότερης περίπτωσης στη χρήση προβολών βέλτιστης περίπτωσης ή οτιδήποτε μεταξύ αυτών των τελικών σημείων. Τέλος, οι οργανισμοί λαμβάνουν υπόψη τους την αβεβαιότητα όσον αφορά τις υποθέσεις που έγιναν ή άλλες πληροφορίες που χρησιμοποιούνται στην εκτίμηση κινδύνου. Η αβεβαιότητα στις υποθέσεις μπορεί να επηρεάσει την ανοχή του οργανωτικού κινδύνου. Για παράδειγμα, οι υποθέσεις που βασίζονται στην έλλειψη συγκεκριμένων ή αξιόπιστων πληροφοριών ενδέχεται να μειώσουν την ανοχή κινδύνου ενός οργανισμού λόγω της αβεβαιότητας που επηρεάζει τις υποθέσεις. Τα ακόλουθα τμήματα παρέχουν ορισμένα αντιπροσωπευτικά παραδείγματα περιοχών όπου μπορούν να εντοπιστούν υποθέσεις/περιορισμοί για τις αξιολογήσεις κινδύνου.

Πηγές απειλών

Οι οργανισμοί καθορίζουν τον τύπο των απειλών που πρέπει να ληφθούν υπόψη κατά τη διάρκεια των αξιολογήσεων κινδύνου και του επιπέδου λεπτομέρειας που απαιτείται για την περιγραφή τέτοιων γεγονότων. Οι περιγραφές των γεγονότων απειλών μπορούν να εκφραστούν με εξαιρετικά γενικούς όρους (π.χ. phishing, κατανεμημένη άρνηση εξυπηρέτησης), με πιο περιγραφικούς όρους χρησιμοποιώντας τακτικές, τεχνικές και διαδικασίες ή με ιδιαίτερα ειδικούς όρους (π.χ. τα ονόματα συγκεκριμένων συστημάτων πληροφοριών , τεχνολογίες, οργανώσεις, ρόλοι ή τοποθεσίες). Επιπλέον, οι οργανισμοί λαμβάνουν υπόψη τους: i) ποιο αντιπροσωπευτικό σύνολο απειλών γεγονότων μπορεί να χρησιμεύσει ως σημείο εκκίνησης για την ταυτοποίηση των ειδικών απειλών γεγονότων στην εκτίμηση κινδύνου, και ii) ποιο βαθμό επιβεβαίωσης απαιτείται για τα γεγονότα απειλών που πρέπει να θεωρηθούν σχετικά για τους σκοπούς της αξιολόγησης κινδύνου. Για παράδειγμα, οι οργανισμοί μπορούν να εξετάσουν μόνο εκείνα τα απειλητικά γεγονότα που έχουν παρατηρηθεί (είτε εσωτερικά είτε από οργανισμούς που είναι εταίροι) ή όλα τα πιθανά γεγονότα απειλών. Ο Πίνακας Ε-2 και ο Πίνακας Ε-3 παρέχουν αντιπροσωπευτικά παραδείγματα στοχευμένων και μη απειλών σε επίπεδο λεπτομέρειας που μπορούν να χρησιμοποιηθούν για αξιολογήσεις κινδύνου σε όλες τις βαθμίδες. Μεγαλύτερη λεπτομέρεια μπορούν να βρεθούν σε πολλαπλές πηγές (π.χ. απαρίθμηση και ταξινόμηση κοινής επίθεσης [CAPEC]).

Ευπάθειες και προδιαθεσικές καταστάσεις

Οι οργανισμοί καθορίζουν τους τύπους τρωτών σημείων που πρέπει να λαμβάνονται υπόψη κατά τη διάρκεια των αξιολογήσεων κινδύνου και του επιπέδου λεπτομέρειας που παρέχεται στις περιγραφές ευπάθειας. Οι οργανισμοί καθιστούν ρητή τη διαδικασία που χρησιμοποιείται για τον εντοπισμό των τρωτών σημείων και τυχόν υποθέσεων που σχετίζονται με τη διαδικασία αναγνώρισης ευπάθειας. Εάν εντοπιστούν αυτές οι

πληροφορίες κατά τη διάρκεια του βήματος πλαισίωσης κινδύνου και περιλαμβάνονται ως μέρος της στρατηγικής διαχείρισης οργανωτικού κινδύνου, οι πληροφορίες δεν πρέπει να επαναληφθούν σε κάθε ατομική αξιολόγηση κινδύνου. Τα τρωτά σημεία μπορούν να συσχετιστούν με οργανωτικά συστήματα πληροφοριών (π.χ. υλικό, λογισμικό, υλικολογισμικό, εσωτερικούς ελέγχους και διαδικασίες ασφαλείας) ή τα περιβάλλοντα στα οποία λειτουργούν τα συστήματα αυτά (π.χ. οργανωτική διακυβέρνηση, εξωτερικές σχέσεις, επιχειρηματικές διαδικασίες, αρχιτεκτονικές επιχειρήσεων, πληροφορίες, πληροφορίες αρχιτεκτονικής ασφαλείας). Οι οργανισμοί καθορίζουν επίσης τους τύπους προδιαθέσεων που πρόκειται να ληφθούν υπόψη κατά τη διάρκεια αξιολογήσεων κινδύνου, όπως, για παράδειγμα, αρχιτεκτονικές και τεχνολογίες που χρησιμοποιούνται, περιβάλλοντα λειτουργίας και προσωπικό. Ο Πίνακας F-4 παρέχει αντιπροσωπευτικά παραδείγματα τέτοιων συνθηκών.

Πιθανότητα

Οι οργανισμοί καθιστούν ρητή τη διαδικασία που χρησιμοποιείται για τη διεξαγωγή προσδιορισμών πιθανότητας και τυχόν υποθέσεις που σχετίζονται με τη διαδικασία προσδιορισμού πιθανότητας. Εάν εντοπιστούν αυτές οι πληροφορίες κατά τη διάρκεια του βήματος πλαισίωσης κινδύνου και περιλαμβάνονται ως μέρος της στρατηγικής διαχείρισης οργανωτικού κινδύνου, οι πληροφορίες δεν χρειάζεται να επαναλαμβάνονται σε κάθε μεμονωμένη αξιολόγηση κινδύνου. Οι οργανωτικές υποθέσεις σχετικά με τον τρόπο προσδιορισμού της πιθανότητας πληροφορούν την Δράση 2-4.

Επιπτώσεις

Οι οργανισμοί καθορίζουν πιθανές δυσμενείς επιπτώσεις όσον αφορά τις οργανωτικές επιχειρήσεις (δηλ. αποστολές, λειτουργίες, εικόνα και φήμη), οργανωτικά περιουσιακά στοιχεία, άτομα, άλλους οργανισμούς και το Έθνος. Οι οργανισμοί καθιστούν ρητή τη διαδικασία που χρησιμοποιείται για τη διεξαγωγή προσδιορισμών επίπτωσης και τυχόν παραδοχές που σχετίζονται με τη διαδικασία προσδιορισμού των επιπτώσεων. Εάν εντοπιστούν αυτές οι πληροφορίες κατά τη διάρκεια του βήματος πλαισίωσης κινδύνου και περιλαμβάνονται ως μέρος της στρατηγικής διαχείρισης οργανωτικού κινδύνου, οι πληροφορίες δεν πρέπει να επαναληφθούν σε κάθε ατομική αξιολόγηση κινδύνου. Οι οργανισμοί αντιμετωπίζουν επιπτώσεις σε ένα επίπεδο λεπτομέρειας που περιλαμβάνει, για παράδειγμα, συγκεκριμένες διαδικασίες επιχειρηματικών διαδικασιών ή πόρων πληροφόρησης (π.χ. πληροφορίες, προσωπικό, εξοπλισμό, κεφάλαια και τεχνολογία πληροφοριών). Οι οργανισμοί ενδέχεται να περιλαμβάνουν πληροφορίες από αναλύσεις επιπτώσεων επιχειρήσεων όσον αφορά την παροχή πληροφοριών επιπτώσεων για αξιολογήσεις κινδύνου. Ο Πίνακας H-2 παρέχει αντιπροσωπευτικά παραδείγματα τύπων επιπτώσεων (π.χ. ζημία) που μπορούν να εξεταστούν από οργανισμούς.

Ανοχή και αβεβαιότητα κινδύνου

Οι οργανισμοί καθορίζουν τα επίπεδα και τους τύπους κινδύνου που είναι αποδεκτά. Η ανοχή κινδύνου καθορίζεται ως μέρος της στρατηγικής διαχείρισης κινδύνου για να εξασφαλιστεί η συνέπεια σε ολόκληρο τον οργανισμό. Οι οργανισμοί παρέχουν επίσης καθοδήγηση σχετικά με τον προσδιορισμό των λόγων για την αβεβαιότητα όταν αξιολογούνται οι παράγοντες κινδύνου, καθώς η αβεβαιότητα σε έναν ή περισσότερους παράγοντες θα διαδοθεί στην αξιολόγηση του επιπέδου κινδύνου και τον τρόπο αντιστάθμισης των ατελών ή εξαρτώμενων από την υπόθεση εκτιμήσεων. Η εξέταση της αβεβαιότητας είναι ιδιαίτερα σημαντική όταν οι οργανισμοί εξετάζουν τις προχωρημένες επίμονες απειλές (Advanced Persistent Threats), καθώς οι αξιολογήσεις της πιθανότητας εμφάνισης απειλών μπορεί να έχουν μεγάλη αβεβαιότητα. Για να αντισταθμιστούν, οι οργανισμοί μπορούν να λάβουν μια ποικιλία προσεγγίσεων για τον προσδιορισμό της πιθανότητας, το εύρος της οποίας ξεκινάει υποθέτοντας την πιθανότητα χειρότερης περίπτωσης (ορισμένα συμβάντα θα συμβούν κάποια στιγμή στο προβλέψιμο μέλλον), και καταλήγει υποθέτοντας ότι εάν δεν έχει παρατηρηθεί ένα συμβάν, είναι απίθανο να συμβεί. Οι οργανισμοί καθορίζουν επίσης ποια επίπεδα κινδύνου (συνδυασμός πιθανότητας και αντίκτυπου) δείχνουν ότι δεν απαιτείται περαιτέρω ανάλυση οποιουδήποτε παράγοντα κινδύνου.

Αναλυτική προσέγγιση

Οι αξιολογήσεις κινδύνου περιλαμβάνουν τόσο τις προσεγγίσεις αξιολόγησης (δηλ. ποσοτικές, ποιοτικές, ημι-ποσοτικές) όσο και τις προσεγγίσεις ανάλυσης (δηλ. προσανατολισμένες σε απειλές, προσανατολισμένα στο περιουσιακό στοιχείο, προσανατολισμένες στην ευπάθεια). Μαζί, οι προσεγγίσεις αξιολόγησης και

ανάλυσης αποτελούν την *αναλυτική προσέγγιση* για την εκτίμηση κινδύνου. Οι οργανισμοί καθορίζουν το επίπεδο λεπτομέρειας και σε ποια μορφή αναλύονται οι απειλές, συμπεριλαμβανομένου του επιπέδου της λεπτομερούς για την περιγραφή των γεγονότων απειλών ή των σεναρίων απειλής. Οι διαφορετικές προσεγγίσεις ανάλυσης μπορούν να οδηγήσουν σε διαφορετικά επίπεδα λεπτομέρειας στον χαρακτηρισμό των ανεπιθύμητων ενεργειών για τα οποία καθορίζονται οι πιθανότητες. Για παράδειγμα, ένα ανεπιθύμητο συμβάν θα μπορούσε να χαρακτηριστεί με διάφορους τρόπους (με αυξανόμενα επίπεδα λεπτομέρειας): i) ένα γεγονός απειλής (για το οποίο η πιθανότητα καθορίζεται λαμβάνοντας τις μέγιστες συνολικές πηγές απειλής), ii) συνδυασμός ενός γεγονότος απειλής και μιας πηγή απειλής, ή iii) ένα λεπτομερές σενάριο απειλής. Γενικά, οι οργανισμοί αναμένεται να απαιτήσουν περισσότερες λεπτομέρειες για εξαιρετικά κρίσιμες επιχειρηματικές λειτουργίες, κοινές υποδομές ή κοινές υπηρεσίες στις οποίες εξαρτώνται πολλαπλές αποστολές ή επιχειρηματικές λειτουργίες (ως κοινά σημεία αποτυχίας) και συστήματα πληροφοριών με υψηλή κρισιμότητα ή ευαισθησία[5]. Οι ιδιοκτήτες επιχειρήσεων μπορούν να ενισχύσουν αυτήν την καθοδήγηση για τα σημαντικά σημεία κινδύνου (συστήματα πληροφοριών, υπηρεσίες ή στοιχεία κρίσιμης υποδομής ιδιαίτερων ανησυχιών) σε τμήματα επιχειρήσεων.

Προσδιορισμός των πηγών πληροφοριών

Δράση 1-4: Προσδιορισμός των πηγών, απειλής, ευπάθειας και επιπτώσεων που θα χρησιμοποιηθούν στην εκτίμηση κινδύνου.

Συμπληρωματική καθοδήγηση: Οι περιγραφικές πληροφορίες επιτρέπουν στους οργανισμούς να είναι σε θέση να καθορίσουν τη συνάφεια των πληροφοριών απειλής και ευπάθειας. Στη βαθμίδα 1, οι περιγραφικές πληροφορίες μπορούν να περιλαμβάνουν, για παράδειγμα, τον τύπο της διαχείρισης κινδύνου και των δομών διακυβέρνησης της ασφάλειας των πληροφοριών που ισχύουν εντός των οργανισμών και τον τρόπο με τον οποίο ο οργανισμός προσδιορίζει και δίνει προτεραιότητα στις κρίσιμες επιχειρηματικές λειτουργίες. Στη βαθμίδα 2, οι περιγραφικές πληροφορίες μπορούν να περιλαμβάνουν, για παράδειγμα, πληροφορίες σχετικά με: i) οργανωτικές αποστολές/επιχειρηματικές διαδικασίες, λειτουργικές διαδικασίες διαχείρισης και ροές πληροφοριών, ii) αρχιτεκτονική επιχειρήσεων, αρχιτεκτονική ασφάλειας πληροφοριών και αρχιτεκτονικές τεχνικών/διαδικασιών ροής των συστημάτων, κοινές υποδομές και κοινόχρηστες υπηρεσίες που εμπίπτουν στο πεδίο εφαρμογής της αξιολόγησης κινδύνου και iii) τα εξωτερικά περιβάλλοντα στα οποία λειτουργούν οι οργανισμοί, συμπεριλαμβανομένων, για παράδειγμα, των σχέσεων και των εξαρτήσεων με εξωτερικούς παρόχους. Τέτοιες πληροφορίες βρίσκονται συνήθως στην αρχιτεκτονική τεκμηρίωση (τεκμηρίωση επιχειρησιακών απόψεων υψηλού επιπέδου), σχέδια επιχειρηματικής συνέχειας και εκθέσεις αξιολόγησης κινδύνου για οργανωτικά συστήματα πληροφοριών, κοινές υποδομές και κοινές υπηρεσίες που εμπίπτουν στο πεδίο εφαρμογής της αξιολόγησης κινδύνου. Στη βαθμίδα 3, οι περιγραφικές πληροφορίες μπορούν να περιλαμβάνουν, για παράδειγμα, πληροφορίες σχετικά με: i) τον σχεδιασμό και τις τεχνολογίες που χρησιμοποιούνται στα οργανωτικά συστήματα πληροφοριών, ii) το περιβάλλον στο οποίο λειτουργούν τα συστήματα, iii) συνδεσιμότητα και εξάρτηση από άλλα συστήματα πληροφοριών, και iv) εξαρτήσεις από κοινές υποδομές ή κοινές υπηρεσίες. Τέτοιες πληροφορίες βρίσκονται στην τεκμηρίωση του συστήματος, στα σχέδια έκτακτης ανάγκης και στις εκθέσεις αξιολόγησης κινδύνου για άλλα συστήματα πληροφοριών, υποδομές και υπηρεσίες.

Πηγές πληροφοριών που περιγράφονται στους πίνακες D-1, E-1, F-1, H-1 και I-1 μπορούν να είναι είτε εσωτερικές είτε εξωτερικές σε οργανισμούς. Οι εσωτερικές πηγές πληροφοριών που μπορούν να δώσουν πληροφορίες τόσο για τις απειλές όσο και για τα τρωτά σημεία μπορούν να περιλαμβάνουν, για παράδειγμα, εκθέσεις αξιολόγησης κινδύνου, αναφορές περιστατικών, αρχεία καταγραφής ασφαλείας και αποτελέσματα παρακολούθησης. Να σημειωθεί ότι εσωτερικά, οι πληροφορίες από τις εκθέσεις αξιολόγησης κινδύνου σε μία βαθμίδα μπορούν να χρησιμεύσουν ως εισροές σε αξιολογήσεις κινδύνου σε άλλες βαθμίδες. Οι ιδιοκτήτες επιχειρήσεων ενθαρρύνονται να εντοπίζουν όχι μόνο τις συνηθισμένες υπηρεσίες υποδομής ή/και υποστήριξης, αλλά και εκείνες που μπορούν να χρησιμοποιήσουν υπό συγκεκριμένες επιχειρησιακές συνθήκες. Οι εξωτερικές πηγές πληροφοριών απειλής μπορούν να περιλαμβάνουν οργανισμούς διασταυρούμενης κοινότητας (π.χ. ομάδα ετοιμότητας έκτακτης ανάγκης υπολογιστών [US-CERT], τομεακούς εταίρους (π.χ. αμυντική βιομηχανική βάση [DIB] χρησιμοποιώντας το περιβάλλον κοινής χρήσης της βιομηχανικής βάσης DoD-Defense [DCISE] , Κέντρα ανταλλαγής πληροφοριών και ανάλυσης [ISACs] για τους τομείς κρίσιμης υποδομής), έρευνα και μη κυβερνητικές οργανώσεις (π.χ. Πανεπιστήμιο Carnegie Mellon, Ινστιτούτο Μηχανικών Λογισμικού) και παρόχους υπηρεσιών ασφαλείας). Οργανισμοί που χρησιμοποιούν εξωτερικές πηγές, λαμβάνουν υπόψη την

[5] Το NIST Special Publication 800-60 συζητά τις έννοιες της κρισιμότητας και της ευαισθησίας των πληροφοριών σε σχέση με την κατηγοριοποίηση της ασφάλειας.

επικαιρότητα, την εξειδίκευση και τη συνάφεια των πληροφοριών απειλής. Παρόμοια με τις πηγές πληροφοριών απειλής, οι πηγές πληροφοριών ευπάθειας μπορούν επίσης να είναι είτε εσωτερικές είτε εξωτερικές σε οργανισμούς (βλ. Πίνακα F-1). Οι εσωτερικές πηγές μπορούν να περιλαμβάνουν, για παράδειγμα, εκθέσεις αξιολόγησης ευπάθειας. Οι εξωτερικές πηγές πληροφοριών ευπάθειας είναι παρόμοιες με τις πηγές που προσδιορίστηκαν παραπάνω για πληροφορίες απειλής. Όπως περιγράφεται στον Πίνακα F-1, οι πληροφορίες σχετικά με τις συνθήκες προδιάθεσης μπορούν να βρεθούν σε διάφορες πηγές, όπως, για παράδειγμα, περιγραφές συστημάτων πληροφοριών, περιβάλλοντος λειτουργίας, κοινών υπηρεσιών, κοινών υποδομών και αρχιτεκτονικής επιχειρήσεων. Όπως περιγράφεται στον Πίνακα H-1, οι πηγές πληροφοριών επιπτώσεων μπορούν να περιλαμβάνουν, για παράδειγμα, αναλύσεις επιπτώσεων αποστολής/επιχειρηματικών επιπτώσεων, αποθέματα στοιχείων συστήματος πληροφοριών και κατηγοριοποιήσεις ασφαλείας. Η κατηγοριοποίηση της ασφάλειας αποτελεί τον προσδιορισμό των πιθανών επιπτώσεων που προκύπτουν ορισμένα συμβάντα που θέτουν σε κίνδυνο τα συστήματα πληροφοριών και πληροφοριών που απαιτούνται από τον οργανισμό για να επιτύχουν τις αποστολές του, να προστατεύσουν τα περιουσιακά του στοιχεία, να εκπληρώσουν τις νομικές ευθύνες της, να διατηρήσουν τις καθημερινές του λειτουργίες και τα άτομα. Οι κατηγορίες ασφαλείας πρέπει να χρησιμοποιούνται σε συνδυασμό με πληροφορίες ευπάθειας και απειλής για την αξιολόγηση του κινδύνου για οργανωτικές επιχειρήσεις και περιουσιακά στοιχεία, άτομα, άλλους οργανισμούς και το Έθνος. Οι κατηγορίες ασφαλείας αποτελούν μια αρχική περίληψη των επιπτώσεων όσον αφορά τις αποτυχίες για την επίτευξη των στόχων ασφαλείας της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας και ενημερώνονται από τους τύπους βλάβης που παρουσιάζονται στον Πίνακα H-2.

Προσδιορισμός του μοντέλου κινδύνου και αναλυτική προσέγγιση

Δράση:1-5: Προσδιορισμός του μοντέλου κινδύνου και αναλυτική περιγραφή που θα χρησιμοποιηθεί στην αξιολόγηση κινδύνου.

Συμπληρωματική καθοδήγηση: Οι οργανισμοί καθορίζουν ένα ή περισσότερα μοντέλα κινδύνου για χρήση κατά τη διεξαγωγή αξιολογήσεων κινδύνου (βλ. Ενότητα 3.3.1) και προσδιορίζουν ποιο μοντέλο πρόκειται να χρησιμοποιηθεί για την αξιολόγηση κινδύνου. Για τη διευκόλυνση της αμοιβαιότητας των αποτελεσμάτων αξιολόγησης, τα μοντέλα κινδύνου περιλαμβάνουν ή μπορούν να μεταφραστούν σε παράγοντες κινδύνου (δηλ. απειλή, ευπάθεια, αντίκτυπο, πιθανότητα και προδιάθεση) που ορίζονται στα παραρτήματα. Οι οργανισμοί προσδιορίζουν επίσης τη συγκεκριμένη αναλυτική προσέγγιση που θα χρησιμοποιηθεί για την αξιολόγηση κινδύνου, συμπεριλαμβανομένης της προσέγγισης αξιολόγησης (δηλ. Ποσοτικής, ποιοτικής, ημι-ποσοτικής) και της προσέγγισης ανάλυσης (δηλ. προσανατολισμένες σε απειλές, προσανατολισμένες σε περιουσιακά στοιχεία, προσανατολισμένες στις ευπάθειες). Για κάθε συντελεστή κινδύνου, τα παραρτήματα περιλαμβάνουν τρεις κλίμακες αξιολόγησης (μία ποιοτική και δύο ημι-ποσοτικές κλίμακες) με αντίστοιχα διαφορετικές αναπαραστάσεις. Οι οργανισμοί συνήθως καθορίζουν (ή επιλέγουν και προσαρμόζουν από τα παραρτήματα) τις κλίμακες αξιολόγησης που πρέπει να χρησιμοποιηθούν στις αξιολογήσεις κινδύνου τους, σχολιάζοντας με παραδείγματα για συγκεκριμένες τιμές και καθορίζοντας σημεία τέλους και αρχής μεταξύ των κάδων για ημιποσοτικές προσεγγίσεις. Επιπλέον, οι ιδιοκτήτες επιχειρήσεων μπορούν να παράσχουν περαιτέρω σχολιασμούς με παραδείγματα αποστολής/επιχειρήσεων. Οι οργανισμοί μπορούν να εντοπίσουν διαφορετικές κλίμακες αξιολόγησης που θα χρησιμοποιηθούν σε διαφορετικές συνθήκες. Για παράδειγμα, για συστήματα χαμηλής επίπτωσης, οι οργανισμοί θα μπορούσαν να χρησιμοποιήσουν ποιοτικές τιμές, ενώ για συστήματα μέτριας και υψηλής επίπτωσης, θα μπορούσαν να χρησιμοποιηθούν οι ημι-ποσοτικές τιμές (0-100). Όπως αναλύεται στην ειδική δημοσίευση 800-39, δράση 1-1, παραδοχές κινδύνου, οι οργανισμοί ποικίλλουν στα σχετικά βάρη που εφαρμόζονται σε παράγοντες κινδύνου. Επομένως, αυτή η κατευθυντήρια γραμμή δεν καθορίζει τους αλγόριθμους για τον συνδυασμό ημι-ποσοτικών τιμών. Τα μοντέλα κινδύνου για συγκεκριμένες οργανώσεις περιλαμβάνουν αλγόριθμους (π.χ. τύποι, πίνακες, κανόνες) για τον συνδυασμό των παραγόντων κινδύνου. Εάν ένα μοντέλο κινδύνου που σχετίζεται με τον οργανισμό δεν παρέχεται στη στρατηγική διαχείρισης κινδύνου ως μέρος του βήματος πλαισίωσης κινδύνου, τότε μέρος αυτού του έργου είναι να καθορίσει τους αλγόριθμους για τον συνδυασμό των τιμών. Οι αλγόριθμοι για τον συνδυασμό των παραγόντων κινδύνου αντικατοπτρίζουν την ανοχή του οργανωτικού κινδύνου (βλ. συμπληρωματική καθοδήγηση στην δράση 2-4 για παραδείγματα). Τα μοντέλα κινδύνου ειδικά για την οργάνωση εξευγενίζονται ως μέρος της προετοιμασίας για αξιολόγηση κινδύνου από: i) τον προσδιορισμό του μοντέλου κινδύνου και τη λογική για τη χρήση του (όταν παρέχονται πολλαπλά μοντέλα κινδύνου που σχετίζονται με την οργάνωση), ii) παρέχοντας πρόσθετα παραδείγματα για τις τιμές των παραγόντων κινδύνου και iii) τον προσδιορισμό τυχόν αλγορίθμων ειδικών για την αξιολόγηση (π.χ. αλγόριθμοι ειδικά για τη χρήση μιας τεχνικής ανάλυσης γραφημάτων επίθεσης). Ελλείψει προ υπαρχουσών

μοντέλων κινδύνου που προϋποθέτουν την οργάνωση ή αναλυτικών προσεγγίσεων που ορίζονται στη στρατηγική διαχείρισης κινδύνου οργανωτικού κινδύνου, το μοντέλο κινδύνου και οι αναλυτικές προσεγγίσεις που πρέπει να χρησιμοποιηθούν στην εκτίμηση κινδύνου καθορίζονται και τεκμηριώνονται σε αυτό το έργο.

4.2 Διεξαγωγή εκτίμησης κινδύνου

Το δεύτερο βήμα στην διαδικασία εκτίμησης κινδύνου είναι η *διεξαγωγή* της εκτίμησης κινδύνου. Το ζητούμενο αυτού του βήματος είναι να παραχθεί στο τέλος μια λίστα απειλών οι οποίες μπορούν να μπουν σε σειρά προτεραιότητας ανάλογα με το επίπεδο κινδύνου και να χρησιμοποιηθούν με σκοπό την περαιτέρω πληροφόρηση για την αντιμετώπισή τους. Για να επιτύχει αυτό, οι οργανισμοί αναλύουν τις απειλές, τις ευπάθειες, τις επιπτώσεις, την πιθανότητα καθώς και την αβεβαιότητα που σχετίζεται με τη διαδικασία εκτίμησης κινδύνου. Αυτό το βήμα επίσης περιλαμβάνει τη συλλογή σημαντικών πληροφοριών ως μέρος κάθε δράσης και διεξάγεται σύμφωνα με το πλαίσιο αξιολόγησης κινδύνου που καθορίζεται στο βήμα Προετοιμασία της διαδικασίας εκτίμησης κινδύνου. Η προσδοκία για τις εκτιμήσεις κινδύνου είναι να καλύπτεται επαρκώς ολόκληρος ο χώρος απειλής σύμφωνα με τους συγκεκριμένους ορισμούς, την καθοδήγηση και την κατεύθυνση που καθορίστηκαν κατά το βήμα Προετοιμασίας. Ωστόσο, στην πράξη, η επαρκής κάλυψη εντός των διαθέσιμων πόρων μπορεί να υπαγορεύει τη γενίκευση των πηγών απειλών, των γεγονότων απειλών και των τρωτών σημείων για τη διασφάλιση της πλήρους κάλυψης και την αξιολόγηση συγκεκριμένων, λεπτομερών πηγών, συμβάντων και τρωτών σημείων μόνο όπως απαιτείται για την επίτευξη στόχων αξιολόγησης κινδύνου. Η διεξαγωγή αξιολογήσεων κινδύνου περιλαμβάνει τις ακόλουθες ειδικές εργασίες:

- Προσδιορισμός πηγών απειλών που σχετίζονται με οργανισμούς,
- προσδιορισμός συμβάντων απειλής που θα μπορούσαν να προκληθούν από αυτές τις πηγές,
- προσδιορισμός ευπαθειών εντός των οργανισμών που θα μπορούσαν να αξιοποιηθούν από πηγές απειλής μέσω συγκεκριμένων συμβάντων απειλής και προδιαθεσικών συνθηκών που θα μπορούσαν να επηρεάσουν την επιτυχή εκμετάλλευση,
- προσδιορισμός της πιθανότητας ότι οι αναγνωρισμένες πηγές απειλής θα αρχικοποιήσουν συγκεκριμένα γεγονότα απειλής και την πιθανότητα ότι τα γεγονότα απειλής θα ήταν επιτυχή,
- προσδιορισμός των αρνητικών επιπτώσεων σε οργανωτικές λειτουργίες και περιουσιακά στοιχεία, άτομα, άλλους οργανισμούς και το Έθνος που προκύπτουν από την εκμετάλλευση των τρωτών σημείων από πηγές απειλών (μέσω συγκεκριμένων γεγονότων απειλής) και,
- προσδιορισμός των κινδύνων για την ασφάλεια των πληροφοριών ως συνδυασμό της πιθανότητας εκμετάλλευσης της απειλής των τρωτών σημείων και του αντίκτυπου μιας τέτοιας εκμετάλλευσης, συμπεριλαμβανομένων τυχόν αβεβαιοτήτων που σχετίζονται με τους προσδιορισμούς κινδύνου.

Οι συγκεκριμένες δράσεις παρουσιάζονται με διαδοχικό τρόπο για λόγους σαφήνειας. Ωστόσο, στην πράξη, κάποια επανάληψη μεταξύ των δράσεων είναι και απαραίτητη και αναμενόμενη. Ανάλογα με τον σκοπό της αξιολόγησης κινδύνου, οι οργανισμοί μπορεί να θεωρήσουν ωφέλιμη την αναδιάταξη των δράσεων. Όποιες και αν είναι οι προσαρμογές που κάνουν οι οργανισμοί στα καθήκοντα που περιγράφονται παρακάτω, οι αξιολογήσεις κινδύνου θα πρέπει να πληρούν τον αναφερόμενο σκοπό, το πεδίο εφαρμογής, τις παραδοχές και τους περιορισμούς που έχουν καθοριστεί από τους οργανισμούς που ξεκινούν τις αξιολογήσεις. Για να βοηθηθούν οι οργανισμοί στην εκτέλεση των επιμέρους εργασιών στη διαδικασία αξιολόγησης κινδύνου, παρέχεται ένα σύνολο προτύπων στα Παραρτήματα Δ έως Ι. Αυτά τα παραρτήματα παρέχουν χρήσιμες πληροφορίες για τους οργανισμούς στην αξιολόγηση του κινδύνου και μπορούν επίσης να χρησιμοποιηθούν για την καταγραφή των αποτελεσμάτων αξιολόγησης που παράγονται κατά τη διάρκεια βασικών υπολογισμών και αναλύσεων. Τα πρότυπα είναι υποδειγματικά και μπορούν να προσαρμοστούν από οργανισμούς σύμφωνα με συγκεκριμένες απαιτήσεις οργανωτικής αποστολής/επιχειρήσεων. Η χρήση των προτύπων δεν απαιτείται για τη διεξαγωγή αξιολογήσεων κινδύνου.

Βήμα 2: Διεξαγωγή της εκτίμησης κινδύνου

Προσδιορισμός των πηγών απειλής

Δράση 1-2: Προσδιορισμός και χαρακτηρισμός των πηγών απειλής, συμπεριλαμβανομένων της ικανότητας, πρόθεσης και στόχευσης όσον αφορά εχθρικές απειλές και εύρος επιπτώσεων για μη εχθρικές απειλές.

Συμπληρωματική καθοδήγηση: Οι οργανισμοί εντοπίζουν τις πηγές ανησυχίας και προσδιορίζουν τα χαρακτηριστικά που σχετίζονται με αυτές τις πηγές απειλών. Για εχθρικές πηγές απειλών, πραγματοποιείται αξιολόγηση των δυνατοτήτων, των προθέσεων και της στόχευσης που σχετίζονται με τις πηγές απειλής. Για μη εχθρικές πηγές απειλών, αξιολογείται το δυνητικό εύρος επιπτώσεων από τις πηγές απειλής. Η στρατηγική διαχείρισης κινδύνου και τα αποτελέσματα του βήματος Προετοιμασίας παρέχουν οργανωτική κατεύθυνση και καθοδήγηση για τη διεξαγωγή αναγνώρισης και χαρακτηρισμού της πηγής απειλής, συμπεριλαμβανομένων, για παράδειγμα: i) πηγών για τη λήψη πληροφοριών για την απειλή, ii) πηγές απειλών που πρέπει να ληφθούν υπόψη (κατά τύπο/όνομα), iii) ταξινόμηση απειλών, και iv) τη διαδικασία για τον προσδιορισμό των πηγών απειλής που προκαλούν ανησυχία για την αξιολόγηση κινδύνου. Όπως προσδιορίζεται στην δράση 1-3, οι οργανισμοί κάνουν σαφείς οποιεσδήποτε υποθέσεις σχετικά με τις πηγές απειλών, συμπεριλαμβανομένων των αποφάσεων που αφορούν τον προσδιορισμό των πηγών απειλής όταν δεν είναι διαθέσιμες συγκεκριμένες και αξιόπιστες πληροφορίες για την απειλή. Οι οργανισμοί μπορούν επίσης να δουν τις αντίπαλες πηγές απειλών από μια ευρεία προοπτική, λαμβάνοντας υπόψη τον χρόνο που μπορεί να έχουν αυτές οι πηγές απειλών για να εκμεταλλευτούν οργανωτικά ευπαθή σημεία, την κλίμακα της επίθεσης και την πιθανή χρήση πολλαπλών φορέων επίθεσης. Ο εντοπισμός και ο χαρακτηρισμός των Προηγμένων Επίμονων Απειλών (APT) μπορεί να περιλαμβάνει σημαντική αβεβαιότητα. Οι οργανισμοί σχολιάζουν τέτοιες πηγές απειλών με κατάλληλο σκεπτικό και αναφορές (και παρέχουν ταξινομήσεις όπως απαιτείται).

Προσδιορισμός των συμβάντων απειλής

Δράση 2-2: Προσδιορισμός πιθανών συμβάντων απειλής, της συνάφειας των γεγονότων και των πηγών απειλής που θα μπορούσαν να ξεκινήσουν τα γεγονότα.

Συμπληρωματική καθοδήγηση: Τα συμβάντα απειλών χαρακτηρίζονται από τις πηγές απειλών που θα μπορούσαν να ξεκινήσουν τα γεγονότα, και για τα εχθρικά γεγονότα απειλής αντίστοιχα, τα TTP (tactics, technics, procedures) που χρησιμοποιούνται για την πραγματοποίηση αυτών των επιθέσεων. Οι οργανισμοί ορίζουν αυτά τα συμβάντα απειλής με επαρκή λεπτομέρεια για την επίτευξη του σκοπού της αξιολόγησης κινδύνου. Πολλαπλές πηγές απειλών μπορούν να ξεκινήσουν ένα μόνο συμβάν απειλής. Αντίθετα, μια μεμονωμένη πηγή απειλής μπορεί ενδεχομένως να εκκινήσει οποιοδήποτε από τα πολλαπλά γεγονότα απειλής. Ως εκ τούτου, μπορεί να υπάρχει μια σχέση πολλά προς πολλά μεταξύ των γεγονότων απειλών και των πηγών απειλών που μπορεί ενδεχομένως να αυξήσουν την πολυπλοκότητα της εκτίμησης κινδύνου. Για να καταστεί δυνατή η αποτελεσματική χρήση και επικοινωνία των αποτελεσμάτων αξιολόγησης κινδύνου, οι οργανισμοί προσαρμόζουν τις γενικές περιγραφές των γεγονότων απειλών στους Πίνακες Ε-2 και Ε-3 για να προσδιορίσουν πώς κάθε γεγονός θα μπορούσε ενδεχομένως να βλάψει τις οργανωτικές λειτουργίες (συμπεριλαμβανομένης της αποστολής, των λειτουργιών, της εικόνας ή της φήμης) και περιουσιακά στοιχεία, άτομα, άλλους οργανισμούς ή το Έθνος. Για κάθε γεγονός απειλής που προσδιορίζεται, οι οργανισμοί καθορίζουν τη συνάφεια του συμβάντος. Ο Πίνακας Ε-4 παρέχει μια σειρά τιμών για τη συνάφεια των γεγονότων απειλών. Οι αξίες που επιλέγονται από τους οργανισμούς έχουν άμεση σχέση με την ανοχή οργανωτικού κινδύνου. Όσο μεγαλύτερη είναι η αποστροφή του κινδύνου, τόσο μεγαλύτερο είναι το εύρος των τιμών που εξετάζονται. Οι οργανισμοί που αποδέχονται μεγαλύτερο κίνδυνο ή έχουν μεγαλύτερη ανοχή κινδύνου είναι πιο πιθανό να απαιτούν ουσιαστικά στοιχεία προτού λάβουν σοβαρά υπόψη τα γεγονότα απειλών. Εάν ένα γεγονός απειλής κριθεί άσχετο, δεν δίνεται περαιτέρω εξέταση. Για σχετικά συμβάντα απειλής, οι οργανισμοί εντοπίζουν όλες τις πιθανές πηγές απειλής που θα μπορούσαν να ξεκινήσουν τα γεγονότα. Για χρήση στην δράση 2-4, οι οργανισμοί μπορούν να αναγνωρίσουν κάθε σύζευξη πηγής απειλής και συμβάν απειλής ξεχωριστά, καθώς η πιθανότητα έναρξης και επιτυχίας της απειλής μπορεί να είναι διαφορετική για κάθε σύζευξη. Εναλλακτικά, οι οργανισμοί μπορούν να προσδιορίσουν το σύνολο όλων των πιθανών πηγών απειλής που θα μπορούσαν ενδεχομένως να ξεκινήσουν μια απειλή.

Προσδιορισμός ευπαθειών και προδιαθεσικών καταστάσεων

Δράση 2-3: Προσδιορισμός των τρωτών σημείων και των προδιαθεσικών συνθηκών που επηρεάζουν την πιθανότητα τα ανησυχητικά γεγονότα να οδηγήσουν σε δυσμενείς επιπτώσεις.

Συμπληρωματική καθοδήγηση: Ο πρωταρχικός σκοπός των αξιολογήσεων τρωτότητας είναι η κατανόηση της φύσης και του βαθμού στον οποίο οι οργανισμοί, οι διαδικασίες αποστολής/επιχειρήσεων και τα συστήματα πληροφοριών είναι ευάλωτα σε πηγές απειλών που προσδιορίζονται στην δράση 2-1 και στα γεγονότα απειλών που προσδιορίζονται στην δράση 2-2 που μπορούν να ξεκινήσουν από αυτές τις πηγές απειλών. Τα τρωτά σημεία στο επίπεδο ένα μπορεί να είναι διάχυτα σε όλους τους οργανισμούς και μπορεί να έχουν

ευρείες δυσμενείς επιπτώσεις εάν εκμεταλλευτούν τα γεγονότα απειλών. Για παράδειγμα, η οργανωτική αποτυχία να εξετάσει τις δραστηριότητες της εφοδιαστικής αλυσίδας μπορεί να έχει ως αποτέλεσμα οι οργανισμοί να αποκτήσουν ανατρεπτικά στοιχεία που οι αντίπαλοι θα μπορούσαν να εκμεταλλευτούν για να διαταράξουν τις οργανωτικές αποστολές/επιχειρηματικές λειτουργίες ή να αποκτήσουν ευαίσθητες οργανωτικές πληροφορίες. Τα τρωτά σημεία στο επίπεδο 2 μπορούν να περιγραφούν ως προς την οργανωτική αποστολή/επιχειρηματικές διαδικασίες, την εταιρική αρχιτεκτονική, τη χρήση πολλαπλών συστημάτων πληροφοριών ή κοινές υποδομές/κοινόχρηστες υπηρεσίες. Στο επίπεδο δύο, τα τρωτά σημεία συνήθως διασχίζουν ή εκτείνονται στα όρια του συστήματος πληροφοριών. Τα τρωτά σημεία στο επίπεδο τρία μπορούν να περιγραφούν ως προς τις τεχνολογίες πληροφοριών που χρησιμοποιούνται σε οργανωτικά συστήματα πληροφοριών, τα περιβάλλοντα στα οποία λειτουργούν αυτά τα συστήματα ή/και την έλλειψη ή αδυναμίες σε ελέγχους ασφαλείας για το συγκεκριμένο σύστημα. Υπάρχει δυνητικά μια σχέση πολλά-προς-πολλά μεταξύ των γεγονότων απειλών και των τρωτών σημείων. Πολλαπλά συμβάντα απειλής μπορούν να εκμεταλλευτούν μια μεμονωμένη ευπάθεια και αντιστρόφως, πολλαπλές ευπάθειες μπορούν να εκμεταλλευτούν από ένα μόνο συμβάν απειλής. Η σοβαρότητα μιας ευπάθειας είναι μια εκτίμηση της σχετικής σημασίας του μετριασμού μιας τέτοιας ευπάθειας. Αρχικά, ο βαθμός στον οποίο ο μετριασμός δεν είναι προγραμματισμένος μπορεί να χρησιμεύσει ως υποκατάστατο για τη σοβαρότητα της ευπάθειας. Αφού αξιολογηθούν οι κίνδυνοι που σχετίζονται με μια συγκεκριμένη ευπάθεια, η σοβαρότητα των επιπτώσεων και η έκθεση της ευπάθειας δεδομένων των ελέγχων ασφαλείας που εφαρμόζονται και άλλων τρωτών σημείων μπορούν να ληφθούν υπόψη κατά την αξιολόγηση της σοβαρότητας της ευπάθειας. Οι αξιολογήσεις της σοβαρότητας της τρωτότητας υποστηρίζουν την απόκριση στον κίνδυνο. Τα τρωτά σημεία μπορούν να εντοπιστούν σε διάφορους βαθμούς ευαισθησίας και ειδικότητας. Το επίπεδο λεπτομέρειας που παρέχεται σε κάθε συγκεκριμένη αξιολόγηση τρωτότητας είναι συνεπές με τον σκοπό της αξιολόγησης κινδύνου και τον τύπο των εισροών που απαιτούνται για την υποστήριξη των επακόλουθων προσδιορισμών πιθανότητας και επιπτώσεων.

Λόγω του συνεχώς αυξανόμενου μεγέθους και πολυπλοκότητας των οργανισμών, των διαδικασιών επιχειρήσεων και των συστημάτων πληροφοριών που υποστηρίζουν αυτές τις διαδικασίες, ο αριθμός των τρωτών σημείων τείνει να είναι μεγάλος και μπορεί να αυξήσει τη συνολική πολυπλοκότητα της ανάλυσης. Ως εκ τούτου, οι οργανισμοί έχουν την επιλογή να χρησιμοποιήσουν την εργασία αναγνώρισης τρωτών σημείων για να κατανοήσουν τη γενική φύση των τρωτών σημείων (συμπεριλαμβανομένου του εύρους, του αριθμού και του τύπου) που σχετίζονται με την αξιολόγηση (βλ. δράση 1-3) και να πραγματοποιήσουν μια καταλογογράφηση συγκεκριμένων τρωτών σημείων όπως απαιτείται για να το κάνεις. Οι οργανισμοί καθορίζουν ποιες ευπάθειες σχετίζονται με ποια απειλητικά συμβάντα, προκειμένου να μειώσουν τον χώρο των πιθανών κινδύνων που πρέπει να αξιολογηθούν. Εκτός από τον εντοπισμό τρωτών σημείων, οι οργανισμοί εντοπίζουν επίσης τυχόν προδιαθεσικές συνθήκες που μπορεί να επηρεάσουν την ευαισθησία σε ορισμένα τρωτά σημεία. Προδιαθεσικές συνθήκες που υπάρχουν μέσα σε οργανισμούς (συμπεριλαμβανομένων των διαδικασιών αποστολής/επιχειρήσεων, συστημάτων πληροφοριών και περιβαλλόντων λειτουργίας) μπορούν να συμβάλουν (δηλαδή, να αυξήσουν ή να μειώσουν) την πιθανότητα ένα ή περισσότερα συμβάντα απειλής, να οδηγήσουν σε δυσμενείς επιπτώσεις σε οργανωτικές λειτουργίες, οργανωτικά περιουσιακά στοιχεία, άτομα, άλλους οργανισμούς ή το Έθνος. Οι οργανισμοί καθορίζουν ποιες προδιαθεσικές συνθήκες σχετίζονται με ποια απειλητικά γεγονότα, προκειμένου να μειώσουν τον χώρο των πιθανών κινδύνων που πρέπει να αξιολογηθούν. Οι οργανισμοί αξιολογούν τη διάχυση των προδιαθεσικών συνθηκών για να υποστηρίξουν τον προσδιορισμό του επιπέδου(ων) στο οποίο η απόκριση στον κίνδυνο θα μπορούσε να είναι πιο αποτελεσματική.

Προσδιορισμός πιθανότητας

Δράση 2-4: Καθορισμός της πιθανότητας των συμβάντων απειλών που θα οδηγήσουν σε δυσμενείς επιπτώσεις, λαμβάνοντας υπόψη: i) τα ευπαθή σημεία/προδιαθεσικές καταστάσεις, ii) τα χαρακτηριστικά των πηγών απειλής που μπορούν να πυροδοτήσουν συμβάντα απειλής, και iii) την οργανωτική ευαισθησία που αντικατοπτρίζει τις διασφαλίσεις/αντίμετρα που σχεδιάζονται ή εφαρμόζονται για την παρεμπόδιση τέτοιων συμβάντων.

Συμπληρωματική καθοδήγηση: Οι οργανισμοί υλοποιούν μια διαδικασία τριών βημάτων για να καθορίσουν τη συνολική πιθανότητα των συμβάντων απειλής. Πρώτον, οι οργανισμοί εκτιμούν την πιθανότητα τα γεγονότα απειλής να ξεκινήσουν (για εχθρικά γεγονότα απειλής) ή να προκύψουν (για μη εχθρικά γεγονότα απειλής). Δεύτερον, οι οργανισμοί εκτιμούν την πιθανότητα τα γεγονότα απειλής εφόσον ξεκινήσουν να επιφέρουν δυσμενείς επιπτώσεις στις οργανωτικές λειτουργίες, τα αγαθά, τα άτομα, άλλους οργανισμούς ή το

Έθνος. Τέλος, οι οργανισμοί εκτιμούν τη συνολική πιθανότητα ως συνδυασμό της πιθανότητας πυροδότησης ενός συμβάντος απειλής και της πιθανότητας να αποφέρει σοβαρές επιπτώσεις.

Οι οργανισμοί αξιολογούν την πιθανότητα έναρξης γεγονότος απειλής λαμβάνοντας υπόψη τα χαρακτηριστικά των πηγών απειλής, συμπεριλαμβανομένης της ικανότητας, της πρόθεσης και της στόχευσης (βλ. δράση 2-1 και Παράρτημα D). Εάν τα γεγονότα απειλής απαιτούν περισσότερες δυνατότητες από ό,τι διαθέτουν οι αντίπαλοι (και οι αντίπαλοι γνωρίζουν αυτό το γεγονός), τότε δεν αναμένεται από τους αντίπαλους να ξεκινήσουν τα γεγονότα. Εάν οι αντίπαλοι δεν αναμένουν να επιτύχουν τους επιδιωκόμενους στόχους εκτελώντας απειλητικά γεγονότα, τότε οι αντίπαλοι δεν αναμένεται να ξεκινήσουν τα γεγονότα. Και τέλος, εάν οι αντίπαλοι δεν στοχεύουν ενεργά συγκεκριμένους οργανισμούς ή τις αποστολές/επιχειρηματικές λειτουργίες τους, οι αντίπαλοι δεν αναμένεται να ξεκινήσουν απειλές. Οι οργανισμοί χρησιμοποιούν την κλίμακα αξιολόγησης στον Πίνακα G-2 και παρέχουν ένα σκεπτικό για την αξιολόγηση που επιτρέπει τη ρητή εξέταση της μετατόπισης της αποτροπής και της απειλής. Οι οργανισμοί μπορούν να αξιολογήσουν την πιθανότητα εμφάνισης γεγονότος απειλής (μη εχθρικής) χρησιμοποιώντας τον Πίνακα G-3 και να παρέχουν παρόμοια λογική για την αξιολόγηση.

Οι οργανισμοί αξιολογούν την πιθανότητα τα γεγονότα απειλών να οδηγήσουν σε δυσμενείς επιπτώσεις λαμβάνοντας υπόψη το σύνολο των εντοπισμένων τρωτών σημείων και των προδιαθεσικών συνθηκών (βλ. δράση 2-3 και Παράρτημα F). Για γεγονότα απειλών που ξεκινούν από αντιπάλους, οι οργανισμοί λαμβάνουν υπόψη τα χαρακτηριστικά των σχετικών πηγών απειλών. Για συμβάντα μη αντίπαλης απειλής, οι οργανισμοί λαμβάνουν υπόψη την αναμενόμενη σοβαρότητα και διάρκεια του συμβάντος (όπως περιλαμβάνονται στην περιγραφή του συμβάντος). Οι οργανισμοί χρησιμοποιούν την κλίμακα αξιολόγησης στον Πίνακα G-4 και παρέχουν ένα σκεπτικό για την αξιολόγηση που επιτρέπει τη ρητή εξέταση όπως αναφέρεται παραπάνω. Τα συμβάντα απειλής για τα οποία δεν έχουν εντοπιστεί ευπάθειες ή προδιαθεσικές συνθήκες, έχουν πολύ μικρή πιθανότητα να οδηγήσουν σε δυσμενείς επιπτώσεις. Τέτοια συμβάντα απειλών μπορούν να επισημανθούν και να μετακινηθούν στο τέλος του πίνακα (ή σε ξεχωριστό πίνακα), έτσι ώστε να μπορούν να παρακολουθούνται για εξέταση στις επακόλουθες αξιολογήσεις κινδύνου. Ωστόσο, δεν απαιτείται περαιτέρω εξέταση κατά την τρέχουσα αξιολόγηση.

Η συνολική πιθανότητα ενός γεγονότος απειλής είναι ένας συνδυασμός: (i) της πιθανότητας να συμβεί το συμβάν (π.χ. λόγω ανθρώπινου λάθους ή φυσικής καταστροφής) ή να ξεκινήσει από έναν αντίπαλο· και (ii) την πιθανότητα η έναρξη/εμφάνιση να οδηγήσει σε δυσμενείς επιπτώσεις. Οι οργανισμοί αξιολογούν τη συνολική πιθανότητα γεγονότων απειλών χρησιμοποιώντας δεδομένα από τους Πίνακες G-2, G-3 και G-4. Οποιοσδήποτε συγκεκριμένος αλγόριθμος ή κανόνας για το συνδυασμό των καθορισμένων τιμών πιθανότητας εξαρτάται από: i) τη γενική οργανωτική στάση απέναντι στον κίνδυνο, συμπεριλαμβανομένης της συνολικής ανοχής κινδύνου και της ανοχής στην αβεβαιότητα, ii) ειδικές ανοχές έναντι της αβεβαιότητας σε διαφορετικούς παράγοντες κινδύνου και iii) οργανωτική στάθμιση των παραγόντων κινδύνου. Για παράδειγμα, οι οργανισμοί θα μπορούσαν να χρησιμοποιήσουν οποιονδήποτε από τους ακόλουθους κανόνες (ή θα μπορούσαν να ορίσουν έναν διαφορετικό κανόνα): i) να χρησιμοποιήσουν το μέγιστο από τις δύο τιμές πιθανότητας, ii) χρησιμοποιεί το ελάχιστο από τις δύο τιμές πιθανότητας, iii) εξετάζει την πιθανότητα έναρξης/εμφάνισης μόνο, υποθέτοντας ότι εάν ξεκινήσουν ή συμβούν γεγονότα απειλής, τα γεγονότα θα οδηγήσουν σε δυσμενείς επιπτώσεις, iv) εξετάζει μόνο την πιθανότητα επιπτώσεων, υποθέτοντας ότι εάν τα γεγονότα απειλής θα μπορούσαν να οδηγήσουν σε δυσμενείς επιπτώσεις, οι αντίπαλοι θα ξεκινήσουν τα γεγονότα, ή v) να λάβει ένα σταθμισμένο μέσο όρο των δύο τιμών πιθανότητας. Οι οργανισμοί καθιστούν σαφείς τους κανόνες που χρησιμοποιούνται.

Προσδιορισμός της επίπτωσης

Δράση 2-5: προσδιορισμός των δυσμενών επιπτώσεων που προκαλούνται από γεγονότα απειλής λαμβάνοντας υπόψη: i) τα χαρακτηριστικά των πηγών απειλής που προκαλούν τα γεγονότα, ii) τις ευπάθειες και τις προδιαθεσικές καταστάσεις που προσδιορίστηκαν, iii) την ευαισθησία που αντικατοπτρίζει τις διασφαλίσεις/αντίμετρα που σχεδιάζονται ή εφαρμόζονται για την παρεμπόδιση τέτοιων συμβάντων.

Συμπληρωματική καθοδήγηση: Οι οργανισμοί περιγράφουν τις αρνητικές επιπτώσεις από την άποψη της πιθανής ζημίας που προκαλείται σε οργανωτικές λειτουργίες και περιουσιακά στοιχεία, άτομα, άλλους οργανισμούς ή το Έθνος. Όπου συμβαίνει το συμβάν απειλής και εάν οι επιπτώσεις του συμβάντος περιορίζονται ή εξαπλώνονται, επηρεάζει τη σοβαρότητα της επίπτωσης. Η αξιολόγηση του αντίκτυπου μπορεί να περιλαμβάνει τον εντοπισμό περιουσιακών στοιχείων ή πιθανών στόχων πηγών απειλών, συμπεριλαμβανομένων πόρων πληροφοριών (π.χ. πληροφορίες, αποθήκες δεδομένων, συστήματα πληροφοριών, εφαρμογές, τεχνολογίες πληροφοριών, συνδέσεις επικοινωνιών), άτομα και φυσικούς πόρους (π.χ. κτίρια, τροφοδοτικά), τα οποία μπορεί να επηρεαστούν από απειλητικά γεγονότα. Οι οργανωτικές επιπτώσεις ορίζονται και ιεραρχούνται στις

Βαθμίδες 1 και 2 και κοινοποιούνται στη Βαθμίδα 3 ως μέρος του πλαισίου κινδύνου. Στη Βαθμίδα 3, οι επιπτώσεις σχετίζονται με δυνατότητες συστημάτων πληροφοριών (π.χ. επεξεργασία, εμφάνιση, επικοινωνίες, αποθήκευση και ανάκτηση) και πόρους (π.χ. βάσεις δεδομένων, υπηρεσίες, στοιχεία) που θα μπορούσαν να τεθούν σε κίνδυνο.

Προσδιορισμός του κινδύνου

Δράση 2-6: Προσδιορισμός του κινδύνου για τον οργανισμό που προέρχεται από συμβάντα απειλής λαμβάνοντας υπόψη: i) τις επιπτώσεις που θα αποφέρουν τα συμβάντα απειλής, και ii) την πιθανότητα αυτά τα συμβάντα να προκύψουν.

Συμπληρωματική καθοδήγηση: Οι οργανισμοί αξιολογούν τους κινδύνους από γεγονότα απειλών ως συνδυασμό πιθανότητας και επιπτώσεων. Το επίπεδο κινδύνου που σχετίζεται με αναγνωρισμένα γεγονότα απειλής αντιπροσωπεύει έναν προσδιορισμό του βαθμού στον οποίο οι οργανισμοί απειλούνται από τέτοια γεγονότα. Οι οργανισμοί δηλώνουν ρητά την αβεβαιότητα στους προσδιορισμούς κινδύνου, συμπεριλαμβανομένων, για παράδειγμα, των οργανωτικών παραδοχών και των υποκειμενικών κρίσεων/αποφάσεων. Οι οργανισμοί μπορούν να ταξινομήσουν τη λίστα των γεγονότων απειλών που προκαλούν ανησυχία με βάση το επίπεδο κινδύνου που προσδιορίζεται κατά την αξιολόγηση κινδύνου — με τη μεγαλύτερη προσοχή να δίνεται στα συμβάντα υψηλού κινδύνου. Οι οργανισμοί μπορούν περαιτέρω να ιεραρχήσουν τους κινδύνους στο ίδιο επίπεδο ή με παρόμοιες βαθμολογίες (βλ. Παράρτημα J). Κάθε κίνδυνος αντιστοιχεί σε ένα συγκεκριμένο γεγονός απειλής με ένα επίπεδο αντίκτυπου εάν συμβεί αυτό το συμβάν. Γενικά, το επίπεδο κινδύνου δεν είναι συνήθως υψηλότερο από το επίπεδο επιπτώσεων και η πιθανότητα μπορεί να χρησιμεύσει για τη μείωση του κινδύνου κάτω από αυτό το επίπεδο επιπτώσεων. Ωστόσο, όταν αντιμετωπίζονται ζητήματα διαχείρισης κινδύνου σε ολόκληρο τον οργανισμό με μεγάλο αριθμό αποστολών/επιχειρηματικών λειτουργιών, αποστολών/επιχειρηματικών διαδικασιών και υποστήριξης συστημάτων πληροφοριών, ο αντίκτυπος ως ανώτατο όριο στον κίνδυνο ενδέχεται να μην ισχύει. Για παράδειγμα, όταν πραγματοποιούνται πολλαπλοί κίνδυνοι, ακόμα κι αν κάθε κίνδυνος βρίσκεται σε μέτριο επίπεδο, το σύνολο αυτών των κινδύνων μέτριου επιπέδου θα μπορούσε να συγκεντρωθεί σε υψηλότερο επίπεδο κινδύνου για τους οργανισμούς. Για την αντιμετώπιση καταστάσεων όπου η βλάβη συμβαίνει πολλές φορές, οι οργανισμοί μπορούν να ορίσουν ένα γεγονός απειλής ως πολλαπλά περιστατικά βλάβης και ένα επίπεδο επιπτώσεων που σχετίζεται με τον σωρευτικό βαθμό βλάβης. Κατά την εκτέλεση των δράσεων 2-1 έως 2-5, οι οργανισμοί συγκεντρώνουν βασικές πληροφορίες που σχετίζονται με αβεβαιότητες στις εκτιμήσεις κινδύνου. Αυτές οι αβεβαιότητες προκύπτουν από πηγές όπως το να λείπουν πληροφορίες, υποκειμενικοί προσδιορισμοί και υποθέσεις που έγιναν. Η αποτελεσματικότητα των αποτελεσμάτων της αξιολόγησης κινδύνου καθορίζεται εν μέρει από την ικανότητα των υπευθύνων λήψης αποφάσεων να είναι σε θέση να προσδιορίσουν τη συνεχή εφαρμογή των παραδοχών που γίνονται ως μέρος της αξιολόγησης. Οι πληροφορίες που σχετίζονται με την αβεβαιότητα συγκεντρώνονται και παρουσιάζονται με τρόπο που υποστηρίζει εύκολα τεκμηριωμένες αποφάσεις διαχείρισης κινδύνου.

4.3 Επικοινωνία και κοινοποίηση των πληροφοριών εκτίμησης κινδύνου

Το τρίτο βήμα της διαδικασίας εκτίμησης κινδύνου είναι η επικοινωνία των αποτελεσμάτων της εκτίμησης και η κοινοποίηση των αντίστοιχων πληροφοριών. Αντικείμενο αυτού του βήματος είναι να διασφαλίσει ότι οι υπεύθυνοι για τις λήψεις αποφάσεων μέσα στον οργανισμό έχουν την απαραίτητη πληροφορία που χρειάζονται για να πάρουν τις κατάλληλες αποφάσεις. Η επικοινωνία και η κοινοποίηση των πληροφοριών αποτελείται από δύο βήματα:

- Επικοινωνία των αποτελεσμάτων της εκτίμησης κινδύνου, και
- Κοινοποίηση των πληροφοριών που προέκυψαν κατά την εκτέλεση της εκτίμησης κινδύνου, με σκοπό την υποστήριξη άλλων δραστηριοτήτων διαχείρισης κινδύνου.

Βήμα 3: Επικοινωνία και κοινοποίηση των αποτελεσμάτων της εκτίμησης κινδύνου

Επικοινωνία των αποτελεσμάτων της εκτίμησης κινδύνου

Δράση 3-1: Επικοινωνία των αποτελεσμάτων στους υπεύθυνους για τη λήψη αποφάσεων στον οργανισμό με σκοπό την αντιμετώπιση του κινδύνου.

Συμπληρωματική καθοδήγηση: Οι οργανισμοί μπορούν να κοινοποιούν τα αποτελέσματα της αξιολόγησης κινδύνου με διάφορους τρόπους (π.χ. ενημερώσεις στελεχών, εκθέσεις αξιολόγησης κινδύνου, πίνακες εργαλείων). Τέτοιες επικοινωνίες κινδύνου μπορεί να είναι επίσημες ή ανεπίσημες με το περιεχόμενο και τη μορφή που καθορίζονται από τους οργανισμούς που ξεκινούν και διεξάγουν τις αξιολογήσεις. Οι οργανισμοί παρέχουν καθοδήγηση σχετικά με συγκεκριμένες απαιτήσεις επικοινωνίας και αναφοράς κινδύνου, οι οποίες περιλαμβάνονται στο πλαίσιο της προετοιμασίας για την αξιολόγηση κινδύνου (εάν δεν παρέχεται στη στρατηγική διαχείρισης κινδύνου ως μέρος της εργασίας πλαισίωσης κινδύνου). Οι οργανισμοί δίνουν προτεραιότητα στους κινδύνους στο ίδιο επίπεδο ή με παρόμοια βαθμολογία (βλ. Παράρτημα J). Το Παράρτημα K παρέχει ένα παράδειγμα τύπου πληροφοριών που μπορεί να περιλαμβάνονται σε μια έκθεση αξιολόγησης κινδύνου ή στο προτιμώμενο όχημα για την επικοινωνία κινδύνου.

Κοινοποίηση των πληροφοριών σχετικών με τον κίνδυνο

Δράση 3-2: Διαμοιρασμός πληροφοριών σχετικά με τον κίνδυνο που παράγονται κατά την αξιολόγηση κινδύνου με το κατάλληλο οργανωτικό προσωπικό.

Συμπληρωματική καθοδήγηση: Οι οργανισμοί μοιράζονται πληροφορίες πηγής και ενδιάμεσα αποτελέσματα και παρέχουν καθοδήγηση σχετικά με την κοινή χρήση πληροφοριών που σχετίζονται με τον κίνδυνο. Η ανταλλαγή πληροφοριών πραγματοποιείται κυρίως εντός των οργανισμών, μέσω αναφορών και ενημερώσεων και με την ενημέρωση των δεδομένων που σχετίζονται με τον κίνδυνο με αποδεικτικά στοιχεία για τα αποτελέσματα της αξιολόγησης κινδύνου. Η ανταλλαγή πληροφοριών υποστηρίζεται επίσης από την τεκμηρίωση των πηγών πληροφοριών, των αναλυτικών διαδικασιών και των ενδιάμεσων αποτελεσμάτων (π.χ. συμπληρωμένοι πίνακες στα Παραρτήματα Δ-Ι), έτσι ώστε να μπορούν να διατηρούνται εύκολα οι εκτιμήσεις κινδύνου. Η ανταλλαγή πληροφοριών μπορεί επίσης να πραγματοποιηθεί με άλλους οργανισμούς.

4.4 Διατήρηση της εκτίμησης κινδύνου

Το τέταρτο βήμα στη διαδικασία αξιολόγησης κινδύνου είναι η διατήρηση της αξιολόγησης. Ο στόχος αυτού του βήματος είναι να διατηρείται ενημερωμένη η συγκεκριμένη γνώση σχετικά με τους κινδύνους που αναλαμβάνουν οι οργανισμοί. Τα αποτελέσματα των αξιολογήσεων κινδύνου ενημερώνουν τις αποφάσεις διαχείρισης κινδύνου και καθοδηγούν τις αντιμετωπίσεις κινδύνου. Για να υποστηρίξουν τη συνεχή αναθεώρηση των αποφάσεων διαχείρισης κινδύνου (π.χ. αποφάσεις απόκτησης, αποφάσεις εξουσιοδότησης για συστήματα πληροφοριών και κοινούς ελέγχους, αποφάσεις σύνδεσης), οι οργανισμοί διατηρούν αξιολογήσεις κινδύνου για να ενσωματώσουν τυχόν αλλαγές που ανιχνεύονται μέσω της παρακολούθησης κινδύνου. Η παρακολούθηση κινδύνου παρέχει στους οργανισμούς με τα κατάλληλα μέσα και σε συνεχή βάση να: i) καθορίζει την αποτελεσματικότητα των ανταποκρίσεων στον κίνδυνο, ii) προσδιορίζει τις αλλαγές που επηρεάζουν τον κίνδυνο στα συστήματα πληροφοριών του οργανισμού και στα περιβάλλοντα στα οποία λειτουργούν αυτά τα συστήματα, και iii) επαληθεύει τη συμμόρφωση. Η διατήρηση των αξιολογήσεων κινδύνου περιλαμβάνει τις ακόλουθες ειδικές εργασίες:

- Παρακολούθηση παραγόντων κινδύνου που προσδιορίζονται στις αξιολογήσεις κινδύνου σε συνεχή βάση και κατανόηση των επακόλουθων αλλαγών σε αυτούς τους παράγοντες και
- Ενημέρωση των στοιχείων των αξιολογήσεων κινδύνου που αντικατοπτρίζουν τις δραστηριότητες παρακολούθησης που πραγματοποιούνται από οργανισμούς.

Βήμα 4: Διατήρηση της αξιολόγησης

Προσδιορισμός των παραγόντων κινδύνου

Δράση 4-1: Διεξαγωγή συνεχής παρακολούθησης των παραγόντων κινδύνου που συμβάλλουν σε αλλαγές κινδύνου για τις οργανωτικές λειτουργίες και τα περιουσιακά στοιχεία, τα άτομα, άλλους οργανισμούς ή το Έθνος.

Συμπληρωματική καθοδήγηση: Οι οργανισμοί παρακολουθούν σημαντικούς παράγοντες κινδύνου σε συνεχή βάση για να διασφαλίσουν ότι οι πληροφορίες που απαιτούνται για τη λήψη αξιόπιστων αποφάσεων που βασίζονται στον κίνδυνο συνεχίζουν να είναι διαθέσιμες με την πάροδο του χρόνου. Η παρακολούθηση παραγόντων κινδύνου (π.χ. πηγές απειλών και συμβάντα απειλών, ευπάθειες και προδιαθεσικές συνθήκες,

δυνατότητες και πρόθεση αντιπάλων, στόχευση οργανωτικών λειτουργιών, περιουσιακών στοιχείων ή ατόμων) μπορεί να παρέχει κρίσιμες πληροφορίες για τις μεταβαλλόμενες συνθήκες που θα μπορούσαν ενδεχομένως να επηρεάσουν την ικανότητα των οργανισμών να ενεργούν βασικές αποστολές και επιχειρηματικές λειτουργίες. Οι πληροφορίες που προέρχονται από τη συνεχή παρακολούθηση των παραγόντων κινδύνου μπορούν να χρησιμοποιηθούν για την ανανέωση των αξιολογήσεων κινδύνου σε οποιαδήποτε συχνότητα κρίνεται κατάλληλη. Οι οργανισμοί μπορούν επίσης να επιχειρήσουν να καταγράψουν αλλαγές στην αποτελεσματικότητα των μέτρων αντιμετώπισης κινδύνου, προκειμένου να διατηρήσουν το νόμισμα των αξιολογήσεων κινδύνου. Ο στόχος είναι να διατηρηθεί μια συνεχής επίγνωση της κατάστασης σχετικά με τις δομές και τις δραστηριότητες οργανωτικής διακυβέρνησης, τις διαδικασίες αποστολής/επιχειρήσεων, τα πληροφοριακά συστήματα και τα περιβάλλοντα λειτουργίας, και ως εκ τούτου όλων των παραγόντων κινδύνου που μπορεί να επηρεάσουν τον κίνδυνο που αναλαμβάνουν οι οργανισμοί. Επομένως, κατά την εφαρμογή του πλαισίου αξιολόγησης κινδύνου ή του πλαισίου κινδύνου (δηλαδή, εύρος, σκοπός, υποθέσεις, περιορισμοί, ανοχές κινδύνου, προτεραιότητες και συμβιβασμούς), οι οργανισμοί λαμβάνουν υπόψη τον ρόλο που διαδραματίζουν οι παράγοντες κινδύνου στο εκτελούμενο σχέδιο απόκρισης κινδύνου. Για παράδειγμα, αναμένεται να είναι αρκετά σύνηθες η στάση ασφαλείας των πληροφοριακών συστημάτων (δηλαδή οι παράγοντες κινδύνου που μετρούνται σε αυτά τα συστήματα) να αντικατοπτρίζει μόνο ένα μέρος της απόκρισης οργανωτικού κινδύνου, με ενέργειες απόκρισης σε επίπεδο οργανισμού ή αποστολής/ επίπεδο επιχειρηματικής διαδικασίας που παρέχει σημαντικό μέρος αυτής της ανταπόκρισης. Σε τέτοιες περιπτώσεις, η παρακολούθηση μόνο της θέσης ασφαλείας των συστημάτων πληροφοριών πιθανότατα δεν θα παρέχει επαρκείς πληροφορίες για τον προσδιορισμό του συνολικού κινδύνου που διατρέχουν οι οργανισμοί. Πηγές απειλής με υψηλή ικανότητα, με καλούς πόρους και με γνώμονα το σκοπό μπορεί να αναμένεται ότι θα νικήσουν τους κοινώς διαθέσιμους μηχανισμούς προστασίας (π.χ. παρακάμπτοντας ή παραβιάζοντας τέτοιους μηχανισμούς). Έτσι, μέτρα απόκρισης κινδύνου σε επίπεδο διαδικασίας, όπως ο ανασχεδιασμός των διαδικασιών αποστολής/επιχειρήσεων, η σοφή χρήση της τεχνολογίας πληροφοριών ή η χρήση εναλλακτικών διαδικασιών εκτέλεσης, σε περίπτωση παραβιάσεων συστημάτων πληροφοριών, μπορεί να είναι κύρια στοιχεία των σχεδίων αντιμετώπισης οργανωτικού κινδύνου.

Ανανέωση της αξιολόγησης κινδύνου

Δράση 4-2: Ενημέρωση της υπάρχουσας εκτίμησης κινδύνου χρησιμοποιώντας τα αποτελέσματα από τη συνεχή παρακολούθηση των παραγόντων κινδύνου.

Συμπληρωματική καθοδήγηση: Οι οργανισμοί καθορίζουν τη συχνότητα και τις συνθήκες υπό τις οποίες ενημερώνονται οι αξιολογήσεις κινδύνου. Τέτοιοι προσδιορισμοί μπορεί να περιλαμβάνουν, για παράδειγμα, το τρέχον επίπεδο κινδύνου για και/ή τη σημασία των βασικών οργανωτικών αποστολών/επιχειρηματικών λειτουργιών. Εάν έχουν προκύψει σημαντικές αλλαγές (όπως ορίζονται από τις οργανωτικές πολιτικές, την κατεύθυνση ή την καθοδήγηση) από τη στιγμή που πραγματοποιήθηκε η αξιολόγηση κινδύνου, οι οργανισμοί μπορούν να επανεξετάσουν το σκοπό, το πεδίο, τις υποθέσεις και τους περιορισμούς της αξιολόγησης για να καθορίσουν εάν όλες οι εργασίες στη διαδικασία αξιολόγησης κινδύνου χρειάζονται να επαναληφθεί. Διαφορετικά, οι ενημερώσεις συνιστούν μεταγενέστερες εκτιμήσεις κινδύνου, προσδιορίζοντας και αξιολογώντας μόνο τον τρόπο με τον οποίο έχουν αλλάξει επιλεγμένοι παράγοντες κινδύνου, για παράδειγμα: i) εντοπισμός νέων γεγονότων απειλής, τρωτών σημείων, προδιαθεσικών συνθηκών, ανεπιθύμητων συνεπειών ή/και επηρεαζόμενων περιουσιακών στοιχείων και ii) τις εκτιμήσεις των χαρακτηριστικών της πηγής απειλής (π.χ. ικανότητα, πρόθεση, στόχευση, εύρος επιπτώσεων), πιθανότητες και επιπτώσεις. Οι οργανισμοί κοινοποιούν τα αποτελέσματα των επακόλουθων αξιολογήσεων κινδύνου σε οντότητες σε όλες τις βαθμίδες διαχείρισης κινδύνου για να διασφαλίσουν ότι οι υπεύθυνοι υπάλληλοι έχουν πρόσβαση σε κρίσιμες πληροφορίες που απαιτούνται για τη λήψη συνεχών αποφάσεων που βασίζονται στον κίνδυνο.

5. Διαφορές μεταξύ ISO 27005 και NIST 800-30 SP

Υπάρχουν πολλά πλαίσια διαχείρισης κινδύνων του κλάδου που ήδη περιγράφουν τα αναμενόμενα βήματα ή διαδικασίες για τη διαχείριση κινδύνων στον κυβερνοχώρο και της πληροφορικής — και ακόμη περιγράφουν τις αρχές που απαιτούνται για ένα αποτελεσματικό πρόγραμμα διαχείρισης κινδύνου.

Οι πιο συνηθισμένες είναι το NIST 800-30 και το ISO 27005 πρόκειται για κορυφαία πρότυπα που περιγράφουν τις βέλτιστες πρακτικές για τη διεξαγωγή αξιολόγησης κινδύνου ασφάλειας πληροφοριών. Αυτό

που είναι σημαντικό να συνειδητοποιήσουμε είναι ότι δεν περιγράφουν συγκεκριμένες μεθόδους, απλώς καθορίζουν τις προτεινόμενες διαδικασίες που πρέπει να ακολουθηθούν. Υιοθετώντας τέτοια πρότυπα, οι οργανισμοί διασφαλίζουν την υψηλότερη δυνατή ποιότητα της μεθοδολογίας διαχείρισης κινδύνων τους.

5.1 Εκτιμήσεις κινδύνου σύμφωνα με πρότυπο NIST 800-30 SP

Το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) παρέχει μια κατευθυντήρια γραμμή στο έγγραφο που ονομάζεται NIST Special Publication 800-30 revision 1. Είναι επίσης προσαρμόσιμο στις ανάγκες οποιουδήποτε οργανισμού με συγκεκριμένες απαιτήσεις και κυβερνητικά συστήματα πληροφοριών. Γενικά, αντιμετωπίζει τις πιθανές αρνητικές επιπτώσεις σε οργανωτικές λειτουργίες και περιουσιακά στοιχεία, άτομα, άλλους οργανισμούς και τα συμφέροντα της οικονομίας και της εθνικής ασφάλειας των Ηνωμένων Πολιτειών.

Όπως αναφέρεται παραπάνω, η αξιολόγηση κινδύνου μπορεί να πραγματοποιηθεί και στα τρία επίπεδα της ιεραρχίας διαχείρισης κινδύνου:

- Οργανωτικό επίπεδο
- Επίπεδο αποστολής/επιχειρηματικής διαδικασίας
- Επίπεδο πληροφοριακού συστήματος

Επιπλέον, η διαδικασία αξιολόγησης κινδύνου σύμφωνα με το NIST 800-30 έχει τέσσερα κύρια βήματα:

Προετοιμασία για την Εκτίμηση Κινδύνου

Ο στόχος αυτού του βήματος είναι να προσδιορίσει το πλαίσιο της αξιολόγησης κινδύνου που προκύπτει από το βήμα του πλαισίου κινδύνου. Στην πραγματικότητα, περιλαμβάνει λεπτομερή προγραμματισμό που σχετίζεται με τις ακόλουθες βασικές δραστηριότητες:

- Προσδιορισμός του σκοπού και του στόχου της αξιολόγησης.
- Προσδιορισμός του πιθανού εύρους της αξιολόγησης.
- Προσδιορισμός όλων των παραδοχών και των περιορισμών που επηρεάζουν την αξιολόγηση.
- Προσδιορισμός εισροών αξιολόγησης, όπως πηγές απειλής, ευπάθειας και πληροφορίες επιπτώσεων.
- Επανεξέταση του μοντέλου κινδύνου, της προσέγγισης αξιολόγησης και της προσέγγισης ανάλυσης που θα χρησιμοποιηθούν στην αξιολόγηση κινδύνου.

Διεξαγωγή αξιολογήσεων κινδύνου

Με βάση τα αποτελέσματα από το προηγούμενο βήμα, ο στόχος αυτής της φάσης είναι η δημιουργία μιας λίστας κινδύνων για την ασφάλεια των πληροφοριών. Για την επίτευξη αυτού του στόχου απαιτείται η εκτέλεση των παρακάτω δραστηριοτήτων:

- Προσδιορισμός των πηγών απειλών των οργανισμών και των γεγονότων απειλών που θα μπορούσαν να παραχθούν.
- Προσδιορισμός των τρωτών σημείων, της πιθανότητας απειλής εκμετάλλευσης αδυναμιών σε συστήματα πληροφοριών και περιβάλλοντα λειτουργίας.
- Προσδιορισμός πιθανών σεναρίων επιπτώσεων σε συγκεκριμένες οργανωτικές λειτουργίες, περιουσιακά στοιχεία και άτομα.
- Τέλος, Προσδιορισμός των κινδύνων για την ασφάλεια των πληροφοριών. Αυτά αναγνωρίζονται ως συνδυασμός της πιθανότητας εκμετάλλευσης της απειλής των τρωτών σημείων και του αντίκτυπου των εκμεταλλεύσεων. Επίπεδα κινδύνου που λαμβάνονται από τον πίνακα επιπέδου επιπτώσεων με τον πίνακα επιπέδου πιθανοτήτων με βάση τα σενάρια κινδύνου.
- Συνολικά, το αποτέλεσμα των αξιολογήσεων κινδύνου αναμένεται να καλύψει επαρκώς ολόκληρο τον χώρο απειλής σύμφωνα με τους συγκεκριμένους ορισμούς, τις οδηγίες και τις κατευθύνσεις που έχουν καθοριστεί κατά την προετοιμασία.

Επικοινωνία και κοινή χρήση πληροφοριών αξιολόγησης κινδύνου

Αυτό το βήμα περιλαμβάνει την επεξεργασία των αποτελεσμάτων από τις δύο προηγούμενες φάσεις και την περαιτέρω παρουσίασή τους. Προφανώς, οι υπεύθυνοι λήψης αποφάσεων σε ολόκληρο τον οργανισμό

πρέπει να έχουν κατάλληλες πληροφορίες σχετικά με τον κίνδυνο για να ενημερώνουν και να λαμβάνουν τις σωστές αποφάσεις κινδύνου. Επομένως, σε αυτό το στάδιο, είναι απαραίτητο να ρυθμιστεί:

- Πώς πρέπει να κοινοποιούνται τα αποτελέσματα της αξιολόγησης κινδύνου.
- Να καθοριστεί πώς θα μοιραστούν, λαμβάνοντας υπόψη τις πολιτικές του οργανισμού.
- Διατήρηση της Εκτίμησης Κινδύνων.

Η τελευταία φάση της διαδικασίας είναι η συντήρηση. Είναι σημαντικό να συνειδητοποιήσουμε ότι η αξιολόγηση κινδύνου είναι μια διαρκώς εξελισσόμενη διαδικασία. Η παρακολούθηση και η επαναξιολόγηση των παραγόντων κινδύνου οδηγεί σε αποτελεσματική προστασία. Είναι απαραίτητο να ληφθούν υπόψη οι παράγοντες κινδύνου που εντοπίστηκαν καθώς και τυχόν νέοι.

5.2 Εκτιμήσεις κινδύνου σύμφωνα με το πρότυπο ISO/IEC 27005

Ο ISO είναι ένας ανεξάρτητος και μη κυβερνητικός διεθνής οργανισμός τυποποίησης. Η πιο πρόσφατη έκδοση, το ISO/IEC 27005:2018 είναι ένα ευρέως χρησιμοποιούμενο πρότυπο από οργανισμούς για την εφαρμογή διαχείρισης κινδύνων ασφάλειας πληροφοριών και καλύπτει τεχνολογία, ανθρώπους και διαδικασίες στην αξιολόγηση κινδύνου. Επιπλέον, υποστηρίζει τις γενικές έννοιες που καθορίζονται στο ISO/IEC 27001. Παντού έχει σχεδιαστεί για να υποστηρίζει την εφαρμογή ασφάλειας πληροφοριών βάσει κινδύνου. Αυτό το πρότυπο μπορεί να επιτευχθεί σε διάφορους τύπους οργανισμών, όπως εμπορικές επιχειρήσεις, κυβερνητικές υπηρεσίες και μη κερδοσκοπικούς οργανισμούς.

Σε σύγκριση με το NIST 800-30, το ISO 27005 βασίζεται στη συμμόρφωση με τη γενική διαχείριση κινδύνου. Το έγγραφο δεν υιοθετεί μια προσέγγιση που ταιριάζει σε όλους, αλλά παρέχει μια λεπτομερή και ευέλικτη δομή για την κάλυψη των απαιτήσεων.

Η διαδικασία διαχείρισης κινδύνου σύμφωνα με το ISO 27005 έχει έξι φάσεις:

- Καθορισμός πλαισίου
- Εκτίμηση κινδύνου
- Αντιμετώπιση κινδύνου
- Αποδοχή του κινδύνου
- Επικοινωνία κινδύνου
- Παρακολούθηση και επανεξέταση κινδύνου

Οι φάσεις αξιολόγησης κινδύνου αποτελούνται από συστηματικό εντοπισμό, ανάλυση, αξιολόγηση και ιεράρχηση των κινδύνων ασφάλειας πληροφοριών. Επιπλέον, αυτά είναι σύμφωνα με τα κριτήρια και τους στόχους της αξιολόγησης κινδύνου που σχετίζονται με τον οργανισμό.

Προσδιορισμός κινδύνου

Η ουσία αυτού του μέρους είναι να δηλωθεί τι θα μπορούσε να προκαλέσει πιθανή απώλεια για τον οργανισμό. Πρέπει λοιπόν να προσδιοριστούν τα εξής:

- Περιουσιακά στοιχεία, επιχειρηματικές διαδικασίες και κατάλληλες πληροφορίες και υποστήριξη. Ως αποτέλεσμα, λαμβάνουμε μια λίστα περιουσιακών στοιχείων για τα οποία απαιτείται διαχείριση κινδύνου. Επίσης, μια λίστα με τις διαδικασίες των δραστηριοτήτων του οργανισμού που ισχύουν για τα περιουσιακά στοιχεία και τη σημασία τους.
- Απειλές και τρωτά σημεία που ισχύουν για κάθε περιουσιακό στοιχείο. Αδυναμίες του οργανισμού στην τεχνολογία, τους ανθρώπους και τις διαδικασίες, τη διαμόρφωση του πληροφοριακού συστήματος κ.λπ. Όλα αυτά πρέπει να εντοπιστούν.
- Θα πρέπει να προσδιοριστούν οι υφιστάμενοι και οι προγραμματισμένοι έλεγχοι. Μετά την ταυτοποίηση, συνιστάται ο έλεγχος των μέτρων. Αυτό καθιστά δυνατή την αποφυγή απωλειών χρόνου και τρωτών σημείων.
- Επιπτώσεις, που μπορεί να σημαίνουν απώλεια εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας για το στοιχείο. Ως αποτέλεσμα αυτού του βήματος, λίστα σεναρίων συμβάντων με τις συνέπειές τους που σχετίζονται με περιουσιακά στοιχεία και διαδικασίες.

Ανάλυση κινδύνου

Αυτό το μέρος χωρίζεται σε τρία μικρότερα μέρη στο έγγραφο. Αυτό περιλαμβάνει τη μεθοδολογία ανάλυσης κινδύνου, την εκτίμηση επιπτώσεων και τον προσδιορισμό της πιθανότητας ενός επιπέδου κινδύνου. Με βάση τα αποτελέσματα αυτών των τμημάτων, είναι δυνατό να δημιουργηθεί μια λίστα σεναρίων συμβάντων με τις επιπτώσεις και τις πιθανότητες τους. Ως αποτέλεσμα, ανάλογα με τη μεθοδολογία, οι τιμές που αποδίδονται στην πιθανότητα και τον αντίκτυπο μπορεί να είναι ποσοτικές ή ποιοτικές.

Αξιολόγηση κινδύνου

Το τελευταίο μέρος της αξιολόγησης κινδύνου σύμφωνα με το ISO/IEC 27005 είναι η αξιολόγηση κινδύνου. Οι κίνδυνοι πρέπει να ιεραρχούνται σύμφωνα με τα κριτήρια αξιολόγησης κινδύνου που σχετίζονται με το σενάριο του συμβάντος. Ωστόσο, εάν το κριτήριο δεν είναι σημαντικό για την εταιρεία, οι κίνδυνοι με αυτό το κριτήριο ενδέχεται να μην είναι επίσης σημαντικοί. Σε αυτή τη φάση θα πρέπει επίσης να ληφθεί υπόψη η σημασία των περιουσιακών στοιχείων και των διαδικασιών.

No.	ISO 27005	NIST SP 800-30 REVISION 1	COMBINATION TECHNIQUE [5]
		CONTEXT ESTABLISHMENT	
1.	Determination of Risk Assessment Criteria and Scale		
		RISK ASSESSMENT	
2.	Risk Identification	1. Threat Source Identification 2. Threat Event Identification 3. Vulnerability Identification	1. Risk Identification: a). Threat Source Identification; b). Threat Event Identification; c). Vulnerability Identification.
3.	Risk Analysis	4. Determining the Likelihood 5. Determining Impact	2. Risk Analysis: a). Determining the likelihood in the risk scenario; b). Determining the impact on the risk scenario.
4.	Risk Evaluation	6. Determine information security risk level	3. Risk Evaluation: a). Determining the level of information security risk; b). Determining Risk Priority.

Εικόνα 4:Σύγκριση των ISO 27005 και NIST 80-30 SP

6. Μέθοδοι και Εργαλεία για την εκτίμηση κινδύνου

Υπάρχουν διάφορες μέθοδοι και εργαλεία αξιολόγησης κινδύνου που μπορούν να βοηθήσουν στον εντοπισμό του κινδύνου, στην κατάλληλη αξιολόγηση του κινδύνου και στη διαχείριση του κινδύνου

6.1 Μέθοδοι εκτίμησης κινδύνου

Οι μέθοδοι αξιολόγησης κινδύνου διαφέρουν σε διαφορετικούς τομείς και οργανισμούς, αλλά η μέθοδος που υιοθετείται θα πρέπει να ταιριάζει καλύτερα στη διαδικασία οργάνωσης. Οι μέθοδοι αξιολόγησης κινδύνου μπορεί να διαφέρουν μεταξύ των βιομηχανιών και εάν αφορούν γενικές οικονομικές αποφάσεις ή εκτίμηση περιβαλλοντικών, οικολογικών ή κινδύνων για τη δημόσια υγεία.

Μερικές από αυτές τις πιο χρησιμοποιούμενες μεθόδους εκτίμησης κινδύνου περιλαμβάνουν:

1. What-if analysis
2. Fault tree analysis (FTA)
3. Failure mode event analysis (FMEA)
4. Hazard operability analysis (HAZOP)
5. Incident BowTie
6. Event Tree

6.1.1 What-if analysis

Η ανάλυση What-If είναι να εντοπίσει κινδύνους, επικίνδυνες καταστάσεις ή συγκεκριμένες ακολουθίες γεγονότων που θα μπορούσαν να προκαλέσουν ανεπιθύμητες συνέπειες. Η μέθοδος μπορεί να περιλαμβάνει εξέταση πιθανών αποκλίσεων από τον σχεδιασμό, την κατασκευή, την τροποποίηση ή την πρόθεση λειτουργίας. Απαιτεί μια βασική κατανόηση της πρόθεσης της διαδικασίας, μαζί με την ικανότητα διανοητικού συνδυασμού πιθανών αποκλίσεων από την πρόθεση σχεδιασμού που θα μπορούσαν να οδηγήσουν σε ένα περιστατικό. Αυτή η τεχνική είναι πραγματικά επιτυχημένη όταν τα μέλη της ομάδας που συμμετέχουν στην ανάλυση είναι έμπειρα.

6.1.2 Fault Tree Analysis (FTA)

Είναι μια απαγωγική διαδικασία που χρησιμοποιείται για τον προσδιορισμό των διαφόρων συνδυασμών αστοχιών υλικού και λογισμικού και ανθρώπινων λαθών που θα μπορούσαν να προκαλέσουν ανεπιθύμητα συμβάντα (που αναφέρονται ως κορυφαία συμβάντα) σε επίπεδο συστήματος.

Το Fault Tree είναι ένα κατακόρυφο γραφικό μοντέλο που εμφανίζει τους διάφορους συνδυασμούς ανεπιθύμητων συμβάντων που μπορούν να οδηγήσουν σε ένα περιστατικό. Το διάγραμμα αντιπροσωπεύει την αλληλεπίδραση αυτών των αστοχιών και γεγονότων μέσα σε ένα σύστημα. Τα διαγράμματα Fault Tree είναι λογικά μπλοκ διαγράμματα που εμφανίζουν την κατάσταση ενός συστήματος (TopEvent) ως προς τις καταστάσεις των στοιχείων του (βασικά συμβάντα). Ένα διάγραμμα Fault Tree δημιουργείται από πάνω προς τα κάτω ξεκινώντας με το TopEvent (το συνολικό σύστημα) και πηγαίνοντας προς τα πίσω στο χρόνο από εκεί. Δείχνει τις διαδρομές από αυτό το TopEvent που μπορούν να οδηγήσουν σε άλλα προβλέψιμα, ανεπιθύμητα βασικά συμβάντα. Κάθε γεγονός αναλύεται ρωτώντας: «Πώς θα μπορούσε να συμβεί αυτό;» Τα μονοπάτια διασυνδέουν συνεισφέροντα συμβάντα και συνθήκες, χρησιμοποιώντας σύμβολα πύλης (AND, OR). Οι πύλες ΚΑΙ αντιπροσωπεύουν μια κατάσταση στην οποία όλα τα συμβάντα που φαίνονται κάτω από την πύλη πρέπει να υπάρχουν για να συμβεί το συμβάν που φαίνεται πάνω από την πύλη. Μια πύλη OR αντιπροσωπεύει μια κατάσταση στην οποία οποιοδήποτε από τα συμβάντα που φαίνονται κάτω από την πύλη μπορεί να οδηγήσει στο γεγονός που φαίνεται πάνω από την πύλη.

6.1.3 Failure Mode Analysis (FMEA)

Η ανάλυση συμβάντων λειτουργίας αστοχίας (FMEA) μπορεί επίσης να είναι γνωστή ως ανάλυση πιθανών τρόπων αστοχίας και επιπτώσεων, τρόποι αστοχίας, επιδράσεις και ανάλυση κρισιμότητας (FMECA).

Η ανάλυση τρόπων και επιπτώσεων αστοχίας (FMEA) είναι μια προσέγγιση βήμα προς βήμα για τον εντοπισμό όλων των πιθανών αστοχιών σε ένα σχεδιασμό, μια διαδικασία κατασκευής ή συναρμολόγησης ή ένα προϊόν ή μια υπηρεσία. Οι λειτουργίες αποτυχίας σημαίνουν τους τρόπου με τους οποίους κάτι μπορεί να αποτύχει. Οι αποτυχίες είναι τυχόν σφάλματα ή ελαττώματα, ειδικά αυτά που επηρεάζουν τον πελάτη και μπορεί να είναι πιθανά ή πραγματικά. Η ανάλυση επιπτώσεων αναφέρεται στη μελέτη των συνεπειών αυτών των αποτυχιών. Οι αποτυχίες ιεραρχούνται ανάλογα με το πόσο σοβαρές είναι οι συνέπειές τους, πόσο συχνά συμβαίνουν και πόσο εύκολα μπορούν να εντοπιστούν. Ο σκοπός του FMEA είναι να λάβει μέτρα για την εξάλειψη ή τη μείωση των αστοχιών, ξεκινώντας από αυτές που έχουν την υψηλότερη προτεραιότητα.

Η ανάλυση τρόπων αστοχίας και επιπτώσεων τεκμηριώνει επίσης τις τρέχουσες γνώσεις και ενέργειες σχετικά με τους κινδύνους αστοχιών, για χρήση στη συνεχή βελτίωση. Το FMEA χρησιμοποιείται κατά τη διάρκεια του σχεδιασμού για την αποφυγή αστοχιών. Αργότερα χρησιμοποιείται για έλεγχο, πριν και κατά τη διάρκεια της συνεχούς λειτουργίας της διαδικασίας. Στην ιδανική περίπτωση, το FMEA ξεκινά από τα πρώτα εννοιολογικά στάδια του σχεδιασμού και συνεχίζεται καθ' όλη τη διάρκεια ζωής του προϊόντος ή της υπηρεσίας.

6.1.4 Hazard Operability Analysis (HAZOP)

Η Ανάλυση Κινδύνων και Λειτουργικότητας (HAZOP) είναι μια δομημένη και συστηματική τεχνική για την εξέταση του συστήματος και τη διαχείριση κινδύνου. Συγκεκριμένα, το HAZOP χρησιμοποιείται συχνά ως τεχνική για τον εντοπισμό πιθανών κινδύνων σε ένα σύστημα και τον εντοπισμό προβλημάτων λειτουργικότητας που ενδέχεται να οδηγήσουν σε μη συμμορφούμενα προϊόντα. Το HAZOP βασίζεται σε μια θεωρία που υποθέτει ότι τα γεγονότα κινδύνου προκαλούνται από αποκλίσεις από τις προθέσεις σχεδιασμού ή λειτουργίας. Ο εντοπισμός τέτοιων αποκλίσεων διευκολύνεται με τη χρήση συνόλων «κατευθυντήριων λέξεων» ως συστηματικής λίστας προοπτικών απόκλισης. Αυτή η προσέγγιση είναι ένα μοναδικό χαρακτηριστικό της μεθοδολογίας HAZOP που βοηθά στην τόνωση της φαντασίας των μελών της ομάδας κατά την εξερεύνηση πιθανών αποκλίσεων.

6.1.5 Incident Bow Tie

Η μέθοδος ανάλυσης «Incident BowTie» συνδυάζει δύο μεθόδους ανάλυσης. Ανάλυση κινδύνου BowTie και ανάλυση περιστατικών Tripod. Η μέθοδος συγκεντρώνει τα πλεονεκτήματα και των δύο μεθόδων. Οι πληροφορίες από την ανάλυση BowTie μπορούν να χρησιμοποιηθούν ως δεδομένα για την ανάλυση περιστατικού, εξετάζοντάς την από μια ευρύτερη οπτική γωνία και διασφαλίζοντας ότι λαμβάνονται υπόψη όλα τα πιθανά σενάρια. Η είσοδος από την ανάλυση περιστατικών Tripod μπορεί να χρησιμοποιηθεί για να γίνει η ανάλυση BowTie πιο ρεαλιστική και ενημερωμένη, χρησιμοποιώντας πραγματικά δεδομένα. Δημιουργεί ένα επιπλέον επίπεδο στο διάγραμμα BowTie, καθιστώντας δυνατή την προσθήκη πιο συγκεκριμένων πληροφοριών στην ανάλυση κινδύνου. Οι δύο μέθοδοι έχουν σημαντική ομοιότητα στην τεχνική ανάλυσης. τα εμπόδια.

Και για τις δύο μεθόδους χρησιμοποιούνται φραγμοί για να δείξουν τι γίνεται για την αποτροπή περιστατικών ή συμβάντων (BowTie) ή για να δείξουν πού βρίσκονται οι αποτυχίες (Τρίποδο). Για τη δημιουργία ενός διαγράμματος «Incident BowTie», τα στοιχεία και από τις δύο μεθόδους συνδέονται στο επίπεδο των φραγμών, καθιστώντας δυνατή τη συλλογή πληροφοριών σχετικά με αυτά τα εμπόδια από δύο οπτικές γωνίες.

6.1.6 Event Tree Analysis

Η μέθοδος ανάλυσης Δέντρου Συμβάντων είναι μια επαγωγική μέθοδος από κάτω προς τα πάνω. Χρησιμοποιεί γενικές πληροφορίες για την ανάλυση συγκεκριμένων πληροφοριών. Το διάγραμμα που δημιουργείται δίνει μια οριζόντια γραφική αναπαράσταση του λογικού μοντέλου που προσδιορίζει τα πιθανά αποτελέσματα μετά από ένα συμβάν εκκίνησης. Η ακολουθία συμβάντων επηρεάζεται είτε από την επιτυχία είτε από την αποτυχία των ισχυόντων φραγμών ή των λειτουργιών/συστημάτων ασφαλείας. Η ακολουθία γεγονότων οδηγεί σε ένα σύνολο πιθανών συνεπειών. Κάθε συνδυασμός επιτυχιών ή αποτυχιών εμποδίων οδηγεί σε μια συγκεκριμένη συνέπεια ή γεγονός. Η μέθοδος μπορεί επίσης να χρησιμοποιηθεί ποσοτικά για τον υπολογισμό της πιθανότητας κάθε αποτελέσματος ή συνέπειας δίνοντας την πιθανότητα αποτυχίας κάθε φραγμού.

6.2 Εργαλεία εκτίμησης κινδύνου

6.2.1 Risk Matrix

Ο πίνακας κινδύνου είναι ένα απλό, οπτικό εργαλείο που μπορεί να χρησιμοποιηθεί για να προσδιοριστούν τα επίπεδα κινδύνου. Αν και υπάρχουν ορισμένοι περιορισμοί στους πίνακες κινδύνου – εν μέρει λόγω της απλότητάς τους – υπάρχουν πολλά οφέλη. Για όσους εργάζονται στη διαχείριση κινδύνων, καθώς και για όσους βρίσκονται σε ανώτερες θέσεις, παρέχουν μια προσβάσιμη επισκόπηση των κινδύνων που αντιμετωπίζει ένας οργανισμός, διευκολύνοντας ενδεχομένως τον τρόπο αντιμετώπισης των κινδύνων.

Όλοι οι πίνακες κινδύνου ακολουθούν την ίδια βασική δομή. Είναι συνήθως πίνακες 5x5 που δείχνουν την πιθανότητα εμφάνισης κινδύνων κατά μήκος του άξονα Y και τη σοβαρότητα των συνεπειών τους κατά μήκος του άξονα X. Κάθε άξονας ακολουθεί μια κλίμακα από πολύ χαμηλό έως πολύ υψηλό. Οι κίνδυνοι που θα μπορούσε να αντιμετωπίσει ο οργανισμός σας τοποθετούνται στη μήτρα κινδύνου ανάλογα με το πού εμπίπτουν σε αυτήν την κλίμακα. Αυτό σας βοηθά να προσδιορίσετε τα επίπεδα κινδύνου.

Πιθανότητα x Συνέπεια = Επίπεδο Κινδύνου

Εάν ο κίνδυνος είναι υψηλός στην κλίμακα πιθανότητας και υψηλός στην κλίμακα συνεπειών, μπορείτε να ορίσετε το επίπεδο κινδύνου ως πολύ υψηλό. Αντίθετα, εάν ο κίνδυνος πέσει χαμηλά στην κλίμακα πιθανότητας και χαμηλός στην κλίμακα συνεπειών, το επίπεδο κινδύνου θα ήταν πολύ χαμηλό.

Μέσα σε μια μήτρα κινδύνου, τα επίπεδα κινδύνου επισημαίνονται περαιτέρω με ένα σύστημα με χρωματική κωδικοποίηση. Ένας κίνδυνος που έχει συνολικά χαμηλό επίπεδο κινδύνου είναι ο χρωματικά κωδικοποιημένος πράσινος. Εάν είναι μεσαίο, εμφανίζεται με κίτρινο ή πορτοκαλί χρώμα. Ένας συνολικός υψηλός κίνδυνος απεικονίζεται με κόκκινο χρώμα. Αυτό το σύστημα χρωμάτων καθιστά εύκολη την γρήγορη κατανόηση των επιπέδων κινδύνου.

Παρά αυτή τη βασική δομή, οι πίνακες κινδύνου μπορεί να διαφέρουν σημαντικά ανάλογα με τον οργανισμό και τον τρόπο με τον οποίο χρησιμοποιούνται.

Για παράδειγμα, ο άξονας πιθανότητας μπορεί να χωριστεί σε πιο συγκεκριμένες κατηγορίες όπως «βέβαιο», «πιθανό», «απίθανο» και «σπάνιο». Οι κατηγορίες κατά μήκος του άξονα των συνεπειών θα μπορούσαν να ονομαστούν «πολύ χαμηλή», «χαμηλή», «μέτρια», «υψηλή» και «ακραία» ή «καταστροφική». Το πώς θα χαρακτηριστούν αυτές οι κατηγορίες εξαρτάται αποκλειστικά από τον οργανισμό.

Ας ρίξουμε μια ματιά σε ένα παράδειγμα πίνακα κινδύνου.

		Likelihood of Risk Scenario				
		Rare/Remote /Improbable	Unlikely/Seldom	Possible	Probable/Likely	Almost Certain/Frequent
Severity of Business Impact	Severe	Medium	Medium	High	Extreme	Extreme
	Large	Medium	Medium	Medium	High	Extreme
	Moderate	Low	Medium	Medium	Medium	High
	Small	Minute	Low	Medium	Medium	Medium
	Insignificant	Minute	Minute	Low	Medium	Medium

Πίνακας 5.2.1: Risk Matrix

Αρχικά, δημιουργείται μια λίστα με τις απειλές κατά του οργανισμού χωρισμένες σε κατηγορίες όπως φαίνεται στις παρακάτω εικόνες.

Risk Identifier	Risk Event Type (Level 2)	Risk Exposure (Level 1)	Risk Description	Risk Owner(s)	Risk Type
Unique identifier	*Fixed choice*	*Fixed choice*	*Free Text*	*Free text*	*Fixed choice*
RISK001	Cybercrime - Business Email Compromise	Cybercrime	Significant fraud event arising from fraudulent payment to a person impersonating a senior executive.	CFO	Cyber and IT
RISK002	Cybercrime - Ransomware	Cybercrime	Significant system downtime on customer service workstations due to an uncontrolled ransomware outbreak.	Head of Retail	Cyber and IT

Πίνακας 5.2.2: Καταχώρηση απειλών

Inherent Risk Assessment Output				Control Assessment Output	
Description of Risk and Impact	Likelihood	Impact	Inherent Risk	Existing Mitigating Controls	Control Effectiveness
Free text	*Fixed choice*	*Fixed choice*	*Calculated*	*Free text*	*Fixed choice*
We suffer a coordinated operation of multiple claims against existing retirement funds to fraudsters impersonating existing clients, based on what appears to be authentic paperwork and knowledgeable calls to our customer service line. We fail to recover the payments. Such a fraud requires a well-informed, coordinated operation.	Rare/Remote/Improbable	Large	Medium	• Payment procedures using phasing and delay mechanisms to identify potentially fraudulent claims and prevent outflow of funds. • Payment claims of greater than $100,000 must be lodged physically and identification sighted.	Effective
We suffer a significant outage to customer service workstations due to a ransomware outbreak. This inhibits our ability to serve customers effectively. There are also secondary financial and brand impacts.	Almost Certain/Frequent	Large	Extreme	• Desktop and network anti-malware software installed and updated regularly. • Forensic and diagnostics support available on demand.	Partially Effective

Πίνακας 5.2.3: Καταχώρηση απειλών

Residual Risk Assessment Output					Residual Gap
Likelihood	Impact	Residual Risk	Risk Tolerance	Frequency / Next Risk Assessment	Issues identified
ːe	*Fixed choice*	*Calculated*	*Fixed choice*	*Free text*	*Free text*
Rare/Remote/Improbable	Moderate	Low	Low	Annual	• Failure to adequately identify the claimant when not physically present. • No mechanism to detect clustering of retirement fund claims across multiple customer service staff. • Staff not trained to identify high-risk payment situations.
ːable/Likely	Large	High	Low	Annual	• No protection against Day 0-type attacks. • No early-warning system for malware tailored specifically for our systems.

Πίνακας 5.2.4: Καταχώρηση απειλών

Management Plan to Address Residual Gap					
Plan of Action & Milestones	Action Owner	Action Status	Date of Update	Target Completion Date	Actual Completion Date
ː *Text*	*Free Text*	*Fixed Choice*	*Free text*	*Free text*	*Free text*
• Modify procedures so that payment claims of greater than $25,000 must be lodged physically and identification sighted. • Modify procedures to cross-check contact and account details out of band.	SVP, Customer Service Division	Solution implemented — waiting on acceptance			1-Σεπ-23
• Extend postclaim, prepayment fraud detection capability to detect claims clustering. • Train staff to ask profiling questions.	CSO	Solution in progress			

Πίνακας 5.2.5: Καταχώρηση απειλών

Έπειτα, δημιουργείται ένας πίνακας αξιολόγησης αντικτύπου (impact assessment), όπως φαίνεται παρακάτω:

Business Impact	Financial Impact	Customer Impact	Opportunity Impact	Shareholder Impact
Severe	Insolvency, or negative profit outlook.	Complete failure of service across multiple lines of business >= 5 minutes.	We lose rights to our IP. Competitor gains first-mover advantage.	Attributable negative share price movement >= 10%.
Large	Material financial loss (as formally defined), or loss above the board-reportable threshold.	Failure (partial or complete) of service across multiple lines of business < 5 minutes, or complete failure across a single line of business >= 1 day.	Compromise of IP or trade secret, and competitor generates significant market share using it.	Attributable negative share price movement >= 5% but < 10%.
Moderate	Financial loss greater than budget allowance, requiring budget adjustment across multiple lines of business.	Partial service disruption in a single line of business >= 1 day, or total service disruption in a single line of business >= 1 hour.	Compromise of IP or trade secret, but we are able to recover through legal or other means.	Attributable negative share price movement >= 1% but < 5%.
Small	Financial loss greater than budget allowance, requiring budget adjustment within a single line of business.	Partial service disruption in a single line of business < 1 day, or total disruption in a single line of business < 1 hour, or attributable rise in daily call center load >= 20%.	Competitor gains insight into our IP and generates inferior competitive offering.	Attributable negative share price movement < 1%.
Insignificant	Financial loss within annual budget allowance.	Insignificant service disruption, or attributable rise in daily call center load < 20%.	IP or trade secret leaked prior to planned release.	Attributable negative share price movement insignificant (< 0.1%).

Πίνακας 5.2.6: Αξιολόγηση αντικτύπου

Στην συνέχεια, δημιουργείται ο πίνακας αξιολόγησης πιθανοτήτων:

Likelihood Level	Likelihood Criteria	
	Likelihood of occurrence in next 12 months	**Frequency in years**
Rare/Remote/Improbable	Less than 5%	Every 10+years
Unlikely/Seldom	5% - 20%	Every 5-10 years
Possible	20% to 50%	Every 3-5 years
Probable/Likely	50% to 80%	Every 2-3 years
Almost Certain/Frequent	Greater than 80%	Every year

Πίνακας 5.2.6: Αξιολόγησης πιθανοτήτων

Και με βάση όλες αυτές τις πληροφορίες δημιουργείται ο πίνακας κινδύνου 5.2.1 που είδαμε παραπάνω.

6.2.2 DERA (Deloitte Enterprise Risk Assessment)

Επισκόπηση

Το DERA είναι ένα διαδικτυακό, τυποποιημένο και αυτοματοποιημένο εργαλείο που χρησιμοποιείται ευρέως από τη συμβουλευτική εταιρεία ¨Deloitte¨ και επιτρέπει αξιολογήσεις κινδύνου σε έναν οργανισμό, περιλαμβάνοντας τους κινδύνους Οικονομικού Εγκλήματος, Συμμόρφωσης και λειτουργικών κινδύνων.

Προκλήσεις αξιολόγησης κινδύνου σε επιχειρηματικό επίπεδο

• Αύξηση των ρυθμιστικών προσδοκιών.
• Κόστος συμμόρφωσης.
• Ασυνεπείς και αποκεντρωμένες μέθοδοι εκτίμησης κινδύνων.
• Και οι χειροκίνητες και επιρρεπείς σε σφάλματα διαδικασίες μαστίζουν τους οργανισμούς.

Οι διπλές προσπάθειες σε τομείς λειτουργικού, τεχνολογικού, ρυθμιστικού, οικονομικού και στρατηγικού κινδύνου μπορούν να προσθέσουν επιπλέον εργασία που επιβραδύνει τη διαδικασία. Οι διαχειριστές κινδύνων συχνά δεν διαθέτουν τη διαδρομή ελέγχου και τις αυτοματοποιημένες ροές εργασίας για να γνωρίζουν ποιες αξιολογήσεις βρίσκονται στη διαδικασία, ποιες είναι εκκρεμείς, σε κίνδυνο ή ολοκληρωμένες και πότε. Αυτό καθιστά δύσκολη την απομόνωση όπου υπάρχουν μεγάλα κενά και δεν υπάρχει εύκολος τρόπος να συγκεντρωθούν οι πληροφορίες σε έναν εκτελεστικό πίνακα εργαλείων ή σε άλλες απαιτούμενες αναφορές. Αυτό που χρειάζεται είναι ένα εργαλείο που μπορεί να εξορθολογήσει τη διαδικασία αξιολόγησης κινδύνου.

Η λύση DERA είναι ένα πολυδιάστατο, σε βάθος, εργαλείο που καθοδηγεί την επιχείρηση βήμα-βήμα σε μια αξιολόγηση κινδύνου ολόκληρου του οργανισμού. Η προσέγγισή αυτή εξισορροπεί εγγενείς παράγοντες κινδύνου, ελέγχους και υπολειπόμενους παράγοντες κινδύνου, με αποτέλεσμα ένα ισχυρό σχέδιο δράσης. Οι ενσωματωμένες αναλυτικές τεχνικές βοηθούν στην αξιολόγηση των κινδύνων σε ρυθμιστικούς τομείς, τομείς συμμόρφωσης και άλλους λειτουργικούς τομείς. Γενικότερα με το εργαλείο DERA επιτυγχάνεται:

• Ο προσδιορισμός και η αξιολόγηση πιθανών κινδύνων που μπορεί να επηρεάσουν αρνητικά ολόκληρο τον οργανισμό ή ένα συγκεκριμένο προϊόν ή μια επιχειρηματική γραμμή.
• Η αξιολόγηση των ελέγχων που έχει εφαρμόσει ο οργανισμός για τον μετριασμό αυτών των πιθανών κινδύνων.
• Ο προσδιορισμός του εναπομείναντα κινδύνου που σχετίζεται με τον οργανισμό ή ένα συγκεκριμένο προϊόν ή μια επιχειρηματική γραμμή.

Το εργαλείο DERA αποτελείται από τα εξής:

Risk Dashboard

• Η DERA παρέχει μια πλατφόρμα όπως φαίνεται στην παρακάτω εικόνα για το σχεδιασμό και την εφαρμογή μιας αξιολόγησης κινδύνου σε επίπεδο επιχείρησης χρησιμοποιώντας τόσο ποσοτικά όσο και ποιοτικά μέτρα για την αξιολόγηση του κινδύνου με βάση τα προϊόντα και τις υπηρεσίες του ιδρύματος, τους πελάτες και τους υπαλλήλους, τους πωλητές και τους προμηθευτές, τα κανάλια, τις γεωγραφικές περιοχές κ.λπ.

Εικόνα 5.2.2: DERA Risk Dashboard

Survey Tracking

• Διαχειρίζεται τη διαδικασία πλήρους ροής εργασιών έρευνας - από την ανάθεση έως την ολοκλήρωση.

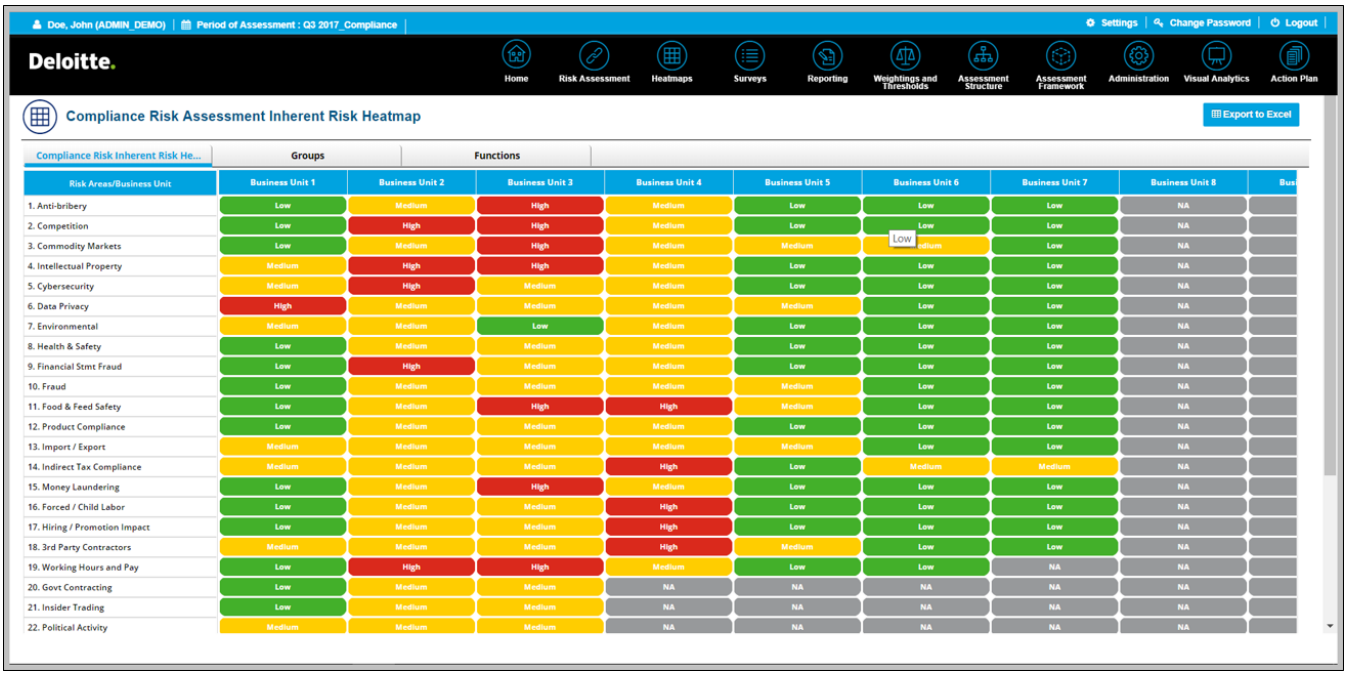
• Παρέχει παρακολούθηση ανά νομική οντότητα, τμήμα, περιοχή και επιχείρηση.

Εικόνα 5.2.2: Survey Tracking

Heatmaps

• Επιτρέπει ένα μόνο σημείο συγκέντρωσης σε κάθε επίπεδο του οργανισμού (π.χ. σειρά προϊόντων, επιχειρηματική γραμμή, νομική οντότητα, χώρα ή περιοχή).

• Εμφανίζει αποτελέσματα σε όλες τις μονάδες αξιολόγησης και σε όλες τις περιοχές κινδύνου χρησιμοποιώντας έναν χάρτη θερμότητας για όλη την επιχείρηση.



Εικόνα 5.2.2: Heatmaps

Reporting

• Διευκολύνει τη συγκεντρωτική αναφορά για να υποστηρίξει μια ολιστική άποψη του επιχειρηματικού κινδύνου και τη λήψη στρατηγικών αποφάσεων.

Δείγματα αναφορών δεδομένων δίνονται παρακάτω:

Risk Area/Regulation	Inherent Risk Rating	Controls Risk Rating	Residual Risk Rating	Residual Risk Trending Y-o-Y
Risk Area 1	Very High	Improvement needed	High	↑
Reg 2	High	Satisfactory with Exceptions	High	
Risk Area 3	High	Satisfactory with Exceptions	High	
Reg 4	Very High	Improvement needed	Moderate	
Risk Area 5	Very High	Satisfactory with Exceptions	Moderate	↓
Reg 6	Very High	Satisfactory with Exceptions	Moderate	↓
Risk Area 7	High	Improvement needed	Moderate	↓
Reg 8	High	Improvement needed	Moderate	↓
Risk Area 9	High	Improvement needed	Moderate	
Reg 10	High	Satisfactory with Exceptions	Moderate	
Risk Area 11	High	Satisfactory with Exceptions	Moderate	
Reg 12	High	Satisfactory with Exceptions	Moderate	
Risk Area 13	High	Satisfactory with Exceptions	Moderate	↓
Reg 14	High	Satisfactory with Exceptions	Moderate	↑
Risk Area 15	High	Satisfactory with Exceptions	Moderate	↓
Reg 16	High	Satisfactory with Exceptions	Moderate	
Risk Area 17	High	Satisfactory with Exceptions	Moderate	↔
Reg 18	High	Satisfactory	Moderate	
Risk Area 19	High	Satisfactory	Moderate	↓
Reg 20	High	Satisfactory	Moderate	↓
Risk Area 21	High	Satisfactory	Moderate	

Εικόνα 5.2.2: Reporting

Ut consectetur nulla vel nisi pharetra, non suscipit nisi posuere. Donec suscipit dui in arcu mollis, vel venenatis erat rutrum. Vestibulum imperdiet dolor et blandit posuere.

Override Residual Rationale
Quisque fringilla est et velit bibendum, nec pharetra turpis eleifend.

Inherent Risk Rating Drivers
Internal Inherent
Maecenas sagittis felis facilisis gravida dictum. Aenean varius purus sit amet orci consequat, ut aliquet urna pulvinar. Praesent maximus commodo dolor a facilisis. Suspendisse ornare, elit vitae cursus luctus, ante nibh vestibulum arcu, ac placerat est nunc quis purus.
External Inherent
Phasellus facilisis, orci quis laoreet fermentum, tellus ante feugiat justo, vel dapibus ipsum purus at purus. Mauris consequat eu justo a condimentum. Sed at euismod orci, ac volutpat sem. Vivamus tristique eget massa ut porttitor.

Control Type	Improvement Areas
Governance, Oversight & Staffing	Phasellus nunc massa, laoreet in ornare at, mattis at mi. Sed nisi justo, pulvinar eget interdum sit amet, ultricies id magna. Vivamus blandit, sem sit amet aliquet dapibus, mi urna hendrerit eros, nec malesuada est neque ac ipsumibero, in efficitur metus magna eu velit.
Training	Phasellus nunc massa, laoreet in ornare at, mattis at mi. Sed nisi justo, pulvinar eget interdum sit amet, ultricies id magna. Vivamus blandit, sem sit amet aliquet dapibus, mi urna hendrerit eros, nec malesuada est neque ac ipsumibero, in efficitur metus magna eu velit.
Preventive Control Activities	Phasellus nunc massa, laoreet in ornare at, mattis at mi. Sed nisi justo, pulvinar eget interdum sit amet, ultricies id magna. Vivamus blandit, sem sit amet aliquet dapibus, mi urna hendrerit eros, nec malesuada est neque ac ipsumibero, in efficitur metus magna eu velit.
Detective Controls	Phasellus nunc massa, laoreet in ornare at, mattis at mi. Sed nisi justo, pulvinar eget interdum sit amet, ultricies id magna. Vivamus blandit, sem sit amet aliquet dapibus, mi urna hendrerit eros, nec malesuada est neque ac ipsumibero, in efficitur metus magna eu velit.

	Trending Analysis		
	Inherent	Control	Residual
CRA 2017			
CRA 2018			

Control Type	Year 2017	Year 2018
Policies & Procedures		
Governance, Oversight & Staffing		
Training	NA	
Preventive Control Activities		
Detective Controls		
Control Effectiveness	NA	
Overall Control Rating		

Εικόνα 5.2.2: Detailed Summary

6.2.3 spiraPlan by Infectra

Το SpiraPlan είναι μια πλατφόρμα διαχείρισης προγραμματισμού, η ναυαρχίδα της Inflectra, που εστιάζει στη διαχείριση κινδύνου για οργανισμούς όλων των μεγεθών και από όλους τους κλάδους.

Τώρα στην 6η έκδοσή του, το SpiraPlan βοηθά τους χρήστες να ευθυγραμμίσουν τους στρατηγικούς στόχους με τις βασικές τεχνικές διαχείρισης κινδύνου και βοηθά στην παρακολούθηση του κινδύνου εντός της επιχείρησης.

Αυτή η λύση all-in-one συνδυάζει τη διαχείριση δοκιμών, την παρακολούθηση σφαλμάτων και την ιχνηλασιμότητα απαιτήσεων, με ένα πλήρες σύνολο λειτουργιών για τη διαχείριση προγραμμάτων και χαρτοφυλακίου, τον προγραμματισμό εκδόσεων, τη διαχείριση πόρων και κινδύνου.

Με το SpiraPlan, οι ομάδες μπορούν να έχουν πρόσβαση σε κινδύνους από έναν κεντρικό κόμβο – μια ενότητα για τον εντοπισμό κινδύνων, τον έλεγχο των ελλείψεων, τον προσδιορισμό των απαντήσεων και την ανάπτυξη βημάτων που μπορούν να παρακολουθηθούν μέχρι το κλείσιμο.

Στο SpiraPlan, ο κίνδυνος είναι ένας ξεχωριστός τύπος τεχνουργήματος με τους δικούς του τύπους (επιχειρηματικό, τεχνικό, χρονοδιάγραμμα, κ.λπ.), χαρακτηριστικά και ροές εργασίας. Η πλατφόρμα επιτρέπει στους χρήστες να αναλύουν και να κατηγοριοποιούν τον κίνδυνο με βάση παραμέτρους όπως η πιθανότητα, ο αντίκτυπος και η έκθεση.

Εικόνα 5.2.3: Risk Summary, spiraPlan

Με ενσωματωμένη υποστήριξη για διαδρομές ελέγχου κινδύνου, το SpiraPlan είναι ιδανικό για ομάδες που πρέπει να διατηρούν ένα επικυρωμένο σύστημα με λειτουργίες ροής εργασιών κινδύνου, συμπεριλαμβανομένων ηλεκτρονικών υπογραφών. Το τυπικό μενού αναφορών SpiraPlan επιτρέπει στους χρήστες να δημιουργούν αναφορές κινδύνου σε διάφορες μορφές.

Η διαχείριση κινδύνου σε πραγματικό χρόνο επιτυγχάνεται μέσω γραφικών στοιχείων πινάκων εργαλείων SpiraPlan: ένα μητρώο κινδύνου και έναν κύβο κινδύνου. Το SpiraPlan μπορεί να προσπελαστεί ως SaaS ή on-premise και διαθέτει περισσότερες από 60 ενσωματώσεις για να βοηθήσει τα παλαιού τύπου συστήματα και τα σύγχρονα εργαλεία να βελτιστοποιήσουν τις διαδικασίες και την επιχειρηματική τους ανάπτυξη.

7.Συμπεράσματα και μελλοντική έρευνα

7.1 Συμπεράσματα

Τα συμπεράσματα για τη διαδικασία διαχείρισης κινδύνου μπορεί να διαφέρουν ανάλογα με το συγκεκριμένο πλαίσιο και την οργάνωση. Ωστόσο, εδώ είναι μερικά κοινά και βασικά συμπεράσματα που μπορούν να εξαχθούν από τη διαδικασία διαχείρισης κινδύνου:

- *Προσδιορισμός κινδύνου*: Η διαδικασία διαχείρισης κινδύνου επιτρέπει στους οργανισμούς να εντοπίζουν και να αξιολογούν συστηματικά πιθανούς κινδύνους που θα μπορούσαν να επηρεάσουν τους στόχους τους. Αυτό βοηθά στην προληπτική αντιμετώπιση αυτών των κινδύνων και στη λήψη κατάλληλων μέτρων για τον μετριασμό ή την αποφυγή τους.
- *Εκτίμηση Κινδύνων*: Με την αξιολόγηση της πιθανότητας και του πιθανού αντίκτυπου των εντοπισμένων κινδύνων, οι οργανισμοί αποκτούν μια σαφέστερη κατανόηση του τοπίου κινδύνου τους.

Αυτή η αξιολόγηση τους επιτρέπει να ιεραρχούν τους κινδύνους με βάση τη σημασία τους, επιτρέποντας την κατανομή πόρων και προσπαθειών σε περιοχές με τον υψηλότερο δυνατό αντίκτυπο.

- *Μετριασμός κινδύνου*: Η διαδικασία διαχείρισης κινδύνου βοηθά στην ανάπτυξη και εφαρμογή αποτελεσματικών στρατηγικών μετριασμού του κινδύνου. Αυτό μπορεί να περιλαμβάνει την εφαρμογή ελέγχων, την ανάπτυξη σχεδίων έκτακτης ανάγκης, τη μεταφορά κινδύνων μέσω ασφάλισης ή την πραγματοποίηση λειτουργικών αλλαγών για την ελαχιστοποίηση της πιθανότητας ή του αντίκτυπου των εντοπισμένων κινδύνων.
- *Παρακολούθηση κινδύνου*: Η συνεχής παρακολούθηση των κινδύνων είναι ζωτικής σημασίας για να διασφαλιστεί ότι τα μέτρα μετριασμού του κινδύνου παραμένουν αποτελεσματικά και σχετικά με την πάροδο του χρόνου. Οι τακτικές αναθεωρήσεις και ενημερώσεις των προφίλ κινδύνου βοηθούν τους οργανισμούς να παραμένουν ενημερωμένοι για τις αλλαγές στο περιβάλλον κινδύνου και να ανταποκρίνονται άμεσα σε αναδυόμενους κινδύνους.
- *Επικοινωνία Κινδύνων*: Η αποτελεσματική διαχείριση κινδύνων περιλαμβάνει σαφή και έγκαιρη επικοινωνία των κινδύνων στα σχετικά ενδιαφερόμενα μέρη, συμπεριλαμβανομένων των ανώτερων στελεχών, των εργαζομένων, των πελατών και των συνεργατών. Τα συμπεράσματα που προκύπτουν από τη διαδικασία διαχείρισης κινδύνων θα πρέπει να τονίζουν τη σημασία της διαφανούς και ανοιχτής επικοινωνίας για την ενίσχυση της συνειδητοποίησης των κινδύνων και τη διασφάλιση συντονισμένης απόκρισης στους κινδύνους.
- *Κουλτούρα κινδύνου*: Η διαδικασία διαχείρισης κινδύνου συμβάλλει στην ανάπτυξη μιας κουλτούρας επίγνωσης του κινδύνου εντός του οργανισμού. Με την ενσωμάτωση της διαχείρισης κινδύνου στις διαδικασίες λήψης αποφάσεων και την προώθηση της λογοδοσίας σε όλα τα επίπεδα, οι οργανισμοί μπορούν να καλλιεργήσουν μια προορατική και ανθεκτική κουλτούρα που ενστερνίζεται τη διαχείριση κινδύνου ως βασική επιχειρηματική πρακτική.
- *Συνεχής Βελτίωση*: Η διαχείριση κινδύνου είναι μια επαναληπτική διαδικασία που απαιτεί συνεχή αξιολόγηση και βελτίωση. Τα συμπεράσματα θα πρέπει να τονίσουν την ανάγκη για περιοδικές αναθεωρήσεις του πλαισίου διαχείρισης κινδύνου, διδαχής από προηγούμενες εμπειρίες και ενσωμάτωσης διδαγμάτων για την ενίσχυση της αποτελεσματικότητας των μελλοντικών προσπαθειών διαχείρισης κινδύνου.
- *Οργανωτική ανθεκτικότητα*: Τελικά, η διαδικασία διαχείρισης κινδύνου στοχεύει στην ενίσχυση της οργανωτικής ανθεκτικότητας επιτρέποντας τον προληπτικό εντοπισμό, αξιολόγηση και μετριασμό του κινδύνου. Τα συμπεράσματα που εξάγονται θα πρέπει να τονίζουν τη σημασία της οικοδόμησης ενός ανθεκτικού οργανισμού που μπορεί να προσαρμοστεί και να ανταποκριθεί στους κινδύνους, διατηρώντας παράλληλα την ικανότητά του να επιτυγχάνει στρατηγικούς στόχους.

Να σημειωθεί ότι, αυτά τα συμπεράσματα θα πρέπει να προσαρμόζονται στον συγκεκριμένο οργανισμό και στο πλαίσιο διαχείρισης κινδύνου του, λαμβάνοντας υπόψη τις ειδικές απαιτήσεις του κλάδου και τις ρυθμιστικές εκτιμήσεις.

7.2 Μελλοντική έρευνα

Οι μελλοντικές εργασίες για τη διαχείριση κινδύνων περιλαμβάνουν την παραμονή μπροστά από τις αναδυόμενες προκλήσεις και τα εξελισσόμενα τοπία κινδύνου. Ακολουθούν ορισμένοι βασικοί τομείς εστίασης για μελλοντικές προσπάθειες διαχείρισης κινδύνου:

- *Τεχνολογικές εξελίξεις*: Καθώς η τεχνολογία συνεχίζει να προοδεύει γρήγορα, οι οργανισμοί πρέπει να είναι προετοιμασμένοι για αναδυόμενους κινδύνους που σχετίζονται με την ασφάλεια στον κυβερνοχώρο, τις παραβιάσεις δεδομένων, την τεχνητή νοημοσύνη, τον αυτοματισμό και τον ψηφιακό μετασχηματισμό. Οι μελλοντικές εργασίες για τη διαχείριση κινδύνων θα περιλαμβάνουν την ανάπτυξη ισχυρών στρατηγικών για την αντιμετώπιση αυτών των κινδύνων και τη διασφάλιση της ασφαλούς και ηθικής χρήσης της τεχνολογίας.
- *Κλιματική Αλλαγή και Περιβαλλοντικοί Κίνδυνοι*: Η αυξανόμενη αναγνώριση της κλιματικής αλλαγής και ο δυνητικός αντίκτυπός της στις επιχειρήσεις απαιτεί τη διαχείριση κινδύνων για την ενσωμάτωση περιβαλλοντικών κινδύνων. Οι μελλοντικές εργασίες θα περιλαμβάνουν την αξιολόγηση και τη διαχείριση κινδύνων που σχετίζονται με ακραία καιρικά φαινόμενα, τη σπανιότητα των πόρων, τις κανονιστικές αλλαγές και τη μετάβαση σε μια οικονομία χαμηλών εκπομπών άνθρακα.

- *Κίνδυνοι εφοδιαστικής αλυσίδας*: Η παγκοσμιοποίηση και οι διασυνδεδεμένες αλυσίδες εφοδιασμού έχουν αυξήσει την πολυπλοκότητα και την ευπάθεια των δικτύων εφοδιαστικής αλυσίδας. Οι μελλοντικές προσπάθειες διαχείρισης κινδύνου θα επικεντρωθούν στον εντοπισμό και τον μετριασμό των κινδύνων που σχετίζονται με διακοπές προμηθευτών, γεωπολιτική αστάθεια, εμπορικές συγκρούσεις και εξαρτήσεις από κρίσιμους πόρους.
- *Κανονιστική συμμόρφωση*: Τα ρυθμιστικά τοπία εξελίσσονται διαρκώς και οι οργανισμοί πρέπει να προσαρμόζουν τις πρακτικές διαχείρισης κινδύνου για να ανταποκρίνονται στις μεταβαλλόμενες απαιτήσεις συμμόρφωσης. Οι μελλοντικές εργασίες θα περιλαμβάνουν την παρακολούθηση και την κατανόηση των κανονιστικών αλλαγών, την αξιολόγηση των επιπτώσεών τους στον οργανισμό και τη διασφάλιση της συνεχούς συμμόρφωσης για την αποφυγή νομικών κινδύνων και κινδύνων για τη φήμη.
- Αναδυόμενοι Κίνδυνοι και Μαύροι Κύκνοι (Black Swans[6]): Η διαχείριση κινδύνων πρέπει να είναι ευέλικτη και προσαρμοστική για την αντιμετώπιση αναδυόμενων κινδύνων που μπορεί να μην έχουν προηγουμένως εντοπιστεί ή προβλεφθεί. Οι μελλοντικές εργασίες θα περιλαμβάνουν την ανάπτυξη συστημάτων έγκαιρης προειδοποίησης, τον σχεδιασμό σεναρίων και την καλλιέργεια μιας κουλτούρας συνειδητοποίησης κινδύνου για τον εντοπισμό και την αποτελεσματική αντιμετώπιση των αναδυόμενων κινδύνων.
- *Ανάλυση δεδομένων και μοντελοποίηση κινδύνων*: Με την αυξανόμενη διαθεσιμότητα δεδομένων και τις προόδους στα αναλυτικά στοιχεία, η διαχείριση κινδύνου μπορεί να αξιοποιήσει την προγνωστική ανάλυση και τις τεχνικές μοντελοποίησης κινδύνου για να βελτιώσει την αξιολόγηση κινδύνου και τη λήψη αποφάσεων. Οι μελλοντικές εργασίες θα περιλαμβάνουν τη χρήση γνώσεων που βασίζονται σε δεδομένα για τον εντοπισμό προτύπων, την πρόβλεψη των κινδύνων και τη βελτιστοποίηση των στρατηγικών μετριασμού του κινδύνου.
- *Ενσωμάτωση Διαχείρισης Κινδύνων Επιχειρήσεων*: Οι οργανισμοί αναγνωρίζουν την ανάγκη να ενσωματώσουν τη διαχείριση κινδύνου σε όλα τα επίπεδα και τις λειτουργίες του οργανισμού. Οι μελλοντικές εργασίες θα περιλαμβάνουν την ευθυγράμμιση της διαχείρισης κινδύνου με τα πλαίσια στρατηγικού σχεδιασμού, διαχείρισης απόδοσης και διακυβέρνησης για να διασφαλιστεί μια ολιστική και ολοκληρωμένη προσέγγιση στη διαχείριση κινδύνου.
- *Συμπεριφορικά και πολιτισμικά ζητήματα*: Η κατανόηση της ανθρώπινης συμπεριφοράς και της οργανωσιακής κουλτούρας είναι κρίσιμης σημασίας για την αποτελεσματική διαχείριση κινδύνου. Οι μελλοντικές εργασίες θα επικεντρωθούν στην αντιμετώπιση των προκαταλήψεων συμπεριφοράς, στην προώθηση κουλτούρων με επίγνωση του κινδύνου και στην ενσωμάτωση της διαχείρισης κινδύνου στις καθημερινές διαδικασίες λήψης αποφάσεων.
- *Συνεργασία*: Δεδομένης της διασυνδεδεμένης φύσης των κινδύνων, οι μελλοντικές προσπάθειες διαχείρισης κινδύνων θα δώσουν έμφαση στη συνεργασία και τις συνεργασίες με εξωτερικούς ενδιαφερόμενους φορείς, όπως ενώσεις του κλάδου, ρυθμιστικές αρχές, εμπειρογνώμονες και ομοτίμους οργανισμούς. Η ανταλλαγή βέλτιστων πρακτικών, γνώσης και εμπειριών μπορεί να βοηθήσει τους οργανισμούς να αντιμετωπίσουν συλλογικά τους κοινούς κινδύνους πιο αποτελεσματικά.
- *Συνεχής Βελτίωση και Μάθηση*: Η διαχείριση κινδύνου είναι μια συνεχής διαδικασία που απαιτεί συνεχή βελτίωση και μάθηση. Οι μελλοντικές εργασίες θα περιλαμβάνουν τη συλλογή διδαγμάτων, τη διεξαγωγή ανασκοπήσεων μετά το περιστατικό και τη βελτίωση των πρακτικών διαχείρισης κινδύνου για να διασφαλιστεί ότι οι οργανισμοί παραμένουν ανθεκτικοί και ανταποκρινόμενοι στους εξελισσόμενους κινδύνους.

Εστιάζοντας σε αυτούς τους τομείς, οι οργανισμοί μπορούν να ενισχύσουν τις ικανότητές τους διαχείρισης κινδύνων και να περιηγηθούν με σιγουριά στο όλο και πιο περίπλοκο και αβέβαιο επιχειρηματικό περιβάλλον.

[6] Black Swans: Ένας μαύρος κύκνος είναι ένα απρόβλεπτο γεγονός που είναι πέρα από αυτό που συνήθως αναμένεται από μια κατάσταση και έχει δυνητικά σοβαρές συνέπειες.

8.Βιβλιογραφία

1. Agile Project & Program Management Software - Inflectra. (n.d.). Retrieved April 27, 2023, from www.inflectra.com website: https://www.inflectra.com/SpiraPlan/default.aspx?utm_source=STH.com&utm_medium=SpiraPlan&utm_campaign=RiskManagement
2. Barton, T. L., Shenkir, W. G., & Walker, P. L. (2002). Making enterprise risk management pay off. Retrieved from https://www.semanticscholar.org/paper/c7212b388c96671b9671010d3ff61165100cbd3b
3. Claude, M., Khushbu, P., & Deepti, G. (2021, May 6). Toolkit: Sample IT Risk Register. Retrieved March 28, 2023, from Gartner website: https://www.gartner.com/en/documents/2346515
4. Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce. (2019). Publications | CSRC. Retrieved from Nist.gov website: https://csrc.nist.gov/publications
5. Culp, S. (2020, October 20). Why Risk Management Is More Important Than Ever. Retrieved August 29, 2022, from Forbes website: https://www.forbes.com/sites/steveculp/2020/10/01/why-risk-management-is-more-important-than-ever/?sh=3333434430b6
6. Deloitte. (n.d.). A Web-based Enterprise Risk Assessment Solution – DERA. Retrieved March 28, 2023, from Deloitte United States website: https://www2.deloitte.com/us/en/pages/advisory/solutions/enterprise-risk-assessment-solution-dera.html
7. Dickinson, G. D. (2001). Enterprise risk management: Its origins and conceptual foundation. *The Geneva Papers on Risk and Insurance - Issues and Practice*, *26*, 360–366. https://doi.org/10.1111/1468-0440.00121
8. Fenz, S., Heurix, J., & and Pechstein, T. (2014). *Current challenges in information security risk management* (Vol. 22, pp. 410–430). Emerald Group Publishing Limited. Retrieved from https://doi.org/10.1108/IMCS-07-2013-0053
9. Fikri, A., Putra, F., Suryanto, Y., & Ramli, K. (2019). Risk Assessment Using NIST SP 80030 Revision 1 and ISO 27005 Combination Technique in ProfitBased Organization: Case Study of ZZZ Information System Application in ABC Agency. *Procedia Computer Science*, *161*, 1206–1215. https://doi.org/10.1016/j.procs.2019.11.234
10. Gordon, L. A., Loeb, M. P., & Tseng, C.-Y. (2009). Enterprise risk management and firm performance: A contingency perspective. *Journal of Accounting and Public Policy*, *28*, 301–327. https://doi.org/10.1016/J.JACCPUBPOL.2009.06.006
11. Hoyt, R., & Liebenberg, A. P. (2010). The value of enterprise risk management. *ERN: Other IO: Empirical Studies of Firms & Markets (Topic)*, *null*, null. https://doi.org/10.1111/j.1539-6975.2011.01413.x
12. ISO - International Organization for Standardization. (2019a, January 10). ISO/IEC 27005:2018. Retrieved from ISO website: https://www.iso.org/standard/75281.html
13. ISO - International Organization for Standardization. (2019b, February 4). ISO/IEC 27002:2013. Retrieved from ISO website: https://www.iso.org/standard/54533.html
14. ISO - International Organization for Standardization. (2019c, August 6). ISO/IEC 27001:2013. Retrieved from ISO website: https://www.iso.org/standard/54534.html
15. ISO 27005 | IT Governance UK. (2016). Retrieved from Itgovernance.co.uk website: https://www.itgovernance.co.uk/iso27005
16. Kaplan, R. S., & Mikes, A. (2012, June). Managing Risks: A New Framework. Retrieved from Harvard Business Review website: https://hbr.org/2012/06/managing-risks-a-new-framework
17. Κάτσικας, Σ., Γκρίτζαλης, Δ., & Γκρίτζαλης, Σ. (n.d.). Ανάλυση, Αποτίμηση και Διαχείριση Επικινδυνότητας Π.Σ. - (Στηρίζεται στο κεφ. 11 "Ανάλυση, Αποτίμηση και Διαχείριση Επικινδυνότητας ΠΣ" από το βιβλίο 'Ασφάλεια Πληροφοριακών Συστημάτων»). Retrieved from docplayer.gr website: https://docplayer.gr/32787151-Analysi-apotimisi-kai-diaheirisi-epikindynotitas-p-s.html

18. Kremljak, Z., & Kafol, C. (2014). Types of Risk in a System Engineering Environment and Software Tools for Risk Analysis. *24th DAAAM International Symposium on Intelligent Manufacturing and Automation, 2013*, *69*, 177–183. https://doi.org/10.1016/j.proeng.2014.02.218
19. L. Meulbroek. (2002). The promise and challenge of integrated risk management. *Risk Management and Insurance Review*, *5*, 55–66. https://doi.org/10.1111/1098-1616.00006
20. Lam, J. (2003). Enterprise risk management: From incentives to controls. Retrieved from https://www.semanticscholar.org/paper/217614e7bf2d99caa4f75502b2fead07002c9f4a
21. Liebenberg, A. P., & Hoyt, R. (2003). The determinants of enterprise risk management: Evidence from the appointment of chief risk officers. *SPGMI: Compustat Fundamentals (Topic)*, *null*, null. https://doi.org/10.1111/1098-1616.00019
22. Meulbroek, L. K. (2002). A SENIOR MANAGER'S GUIDE TO INTEGRATED RISK MANAGEMENT. *Journal of Applied Corporate Finance*, *14*, 56–70. https://doi.org/10.1111/j.1745-6622.2002.tb00449.x
23. Ni, H., Chen, A., & Chen, N. (2010). Some extensions on risk matrix approach. *Safety Science*, *48*(10), 1269–1278. https://doi.org/10.1016/j.ssci.2010.04.005
24. NIST. (2000). National Institute of Standards and Technology | NIST. Retrieved from NIST website: https://www.nist.gov/
25. Nocco, B. W., & Stulz, R. M. (2006). Enterprise risk management: Theory and practice. *Risk Management & Analysis in Financial Institutions EJournal*, *null*, null. https://doi.org/10.2139/ssrn.921402
26. RoldánMolina, G., AlmacheCueva, M., SilvaRabadão, C., Yevseyeva, I., & BastoFernandes, V. (2017). A Comparison of Cybersecurity Risk Analysis Tools. *CENTERIS 2017International Conference on ENTERprise Information Systems / ProjMAN 2017International Conference on Project MANagement / HCist 2017International Conference on Health and Social Care Information Systems and Technologies, CENTERIS/ProjMAN/HCist 2017*, *121*, 568–575. https://doi.org/10.1016/j.procs.2017.11.075
27. Ross, R. S. (2012, September 17). Guide for Conducting Risk Assessments. Retrieved from NIST website: https://www.nist.gov/publications/guide-conducting-risk-assessments
28. T. Aabo, Fraser, J., & Simkins, B. (2004). The rise and evolution of the chief risk officer: Enterprise risk management at hydro one. *Risk Management EJournal*, *null*, null. https://doi.org/10.1111/J.1745-6622.2005.00045.X

9.Παραρτήματα

Παράρτημα D

Αυτό το παράρτημα παρέχει: i) περιγραφή των δυνητικά χρήσιμων εισροών για την εργασία εντοπισμού πηγής απειλής, ii) μια υποδειγματική ταξινόμηση των πηγών απειλής ανά τύπο, περιγραφή και παράγοντες κινδύνου (δηλαδή χαρακτηριστικά) που χρησιμοποιούνται για την αξιολόγηση της πιθανότητας ή/και του αντίκτυπου αυτών των πηγών απειλής να προκαλέσουν γεγονότα απειλής, iii) ένα υποδειγματικό σύνολο προσαρμοσμένων κλιμάκων αξιολόγησης για την αξιολόγηση αυτών των παραγόντων κινδύνου και iv) υποδείγματα για τη σύνοψη και τεκμηρίωση των αποτελεσμάτων της εργασίας 2-1 εντοπισμού πηγής απειλής. Η ταξινόμηση και οι κλίμακες αξιολόγησης στο παρόν προσάρτημα μπορούν να χρησιμοποιηθούν από τους οργανισμούς ως σημείο εκκίνησης με κατάλληλη προσαρμογή για την προσαρμογή στις συνθήκες του εκάστοτε οργανισμού. Οι πίνακες D-7 και D-8, αποτελέσματα της Εργασίας 2-1, παρέχουν σχετικές εισροές στους πίνακες κινδύνου του Παραρτήματος Ι.

Description	Provided To		
	Tier 1	Tier 2	Tier 3

From Tier 1: (Organization level)
- Sources of threat information deemed to be credible (e.g., open source and/or classified threat reports, previous risk/threat assessments). (**Section 3.1**, **Task 1-4**)
- Threat source information and guidance specific to Tier 1 (e.g., threats related to organizational governance, core missions/business functions, management/operational policies, procedures, and structures, external mission/business relationships).
- Taxonomy of threat sources, annotated by the organization, if necessary. (**Table D-2**)
- Characterization of adversarial and non-adversarial threat sources.
  - Assessment scales for assessing adversary capability, intent, and targeting, annotated by the organization, if necessary. (**Table D-3, Table D-4, Table D-5**)
  - Assessment scale for assessing the range of effects, annotated by the organization, if necessary. (**Table D-6**)
- Threat sources identified in previous risk assessments, if appropriate.
	No	Yes	Yes
			if not provided by Tier 2

From Tier 2: (Mission/business process level) - Threat source information and guidance specific to Tier 2 (e.g., threats related to mission/business processes, EA segments, common infrastructure, support services, common controls, and external dependencies). - Mission/business process-specific characterization of adversarial and non-adversarial threat sources.	Yes *via RAR*	Yes *via peer sharing*	Yes
From Tier 3: (Information system level) - Threat source information and guidance specific to Tier 3 (e.g., threats related to information systems, information technologies, information system components, applications, networks, environments of operation). - Information system-specific characterization of adversarial and non-adversarial threat sources.	Yes *via RAR*	Yes *via RAR*	Yes *via peer sharing*

Πίνακας 8.1: Παράρτημα D-1-Εισροές-Αναγνώριση πηγών απειλής

Type of Threat Source	Description	Characteristics

ADVERSARIAL
- Individual
  - Outsider
  - Insider
  - Trusted Insider
  - Privileged Insider
- Group
  - Ad hoc
  - Established
- Organization
  - Competitor
  - Supplier
  - Partner
  - Customer
- Nation-State
	Individuals, groups, organizations, or states that seek to exploit the organization's dependence on cyber resources (i.e., information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies).	Capability, Intent, Targeting

ACCIDENTAL - User - Privileged User/Administrator	Erroneous actions taken by individuals in the course of executing their everyday responsibilities.	Range of effects

STRUCTURAL
- Information Technology (IT) Equipment
  - Storage
  - Processing
  - Communications
  - Display
  - Sensor
  - Controller
- Environmental Controls
  - Temperature/Humidity Controls
  - Power Supply
- Software
  - Operating System
  - Networking
  - General-Purpose Application
  - Mission-Specific Application
	Failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances which exceed expected operating parameters.	Range of effects

ENVIRONMENTAL
- Natural or man-made disaster
  - Fire
  - Flood/Tsunami
  - Windstorm/Tornado
  - Hurricane
  - Earthquake
  - Bombing
  - Overrun
- Unusual Natural Event (e.g., sunspots)
- Infrastructure Failure/Outage
  - Telecommunications
  - Electrical Power
	Natural disasters and failures of critical infrastructures on which the organization depends, but which are outside the control of the organization.
	Note: Natural and man-made disasters can also be characterized in terms of their severity and/or duration. However, because the threat source and the threat event are strongly identified, severity and duration can be included in the description of the threat event (e.g., Category 5 hurricane causes extensive damage to the facilities housing mission-critical systems, making those systems unavailable for three weeks).
		Range of effects

Πίνακας 8.2:Παράρτημα D-2-Ταξινόμηση πηγών απειλής

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The adversary has a very sophisticated level of expertise, is well-resourced, and can generate opportunities to support multiple successful, continuous, and coordinated attacks.
High	80-95	8	The adversary has a sophisticated level of expertise, with significant resources and opportunities to support multiple successful coordinated attacks.
Moderate	21-79	5	The adversary has moderate resources, expertise, and opportunities to support multiple successful attacks.
Low	5-20	2	The adversary has limited resources, expertise, and opportunities to support a successful attack.
Very Low	0-4	0	The adversary has very limited resources, expertise, and opportunities to support a successful attack.

Πίνακας 8.3:Παράρτημα D-3-Κλίμακα αξιολόγησης-Χαρακτηριστικά ικανότητας επιτιθέμενου

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The adversary seeks to undermine, severely impede, or destroy a core mission or business function, program, or enterprise by exploiting a presence in the organization's information systems or infrastructure. The adversary is concerned about disclosure of tradecraft only to the extent that it would impede its ability to complete stated goals.
High	80-95	8	The adversary seeks to undermine/impede critical aspects of a core mission or business function, program, or enterprise, or place itself in a position to do so in the future, by maintaining a presence in the organization's information systems or infrastructure. The adversary is very concerned about minimizing attack detection/disclosure of tradecraft, particularly while preparing for future attacks.
Moderate	21-79	5	The adversary seeks to obtain or modify specific critical or sensitive information or usurp/disrupt the organization's cyber resources by establishing a foothold in the organization's information systems or infrastructure. The adversary is concerned about minimizing attack detection/disclosure of tradecraft, particularly when carrying out attacks over long time periods. The adversary is willing to impede aspects of the organization's missions/business functions to achieve these ends.
Low	5-20	2	The adversary actively seeks to obtain critical or sensitive information or to usurp/disrupt the organization's cyber resources, and does so without concern about attack detection/disclosure of tradecraft.
Very Low	0-4	0	The adversary seeks to usurp, disrupt, or deface the organization's cyber resources, and does so without concern about attack detection/disclosure of tradecraft.

Πίνακας 8.4:Παράρτημα D-4-Χαρακτηριστικά πρόθεσης επιτιθέμενου

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The adversary analyzes information obtained via reconnaissance and attacks to target persistently a specific organization, enterprise, program, mission or business function, focusing on specific high-value or mission-critical information, resources, supply flows, or functions; specific employees or positions; supporting infrastructure providers/suppliers; or partnering organizations.
High	80-95	8	The adversary analyzes information obtained via reconnaissance to target persistently a specific organization, enterprise, program, mission or business function, focusing on specific high-value or mission-critical information, resources, supply flows, or functions, specific employees supporting those functions, or key positions.
Moderate	21-79	5	The adversary analyzes publicly available information to target persistently specific high-value organizations (and key positions, such as Chief Information Officer), programs, or information.
Low	5-20	2	The adversary uses publicly available information to target a class of high-value organizations or information, and seeks targets of opportunity within that class.
Very Low	0-4	0	The adversary may or may not target any specific organizations or classes of organizations.

Πίνακας 8.5: Παράρτημα D-5: Χαρακτηριστικά στόχου επιτιθέμενου

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The effects of the error, accident, or act of nature are **sweeping**, involving almost all of the cyber resources of the [Tier 3: information systems; Tier 2: mission/business processes or EA segments, common infrastructure, or support services; Tier 1: organization/governance structure].
High	80-95	8	The effects of the error, accident, or act of nature are **extensive**, involving most of the cyber resources of the [Tier 3: information systems; Tier 2: mission/business processes or EA segments, common infrastructure, or support services; Tier 1: organization/governance structure], including many critical resources.
Moderate	21-79	5	The effects of the error, accident, or act of nature are **wide-ranging**, involving a significant portion of the cyber resources of the [Tier 3: information systems; Tier 2: mission/business processes or EA segments, common infrastructure, or support services; Tier 1: organization/governance structure], including some critical resources.
Low	5-20	2	The effects of the error, accident, or act of nature are **limited**, involving some of the cyber resources of the [Tier 3: information systems; Tier 2: mission/business processes or EA segments, common infrastructure, or support services; Tier 1: organization/governance structure], but involving no critical resources.
Very Low	0-4	0	The effects of the error, accident, or act of nature are **minimal,** involving few if any of the cyber resources of the [Tier 3: information systems; Tier 2: mission/business processes or EA segments, common infrastructure, or support services; Tier 1: organization/governance structure], and involving no critical resources.

Πίνακας 8.6:Παράρτημα D-6-Κλίμακα αξιολόγησης-Εύρος αποτελεσμάτων για μη αντίπαλες πηγές απειλών

Identifier	Threat Source Source of Information	In Scope	Capability	Intent	Targeting
Organization -defined	Table D-2 and Task 1-4 or Organization-defined	Yes / No	Table D-3 or Organization -defined	Table D-4 or Organization -defined	Table D-5 or Organization -defined

Πίνακας 8.7:Παράρτημα D-7-Πίνακας-αναγνώριση εχθρικών πηγών απειλών

Identifier	Threat Source Source of Information	In Scope	Range of Effects
Organization -defined	Table D-2 and Task 1-4 or Organization-defined	Yes / No	Table D-6 or Organization-defined

Πίνακας 8.8:Παράρτημα D-8-Πίνακας-αναγνώριση μη-εχθρικών πηγών απειλών

Παράρτημα Ε

Το παρόν παράρτημα παρέχει: (i) περιγραφή των δυνητικά χρήσιμων εισροών για την εργασία προσδιορισμού γεγονότων απειλής, (ii) αντιπροσωπευτικά παραδείγματα γεγονότων απειλής που εκφράζονται ως τακτικές, τεχνικές και διαδικασίες (TTP) και μη απειλητικά γεγονότα απειλής, (iii) μια υποδειγματική κλίμακα αξιολόγησης της συνάφειας αυτών των γεγονότων απειλής και (iv) υποδείγματα για τη σύνοψη και τεκμηρίωση των αποτελεσμάτων της εργασίας 2-2 προσδιορισμού απειλής. Οι οργανισμοί μπορούν να εξαλείψουν ορισμένα συμβάντα απειλής από την περαιτέρω εξέταση, εάν δεν έχει εντοπιστεί αντίπαλος με τις απαραίτητες ικανότητες. Οι οργανισμοί μπορούν επίσης να τροποποιήσουν τα συμβάντα απειλής που παρέχονται για να περιγράψουν συγκεκριμένες TTPs με επαρκή λεπτομέρεια και στο κατάλληλο επίπεδο ταξινόμησης. Οι οργανισμοί μπορούν να χρησιμοποιήσουν τα αντιπροσωπευτικά συμβάντα απειλής και τις προβλεπόμενες/αναμενόμενες τιμές για τη συνάφεια των εν λόγω συμβάντων ως σημείο εκκίνησης με προσαρμογή για την προσαρμογή σε

τυχόν ειδικές συνθήκες του οργανισμού. Ο πίνακας E-5, αποτέλεσμα της εργασίας 2-2, παρέχει σχετικές εισροές για τους πίνακες κινδύνου στο προσάρτημα I.

Description	Provided To		
	Tier 1	Tier 2	Tier 3
From Tier 1: (Organization level) - Sources of threat information deemed to be credible (e.g., open source and/or classified threat reports, previous risk/threat assessments. (**Section 3.1, Task 1-4**.) - Threat event information and guidance specific to Tier 1 (e.g., threats related to organizational governance, core missions/business functions, external mission/business relationships, management/operational policies, procedures, and structures). - Exemplary adversarial threat events, annotated by the organization, if necessary. (**Table E-2**) - Exemplary non-adversarial threat events, annotated by the organization, if necessary. (**Table E-3**) - Assessment scale for assessing the relevance of threat events, annotated by the organization, if necessary. (**Table E-4**) - Threat events identified in previous risk assessments, if appropriate.	No	Yes	Yes *If not provided by Tier 2*
From Tier 2: (Mission/business process level) - Threat event information and guidance specific to Tier 2 (e.g., threats related to mission/business processes, EA segments, common infrastructure, support services, common controls, and external dependencies). - Mission/business process-specific characterization of adversarial and non-adversarial threat events.	Yes *Via RAR*	Yes *Via Peer Sharing*	Yes
From Tier 3: (Information system level) - Threat event information and guidance specific to Tier 3 (e.g., threats related to information systems, information technologies, information system components, applications, networks, environments of operation). - Information system-specific characterization of adversarial and non-adversarial threat events. - Incident reports.	Yes *Via RAR*	Yes *Via RAR*	Yes *Via Peer Sharing*

Πίνακας 8.9:Παράρτημα E-1-Εισροές-Αναγνώριση συμβάντων απειλής

Threat Events (Characterized by TTPs)	Description
Perform reconnaissance and gather information.	
Perform perimeter network reconnaissance/scanning.	Adversary uses commercial or free software to scan organizational perimeters to obtain a better understanding of the information technology infrastructure and improve the ability to launch successful attacks.
Perform network sniffing of exposed networks.	Adversary with access to exposed wired or wireless data channels used to transmit information, uses network sniffing to identify components, resources, and protections.
Gather information using open source discovery of organizational information.	Adversary mines publically accessible information to gather information about organizational information systems, business processes, users or personnel, or external relationships that the adversary can subsequently employ in support of an attack.
Perform reconnaissance and surveillance of targeted organizations.	Adversary uses various means (e.g., scanning, physical observation) over time to examine and assess organizations and ascertain points of vulnerability.
Perform malware-directed internal reconnaissance.	Adversary uses malware installed inside the organizational perimeter to identify targets of opportunity. Because the scanning, probing, or observation does not cross the perimeter, it is not detected by externally placed intrusion detection systems.
Craft or create attack tools.	
Craft phishing attacks.	Adversary counterfeits communications from a legitimate/trustworthy source to acquire sensitive information such as usernames, passwords, or SSNs. Typical attacks occur via email, instant messaging, or comparable means; commonly directing users to websites that appear to be legitimate sites, while actually stealing the entered information.
Craft spear phishing attacks.	Adversary employs phishing attacks targeted at high value targets (e.g., senior leaders/executives).
Craft attacks specifically based on deployed information technology environment.	Adversary develops attacks (e.g., crafts targeted malware) that take advantage of adversary knowledge of the organizational information technology environment.
Create counterfeit/spoof website.	Adversary creates duplicates of legitimate websites; when users visit a counterfeit site, the site can gather information or download malware.
Craft counterfeit certificates.	Adversary counterfeits or compromises a certificate authority, so that malware or connections will appear legitimate.
Create and operate false front organizations to inject malicious components into the supply chain.	Adversary creates false front organizations with the appearance of legitimate suppliers in the critical life-cycle path that then inject corrupted/malicious information system components into the organizational supply chain.
Deliver/insert/install malicious capabilities.	
Deliver known malware to internal organizational information systems (e.g., virus via email).	Adversary uses common delivery mechanisms (e.g., email) to install/insert known malware (e. g., malware whose existence is known) into organizational information systems.
Deliver modified malware to internal organizational information systems.	Adversary uses more sophisticated delivery mechanisms than email (e.g., web traffic, instant messaging, FTP) to deliver malware and possibly modifications of known malware to gain access to internal organizational information systems.
Deliver targeted malware for control of internal systems and exfiltration of data.	Adversary installs malware that is specifically designed to take control of internal organizational information systems, identify sensitive information, exfiltrate the information back to adversary, and conceal these actions.
Deliver malware by providing removable media.	Adversary places removable media (e.g., flash drives) containing malware in locations external to organizational physical perimeters but where employees are likely to find the media (e.g., facilities parking lots, exhibits at conferences attended by employees) and use it on organizational information systems.

Πίνακας 8.10:Παράρτημα Ε-2-Περιληπτικά αντιπροσωπευτικά παραδείγματα-Εχθρικά συμβάντα απειλής

Threat Event	Description
Spill sensitive information	Authorized user erroneously contaminates a device, information system, or network by placing on it or sending to it information of a classification/sensitivity which it has not been authorized to handle. The information is exposed to access by unauthorized individuals, and as a result, the device, system, or network is unavailable while the spill is investigated and mitigated.
Mishandling of critical and/or sensitive information by authorized users	Authorized privileged user inadvertently exposes critical/sensitive information.
Incorrect privilege settings	Authorized privileged user or administrator erroneously assigns a user exceptional privileges or sets privilege requirements on a resource too low.
Communications contention	Degraded communications performance due to contention.
Unreadable display	Display unreadable due to aging equipment.
Earthquake at primary facility	Earthquake of organization-defined magnitude at primary facility makes facility inoperable.
Fire at primary facility	Fire (not due to adversarial activity) at primary facility makes facility inoperable.
Fire at backup facility	Fire (not due to adversarial activity) at backup facility makes facility inoperable or destroys backups of software, configurations, data, and/or logs.
Flood at primary facility	Flood (not due to adversarial activity) at primary facility makes facility inoperable.
Flood at backup facility	Flood (not due to adversarial activity) at backup facility makes facility inoperable or destroys backups of software, configurations, data, and/or logs.
Hurricane at primary facility	Hurricane of organization-defined strength at primary facility makes facility inoperable.
Hurricane at backup facility	Hurricane of organization-defined strength at backup facility makes facility inoperable or destroys backups of software, configurations, data, and/or logs.
Resource depletion	Degraded processing performance due to resource depletion.
Introduction of vulnerabilities into software products	Due to inherent weaknesses in programming languages and software development environments, errors and vulnerabilities are introduced into commonly used software products.
Disk error	Corrupted storage due to a disk error.
Pervasive disk error	Multiple disk errors due to aging of a set of devices all acquired at the same time, from the same supplier.
Windstorm/tornado at primary facility	Windstorm/tornado of organization-defined strength at primary facility makes facility inoperable.
Windstorm/tornado at backup facility	Windstorm/tornado of organization-defined strength at backup facility makes facility inoperable or destroys backups of software, configurations, data, and/or logs.

Πίνακας 8.11:Παράρτημα E-3:Αντιπροσωπευτικά παραδείγματα-Μη εχθρικά συμβάντα απειλής

Value	Description
Confirmed	The threat event or TTP has been seen by the organization.
Expected	The threat event or TTP has been seen by the organization's peers or partners.
Anticipated	The threat event or TTP has been reported by a trusted source.
Predicted	The threat event or TTP has been predicted by a trusted source.
Possible	The threat event or TTP has been described by a somewhat credible source.
N/A	The threat event or TTP is not currently applicable. For example, a threat event or TTP could assume specific technologies, architectures, or processes that are not present in the organization, mission/business process, EA segment, or information system; or predisposing conditions that are not present (e.g., location in a flood plain). Alternately, if the organization is using detailed or specific threat information, a threat event or TTP could be deemed inapplicable because information indicates that no adversary is expected to initiate the threat event or use the TTP.

Πίνακας 8.12:Παράρτημα E-4-Σχετικότητα συμβάντων απειλής

Identifier	Threat Event Source of Information	Threat Source	Relevance
Organization -defined	Table E-2, Table E-3, Task 1-4 or Organization-defined	Table D-7, Table D-8 or Organization-defined	Table E-4 or Organization-defined

Πίνακας 8.13:Παράρτημα E-5: Πίνακας-αναγνώριση συμβάντων απειλής

Παράρτημα F

Το παράρτημα αυτό παρέχει: (i) περιγραφή των δυνητικά χρήσιμων εισροών για την εργασία εντοπισμού ευπαθειών και προδιαθεσικών συνθηκών, (ii) μια υποδειγματική ταξινόμηση προδιαθεσικών συνθηκών- (iii) υποδειγματικές κλίμακες αξιολόγησης για την αξιολόγηση της σοβαρότητας των ευπαθειών και της διάχυσης των προδιαθεσικών συνθηκών, και (iv) ένα σύνολο υποδειγμάτων για τη σύνοψη και τεκμηρίωση των αποτελεσμάτων της εργασίας εντοπισμού ευπαθειών και προδιαθεσικών συνθηκών. Η ταξινομία και οι κλίμακες αξιολόγησης στο παρόν προσάρτημα μπορούν να χρησιμοποιηθούν από τους οργανισμούς ως σημείο εκκίνησης με κατάλληλη προσαρμογή για την προσαρμογή σε τυχόν ειδικές συνθήκες του οργανισμού. Οι πίνακες F-3 και F-6, αποτελέσματα της εργασίας 2-3, παρέχουν σχετικές εισροές για τους πίνακες κινδύνου στο παράρτημα I.

Description	Provided To		
	Tier 1	Tier 2	Tier 3

From Tier 1 (Organization level)
- Sources of vulnerability information deemed to be credible (e.g., open source and/or classified vulnerabilities, previous risk/vulnerability assessments, Mission and/or Business Impact Analyses). (**Section 3.1, Task 1-4.**)
- Vulnerability information and guidance specific to Tier 1 (e.g., vulnerabilities related to organizational governance, core missions/business functions, management/operational policies, procedures, and structures, external mission/business relationships).
- Taxonomy of predisposing conditions, annotated by the organization, if necessary. (**Table F-4**)
- Characterization of vulnerabilities and predisposing conditions.
  - Assessment scale for assessing the severity of vulnerabilities, annotated by the organization, if necessary. (**Table F-2**)
  - Assessment scale for assessing the pervasiveness of predisposing conditions, annotated by the organization, if necessary. (**Table F-5**)
  - Business Continuity Plan, Continuity of Operations Plan for the organization, if such plans are defined for the entire organization.
	No	Yes	Yes
			If not provided by Tier 2

From Tier 2: (Mission/business process level) - Vulnerability information and guidance specific to Tier 2 (e.g., vulnerabilities related to organizational mission/business processes, EA segments, common infrastructure, support services, common controls, and external dependencies). - Business Continuity Plans, Continuity of Operations Plans for mission/business processes, if such plans are defined for individual processes or business units.	Yes *Via RAR*	Yes *Via Peer Sharing*	Yes
From Tier 3: (Information system level) - Vulnerability information and guidance specific to Tier 3 (e.g., vulnerabilities related to information systems, information technologies, information system components, applications, networks, environments of operation). - Security assessment reports (i.e., deficiencies in assessed controls identified as vulnerabilities). - Results of monitoring activities (e.g., automated and nonautomated data feeds). - Vulnerability assessments, Red Team reports, or other reports from analyses of information systems, subsystems, information technology products, devices, networks, or applications. - Contingency Plans, Disaster Recovery Plans, Incident Reports. - Vendor/manufacturer vulnerability reports.	Yes *Via RAR*	Yes *Via RAR*	Yes *Via Peer Sharing*

Πίνακας 8.14:Παράρτημα F-1: Εισροές-Ευπάθειες και προδιαθεσικές συνθήκες

TABLE F-2: ASSESSMENT SCALE – VULNERABILITY SEVERITY

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The vulnerability is exposed and exploitable, and its exploitation could result in severe impacts. Relevant security control or other remediation is not implemented and not planned; or no security measure can be identified to remediate the vulnerability.
High	80-95	8	The vulnerability is of high concern, based on the exposure of the vulnerability and ease of exploitation and/or on the severity of impacts that could result from its exploitation. Relevant security control or other remediation is planned but not implemented; compensating controls are in place and at least minimally effective.
Moderate	21-79	5	The vulnerability is of moderate concern, based on the exposure of the vulnerability and ease of exploitation and/or on the severity of impacts that could result from its exploitation. Relevant security control or other remediation is partially implemented and somewhat effective.
Low	5-20	2	The vulnerability is of minor concern, but effectiveness of remediation could be improved. Relevant security control or other remediation is fully implemented and somewhat effective.
Very Low	0-4	0	The vulnerability is not of concern. Relevant security control or other remediation is fully implemented, assessed, and effective.

TABLE F-3: TEMPLATE – IDENTIFICATION OF VULNERABILITIES

Identifier	Vulnerability Source of Information	Vulnerability Severity
Organization-defined	Task 2-3, Task 1-4 or Organization-defined	Table F-2 or Organization-defined

Πίνακας 8.14:Παράρτηματα F-2,F-3-Σοβαρότητα και αναγνώριση ευπαθειών

TABLE F-4: TAXONOMY OF PREDISPOSING CONDITIONS

Type of Predisposing Condition	Description
INFORMATION-RELATED - Classified National Security Information - Compartments - Controlled Unclassified Information - Personally Identifiable Information - Special Access Programs - Agreement-Determined - NOFORN - Proprietary	Needs to handle information (as it is created, transmitted, stored, processed, and/or displayed) in a specific manner, due to its sensitivity (or lack of sensitivity), legal or regulatory requirements, and/or contractual or other organizational agreements.
TECHNICAL - Architectural - Compliance with technical standards - Use of specific products or product lines - Solutions for and/or approaches to user-based collaboration and information sharing - Allocation of specific security functionality to common controls - Functional - Networked multiuser - Single-user - Stand-alone / nonnetworked - Restricted functionality (e.g., communications, sensors, embedded controllers)	Needs to use technologies in specific ways.
OPERATIONAL / ENVIRONMENTAL - Mobility - Fixed-site (specify location) - Semi-mobile - Land-based, Airborne, Sea-based, Space-based - Mobile (e.g., handheld device) - Population with physical and/or logical access to components of the information system, mission/business process, EA segment - Size of population - Clearance/vetting of population	Ability to rely upon physical, procedural, and personnel controls provided by the operational environment.

TABLE F-5: ASSESSMENT SCALE – PERVASIVENESS OF PREDISPOSING CONDITIONS

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Applies to **all** organizational missions/business functions (Tier 1), mission/business processes (Tier 2), or information systems (Tier 3).
High	80-95	8	Applies to **most** organizational missions/business functions (Tier 1), mission/business processes (Tier 2), or information systems (Tier 3).
Moderate	21-79	5	Applies to **many** organizational missions/business functions (Tier 1), mission/business processes (Tier 2), or information systems (Tier 3).
Low	5-20	2	Applies to **some** organizational missions/business functions (Tier 1), mission/business processes (Tier 2), or information systems (Tier 3).
Very Low	0-4	0	Applies to **few** organizational missions/business functions (Tier 1), mission/business processes (Tier 2), or information systems (Tier 3).

Πίνακας 8.15:Παράρτηματα F-4,F-5-Προδιαθεσικές συνθήκες

Identifier	Predisposing Condition Source of Information	Pervasiveness of Condition
Organization-defined	Table F-4, Task 1-4 or Organization-defined	Table F-5 or Organization-defined

Πίνακας 8.16: Παράρτημα F-6-Αναγώριση προδιαθεσικών συνθηκών

Παράρτημα G

Το παρόν παράρτημα παρέχει: (i) μια περιγραφή των δυνητικά χρήσιμων εισροών για την εργασία προσδιορισμού της πιθανότητας55 και (ii) υποδειγματικές κλίμακες αξιολόγησης για την αξιολόγηση της πιθανότητας έναρξης/εμφάνισης γεγονότων απειλής, της πιθανότητας γεγονότων απειλής που οδηγούν σε δυσμενείς επιπτώσεις και της συνολικής πιθανότητας να ξεκινήσουν ή να συμβούν γεγονότα απειλής και να

προκαλέσουν ζημία σε οργανωτικές λειτουργίες, περιουσιακά στοιχεία ή άτομα. Οι κλίμακες αξιολόγησης του παρόντος προσαρτήματος μπορούν να χρησιμοποιηθούν από τους οργανισμούς ως σημείο εκκίνησης με την κατάλληλη προσαρμογή για την προσαρμογή σε τυχόν ειδικές συνθήκες του οργανισμού. Οι πίνακες G-2, G-3, G-4 και G-5, αποτελέσματα της εργασίας 2-4, παρέχουν σχετικές εισροές στους πίνακες κινδύνου του παραρτήματος I.

Description	Provided To		
	Tier 1	Tier 2	Tier 3
From Tier 1 (Organization level) - Likelihood information and guidance specific to Tier 1 (e.g., likelihood information related to organizational governance, core missions/business functions, management/operational policies, procedures, and structures, external mission/business relationships). - Guidance on organization-wide levels of likelihood needing no further consideration. - Assessment scale for assessing the likelihood of threat event initiation (adversarial threat events), annotated by the organization, if necessary. (**Table G-2**) - Assessment scale for assessing the likelihood of threat event occurrence (non-adversarial threat events), annotated by the organization, if necessary. (**Table G-3**) - Assessment scale for assessing the likelihood of threat events resulting in adverse impacts, annotated by the organization, if necessary. (**Table G-4**) - Assessment scale for assessing the overall likelihood of threat events being initiated or occurring and resulting in adverse impacts, annotated by the organization, if necessary. (**Table G-5**)	No	Yes	Yes *If not provided by Tier 2*
From Tier 2: (Mission/business process level) - Likelihood information and guidance specific to Tier 2 (e.g., likelihood information related to mission/business processes, EA segments, common infrastructure, support services, common controls, and external dependencies).	Yes *Via RAR*	Yes *Via Peer Sharing*	Yes
From Tier 3: (Information system level) - Likelihood information and guidance specific to Tier 3 (e.g., likelihood information related to information systems, information technologies, information system components, applications, networks, environments of operation). - Historical data on successful and unsuccessful cyber attacks; attack detection rates. - Security assessment reports (i.e., deficiencies in assessed controls identified as vulnerabilities). - Results of monitoring activities (e.g., automated and nonautomated data feeds). - Vulnerability assessments, Red Team reports, or other reports from analyses of information systems, subsystems, information technology products, devices, networks, or applications. - Contingency Plans, Disaster Recovery Plans, Incident Reports. - Vendor/manufacturer vulnerability reports.	Yes *Via RAR*	Yes *Via RAR*	Yes *Via Peer Sharing*

Πίνακας 8.17: Παράρτημα G-1-Εισροές-Καθορισμός πιθανότητας

TABLE G-2: ASSESSMENT SCALE – LIKELIHOOD OF THREAT EVENT INITIATION (ADVERSARIAL)

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Adversary is **almost certain** to initiate the threat event.
High	80-95	8	Adversary is **highly likely** to initiate the threat event.
Moderate	21-79	5	Adversary is **somewhat likely** to initiate the treat event.
Low	5-20	2	Adversary is **unlikely** to initiate the threat event.
Very Low	0-4	0	Adversary is **highly unlikely** to initiate the threat event.

TABLE G-3: ASSESSMENT SCALE – LIKELIHOOD OF THREAT EVENT OCCURRENCE (NON-ADVERSARIAL)

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Error, accident, or act of nature is **almost certain** to occur; or occurs **more than 100 times a year**.
High	80-95	8	Error, accident, or act of nature is **highly likely** to occur; or occurs **between 10-100 times a year**.
Moderate	21-79	5	Error, accident, or act of nature is **somewhat likely** to occur; or occurs **between 1-10 times a year**.
Low	5-20	2	Error, accident, or act of nature is **unlikely** to occur; or occurs **less than once a year**, but **more than once every 10 years**.
Very Low	0-4	0	Error, accident, or act of nature is **highly unlikely** to occur; or occurs **less than once every 10 years**.

TABLE G-4: ASSESSMENT SCALE – LIKELIHOOD OF THREAT EVENT RESULTING IN ADVERSE IMPACTS

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	If the threat event is initiated or occurs, it is **almost certain** to have adverse impacts.
High	80-95	8	If the threat event is initiated or occurs, it is **highly likely** to have adverse impacts.
Moderate	21-79	5	If the threat event is initiated or occurs, it is **somewhat likely** to have adverse impacts.
Low	5-20	2	If the threat event is initiated or occurs, it is **unlikely** to have adverse impacts.
Very Low	0-4	0	If the threat event is initiated or occurs, it is **highly unlikely** to have adverse impacts.

TABLE G-5: ASSESSMENT SCALE – OVERALL LIKELIHOOD

Likelihood of Threat Event Initiation or Occurrence	Likelihood Threat Events Result in Adverse Impacts				
	Very Low	Low	Moderate	High	Very High
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Moderate	Moderate
Very Low	Very Low	Very Low	Low	Low	Low

Πίνακας 8.18: Παράρτηματα G-2-5

Παράρτημα Η

Το παρόν παράρτημα παρέχει: (i) περιγραφή των χρήσιμων εισροών για την εργασία προσδιορισμού των επιπτώσεων, (ii) αντιπροσωπευτικά παραδείγματα δυσμενών επιπτώσεων σε οργανωτικές λειτουργίες και περιουσιακά στοιχεία, άτομα, άλλους οργανισμούς ή το Έθνος, (iii) υποδειγματικές κλίμακες αξιολόγησης για την εκτίμηση των επιπτώσεων των συμβάντων απειλής και του εύρους των επιπτώσεων των συμβάντων απειλής, και (iv) πρότυπο για τη σύνοψη και τεκμηρίωση των αποτελεσμάτων της εργασίας προσδιορισμού των επιπτώσεων 2-5. Οι κλίμακες αξιολόγησης του παρόντος προσαρτήματος μπορούν να χρησιμοποιηθούν ως σημείο εκκίνησης με κατάλληλη προσαρμογή για την προσαρμογή σε τυχόν ειδικές συνθήκες του οργανισμού. Ο Πίνακας Η-4, αποτέλεσμα της Εργασίας 2-5, παρέχει σχετικές εισροές στους πίνακες κινδύνου του Παραρτήματος Ι.

Description	Provided To		
	Tier 1	Tier 2	Tier 3
From Tier 1 (Organization level) - Impact information and guidance specific to Tier 1 (e.g., impact information related to organizational governance, core missions/business functions, management and operational policies, procedures, and structures, external mission/business relationships). - Guidance on organization-wide levels of impact needing no further consideration. - Identification of critical missions/business functions. - Exemplary set of impacts, annotated by the organization, if necessary. (**Table H-2**) - Assessment scale for assessing the impact of threat events, annotated by the organization, if necessary. (**Table H-3**)	No	Yes	Yes *If not provided by Tier 2*
From Tier 2: (Mission/business process level) - Impact information and guidance specific to Tier 2 (e.g., impact information related to mission/business processes, EA segments, common infrastructure, support services, common controls, and external dependencies). - Identification of high-value assets.	Yes *Via RAR*	Yes *Via Peer Sharing*	Yes
From Tier 3: (Information system level) - Impact information and guidance specific to Tier 3 (e.g., likelihood information affecting information systems, information technologies, information system components, applications, networks, environments of operation). - Historical data on successful and unsuccessful cyber attacks; attack detection rates. - Security assessment reports (i.e., deficiencies in assessed controls identified as vulnerabilities). - Results of continuous monitoring activities (e.g., automated and nonautomated data feeds). - Vulnerability assessments, Red Team reports, or other reports from analyses of information systems, subsystems, information technology products, devices, networks, or applications. - Contingency Plans, Disaster Recovery Plans, Incident Reports.	Yes *Via RAR*	Yes *Via RAR*	Yes *Via Peer Sharing*

Πίνακας 8.19: Παράρτημα H-1-Εισροές-Καθορισμός επιπτώσεων

Type of Impact	Impact

HARM TO OPERATIONS	- Inability to perform current missions/business functions.
	  - In a sufficiently timely manner.
	  - With sufficient confidence and/or correctness.
	  - Within planned resource constraints.
	- Inability, or limited ability, to perform missions/business functions in the future.
	  - Inability to restore missions/business functions.
	  - In a sufficiently timely manner.
	  - With sufficient confidence and/or correctness.
	  - Within planned resource constraints.
	- Harms (e.g., financial costs, sanctions) due to noncompliance.
	  - With applicable laws or regulations.
	  - With contractual requirements or other requirements in other binding agreements (e.g., liability).
	- Direct financial costs.
	- Relational harms.
	  - Damage to trust relationships.
	  - Damage to image or reputation (and hence future or potential trust relationships).

HARM TO ASSETS	- Damage to or loss of physical facilities. - Damage to or loss of information systems or networks. - Damage to or loss of information technology or equipment. - Damage to or loss of component parts or supplies. - Damage to or of loss of information assets. - Loss of intellectual property.
HARM TO INDIVIDUALS	- Injury or loss of life. - Physical or psychological mistreatment. - Identity theft. - Loss of Personally Identifiable Information. - Damage to image or reputation.

HARM TO OTHER ORGANIZATIONS	- Harms (e.g., financial costs, sanctions) due to noncompliance.
	  - With applicable laws or regulations.
	  - With contractual requirements or other requirements in other binding agreements.
	- Direct financial costs.
	- Relational harms.
	  - Damage to trust relationships.
	  - Damage to reputation (and hence future or potential trust relationships).

HARM TO THE NATION	- Damage to or incapacitation of a critical infrastructure sector.
	- Loss of government continuity of operations.
	- Relational harms.
	  - Damage to trust relationships with other governments or with nongovernmental entities.
	  - Damage to national reputation (and hence future or potential trust relationships).
	- Damage to current or future ability to achieve national objectives.
	  - Harm to national security.

Πίνακας 8.20: Παράρτημα H-2-Παραδείγματα δυσμενών επιπτώσεων

TABLE H-3: ASSESSMENT SCALE – IMPACT OF THREAT EVENTS

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	80-95	8	The threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. A severe or catastrophic adverse effect means that, for example, the threat event might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.
Moderate	21-79	5	The threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A serious adverse effect means that, for example, the threat event might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.
Low	5-20	2	The threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A limited adverse effect means that, for example, the threat event might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Very Low	0-4	0	The threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation.

TABLE H-4: TEMPLATE – IDENTIFICATION OF ADVERSE IMPACTS

Type of Impact	Impact Affected Asset	Maximum Impact
Table H-2 or Organization-defined	Table H-2 or Organization-defined	Table H-3 or Organization-defined

Πίνακας 8.21: Παράρτημα Η-3-4-Κλίμακα αξιολόγησης και αναγνώριση δυσμενών

Παράρτημα Ι

Το παράρτημα αυτό παρέχει: (i) περιγραφή των δυνητικά χρήσιμων εισροών για την εργασία προσδιορισμού του κινδύνου, συμπεριλαμβανομένων των εκτιμήσεων για την αβεβαιότητα των προσδιορισμών, (ii) υποδειγματικές κλίμακες αξιολόγησης για την εκτίμηση των επιπέδων κινδύνου, (iii) πίνακες για την περιγραφή του περιεχομένου (δηλ. των εισροών δεδομένων) για ανταγωνιστικούς και μη ανταγωνιστικούς προσδιορισμούς του κινδύνου, και (iv) υποδείγματα για τη σύνοψη και τεκμηρίωση των αποτελεσμάτων της εργασίας 2-6 για τον προσδιορισμό του κινδύνου. Οι κλίμακες αξιολόγησης του παρόντος προσαρτήματος μπορούν να χρησιμοποιηθούν ως σημείο εκκίνησης με κατάλληλη προσαρμογή για την προσαρμογή σε τυχόν ειδικές συνθήκες του οργανισμού. Ο Πίνακας Ι-5 (κίνδυνος αντιδικίας) και ο Πίνακας Ι-7 (κίνδυνος μη αντιδικίας) αποτελούν αποτελέσματα της Εργασίας 2-6.

TABLE I-1: INPUTS – RISK

Description	Provided To		
	Tier 1	Tier 2	Tier 3
From Tier 1 (Organization level) - Sources of risk and uncertainty information identified for organization-wide use (e.g., specific information that may be useful in determining likelihoods such as adversary capabilities, intent, and targeting objectives). - Guidance on organization-wide levels of risk (including uncertainty) needing no further consideration. - Criteria for uncertainty determinations. - List of high-risk events from previous risk assessments. - Assessment scale for assessing the level of risk as a combination of likelihood and impact, annotated by the organization, if necessary. (**Table I-2**) - Assessment scale for assessing level of risk, annotated by the organization, if necessary. (**Table I-3**)	No	Yes	Yes *If not provided by Tier 2*
From Tier 2: (Mission/business process level) - Risk-related information and guidance specific to Tier 2 (e.g., risk and uncertainty information related to mission/business processes, EA segments, common infrastructure, support services, common controls, and external dependencies).	Yes *Via RAR*	Yes *Via Peer Sharing*	Yes
From Tier 3: (Information system level) - Risk-related information and guidance specific to Tier 3 (e.g., likelihood information affecting information systems, information technologies, information system components, applications, networks, environments of operation).	Yes *Via RAR*	Yes *Via RAR*	Yes *Via Peer Sharing*

TABLE I-2: ASSESSMENT SCALE – LEVEL OF RISK (COMBINATION OF LIKELIHOOD AND IMPACT)

Likelihood (Threat Event Occurs and Results in Adverse Impact)	Level of Impact				
	Very Low	Low	Moderate	High	Very High
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

Πίνακας 8.22: Παράρτημα I-1-2-Εισροές Κλίμακα αξιολόγησης-Επίπεδο κινδύνου

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	**Very high risk** means that a threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	80-95	8	**High risk** means that a threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Moderate	21-79	5	**Moderate risk** means that a threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Low	5-20	2	**Low risk** means that a threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Very Low	0-4	0	**Very low risk** means that a threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.

Πίνακας 8.23: Παράρτημα I-3- Επίπεδο κινδύνου

Column	Heading	Content
1	Threat Event	Identify threat event. (**Task 2-2**; **Table E-1**; **Table E-2**; **Table E-5**; **Table I-5**.)
2	Threat Sources	Identify threat sources that could initiate the threat event. (**Task 2-1**; **Table D-1**; **Table D-2**; **Table D-7**; **Table I-5**.)
3	Capability	Assess threat source capability. (**Task 2-1**; **Table D-3**; **Table D-7**; **Table I-5**.)
4	Intent	Assess threat source intent. (**Task 2-1**; **Table D-4**; **Table D-7**; **Table I-5**.)
5	Targeting	Assess threat source targeting. (**Task 2-1**; **Table D-5**; **Table D-7**; **Table I-5**.)
6	Relevance	Determine relevance of threat event. (**Task 2-2**; **Table E-1**; **Table E-4**; **Table E-5**; **Table I-5**.) If the relevance of the threat event does not meet the organization's criteria for further consideration, do not complete the remaining columns.
7	Likelihood of Attack Initiation	Determine likelihood that one or more of the threat sources initiates the threat event, taking into consideration capability, intent, and targeting. (**Task 2-4**; **Table G-1**; **Table G-2**; **Table I-5**.)
8	Vulnerabilities and Predisposing Conditions	Identify vulnerabilities which could be exploited by threat sources initiating the threat event and the predisposing conditions which could increase the likelihood of adverse impacts. (**Task 2-5**; **Table F-1**; **Table F-3**; **Table F-4**; **Table F-6**; **Table I-5**.)
9	Severity Pervasiveness	Assess severity of vulnerabilities and pervasiveness of predisposing conditions. (**Task 2-5**; **Table F-1**; **Table F-2**; **Table F-5**; **Table F-6**; **Table I-5**.)
10	Likelihood Initiated Attack Succeeds	Determine the likelihood that the threat event, once initiated, will result in adverse impact, taking into consideration threat source capability, vulnerabilities, and predisposing conditions. (**Task 2-4**; **Table G-1**; **Table G-4**; **Table I-5**.)
11	Overall Likelihood	Determine the likelihood that the threat event will be initiated and result in adverse impact (i.e., combination of likelihood of attack initiation and likelihood that initiated attack succeeds). (**Task 2-4**; **Table G-1**; **Table G-5**; **Table I-5**.)
12	Level of Impact	Determine the adverse impact (i.e., potential harm to organizational operations, organizational assets, individuals, other organizations, or the Nation) from the threat event. (**Task 2-5**; **Table H-1**, **Table H-2**; **Table H-3**; **Table H-4**; **Table I-5**.)
13	Risk	Determine the level of risk as a combination of likelihood and impact. (**Task 2-6**; **Table I-1**; **Table I-2**; **Table I-3**; **Table I-5**.)

TABLE I-5: TEMPLATE – ADVERSARIAL RISK

1	2	3	4	5	6	7	8	9	10	11	12	13
Threat Event	Threat Sources	Threat Source Characteristics			Relevance	Likelihood of Attack Initiation	Vulnerabilities and Predisposing Conditions	Severity and Pervasiveness	Likelihood Initiated Attack Succeeds	Overall Likelihood	Level of Impact	Risk
		Capability	Intent	Targeting								

Πίνακας 8.24: Παράρτημα Ι-4-5- Περιγραφές ανταγωνιστικού κινδύνου

TABLE I-6: COLUMN DESCRIPTIONS FOR NON-ADVERSARIAL RISK TABLE

Column	Heading	Content
1	Threat Event	Identify threat event. (**Task 2-2**; **Table E-1**; **Table E-3**; **Table E-5**; **Table I-7**.)
2	Threat Sources	Identify threat sources that could initiate the threat event. (**Task 2-1**; **Table D-1**; **Table D-2**; **Table D-8**; **Table I-7**.)
3	Range of Effects	Identify the range of effects from the threat source. (**Task 2-1**; **Table D-1**; **Table D-6**; **Table I-7**.)
4	Relevance	Determine relevance of threat event. (**Task 2-2**; **Table E-1**; **Table E-4**; **Table E-5**; **Table I-7**.) If the relevance of the threat event does not meet the organization's criteria for further consideration, do not complete the remaining columns.
5	Likelihood of Threat Event Occurring	Determine the likelihood that the threat event will occur. (**Task 2-4**; **Table G-1**; **Table G-3**; **Table I-7**.)
6	Vulnerabilities and Predisposing Conditions	Identify vulnerabilities which could be exploited by threat sources initiating the threat event and the predisposing conditions which could increase the likelihood of adverse impacts. (**Task 2-5**; **Table F-1**; **Table F-3**; **Table F-4**; **Table F-6**; **Table I-7**.)
7	Severity Pervasiveness	Assess severity of vulnerabilities and pervasiveness of predisposing conditions. (**Task 2-5**; **Table F-1**; **Table F-2**; **Table F-5**; **Table F-6**; **Table I-5**.)
8	Likelihood Threat Event Results in Adverse Impact	Determine the likelihood that the threat event, once initiated, will result in adverse impact, taking into consideration vulnerabilities and predisposing conditions. (**Task 2-4**; **Table G-1**; **Table G-4**; **Table I-7**.)
9	Overall Likelihood	Determine the likelihood that the threat event will occur and result in adverse impacts (i.e., combination of likelihood of threat occurring and likelihood that the threat event results in adverse impact). (**Task 2-4**; **Table G-1**; **Table G-5**; **Table I-7**.)
10	Level of Impact	Determine the adverse impact (i.e., potential harm to organizational operations, organizational assets, individuals, other organizations, or the Nation) from the threat event. (**Task 2-5**; **Table H-1**, **Table H-2**; **Table H-3**; **Table H-4**; **Table I-7**.)
11	Risk	Determine the level of risk as a combination of likelihood and impact. (**Task 2-6**; **Table I-1**; **Table I-2**; **Table I-3**; **Table I-7**.)

TABLE I-7: TEMPLATE – NON-ADVERSARIAL RISK

1	2	3	4	5	6	7	8	9	10	11
Threat Event	Threat Sources	Range of Effects	Relevance	Likelihood of Event Occurring	Vulnerabilities and Predisposing Conditions	Severity and Pervasiveness	Likelihood Event Results in Adverse Impact	Overall Likelihood	Level of Impact	Risk

Πίνακας 8.25: Παράρτημα I-6-7- Περιγραφές μη-ανταγωνιστικού κινδύνου

Παράρτημα J

Η αξιολόγηση κινδύνου μπορεί να εντοπίσει έναν αριθμό κινδύνων που έχουν παρόμοια βαθμολογία (π.χ. 78, 82, 83) ή επίπεδα (π.χ. μέτριο, υψηλό). Όταν πάρα πολλοί κίνδυνοι συγκεντρώνονται στην ίδια ή περίπου στην ίδια τιμή, οι οργανισμοί χρειάζονται μια μέθοδο για να βελτιώσουν την παρουσίαση των αποτελεσμάτων της αξιολόγησης κινδύνων, ιεραρχώντας τις προτεραιότητες εντός των συνόλων κινδύνων με παρόμοιες τιμές, ώστε να ενημερώσουν καλύτερα τη συνιστώσα αντιμετώπισης κινδύνων της διαδικασίας διαχείρισης κινδύνων. Μια τέτοια μέθοδος θα πρέπει να συνδέεται με την αποστολή/τις επιχειρηματικές απαιτήσεις του οργανισμού, να συνάδει με την ανοχή του οργανισμού σε κινδύνους και να μεγιστοποιεί τη χρήση των διαθέσιμων πόρων. Η ιεράρχηση προτεραιοτήτων αποτελεί βασικό στοιχείο της προστασίας βάσει κινδύνων και καθίσταται αναγκαία όταν οι απαιτήσεις δεν μπορούν να ικανοποιηθούν πλήρως ή όταν οι πόροι δεν επιτρέπουν τον μετριασμό όλων των κινδύνων εντός εύλογου χρονικού πλαισίου. Για να διευκολυνθούν οι τεκμηριωμένες αποφάσεις αντιμετώπισης κινδύνων από τους ανώτερους ηγέτες/στελέχη (π.χ. γιατί ορισμένοι κίνδυνοι μετριάστηκαν ή δεν μετριάστηκαν), τα αποτελέσματα της αξιολόγησης κινδύνων σχολιάζονται ώστε να μπορούν οι εν λόγω υπεύθυνοι λήψης αποφάσεων να γνωρίζουν ή να λαμβάνουν απαντήσεις στις ακόλουθες ερωτήσεις για κάθε κίνδυνο σε ένα σύνολο με παρόμοια βαθμολογία:

Χρονικό πλαίσιο

Σε περίπτωση που ο εντοπισμένος κίνδυνος υλοποιηθεί….

- Πόσο μεγάλος θα ήταν ο *άμεσος* αντίκτυπος στις οργανωτικές λειτουργίες (συμπεριλαμβανομένης της αποστολής, των λειτουργιών, της εικόνας ή της φήμης), στα περιουσιακά στοιχεία του οργανισμού, στα άτομα, σε άλλους οργανισμούς ή στο Έθνος;

- Πόσο υψηλός θα ήταν ο *μελλοντικός* αντίκτυπος στις λειτουργίες του οργανισμού (συμπεριλαμβανομένης της αποστολής, των λειτουργιών, της εικόνας ή της φήμης), στα περιουσιακά στοιχεία του οργανισμού, στα άτομα, σε άλλους οργανισμούς ή στο έθνος;

Οι απαντήσεις στις παραπάνω ερωτήσεις, σε συνδυασμό με την ανοχή του οργανισμού σε κινδύνους, παρέχουν τη βάση για την ιεράρχηση των κινδύνων που βασίζεται στις τρέχουσες και μελλοντικές ανάγκες του οργανισμού. Κατά τη στάθμιση των άμεσων επιπτώσεων έναντι των μελλοντικών επιπτώσεων, οι ανώτεροι ηγέτες πρέπει να αποφασίσουν εάν μια κρίσιμη αποστολή/επιχειρηματική ανάγκη σήμερα δικαιολογεί να θέσει σε κίνδυνο τις μελλοντικές δυνατότητες του οργανισμού. Οι ιδιοκτήτες αποστολών/επιχειρήσεων και οι ειδικοί σε θέματα αποστολών/επιχειρήσεων μπορούν να συμβουλευτούν για να λάβουν τις πιο πλήρεις και ενημερωμένες πληροφορίες σχετικά με τις επιπτώσεις των αποστολών/επιχειρήσεων. Μπορούν να ζητηθούν πληροφορίες από άλλους εμπειρογνώμονες ή εκπροσώπους των ενδιαφερομένων μερών για να ληφθούν πληροφορίες σχετικά με τις άμεσες και τις μελλοντικές επιπτώσεις (π.χ. επικοινωνία με το Γραφείο Προστασίας Δεδομένων Προσωπικού Χαρακτήρα για τις επιπτώσεις σε ιδιώτες).

Συνολικός σωρευτικός αντίκτυπος

- Ποιος είναι ο αναμενόμενος αντίκτυπος από ένα μεμονωμένο περιστατικό της απειλής;

- Εάν ο κίνδυνος μπορεί να υλοποιηθεί περισσότερες από μία φορές, ποιος είναι ο συνολικός αναμενόμενος αντίκτυπος (δηλ. σωρευτική απώλεια) για τη χρονική περίοδο ανησυχίας;

Σημειώστε ότι μια πτυχή του συνολικού αντίκτυπου για τους οργανισμούς είναι το κόστος ανάκαμψης από μια απώλεια εμπιστευτικότητας, ακεραιότητας ή διαθεσιμότητας.

Συνέργειες μεταξύ κινδύνων

Εάν υλοποιηθεί ένας κίνδυνος που συνδέεται στενά με πολλαπλούς κινδύνους, είναι πιθανό να υλοποιηθεί ένα σύμπλεγμα κινδύνων ταυτόχρονα ή σχεδόν ταυτόχρονα. Η διαχείριση των δυσμενών επιπτώσεων από την υλοποίηση ενός κινδύνου μπορεί να είναι δυνατή- η διαχείριση πολλαπλών κινδύνων υψηλού αντίκτυπου που υλοποιούνται ταυτόχρονα μπορεί να αποτελέσει πρόκληση για τις δυνατότητες του οργανισμού και, ως εκ τούτου, χρειάζεται πολύ πιο στενή διαχείριση. Οι ακόλουθες ερωτήσεις αφορούν τις σχέσεις μεταξύ των κινδύνων.

Η υλοποίηση ενός συγκεκριμένου κινδύνου θα έχει ως αποτέλεσμα:

- Υψηλή πιθανότητα ή σχεδόν βεβαιότητα υλοποίησης άλλων αναγνωρισμένων κινδύνων;

- Μεγάλη πιθανότητα ή σχεδόν βεβαιότητα μη υλοποίησης άλλων αναγνωρισμένων κινδύνων;

- Καμία ιδιαίτερη επίπτωση στην υλοποίηση άλλων αναγνωρισμένων κινδύνων;

Εάν ένας κίνδυνος συνδέεται σε μεγάλο βαθμό με άλλους κινδύνους ή θεωρείται πιθανό να οδηγήσει στην υλοποίηση άλλων κινδύνων (είτε ο κίνδυνος είναι η αιτία είτε υλοποιείται ταυτόχρονα), ο κίνδυνος θα πρέπει να έχει υψηλότερη προτεραιότητα από έναν κίνδυνο που δεν έχει ιδιαίτερο αντίκτυπο σε άλλους κινδύνους. Εάν η υλοποίηση ενός κινδύνου μειώνει πράγματι την πιθανότητα υλοποίησης άλλων κινδύνων, τότε δικαιολογείται περαιτέρω ανάλυση για να καθοριστεί ποιοι κίνδυνοι αποκτούν χαμηλότερη προτεραιότητα για τον μετριασμό τους.

Εν κατακλείδι, οι οργανισμοί μπορούν να επωφεληθούν σημαντικά από την τελειοποίηση των αποτελεσμάτων της αξιολόγησης κινδύνων κατά την προετοιμασία του σταδίου της αντιμετώπισης των κινδύνων στη διαδικασία διαχείρισης κινδύνων. Κατά τη διάρκεια του βήματος αντιμετώπισης κινδύνων, το οποίο περιγράφεται στην ειδική έκδοση 800-39 της NIST, οι οργανισμοί: i) αναλύουν τις διάφορες κατευθύνσεις δράσης, ii) διεξάγουν αναλύσεις κόστους-οφέλους, iii) αντιμετωπίζουν ζητήματα επεκτασιμότητας για εφαρμογές μεγάλης κλίμακας, iv) εξετάζουν τις αλληλεπιδράσεις/εξαρτήσεις μεταξύ των προσεγγίσεων μετριασμού κινδύνων (π.χ. εξαρτήσεις μεταξύ των ελέγχων ασφαλείας) και v) αξιολογούν άλλους παράγοντες που επηρεάζουν τις οργανωτικές αποστολές/επιχειρησιακές λειτουργίες. Επιπλέον, οι οργανισμοί αντιμετωπίζουν ζητήματα κόστους, χρονοδιαγράμματος και επιδόσεων που σχετίζονται με τα πληροφοριακά συστήματα και την υποδομή τεχνολογίας πληροφοριών που υποστηρίζουν τις οργανωτικές αποστολές/επιχειρησιακές λειτουργίες.

Παράρτημα Κ

Το παράρτημα παρέχει τα βασικά στοιχεία πληροφοριών που μπορούν να χρησιμοποιήσουν οι οργανισμοί για **να** κοινοποιήσουν τα αποτελέσματα των αξιολογήσεων κινδύνου. Τα αποτελέσματα των αξιολογήσεων κινδύνου παρέχουν στους υπεύθυνους λήψης αποφάσεων μια κατανόηση του κινδύνου ασφάλειας πληροφοριών για τις οργανωτικές λειτουργίες και τα περιουσιακά στοιχεία, τα άτομα, τους άλλους οργανισμούς ή το Έθνος που απορρέει από τη λειτουργία και τη χρήση των οργανωτικών συστημάτων πληροφοριών και των

περιβαλλόντων στα οποία λειτουργούν τα εν λόγω συστήματα. Τα ουσιώδη στοιχεία των πληροφοριών σε μια εκτίμηση κινδύνου μπορούν να περιγραφούν σε τρία τμήματα της έκθεσης εκτίμησης κινδύνου (ή σε οποιοδήποτε άλλο μέσο επιλέγουν οι οργανισμοί για να μεταφέρουν τα αποτελέσματα της εκτίμησης): (i) μια σύνοψη, (ii) το κύριο σώμα που περιέχει λεπτομερή αποτελέσματα της αξιολόγησης κινδύνων, και (iii) υποστηρικτικά παραρτήματα.

Περίληψη

- Αναφέρετε την ημερομηνία της αξιολόγησης κινδύνου.
- Συνοψίστε τον σκοπό της αξιολόγησης κινδύνου.
- Περιγράψτε το πεδίο εφαρμογής της αξιολόγησης κινδύνων.
- Για τις αξιολογήσεις κινδύνων της βαθμίδας 1 και 2, προσδιορίστε: οργανωτικές δομές διακυβέρνησης ή διαδικασίες που σχετίζονται με την αξιολόγηση (π.χ. εκτελεστικό όργανο [λειτουργία] κινδύνου, διαδικασία προϋπολογισμού, διαδικασία απόκτησης, διαδικασία σχεδιασμού συστημάτων, επιχειρησιακή αρχιτεκτονική, αρχιτεκτονική ασφάλειας πληροφοριών, οργανωτικές αποστολές/επιχειρησιακές λειτουργίες, διαδικασίες αποστολής/επιχειρησιακής δραστηριότητας, συστήματα πληροφοριών που υποστηρίζουν τις διαδικασίες αποστολής/επιχειρησιακής δραστηριότητας).
- Για τις αξιολογήσεις κινδύνου της βαθμίδας 3, προσδιορίστε: το όνομα του συστήματος πληροφοριών και τη θέση (τις θέσεις), την κατηγοριοποίηση ασφαλείας και το όριο του συστήματος πληροφοριών (π.χ. εξουσιοδότηση).
- Αναφέρετε αν πρόκειται για αρχική ή μεταγενέστερη αξιολόγηση κινδύνου. Εάν πρόκειται για μεταγενέστερη αξιολόγηση κινδύνου, αναφέρετε τις περιστάσεις που προκάλεσαν την επικαιροποίηση και συμπεριλάβετε παραπομπή στην προηγούμενη έκθεση αξιολόγησης κινδύνου.
- Περιγράψτε το συνολικό επίπεδο κινδύνου (π.χ. πολύ χαμηλό, χαμηλό, μέτριο, υψηλό ή πολύ υψηλό).
- Αναφέρετε τον αριθμό των κινδύνων που εντοπίστηκαν για κάθε επίπεδο κινδύνου (π.χ. πολύ χαμηλό, χαμηλό, μέτριο, υψηλό ή πολύ υψηλό).

Σώμα της έκθεσης

- Περιγράψτε τον σκοπό της αξιολόγησης κινδύνων, συμπεριλαμβανομένων των ερωτημάτων που πρέπει να απαντηθούν από την αξιολόγηση. Για παράδειγμα:

Πώς η χρήση μιας συγκεκριμένης τεχνολογίας πληροφοριών θα μπορούσε δυνητικά να μεταβάλει τον κίνδυνο για τις οργανωτικές αποστολές/επιχειρησιακές λειτουργίες, εάν χρησιμοποιηθεί σε συστήματα πληροφοριών που υποστηρίζουν αυτές τις αποστολές/επιχειρησιακές λειτουργίες- ή

- Πώς τα αποτελέσματα της αξιολόγησης κινδύνου πρόκειται να χρησιμοποιηθούν στο πλαίσιο του ΣΔΑΚ (π.χ. αρχική αξιολόγηση κινδύνου που θα χρησιμοποιηθεί για την προσαρμογή των βασικών γραμμών ελέγχου ασφάλειας ή/και για την καθοδήγηση και ενημέρωση άλλων αποφάσεων και θα χρησιμεύσει ως αφετηρία για μεταγενέστερες αξιολογήσεις κινδύνου- μεταγενέστερη αξιολόγηση κινδύνου για την ενσωμάτωση των αποτελεσμάτων των αξιολογήσεων ελέγχου ασφάλειας και την ενημέρωση των αποφάσεων αδειοδότησης- μεταγενέστερη αξιολόγηση κινδύνου για την υποστήριξη της ανάλυσης εναλλακτικών τρόπων δράσης για την αντιμετώπιση κινδύνων- μεταγενέστερη αξιολόγηση κινδύνου με βάση την παρακολούθηση κινδύνων για τον εντοπισμό νέων απειλών ή τρωτών σημείων- μεταγενέστερες αξιολογήσεις κινδύνου για την ενσωμάτωση γνώσεων που αποκτήθηκαν από περιστατικά ή επιθέσεις).
- Προσδιορισμός παραδοχών και περιορισμών.
- Περιγραφή των εισροών ανοχής κινδύνου στην αξιολόγηση κινδύνου (συμπεριλαμβανομένου του εύρους των συνεπειών που πρέπει να ληφθούν υπόψη).
- Προσδιορίστε και περιγράψτε το μοντέλο κινδύνου και την αναλυτική προσέγγιση- παρέχετε αναφορά ή συμπεριλάβετε ως παράρτημα, προσδιορίζοντας τους παράγοντες κινδύνου, τις κλίμακες τιμών και τους αλγορίθμους για τον συνδυασμό των τιμών.
- Να αιτιολογηθεί κάθε απόφαση που σχετίζεται με τον κίνδυνο κατά τη διαδικασία εκτίμησης κινδύνου.
- Περιγράψτε τις αβεβαιότητες στο πλαίσιο της διαδικασίας εκτίμησης κινδύνου και πώς αυτές οι αβεβαιότητες επηρεάζουν τις αποφάσεις.
- Εάν η αξιολόγηση κινδύνου περιλαμβάνει οργανωτικές αποστολές/επιχειρησιακές λειτουργίες, περιγράψτε τις αποστολές/λειτουργίες (π.χ., τις αποστολές/επιχειρησιακές διαδικασίες που υποστηρίζουν τις αποστολές/λειτουργίες, τις διασυνδέσεις και τις εξαρτήσεις μεταξύ σχετικών αποστολών/επιχειρησιακών λειτουργιών και την τεχνολογία πληροφοριών που υποστηρίζει τις αποστολές/επιχειρησιακές λειτουργίες).

- Εάν η αξιολόγηση κινδύνου περιλαμβάνει οργανωτικά πληροφοριακά συστήματα, περιγράψτε τα συστήματα (π.χ. τις αποστολές/επιχειρησιακές λειτουργίες που υποστηρίζει το σύστημα, τις ροές πληροφοριών από/προς τα συστήματα και τις εξαρτήσεις από άλλα συστήματα, κοινές υπηρεσίες ή κοινές υποδομές).

- Συνοψίστε τα αποτελέσματα της αξιολόγησης κινδύνου (π.χ. με τη χρήση πινάκων ή γραφικών παραστάσεων), σε μορφή που επιτρέπει στους υπεύθυνους λήψης αποφάσεων να κατανοήσουν γρήγορα τον κίνδυνο (π.χ. αριθμός των συμβάντων απειλής για διαφορετικούς συνδυασμούς πιθανότητας και επιπτώσεων, το σχετικό ποσοστό των συμβάντων απειλής σε διαφορετικά επίπεδα κινδύνου).

- Προσδιορίστε το χρονικό πλαίσιο για το οποίο ισχύει η αξιολόγηση κινδύνου (δηλαδή, το χρονικό πλαίσιο για το οποίο η αξιολόγηση προορίζεται να υποστηρίξει αποφάσεις).

- Καταγράψτε τους κινδύνους που οφείλονται σε αντίπαλες απειλές (βλέπε πίνακα F-1).

- Καταγράψτε τους κινδύνους που οφείλονται σε μη αντίπαλες απειλές (βλέπε πίνακα F-2).

Παραρτήματα

- Κατάλογος παραπομπών και πηγών πληροφοριών.

- Καταγράψτε την ομάδα ή τα άτομα που διεξάγουν την αξιολόγηση κινδύνων, συμπεριλαμβανομένων των στοιχείων επικοινωνίας.

- Καταγράψτε τις λεπτομέρειες της εκτίμησης κινδύνου και τυχόν υποστηρικτικά στοιχεία (π.χ. πίνακες D-7, D-8, E-5, F-3, F-6, H-4), όπως απαιτείται για την κατανόηση και την επαναχρησιμοποίηση των αποτελεσμάτων (π.χ. για την αμοιβαιότητα, για επόμενες εκτιμήσεις κινδύνου, για να χρησιμεύσουν ως στοιχεία για τις εκτιμήσεις κινδύνου βαθμίδων 1 και 2).

Παράρτημα L

TASK	TASK DESCRIPTION
Step 1: Prepare for Risk Assessment	
TASK 1-1 IDENTIFY PURPOSE **Section 3.1**	Identify the purpose of the risk assessment in terms of the information that the assessment is intended to produce and the decisions the assessment is intended to support.
TASK 1-2 IDENTIFY SCOPE **Section 3.1**	Identify the scope of the risk assessment in terms of organizational applicability, time frame supported, and architectural/technology considerations.
TASK 1-3 IDENTIFY ASSUMPTIONS AND CONSTRAINTS **Section 3.1**	Identify the specific assumptions and constraints under which the risk assessment is conducted.
TASK 1-4 IDENTIFY INFORMATION SOURCES **Section 3.1**	Identify the sources of descriptive, threat, vulnerability, and impact information to be used in the risk assessment.
TASK 1-5 IDENTIFY RISK MODEL AND ANALYTIC APPROACH **Section 3.1**	Identify the risk model and analytic approach to be used in the risk assessment.
Step 2: Conduct Risk Assessment	
TASK 2-1 IDENTIFY THREAT SOURCES **Section 3.2, Appendix D**	Identify and characterize threat sources of concern, including capability, intent, and targeting characteristics for adversarial threats and range of effects for non-adversarial threats.
TASK 2-2 IDENTIFY THREAT EVENTS **Section 3.2, Appendix E**	Identify potential threat events, relevance of the events, and the threat sources that could initiate the events.
TASK 2-3 IDENTIFY VULNERABILITIES AND PREDISPOSING CONDITIONS **Section 3.2, Appendix F**	Identify vulnerabilities and predisposing conditions that affect the likelihood that threat events of concern result in adverse impacts.

Πίνακας 8.26: Παράρτημα J- Σύνοψη δράσεων αξιολόγησης κινδύνου

TASK	TASK DESCRIPTION
TASK 2-4 DETERMINE LIKELIHOOD **Section 3.2, Appendix G**	Determine the likelihood that threat events of concern result in adverse impacts, considering: (i) the characteristics of the threat sources that could initiate the events; (ii) the vulnerabilities/predisposing conditions identified; and (iii) the organizational susceptibility reflecting the safeguards/countermeasures planned or implemented to impede such events.
TASK 2-5 DETERMINE IMPACT **Section 3.2, Appendix H**	Determine the adverse impacts from threat events of concern, considering: (i) the characteristics of the threat sources that could initiate the events; (ii) the vulnerabilities/predisposing conditions identified; and (iii) the organizational susceptibility reflecting the safeguards/countermeasures planned or implemented to impede such events.
TASK 2-6 DETERMINE RISK **Section 3.2, Appendix I**	Determine the risk to the organization from threat events of concern considering: (i) the impact that would result from the events; and (ii) the likelihood of the events occurring.
Step 3: Communicate and Share Risk Assessment Results	
TASK 3-1 COMMUNICATE RISK ASSESSMENT RESULTS **Section 3.3, Appendix K**	Communicate risk assessment results to organizational decision makers to support risk responses.
TASK 3-2 SHARE RISK-RELATED INFORMATION **Section 3.3**	Share risk-related information produced during the risk assessment with appropriate organizational personnel.
Step 4: Maintain Risk Assessment	
TASK 4-1 MONITOR RISK FACTORS **Section 3.4**	Conduct ongoing monitoring of the risk factors that contribute to changes in risk to organizational operations and assets, individuals, other organizations, or the Nation.
TASK 4-2 UPDATE RISK ASSESSMENT **Section 3.4**	Update existing risk assessment using the results from ongoing monitoring of risk factors.

Πίνακας 8.27: Παράρτημα J- Σύνοψη δράσεων αξιολόγησης κινδύνου

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

Η κάτωθι υπογεγραμμένη **ΑΓΓΕΛΙΔΟΥ ΜΑΡΙΑ** του **Αντωνίου,** με αριθμό μητρώου **cscyb2002** φοιτήτρια του Προγράμματος Μεταπτυχιακών Σπουδών της Κυβερνοασφάλειας του **ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ** της σχολής ΜΗΧΑΝΙΚΩΝ του Τμήματος **ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ**,

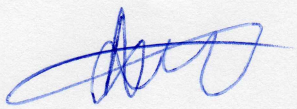
δηλώνω υπεύθυνα ότι:

«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, του Ιδρύματος όσο και δικής μου.

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

Επιθυμώ την απαγόρευση πρόσβασης στο πλήρες κείμενο της εργασίας μου, μέχρι την βαθμολόγηση της και έγκριση του επιβλέποντος καθηγητή.»

Η ΔΗΛΟΥΣΑ
ΑΓΓΕΛΙΔΟΥ ΜΑΡΙΑ του **ΑΝΤΩΝΙΟΥ**



(Υπογραφή φοιτητή)