ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Π.Μ.Σ. «ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΤΕΧΝΗΤΗΣ ΝΟΗΜΟΣΥΝΗΣ»

««Ενίσχυση της Επιχειρησιακής Συνέχειας και της Οργανωσιακής Ανθεκτικότητας μέσω Τοπικών Μεγάλων Γλωσσικών Μοντέλων»

Επιβλέπων Καθηγητής: Στέφανος Γκρίτζαλης,

Ονοματεπώνυμο:	E–mail:	A.M.:
Πολίτης Κωνσταντίνος	konstantinos_politis@ssl-unipi.gr	Mte24026

Πειραιάς
12/02/2026

Περίληψη

Η παρούσα πτυχιακή εργασία εξετάζει τη σύγκλιση της Διοικητικής Επιστήμης και της Τεχνητής Νοημοσύνης στον κρίσιμο τομέα της Επιχειρησιακής Συνέχειας, με στόχο την ενίσχυση της οργανωσιακής ανθεκτικότητας. Αρχικά, αναλύεται διεξοδικά το κανονιστικό πλαίσιο των διεθνών προτύπων ISO 22301 και ISO/IEC 27001, εστιάζοντας στον κύκλο Plan – Do – Check - Act (PDCA) και στη μεθοδολογία της Ανάλυσης Επιχειρησιακών Επιπτώσεων (BIA). Στη συνέχεια, η μελέτη μεταβαίνει στην πρακτική εφαρμογή, διερευνώντας τη δυνατότητα αξιοποίησης ενός τοπικού Μεγάλου Γλωσσικού Μοντέλου (Local LLM), συγκεκριμένα του Mistral 7B, ως ψηφιακού συμβούλου συμμόρφωσης σε περιβάλλον Μικρομεσαίας Επιχείρησης, διασφαλίζοντας παράλληλα την ιδιωτικότητα των δεδομένων μέσω τοπικής εκτέλεσης. Μέσω της υλοποίησης αρχιτεκτονικής RAG (Retrieval-Augmented Generation) και της προσομοίωσης σεναρίου επίθεσης Ransomware, η έρευνα τεκμηριώνει ότι η Τεχνητή Νοημοσύνη δύναται να ανακαλέσει με ακρίβεια κρίσιμες πολιτικές ασφαλείας και να υποστηρίξει τη λήψη αποφάσεων υπό πίεση, υπό την προϋπόθεση ότι συνδυάζεται με κατάλληλο σχεδιασμό εντολών (prompt engineering) και ανθρώπινη επίβλεψη.

Abstract

This thesis explores the convergence of Business Continuity Management and Artificial Intelligence, aiming to enhance organizational resilience through innovative technological solutions. Initially, it provides a comprehensive theoretical analysis of ISO 22301 and ISO/IEC 27001 international standards, focusing on the PDCA cycle and the Business Impact Analysis (BIA) methodology as foundations for effective governance. Subsequently, the study practically investigates the feasibility of utilizing a Local Large Language Model (Local LLM), specifically Mistral 7B, as a compliance advisor within an SME environment, while ensuring data privacy through offline execution. Through the implementation of a Retrieval-Augmented Generation (RAG) architecture and the simulation of a Ransomware attack scenario, the research demonstrates that AI can accurately retrieve security policies and support decision-making processes, provided that it is supported by robust prompt engineering and maintained under human oversight to mitigate inherent technical limitations.

Ευχαριστίες

Η ολοκλήρωση της παρούσας μεταπτυχιακής διατριβής αποτελεί το επιστέγασμα μιας απαιτητικής αλλά και εξαιρετικά δημιουργικής πορείας. Η εκπόνησή της δεν θα ήταν δυνατή χωρίς την καθοδήγηση και την υποστήριξη ανθρώπων στους οποίους οφείλω θερμές ευχαριστίες.

Πρωτίστως, θα ήθελα να εκφράσω τη βαθιά μου ευγνωμοσύνη στον επιβλέποντα καθηγητή μου, κ. Στέφανο Γκρίτζαλη, για την τιμή που μου έκανε να μου αναθέσει το συγκεκριμένο θέμα, καθώς και για την εμπιστοσύνη που μου έδειξε καθ' όλη τη διάρκεια της έρευνας. Οι εύστοχες παρατηρήσεις του, η επιστημονική του καθοδήγηση και η διάθεσή του να μοιραστεί την πολύτιμη εμπειρία του, υπήρξαν καθοριστικοί παράγοντες για την άρτια ολοκλήρωση του εγχειρήματος.

Τέλος, ένα μεγάλο ευχαριστώ οφείλω στην οικογένειά μου. Στους γονείς μου, για την αμέριστη ηθική και υλική υποστήριξη που μου παρείχαν, καθώς και για την υπομονή και την πίστη τους στις δυνατότητές μου. Η δική τους θυσία και ενθάρρυνση αποτέλεσαν το θεμέλιο για κάθε ακαδημαϊκό και επαγγελματικό μου βήμα.

Περιεχόμενα

1. Εισαγωγή 1
2. Βασικές Έννοιες και Ορισμοί 2
2.1 Επιχειρησιακή Συνέχεια (Business Continuity) 3
2.2 Διαχείριση Κρίσεων (Crisis Management) 3
2.3 Κρίσιμες Υποδομές και Πόροι (Critical Infrastructure & Resources) 3
2.3 Η Σημασία για τον Οργανισμό 5
3. Επιχειρησιακή Συνέχεια 5
3.1 Τα Πρότυπα της Επιχειρησιακής Συνέχειας 5
3.2 BCMS Συμφώνως ISO 8
3.2.1 PLAN Phase - Σχεδιασμός του BCMS 10
3.2.2 DO Phase - Υλοποίηση και λειτουργία του BCMS 11
3.2.3 CHECK Phase - Παρακολούθηση, έλεγχος και ανασκόπηση 11
3.2.4 ACT Phase - Διορθωτικές ενέργειες και συνεχής βελτίωση 12
3.3 Σχεδιασμός του BCMS 12
3.3.1 Context Establishment 12
3.3.2 Ηγεσία και δέσμευση της διοίκησης (Leadership) 18
3.3.3 Πολιτική και στόχοι επιχειρησιακής συνέχειας (Business Continuity Policy & Objectives) 20
3.4 Υλοποίηση και λειτουργία του BCMS 22
3.4.1 Business Impact Analysis 22
3.4.2 Αξιολόγηση κινδύνων (Risk Assessment) 25
3.4.3 Στρατηγικές επιχειρησιακής συνέχειας 26
3.4.4 Incident Response Teams 29
3.4.5 Business Continuity Plans και Playbooks 31
3.5 Παρακολούθηση, έλεγχος και ανασκόπηση 33
3.5.1 Continuous Monitoring and Review 34

3.5.2 Internal Audit 34
3.5.3 Management Review 34
3.6 Διορθωτικές ενέργειες και συνεχής βελτίωση 35
3.6.1 Μη συμμορφώσεις (non-conformities) και διορθωτικές ενέργειες (corrective actions) 35
3.6.2 Συνεχής βελτίωση και ενσωμάτωσή της σε ολόκληρο τον κύκλο PDCA 36
4. Πρακτική Αξιοποίηση της Τεχνητής Νοημοσύνης στην Επιχειρησιακή Συνέχεια 38
4.1 Εισαγωγή 38
4.2 Περιβάλλον Υλοποίησης & Τεχνολογικό Υπόβαθρο 38
4.2.1 Ανάλυση Στοίβας Λογισμικού (Software Stack Analysis) 39
4.2.2 Το Επιχειρησιακό Σενάριο: "Alpha Logistics" & Ransomware 42
4.3 Πειραματική Διαδικασία & Εκτέλεση Σεναρίου 43
4.3.1 Εισαγωγή και Διανυσματοποίηση Της Επιχειρησιακής Γνώσης 43
4.3.2 Σύνταξη Εξειδικευμένης Εντολής και Τελική Εκτέλεση 48
5. Συμπεράσματα, Αξιολόγηση και Μελλοντικές Επεκτάσεις 51
6. Βιβλιογραφία 54

Πίνακας Εικόνων

Εικόνα 1: Επιτυχής Δημιουργία Database 47
Εικόνα 2: Τελικό Prompt 50
Εικόνα 3: Απάντηση του Μοντέλου 51

Πίνακας Πινάκων και Διαγραμμάτων

Πίνακας 1: Σύγκριση Προτύπων ISO 22301 και NIST SP 800-34 7
Διάγραμμα 1: Μείωση Παραισθήσεων (Hallucinations) μέσω Σταδιακής Βελτιστοποίησης Εντολών 49

1. Εισαγωγή

Στο σύγχρονο, εξαιρετικά ασταθές και διασυνδεδεμένο επιχειρηματικό περιβάλλον, η έννοια της "σταθερότητας" έχει πάψει να θεωρείται δεδομένη. Οργανισμοί κάθε μεγέθους, από πολυεθνικές εταιρείες έως μικρομεσαίες επιχειρήσεις (ΜμΕ), λειτουργούν υπό τη διαρκή απειλή διαταρακτικών γεγονότων, τα οποία κυμαίνονται από φυσικές καταστροφές και γεωπολιτικές αναταράξεις έως, κυρίως, εξελιγμένες κυβερνοεπιθέσεις. Σε αυτό το πλαίσιο, η ικανότητα ενός οργανισμού να απορροφά τους κραδασμούς, να προσαρμόζεται και να συνεχίζει την παροχή των κρίσιμων λειτουργιών του —η Επιχειρησιακή Συνέχεια (Business Continuity)— αναδεικνύεται σε στρατηγική προτεραιότητα επιβίωσης και όχι απλώς σε μια τυπική διαδικασία κανονιστικής συμμόρφωσης.

Η παρούσα πτυχιακή εργασία εστιάζει στη μελέτη, την ανάλυση και την πρακτική εφαρμογή πλαισίων Επιχειρησιακής Συνέχειας, με στόχο την ενίσχυση της οργανωσιακής ανθεκτικότητας (organizational resilience). Η πολυπλοκότητα των σύγχρονων επιχειρησιακών διεργασιών και η εξάρτηση από ψηφιακές υποδομές καθιστούν ανεπαρκή την εμπειρική διαχείριση κρίσεων. Αντιθέτως, απαιτείται η υιοθέτηση δομημένων, διεθνώς αναγνωρισμένων προτύπων, τα οποία προσφέρουν μεθοδολογία, κοινή γλώσσα και μετρήσιμους στόχους. Κεντρικό ρόλο σε αυτή την προσπάθεια διαδραματίζει το πρότυπο ISO 22301, το οποίο θέτει τις παγκόσμιες προδιαγραφές για τα Συστήματα Διαχείρισης Επιχειρησιακής Συνέχειας (BCMS), σε συνδυασμό με το ISO/IEC 27001, το οποίο θωρακίζει την ασφάλεια των πληροφοριών.

Το θεωρητικό μέρος της εργασίας εμβαθύνει στη φιλοσοφία και τις απαιτήσεις αυτών των προτύπων. Αναλύεται διεξοδικά ο κύκλος Plan-Do-Check-Act (PDCA), ο οποίος αποτελεί τον μηχανισμό συνεχούς βελτίωσης της ετοιμότητας του οργανισμού. Ιδιαίτερη έμφαση δίνεται στις κρίσιμες διαδικασίες της Ανάλυσης Επιχειρησιακών Επιπτώσεων (Business Impact Analysis - BIA) και της Αξιολόγησης Κινδύνων (Risk Assessment). Μέσω αυτών, ένας οργανισμός καλείται να χαρτογραφήσει τις λειτουργίες του, να εντοπίσει τις αλληλεξαρτήσεις πόρων και να καθορίσει με ακρίβεια τους χρόνους ανάκαμψης (RTO, RPO, MTPD) που διαχωρίζουν την επιβίωση από την κατάρρευση. Η κατανόηση αυτού του θεωρητικού πλαισίου είναι απαραίτητη, καθώς αποτελεί τη "γνωσιακή βάση" πάνω στην οποία πρέπει να λαμβάνονται αποφάσεις υπό συνθήκες πίεσης.

Ωστόσο, η ύπαρξη σχεδίων και διαδικασιών στα χαρτιά δεν εγγυάται την επιτυχή εφαρμογή τους την ώρα της κρίσης. Η διαχείριση του τεράστιου όγκου πληροφορίας που περιέχεται στα εγχειρίδια πολιτικής, ειδικά σε στιγμές πανικού όπως κατά τη διάρκεια μιας επίθεσης Ransomware, αποτελεί πρόκληση για τον ανθρώπινο παράγοντα. Εδώ εντοπίζεται το πεδίο καινοτομίας της παρούσας μελέτης: η διερεύνηση του ρόλου της Τεχνητής Νοημοσύνης (AI) ως υποστηρικτικού εργαλείου στη διαχείριση της Επιχειρησιακής Συνέχειας.

Συγκεκριμένα, η εργασία εξετάζει τη δυνατότητα αξιοποίησης Μεγάλων Γλωσσικών Μοντέλων (Large Language Models - LLMs) για την άμεση ανάκληση πληροφοριών συμμόρφωσης και την παροχή κατευθύνσεων βάσει πολιτικής. Αναγνωρίζοντας όμως τους κινδύνους που ελλοχεύουν στη χρήση δημόσιων εργαλείων AI (όπως η διαρροή ευαίσθητων εταιρικών δεδομένων στο Cloud), η μελέτη προτείνει και δοκιμάζει πρακτικά μια αρχιτεκτονική Τοπικής Εκτέλεσης (Local Inference).

Στο πρακτικό μέρος, υλοποιείται ένα πείραμα προσομοίωσης κρίσης σε μια υποθετική εταιρεία ("Alpha Logistics"), όπου ένα τοπικό μοντέλο AI (Mistral 7B), ενισχυμένο με τεχνικές RAG (Retrieval-Augmented Generation), καλείται να λειτουργήσει ως "Ψηφιακός Σύμβουλος Κρίσης". Στόχος είναι να αποδειχθεί ότι η σύγχρονη τεχνολογία μπορεί να γεφυρώσει το χάσμα μεταξύ της "βαριάς" θεωρίας των προτύπων ISO και της άμεσης επιχειρησιακής ανάγκης, προσφέροντας λύσεις που είναι ταυτόχρονα έξυπνες, άμεσες και, κυρίως, απόλυτα ασφαλείς ως προς την ιδιωτικότητα των δεδομένων.

Συνοψίζοντας, η εργασία αυτή φιλοδοξεί να αποτελέσει έναν οδηγό για τη σύγκλιση της Διοικητικής Επιστήμης και της Πληροφορικής, αποδεικνύοντας ότι η ανθεκτικότητα στο μέλλον θα βασίζεται στον αρμονικό συνδυασμό αυστηρών διαδικασιών και προηγμένων τεχνολογικών εργαλείων.

2. Βασικές Έννοιες και Ορισμοί

Η κατανόηση των ορισμών της Επιχειρησιακής Συνέχειας, της Διαχείρισης Κρίσεων και των Κρίσιμων Υποδομών είναι απαραίτητη προτού αναλυθούν τα κανονιστικά πρότυπα και οι μεθοδολογίες υλοποίησης που παρουσιάζονται στα επόμενα κεφάλαια.

2.1 Επιχειρησιακή Συνέχεια (Business Continuity)

Ως Επιχειρησιακή Συνέχεια (Business Continuity - BC) ορίζεται η ικανότητα ενός οργανισμού να συνεχίζει την παράδοση προϊόντων ή την παροχή υπηρεσιών σε αποδεκτά προκαθορισμένα επίπεδα μετά από ένα διαταρακτικό (disruptive) γεγονός. Η Επιχειρησιακή Συνέχεια δεν αφορά απλώς την αποκατάσταση των συστημάτων πληροφορικής (κάτι που εμπίπτει στο Disaster Recovery), αλλά καλύπτει το σύνολο της λειτουργίας: ανθρώπινους πόρους, κτιριακές εγκαταστάσεις, εφοδιαστική αλυσίδα, επικοινωνίες και φήμη.

Ουσιαστικά, στόχος της BC είναι η δημιουργία ενός συστήματος πρόληψης και ανάκαμψης, το Business Continuity Management System (BCMS), ώστε ο οργανισμός να μην "παραλύσει" κατά τη διάρκεια μιας κρίσης, αλλά να διατηρήσει τις ζωτικές του λειτουργίες ενεργές.

2.2 Διαχείριση Κρίσεων (Crisis Management)

Η Διαχείριση Κρίσεων (Crisis Management) είναι η διαδικασία μέσω της οποίας ένας οργανισμός διαχειρίζεται ένα ευρύτερο διαταρακτικό και απροσδόκητο γεγονός που απειλεί να βλάψει τον οργανισμό, τα ενδιαφερόμενα μέρη του ή το ευρύ κοινό.

Σε αντίθεση με την Επιχειρησιακή Συνέχεια που εστιάζει στο *λειτουργικό* κομμάτι ("πώς θα συνεχίσει να δουλεύει η παραγωγή"), η Διαχείριση Κρίσεων εστιάζει στο *στρατηγικό* και *επικοινωνιακό* κομμάτι ("πώς λαμβάνουμε αποφάσεις υπό πίεση και πώς προστατεύουμε τη φήμη μας"). Για να είναι αποτελεσματική η διαχείριση μιας κρίσης απαιτείται γρήγορη λήψη αποφάσεων, συντονισμό διαφορετικών ομάδων και διαφανή επικοινωνία με το εσωτερικό και εξωτερικό περιβάλλον.

2.3 Κρίσιμες Υποδομές και Πόροι (Critical Infrastructure & Resources)

Η έννοια της επιχειρησιακής συνέχειας είναι άρρηκτα συνδεδεμένη με τη διαθεσιμότητα των πόρων που απαιτούνται για την εκτέλεση των δραστηριοτήτων ενός οργανισμού. Σύμφωνα με το ISO 22301, ως «πόροι» (resources) νοούνται όλα τα περιουσιακά στοιχεία, ανθρώπινα ή υλικά, που είναι απαραίτητα για τη λειτουργία, την παράδοση προϊόντων, υπηρεσιών και γενικότερα την επίτευξη των στόχων.

Η αναγνώριση και η χαρτογράφηση αυτών των πόρων αποτελεί το πρώτο βήμα για την κατανόηση των εξαρτήσεων του οργανισμού. Οι πόροι αυτοί κατηγοριοποιούνται συνήθως στις ακόλουθες πέντε (5) βασικές κατηγορίες:

1. **Ανθρώπινο Δυναμικό (People):** Ο σημαντικότερος πόρος για κάθε οργανισμό. Στο πλαίσιο της επιχειρησιακής συνέχειας, η ανάλυση δεν αφορά μόνο τον αριθμό των εργαζομένων, αλλά κυρίως τις εξειδικευμένες δεξιότητες και γνώσεις (skills & knowledge) που κατέχουν.
2. **Κτιριακές Εγκαταστάσεις και Φυσικό Περιβάλλον (Premises):** Αφορά τους φυσικούς χώρους όπου διεξάγονται οι εργασίες, όπως τα κεντρικά γραφεία, οι γραμμές παραγωγής, οι αποθήκες ή τα εμπορικά καταστήματα. Για παράδειγμα η απώλεια πρόσβασης σε μια κρίσιμη εγκατάσταση (π.χ. λόγω πυρκαγιάς ή πλημμύρας) απαιτεί άμεση ενεργοποίηση εναλλακτικών χώρων εργασίας (Disaster Recovery Sites) ή μετάβαση σε καθεστώς τηλεργασίας, εφόσον η φύση της εργασίας το επιτρέπει.
3. **Τεχνολογία και Εξοπλισμός (Technology & Equipment):** Περιλαμβάνει τόσο τις Τεχνολογίες Πληροφορικής και Επικοινωνιών (ICT), όπως servers, δίκτυα, εφαρμογές, όσο και τον επιχειρησιακό εξοπλισμό (Operational Technology - OT), όπως είναι τα μηχανήματα παραγωγής, τα οχήματα logistics ή ιατρικά μηχανήματα.
4. **Πληροφορία και Δεδομένα (Information & Data):** Στην ψηφιακή εποχή, τα δεδομένα αποτελούν συχνά το πολυτιμότερο περιουσιακό στοιχείο. Περιλαμβάνουν ηλεκτρονικά αρχεία, βάσεις δεδομένων, πνευματική ιδιοκτησία, αλλά και φυσικά αρχεία (hard copies) που είναι ζωτικά για τη λειτουργία (π.χ. νομικά συμβόλαια). Η ακεραιότητα, η εμπιστευτικότητα και κυρίως η διαθεσιμότητα των δεδομένων είναι κρίσιμη. Εδώ εισάγονται οι έννοιες του RPO (Recovery Point Objective), δηλαδή πόσα δεδομένα μπορεί να αντέξει να χάσει ο οργανισμός χωρίς να καταστραφεί.
5. **Προμηθευτές και Συνεργάτες (Suppliers & Partners):** Αφορά το εξωτερικό οικοσύστημα του οργανισμού, γνωστό ως εφοδιαστική αλυσίδα (Supply Chain). Κανένας οργανισμός δεν λειτουργεί σε κενό· εξαρτάται από τρίτους για την παροχή πρώτων υλών, υπηρεσιών υποστήριξης (outsourcing), ενέργειας, τηλεπικοινωνιών ή υπηρεσιών Cloud. Μια διακοπή στη λειτουργία ενός κρίσιμου προμηθευτή (π.χ. του Cloud Provider ή του προμηθευτή ρεύματος)

επηρεάζει άμεσα την ικανότητα του οργανισμού να παραδώσει το προϊόν του, μεταφέροντας τον κίνδυνο από τον συνεργάτη στον ίδιο τον οργανισμό.

6. **Αλληλεξαρτήσεις Πόρων (Interdependencies):** Είναι κρίσιμο να σημειωθεί ότι οι παραπάνω πόροι δεν λειτουργούν μεμονωμένα. Υπάρχουν ισχυρές αλληλεξαρτήσεις: το ανθρώπινο δυναμικό χρειάζεται εγκαταστάσεις και τεχνολογία για να εργαστεί, ενώ η τεχνολογία απαιτεί ενέργεια (από προμηθευτές) και δεδομένα για να λειτουργήσει. Η χαρτογράφηση αυτών των αλληλεξαρτήσεων είναι που καθιστά το Business Continuity Management System (BCMS) ένα ολοκληρωμένο σύστημα και όχι απλώς μια λίστα ελέγχου.

2.3 Η Σημασία για τον Οργανισμό

Η υιοθέτηση σχεδίων Επιχειρησιακής Συνέχειας και Διαχείρισης Κρίσεων έχει πλέον μετατραπεί από προαιρετική πολυτέλεια σε θεμελιώδη προϋπόθεση βιωσιμότητας. Η κρισιμότητά τους έγκειται στο ότι η ικανότητα ταχείας ανάκαμψης καθορίζει την επιβίωση του οργανισμού μετά από καταστροφικά συμβάντα, όπως φυσικές καταστροφές ή κυβερνοεπιθέσεις, ενώ παράλληλα διασφαλίζει την απαραίτητη συμμόρφωση με το ρυθμιστικό πλαίσιο και τις συμβατικές υποχρεώσεις. Επιπροσθέτως, η οργανωμένη αντίδραση θωρακίζει τη φήμη και το κύρος της επιχείρησης, ενισχύοντας την εμπιστοσύνη των ενδιαφερόμενων μερών και αποτρέποντας ανεπανόρθωτες βλάβες στο brand name. Αυτή η επιτακτική ανάγκη για δομημένη προετοιμασία και ανθεκτικότητα καθιστά αναγκαία την υιοθέτηση αναγνωρισμένων μεθοδολογιών και προτύπων, τα οποία αναλύονται διεξοδικά στο επόμενο κεφάλαιο, θέτοντας το πλαίσιο για την αποτελεσματική οργάνωση της επιχειρησιακής συνέχειας.

3. Επιχειρησιακή Συνέχεια

3.1 Τα Πρότυπα της Επιχειρησιακής Συνέχειας

Στο πεδίο της Επιχειρησιακής Συνέχειας, η ύπαρξη και η τήρηση δομημένων πλαισίων αναφοράς αποτελεί προϋπόθεση για συστηματική προετοιμασία και αποτελεσματική απόκριση σε διαταραχές. Τα πλαίσια πρέπει να προσφέρουν ολοκληρωμένες κατευθυντήριες γραμμές και βέλτιστες πρακτικές, βοηθώντας τους οργανισμούς να εντοπίζουν, να αξιολογούν και να διαχειρίζονται τους κινδύνους που απορρέουν από απρόβλεπτα περιστατικά. Εστιάζουμε σε δύο καίρια πρότυπα, τα οποία έχουν ευρέως υιοθετηθεί σε διαφορετικούς κλάδους ως σημείο

αναφοράς για την οργάνωση και λειτουργία ενός Business Continuity Management System (BCMS): το ISO 22301, που θέτει τις διεθνείς απαιτήσεις για τη δομημένη διαχείριση της επιχειρησιακής συνέχειας, και τον οδηγό NIST SP 800-34, ο οποίος αποτελεί βασικό πλαίσιο για τη σχεδίαση σχεδίων συνέχισης λειτουργίας σε περιβάλλοντα πληροφοριακών συστημάτων. Στο πλαίσιο της παρούσας εργασίας, το NIST SP 800-34 εξετάζεται συγκριτικά με το ISO 22301, με στόχο να αναδειχθούν οι διαφορές τους ως προς το αντικείμενο, την εστίαση και τον τρόπο οργάνωσης της επιχειρησιακής συνέχειας.

Το ISO 22301 αποτελεί το διεθνώς αναγνωρισμένο πρότυπο που καθορίζει τις απαιτήσεις για τη δημιουργία, εφαρμογή, λειτουργία, παρακολούθηση, ανασκόπηση, συντήρηση και συνεχή βελτίωση ενός Συστήματος Διαχείρισης Επιχειρησιακής Συνέχειας (Business Continuity Management System – BCMS). Σκοπός του είναι να υποστηρίξει τους οργανισμούς στην οργανωμένη προετοιμασία, στην έγκαιρη απόκριση και στην αποτελεσματική ανάκαμψη από απρόβλεπτα και διαταρακτικά συμβάντα, όπως σοβαρές τεχνικές αστοχίες, φυσικές καταστροφές ή κυβερνοεπιθέσεις. Το πρότυπο παρέχει ένα ολοκληρωμένο πλαίσιο για τον συστηματικό εντοπισμό απειλών, την αξιολόγηση των επιπτώσεών τους στις κρίσιμες λειτουργίες του οργανισμού, καθώς και για τον σχεδιασμό, την τεκμηρίωση και τη διαχείριση στρατηγικών και σχεδίων συνέχειας της λειτουργίας. Είναι εφαρμόσιμο σε οργανισμούς κάθε μεγέθους και κλάδου, δημόσιους ή ιδιωτικούς, και δίνει ιδιαίτερη έμφαση στην έννοια της ανθεκτικότητας (resilience), προωθώντας μια δομημένη, τεκμηριωμένη και στρατηγική προσέγγιση στην επιχειρησιακή συνέχεια.

Το NIST SP 800-34, με πλήρη τίτλο *Contingency Planning Guide for Federal Information Systems*, αποτελεί έναν από τους βασικούς οδηγούς του National Institute of Standards and Technology (NIST) για τη συνέχεια και την ανθεκτικότητα πληροφοριακών συστημάτων, παρέχοντας αναλυτικές κατευθύνσεις για τον σχεδιασμό, την τεκμηρίωση, τη συντήρηση και τη δοκιμή αποτελεσματικών σχεδίων αντιμετώπισης έκτακτων καταστάσεων. Εστιάζει πρωτίστως σε ομοσπονδιακές υπηρεσίες των ΗΠΑ, αλλά οι αρχές του μπορούν να αξιοποιηθούν ευρύτερα, καθώς καλύπτει ολόκληρο τον κύκλο ζωής της συνέχειας λειτουργίας ενός πληροφοριακού συστήματος, από την ανάλυση επιπτώσεων (Business Impact Analysis) και τη διαμόρφωση στρατηγικών ανάκαμψης, έως την ανάπτυξη, ενημέρωση και περιοδική δοκιμή των σχεδίων. Ως μέρος της σειράς NIST Special Publication 800, εντάσσεται στο γενικότερο πλαίσιο της κυβερνοασφάλειας και της διασφάλισης πληροφοριών, δίνοντας έμφαση στην προετοιμασία, στη

δομημένη διαδικασία ανάκαμψης και στη συστηματική επαλήθευση της αποτελεσματικότητας των σχεδίων.

Πίνακας 1: Σύγκριση Προτύπων ISO 22301 και NIST SP 800-34

Πρότυπο / Κριτήριο	ISO 22301	NIST SP 800-34
Μεθοδολογία	Κύκλος PDCA (Plan – Do – Check - Act). Requirements για να στηθεί, να λειτουργεί και να βελτιώνεται ένα πλήρες BCMS σε επίπεδο οργανισμού.	Handbook για contingency planning για σχέδια συνέχειας σε IT συστήματα περιγράφει βήματα (BIA, στρατηγικές, σχέδια, testing)
Κύριο Objective	Ορίζει απαιτήσεις για BCMS που εξασφαλίζει τη συνέχιση κρίσιμων λειτουργιών μετά από διαταραχές, με έμφαση στην οργανωσιακή ανθεκτικότητα.	Καθοδηγεί οργανισμούς (κυρίως ομοσπονδιακές υπηρεσίες ΗΠΑ) να φτιάξουν, να συντηρούν και να δοκιμάζουν contingency plans για πληροφοριακά συστήματα.
Βασικά Features	Τυποποιημένες clauses Ενσωμάτωση BIA, risk, strategies, plans, testing, continual improvement. Sector-agnostic, εφαρμόζεται από μικρές έως πολύ μεγάλες επιχειρήσεις.	Detailed βήματα για BIA, recovery strategies, plan development, maintenance, testing. Έμφαση σε system-level recovery (IT) αντί για ολιστικό BCMS.
Target Audience	Οποιοσδήποτε οργανισμός (δημόσιος/ιδιωτικός), κάθε κλάδος, κάθε μέγεθος, που θέλει δομημένο BCMS και πιθανή πιστοποίηση.	Κυρίως US Federal agencies, αλλά και άλλοι οργανισμοί που θέλουν δομημένο contingency planning για τα information systems τους.
Scope	Καλύπτει επιχειρησιακές λειτουργίες συνολικά (processes, people, facilities, IT, third parties). Δεν περιορίζεται σε IT, ούτε σε συγκεκριμένο κλάδο.	Καλύπτει πληροφοριακά συστήματα: IT assets, εφαρμογές, δεδομένα, υποδομές, υποστηρικτικές λειτουργίες που σχετίζονται με αυτά.
Focus	BCMS ως σύστημα διαχείρισης.	Ανάπτυξη και συντήρηση contingency plans για IT.

Συνοψίζοντας, το ISO 22301 λειτουργεί ως πλήρες σύστημα διαχείρισης επιχειρησιακής συνέχειας (BCMS) σε επίπεδο οργανισμού, με δομή PDCA, τυποποιημένες απαιτήσεις και δυνατότητα πιστοποίησης, καλύπτοντας διαδικασίες, ανθρώπους, υποδομές και IT. Αντίθετα, το NIST SP 800-34 αποτελεί κυρίως πρακτικό οδηγό για contingency planning σε πληροφοριακά συστήματα, με έμφαση σε BIA, στρατηγικές ανάκαμψης και ανάπτυξη/δοκιμή σχεδίων για IT. Το ISO 22301 έχει ευρύ, οριζόντιο scope και sector-agnostic χαρακτήρα, ενώ το NIST SP 800-34 είναι περισσότερο US-centric και IT-centric, χωρίς να συγκροτεί από μόνο του ένα πλήρες BCMS. Για τον σκοπό μιας ολιστικής προσέγγισης Business Continuity σε οργανωσιακό επίπεδο και στο

πλαίσιο της παρούσας εργασίας, το ISO 22301 προσφέρει πιο δομημένο και στρατηγικό πλαίσιο σε σχέση με το NIST SP 800-34.

3.2 BCMS Συμφώνως ISO

Ένα ολοκληρωμένο Σύστημα Διαχείρισης Επιχειρησιακής Συνέχειας (Business Continuity Management System - BCMS) δεν είναι απλώς ένα "σχέδιο έκτακτης ανάγκης", αλλά ένα δομημένο σύστημα διαχείρισης που περιλαμβάνει πολιτικές, ρόλους, διαδικασίες, αναλύσεις επιπτώσεων, στρατηγικές συνέχειας, σχέδια απόκρισης και μηχανισμούς συνεχούς βελτίωσης. Στόχος του είναι να διασφαλίζει ότι οι κρίσιμες λειτουργίες του οργανισμού μπορούν να συνεχιστούν ή να αποκατασταθούν μέσα σε αποδεκτά χρονικά όρια μετά από διαταραχές.

Κεντρικό σημείο αναφοράς αποτελεί το ISO 22301, το οποίο καθορίζει τι πρέπει να περιλαμβάνει ένα αποτελεσματικό BCMS: από τον καθορισμό του πλαισίου και του scope, μέχρι τη διενέργεια Business Impact Analysis, τον σχεδιασμό στρατηγικών συνέχειας, τη σύνταξη σχεδίων, τις ασκήσεις και τη συνεχή βελτίωση. Ωστόσο, για να μην μείνει το BCMS σε θεωρητικό επίπεδο, είναι κρίσιμο να το εντάξουμε σε έναν σαφή κύκλο ζωής διαχείρισης. Το ISO/IEC 27001 είναι το αντίστοιχο διεθνές πρότυπο για τα Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών (ISMS) και βασίζεται σε έναν σαφή κύκλο PLAN - DO - CHECK - ACT (PDCA), ώστε η ασφάλεια πληροφοριών να αντιμετωπίζεται ως συνεχής, επαναλαμβανόμενη διαδικασία και όχι ως εφάπαξ έργο.

Ο συνδυασμός των δύο προτύπων προσφέρει ένα ισχυρό πλαίσιο: το ISO 22301 προσδιορίζει τι πρέπει να περιλαμβάνει ένα αποτελεσματικό BCMS, ενώ το ISO/IEC 27001, μέσω του κύκλου PDC, μας δίνει πώς οργανώνουμε αυτό το σύστημα σε έναν ζωντανό κύκλο σχεδιασμού, υλοποίησης, ελέγχου και βελτίωσης.

Αφού παρουσιάστηκαν ο ρόλος του ISO 22301 ως βασικού πλαισίου για τη δομή και τις απαιτήσεις ενός BCMS και του ISO/IEC 27001 ως γενικού συστήματος διαχείρισης που οργανώνει τις σχετικές διεργασίες στον κύκλο PLAN - DO - CHECK - ACT, κρίνεται αναγκαίο να εξεταστούν και τα επιμέρους πρότυπα της ίδιας οικογένειας που εξειδικεύουν κρίσιμες πτυχές της επιχειρησιακής συνέχειας και της ασφάλειας πληροφοριών. Τα πρότυπα αυτά δεν λειτουργούν ανεξάρτητα, αλλά συμπληρώνουν τον κεντρικό κορμό, προσφέροντας πιο αναλυτική καθοδήγηση για δραστηριότητες όπως η ανάλυση επιπτώσεων, ο σχεδιασμός στρατηγικών και σχεδίων, η διαχείριση περιστατικών και η οργανωμένη αντιμετώπιση κρίσεων.

1. **ISO 22313:2020:** λειτουργεί ως οδηγός εφαρμογής του ISO 22301. Δεν εισάγει νέες απαιτήσεις, αλλά εξηγεί, με πρακτικά παραδείγματα και επεξηγήσεις, πώς μπορεί ένας οργανισμός να ανταποκριθεί στις απαιτήσεις του 22301. Αναλύει αναλυτικότερα ζητήματα όπως η ανάλυση πλαισίου, η BIA, οι στρατηγικές συνέχειας, η τεκμηρίωση σχεδίων, η εκπαίδευση, οι ασκήσεις και η ανασκόπηση, διευκολύνοντας τη μετάφραση της θεωρίας σε πρακτική εφαρμογή.
2. **ISO 22317:2021:** εστιάζει αποκλειστικά στη μεθοδολογία Business Impact Analysis. Περιγράφει βήμα-βήμα πώς ένας οργανισμός πρέπει να εντοπίζει κρίσιμες διεργασίες, να ορίζει κριτήρια επιπτώσεων, να αξιολογεί τις επιπτώσεις διακοπής, να προσδιορίζει χρονικά όρια όπως MTPD, RTO, RPO και να προτεραιοποιεί διεργασίες και πόρους. Ουσιαστικά παρέχει ένα αναλυτικό πλαίσιο για να σχεδιάζεται BIA με συνέπεια και τεκμηρίωση, πάνω στο οποίο "χτίζονται" οι στρατηγικές και τα σχέδια BC.
3. **ISO 22332:2021:** δίνει οδηγίες για το πώς πρέπει να είναι δομημένα και τι να περιέχουν τα σχέδια και οι διαδικασίες επιχειρησιακής συνέχειας. Περιγράφει στοιχεία όπως σκοπός, πεδίο εφαρμογής, ρόλοι, triggers ενεργοποίησης, βήματα απόκρισης, επικοινωνία, dependencies και απαιτήσεις πληροφόρησης. Στόχος του είναι να βοηθήσει τους οργανισμούς να σχεδιάζουν BC plans που είναι σαφή, εφαρμόσιμα σε πραγματικές συνθήκες και εύκολα στη χρήση από τις ομάδες που τα ενεργοποιούν σε διαταραχές.
4. **ISO 22361:2022:** αφορά τη διαχείριση κρίσεων σε επίπεδο οργανισμού. Δεν εστιάζει μόνο σε τεχνικές πτυχές αλλά στη στρατηγική και διοικητική διάσταση: καθορίζει αρχές crisis management, περιγράφει πώς δομείται το crisis management framework, ποιοι είναι οι ρόλοι και οι αρμοδιότητες της ομάδας κρίσης, πώς λαμβάνονται αποφάσεις υπό πίεση και πώς οργανώνεται η εσωτερική και εξωτερική επικοινωνία σε κρίσιμες καταστάσεις. Λειτουργεί συμπληρωματικά προς την επιχειρησιακή συνέχεια, καλύπτοντας τη φάση όπου ένα περιστατικό εξελίσσεται σε κρίση υψηλού αντίκτυπου.
5. **ISO/IEC 27002:2022:** είναι ένας αναλυτικός κατάλογος και οδηγός για τα controls ασφάλειας πληροφοριών. Δεν περιγράφει σύστημα διαχείρισης, αλλά δίνει λεπτομερείς περιγραφές μέτρων (τεχνικών, οργανωτικών, φυσικών κ.λπ.), οργανωμένων σε θεματικές κατηγορίες. Για κάθε control εξηγεί τον σκοπό, τη λειτουργία και ενδεικτικούς τρόπους υλοποίησης. Χρησιμοποιείται ως "toolbox" από

οργανισμούς που εφαρμόζουν το ISO/IEC 27001, αλλά και γενικότερα, για να επιλέγουν και να σχεδιάζουν κατάλληλα μέτρα ασφάλειας, συμπεριλαμβανομένων αυτών που σχετίζονται με επιχειρησιακή συνέχεια και αντιμετώπιση ransomware.

6. **ISO/IEC 27035-1:2023:** θέτει τις βασικές αρχές και το γενικό μοντέλο κύκλου ζωής της διαχείρισης περιστατικών ασφάλειας πληροφοριών. Περιγράφει έννοιες όπως incident, event, weakness, και καθορίζει τον κύκλο: προετοιμασία, αναγνώριση και αναφορά, αξιολόγηση και κλιμάκωση, απόκριση, αποκατάσταση και lessons learned. Στόχος του είναι να βοηθήσει τους οργανισμούς να δομήσουν μια συνεπή, επαναλαμβανόμενη διαδικασία incident management, η οποία συνδέεται τόσο με το ISMS όσο και με τα σχέδια επιχειρησιακής συνέχειας.
7. **ISO/IEC 27035-2:2023:** εξειδικεύει το μέρος 1, εστιάζοντας σε σχεδιασμό και υλοποίηση incident response plans και διαδικασιών. Περιγράφει πώς ο οργανισμός αναπτύσσει πολιτικές, ρόλους (π.χ. Incident Response Team), playbooks και λεπτομερή βήματα απόκρισης για διαφορετικούς τύπους περιστατικών (όπως ransomware, data breaches κ.λπ.). Παρέχει επίσης κατευθύνσεις για testing, ασκήσεις, συνεργασία με τρίτους και συνεχή βελτίωση των σχεδίων, ώστε η απόκριση σε περιστατικά να είναι συντονισμένη, έγκαιρη και αποτελεσματική.

3.2.1 PLAN Phase - Σχεδιασμός του BCMS

Στη φάση Plan ο οργανισμός θέτει τα θεμέλια του BCMS. Καθορίζει το context του οργανισμού (εσωτερικό και εξωτερικό περιβάλλον), αναγνωρίζει τα ενδιαφερόμενα μέρη και τις ανάγκες/προσδοκίες τους, ορίζει το scope του BCMS και διαμορφώνει την πολιτική επιχειρησιακής συνέχειας και τους στρατηγικούς στόχους του. Παράλληλα, η ανώτατη διοίκηση αναλαμβάνει σαφή δέσμευση για την υποστήριξη του BCMS, κατανέμει ρόλους και αρμοδιότητες, ενσωματώνει την επιχειρησιακή συνέχεια στη συνολική διακυβέρνηση του οργανισμού και διασφαλίζει ότι υπάρχουν οι απαραίτητοι πόροι, ικανότητες και μηχανισμοί τεκμηρίωσης.

Ιδιαίτερη έμφαση δίνεται στη δομημένη τεκμηρίωση: πολιτικές, διαδικασίες, μητρώα, καθώς και σαφής ορισμός του πώς θα παρακολουθούνται, θα ενημερώνονται και θα ελέγχονται στο μέλλον. Το Plan phase, επομένως, εστιάζει στο να δημιουργηθεί ένα συνεκτικό πλαίσιο

κανόνων, ρόλων και στόχων, πάνω στο οποίο θα «πατήσουν» οι επιχειρησιακές δραστηριότητες του BCMS.

3.2.2 DO Phase - Υλοποίηση και λειτουργία του BCMS

Στη φάση DO ο οργανισμός υλοποιεί όσα σχεδιάστηκαν στη φάση PLAN και θέτει στην πράξη το BCMS. Τεκμηριώνει και ενεργοποιεί τις στρατηγικές και τα σχέδια επιχειρησιακής συνέχειας, υλοποιεί τεχνικά και οργανωτικά μέτρα (όπως backup, εναλλακτικά sites, διαδικασίες ανάκαμψης IT) και εκπαιδεύει το προσωπικό στον ρόλο του σε περίπτωση διαταραχής. Στο πλαίσιο του DO πραγματοποιούνται επίσης η Business Impact Analysis (BIA) και η αξιολόγηση κινδύνων (risk assessment), ώστε να εντοπιστούν οι κρίσιμες διεργασίες, να αποτυπωθούν οι επιχειρησιακές απαιτήσεις και να επιλεγούν κατάλληλες στρατηγικές συνέχειας. Μέσα από τη BIA προσδιορίζονται οι αποδεκτοί χρόνοι διακοπής: ο Recovery Time Objective (RTO), δηλαδή ο μέγιστος αποδεκτός χρόνος εκτός λειτουργίας χωρίς μη αποδεκτές επιπτώσεις, ο Recovery Point Objective (RPO), δηλαδή η μέγιστη αποδεκτή απώλεια δεδομένων (πόσο πίσω στον χρόνο «γυρίζει» ο οργανισμός κατά την ανάκαμψη), και ο Maximum Tolerable Period of Disruption (MTPD), το απόλυτο όριο αντοχής μιας διεργασίας πέρα από το οποίο οι συνέπειες γίνονται καταστροφικές ή μη αναστρέψιμες. Σχεδιαστικά, ο RTO πρέπει να είναι πάντοτε μικρότερος από τον MTPD, ώστε τα μέτρα και οι στρατηγικές συνέχειας να στοχεύουν σε αποκατάσταση πολύ πριν ο οργανισμός πλησιάσει το «σημείο μη επιστροφής». Το ISO 22301 θέτει τις βασικές απαιτήσεις για BIA, risk assessment, στρατηγικές και σχέδια συνεχούς λειτουργίας, ενώ τα ISO 22313 και ISO 22317 παρέχουν λεπτομερέστερη καθοδήγηση για BIA και προσέγγιση κινδύνων, και τα ISO/IEC 27001, 27002, 27035-1, 27035-2, καθώς και το ISO 22332 και όπου χρειάζεται το ISO 22361, υποστηρίζουν την υλοποίηση μέτρων ασφάλειας, απόκρισης σε περιστατικά και δομημένων σχεδίων/διαδικασιών που κάνουν το BCMS λειτουργικό στην πράξη.

3.2.3 CHECK Phase - Παρακολούθηση, έλεγχος και ανασκόπηση

Στη φάση CHECK ο οργανισμός ελέγχει αν το BCMS λειτουργεί όπως σχεδιάστηκε. Παρακολουθεί την απόδοση μέσω δεικτών (KPIs), αναλύει αποτελέσματα ασκήσεων και δοκιμών, εξετάζει συμβάντα και σχετικές αποκλίσεις, διενεργεί εσωτερικούς ελέγχους και πραγματοποιεί ανασκόπηση από τη διοίκηση. Στόχος είναι να διαπιστωθεί αν τα σχέδια, τα μέτρα και οι διαδικασίες πράγματι επιτυγχάνουν τους στόχους (objectives) επιχειρησιακής συνέχειας. Το ISO 22301 και το ISO/IEC 27001 ορίζουν τις απαιτήσεις για monitoring, internal audit και

management review, ενώ τα ISO/IEC 27035-1, 27035-2 και το ISO 22361 προσθέτουν πλαίσιο για αποτίμηση της αποτελεσματικότητας στην απόκριση σε περιστατικά και κρίσεις.

3.2.4 ACT Phase - Διορθωτικές ενέργειες και συνεχής βελτίωση

Στη φάση Act ο οργανισμός αξιοποιεί τα ευρήματα του CHECK για να βελτιώσει το BCMS. Εντοπίζει μη συμμορφώσεις, κενά και αδυναμίες, ορίζει διορθωτικές ενέργειες και προσαρμόζει πολιτικές, διαδικασίες, BIA, στρατηγικές και σχέδια. Τα διδάγματα από ασκήσεις, περιστατικά και κρίσεις μετατρέπονται σε συγκεκριμένες αλλαγές, ώστε ο οργανισμός να γίνει πιο ανθεκτικός. Το ISO 22301 και το ISO/IEC 27001 δίνουν τις γενικές απαιτήσεις για corrective actions και continual improvement, ενώ τα ISO/IEC 27035-1, 27035-2, το ISO 22317, το ISO 22332 και το ISO 22361 υποστηρίζουν το πώς επανεξετάζονται και επικαιροποιούνται BIA, σχέδια, playbooks και δομές crisis/incident management μετά από πραγματική εμπειρία.

3.3 Σχεδιασμός του BCMS

3.3.1 Context Establishment

Στο BCMS, το *context establishment* είναι το πρώτο και πιο κρίσιμο βήμα της φάσης Plan. Ο οργανισμός σταματά να μιλά γενικά για "συνέχεια λειτουργίας" και απαντά σε ένα βασικό ερώτημα: *«Σε τι περιβάλλον λειτουργώ και τι μπορεί να επηρεάσει την ικανότητά μου να συνεχίσω;»*. Αυτό σημαίνει ότι εντοπίζει και αναλύει εξωτερικούς και εσωτερικούς παράγοντες που σχετίζονται με τους στόχους του, τα προϊόντα/υπηρεσίες και το ρίσκο που είναι διατεθειμένος να αναλάβει. Εξωτερικό πλαίσιο είναι, για παράδειγμα, το πολιτικό και ρυθμιστικό περιβάλλον, οι τεχνολογικές τάσεις, η οικονομική κατάσταση και οι εξαρτήσεις από κρίσιμους προμηθευτές. Εσωτερικό πλαίσιο είναι η οργανωτική δομή, οι βασικές διεργασίες, οι πόροι, η κουλτούρα, τα υφιστάμενα management systems και οι εσωτερικές εξαρτήσεις. Όλα αυτά "κουμπώνουν" τελικά στον καθορισμό του scope του BCMS: ποια τμήματα, εγκαταστάσεις, προϊόντα/υπηρεσίες και δραστηριότητες καλύπτει το σύστημα.

Ο καθορισμός του εξωτερικού πλαίσιού αφορά τη συστηματική κατανόηση του περιβάλλοντος μέσα στο οποίο λειτουργεί ο οργανισμός και κατ' επέκταση το BCMS. Σε αυτό το στάδιο εξετάζονται παράγοντες όπως το νομικό και ρυθμιστικό πλαίσιο, οι κλαδικές ιδιαιτερότητες, η οικονομική συγκυρία, οι τεχνολογικές εξελίξεις, οι κοινωνικές και περιβαλλοντικές συνθήκες, καθώς και η γεωπολιτική σταθερότητα. Παράλληλα, αξιολογούνται οι εξαρτήσεις από κρίσιμες υποδομές και βασικούς παρόχους υπηρεσιών, όπως είναι η ενέργεια, οι

τηλεπικοινωνίες και τα δίκτυα δεδομένων. Η ανάλυση αυτή επιτρέπει στον οργανισμό να εντοπίσει εξωτερικούς παράγοντες που μπορούν να προκαλέσουν ή να επιτείνουν διαταραχές στις βασικές του λειτουργίες.

Η αποτύπωση του εξωτερικού context δεν αποτελεί απλή περιγραφή του περιβάλλοντος, αλλά λειτουργεί ως καθοδηγητικό πλαίσιο για τον σχεδιασμό του BCMS. Μέσα από αυτήν την ανάλυση προσδιορίζονται οι κυριότερες εξωτερικές απειλές, οι ευκαιρίες για ενίσχυση της ανθεκτικότητας, καθώς και οι πιέσεις και απαιτήσεις που ασκούνται στον οργανισμό από την αγορά, τους ρυθμιστές και τα ενδιαφερόμενα μέρη. Με αυτόν τον τρόπο, οι στόχοι επιχειρησιακής συνέχειας, οι στρατηγικές και τα σχέδια που θα αναπτυχθούν στη συνέχεια βασίζονται σε μια ρεαλιστική κατανόηση του εξωτερικού περιβάλλοντος και όχι σε θεωρητικές υποθέσεις.

Το εσωτερικό πλαίσιο αφορά τα χαρακτηριστικά του ίδιου του οργανισμού, τα οποία επηρεάζουν άμεσα την ικανότητά του να σχεδιάσει, να εφαρμόσει και να διατηρήσει ένα αποτελεσματικό BCMS. Στο πλαίσιο αυτό εξετάζονται η οργανωτική δομή, τα επίπεδα ευθύνης και λήψης αποφάσεων, οι βασικές επιχειρησιακές διεργασίες και οι κρίσιμες λειτουργίες που στηρίζουν τα προϊόντα και τις υπηρεσίες του οργανισμού. Επιπλέον, αξιολογούνται οι διαθέσιμοι πόροι (ανθρώπινοι, τεχνικοί και οικονομικοί), οι τεχνολογικές υποδομές, η ωριμότητα σε θέματα διαχείρισης κινδύνου και ασφάλειας πληροφοριών, καθώς και η οργανωσιακή κουλτούρα σε σχέση με τη συνέχεια λειτουργίας.

Η συστηματική κατανόηση του εσωτερικού context επιτρέπει την αναγνώριση τόσο των δυνατών σημείων όσο και των αδυναμιών του οργανισμού, τα οποία θα επηρεάσουν τον σχεδιασμό και την υλοποίηση του BCMS. Παράλληλα, λαμβάνονται υπόψη τυχόν υφιστάμενα συστήματα διαχείρισης (όπως ένα ISMS), έτσι ώστε να αναζητηθούν συνέργειες και να αποφευχθούν επικαλύψεις. Η ενσωμάτωση του BCMS στο ευρύτερο πλαίσιο διακυβέρνησης και λειτουργίας του οργανισμού ενισχύει τη συνοχή, μειώνει τον κίνδυνο αποσπασματικών πρωτοβουλιών και διευκολύνει την αποδοχή του συστήματος από τα εμπλεκόμενα μέρη.

Κατά τον καθορισμό του πλαίσιού είναι απαραίτητο να ληφθούν οι υπόψη και να αναλυθούν επαρκώς οι παρακάτω παράγοντες που δύναται να επηρεάσουν:

- **Νομικές, ρυθμιστικές και συμβατικές υποχρεώσεις**

Οι νομικές, ρυθμιστικές και συμβατικές υποχρεώσεις αποτελούν κρίσιμο παράγοντα κατά τον καθορισμό του πλαισίου ενός BCMS και είναι απαραίτητο να καταγραφούν και να αναλυθούν

κατά τον καθορισμό του εξωτερικού πλαισίου. Ο οργανισμός καλείται να εντοπίσει και να τεκμηριώσει τους νόμους, τους κανονισμούς και τις κατευθυντήριες οδηγίες που επηρεάζουν την επιχειρησιακή συνέχεια. Αυτό μπορεί να περιλαμβάνει απαιτήσεις για ελάχιστα επίπεδα διαθεσιμότητας, υποχρέωση ύπαρξης τεκμηριωμένων σχεδίων συνέχειας, υποχρεώσεις αναφοράς περιστατικών ή διακοπών σε εποπτικές αρχές, καθώς και απαιτήσεις για την προστασία δεδομένων και την ασφάλεια πληροφοριών. Η συμμόρφωση με το ρυθμιστικό πλαίσιο δεν αποτελεί μόνο νομική υποχρέωση, αλλά και βασικό παράγοντα προστασίας της φήμης και της αξιοπιστίας του οργανισμού.

Παράλληλα, στον ίδιο άξονα εξετάζονται οι συμβατικές υποχρεώσεις που απορρέουν από συμφωνίες με πελάτες, προμηθευτές και άλλους συνεργάτες. Τέτοιες συμβάσεις μπορεί να περιλαμβάνουν συμβατικά καθορισμένους χρόνους αποκατάστασης, ρήτρες για καθυστέρηση ή διακοπή υπηρεσίας, απαιτήσεις για περιοδικές δοκιμές επιχειρησιακής συνέχειας ή ρήτρες ειδοποίησης σε περίπτωση διαταραχής. Η καταγραφή και η ανάλυση των υποχρεώσεων αυτών επιτρέπουν στον οργανισμό να μεταφράσει τις εξωτερικές απαιτήσεις σε συγκεκριμένες προδιαγραφές για το BCMS και να διασφαλίσει ότι οι στόχοι και τα σχέδια συνέχειας είναι συμβατά με τις νομικές και συμβατικές του δεσμεύσεις.

- **Ενδιαφερόμενα μέρη (Interested parties)**

Τα ενδιαφερόμενα μέρη αποτελούν βασικό στοιχείο του πλαισίου μέσα στο οποίο λειτουργεί το BCMS. Ως interested parties θεωρούνται όλα τα άτομα ή οι οντότητες που επηρεάζουν, επηρεάζονται ή θεωρούν ότι επηρεάζονται από την απόδοση του συστήματος επιχειρησιακής συνέχειας, είτε άμεσα είτε έμμεσα. Σε αυτά περιλαμβάνονται η ανώτατη διοίκηση, οι εργαζόμενοι, τα κρίσιμα τμήματα του οργανισμού, οι πελάτες, οι προμηθευτές, οι πάροχοι κρίσιμων υπηρεσιών, οι ρυθμιστικές αρχές, οι μέτοχοι και, όπου ενδείκνυται, η τοπική κοινωνία και οι αρχές εκτάκτων αναγκών. Η διαδικασία αποτύπωσης των ενδιαφερόμενων μερών πρέπει να είναι οργανωμένη και τεκμηριωμένη, ώστε να υπάρχει σαφήνεια ως προς το ποιοι θεωρούνται κρίσιμοι για τη συνέχεια λειτουργίας.

Πέρα από την απλή καταγραφή, ο οργανισμός καλείται να κατανοήσει σε βάθος τις ανάγκες, τις προσδοκίες και τις απαιτήσεις των interested parties. Αυτό μπορεί να περιλαμβάνει απαιτήσεις για συγκεκριμένους χρόνους αποκατάστασης, ελάχιστα επίπεδα υπηρεσίας κατά τη διάρκεια διακοπών, υποχρεώσεις ενημέρωσης σε περίπτωση συμβάντων, συμβατικές δεσμεύσεις

και ρυθμιστικές απαιτήσεις. Η ανάλυση αυτή τροφοδοτεί άμεσα τη διαμόρφωση των στόχων επιχειρησιακής συνέχειας και την επιλογή των κατάλληλων στρατηγικών και μέτρων. Με τον τρόπο αυτό, το BCMS δεν σχεδιάζεται με βάση αφηρημένες επιδιώξεις, αλλά αντανακλά τις πραγματικές ανάγκες και υποχρεώσεις του οργανισμού έναντι των βασικών του ενδιαφερόμενων μερών.

- **Πεδίο εφαρμογής (Scope) του BCMS**

Ο καθορισμός του πεδίου εφαρμογής του BCMS είναι κρίσιμο βήμα, καθώς ορίζει με ακρίβεια τα όρια μέσα στα οποία θα λειτουργεί το σύστημα. Στο σημείο αυτό ο οργανισμός προσδιορίζει ποιες δραστηριότητες, προϊόντα/υπηρεσίες, τοποθεσίες, υποδομές, πληροφοριακά συστήματα και οργανωτικές μονάδες καλύπτονται από το BCMS. Εξίσου σημαντική είναι και η τεκμηρίωση των εξαιρέσεων, δηλαδή των περιοχών που δεν εντάσσονται στο πεδίο εφαρμογής, μαζί με τους λόγους γι' αυτήν την απόφαση. Η σαφήνεια στο scope αποτρέπει παρερμηνείες και βοηθά όλες τις εμπλεκόμενες πλευρές να κατανοήσουν τι ακριβώς καλύπτει και τι δεν καλύπτει το σύστημα επιχειρησιακής συνέχειας.

Ένα προσεκτικά διαμορφωμένο scope διευκολύνει επίσης την ευθυγράμμιση του BCMS με άλλα συστήματα διαχείρισης που λειτουργούν στον οργανισμό. Σε περιβάλλον όπου συνυπάρχουν, για παράδειγμα, ISMS, είναι σημαντικό να παραμένει σαφές πού συμπίπτει και πού διαφοροποιείται το πεδίο εφαρμογής του BCMS. Επιπλέον, η τεκμηρίωση του scope αποτελεί βασικό στοιχείο τόσο για διαδικασίες εσωτερικού ελέγχου (internal audit) και ανασκόπησης από τη διοίκηση, όσο και για τυχόν εξωτερικές αξιολογήσεις ή πιστοποιήσεις. Καθίσταται έτσι θεμέλιο για κάθε επόμενη δραστηριότητα σχεδιασμού και υλοποίησης μέσα στο BCMS.

- **Όρεξη κινδύνου και κριτήρια επιπτώσεων (Risk Appetite & Impact Criteria)**

Κατά τον καθορισμό του πλαισίου, ο οργανισμός καλείται να αποσαφηνίσει την risk appetite του ή αλλιώς την "όρεξη κινδύνου" του σε σχέση με τη διακοπή λειτουργίας. Η όρεξη κινδύνου εκφράζει το επίπεδο αβεβαιότητας και διαταραχής που είναι διατεθειμένη να αποδεχθεί η διοίκηση, πριν θεωρηθεί ότι οι επιπτώσεις είναι μη ανεκτές. Η αποσαφήνιση αυτή συνδέεται άμεσα με τη στρατηγική του οργανισμού, τη νομική και ρυθμιστική του θέση, την ανοχή πελατών και ενδιαφερόμενων μερών σε διακοπές, καθώς και με την ευρύτερη κουλτούρα διαχείρισης

κινδύνου. Η όρεξη κινδύνου αποτυπώνεται συχνά σε ποιοτικούς και ποσοτικούς όρους και αποτελεί καθοδηγητικό σημείο αναφοράς για όλες τις επόμενες αποφάσεις.

Παράλληλα, προσδιορίζονται οι τύποι και τα κριτήρια επιπτώσεων (impact types and criteria) που θα χρησιμοποιηθούν στη Business Impact Analysis και στην αξιολόγηση κινδύνων. Τα κριτήρια αυτά συνήθως καλύπτουν διαστάσεις όπως οικονομικές επιπτώσεις, νομικές και ρυθμιστικές συνέπειες, επιπτώσεις στη λειτουργική ικανότητα, στη φήμη και στην ασφάλεια ή υγεία ενδιαφερόμενων. Για κάθε κριτήριο ορίζονται επίπεδα σοβαρότητας και αντίστοιχα όρια αποδοχής, ώστε να είναι δυνατή η συγκρίσιμη αξιολόγηση διαφορετικών σεναρίων διακοπής. Από τα κριτήρια αυτά προκύπτουν στη συνέχεια οι στόχοι ανάκαμψης (RTO, RPO, MTPD) και η προτεραιοποίηση διεργασιών και μέτρων, συνδέοντας έτσι άμεσα το context με τον πρακτικό σχεδιασμό της επιχειρησιακής συνέχειας. . Τέλος είναι σημαντικό να τονιστεί η διαφορά μεταξύ των consequence και impact types. Ο όρος *consequence type* αναφέρεται στις κατηγορίες συνεπειών ενός συγκεκριμένου συμβάντος κινδύνου. Αντίθετα, οι *impact types* χρησιμοποιούνται για να περιγράψουν τις επιπτώσεις από τη διακοπή μιας δραστηριότητας ή υπηρεσίας στον χρόνο, με βάση κατάλληλα κριτήρια (π.χ. οικονομικός αντίκτυπος, συμμόρφωση, λειτουργική ικανότητα, φήμη).

- **Κρίσιμα προϊόντα και υπηρεσίες**

Στο πλαίσιο του καθορισμού του context, ιδιαίτερη σημασία έχει η αναγνώριση των κρίσιμων προϊόντων και υπηρεσιών του οργανισμού. Κρίσιμα θεωρούνται εκείνα τα προϊόντα ή οι υπηρεσίες των οποίων η διακοπή θα είχε σημαντικές ή μη αποδεκτές επιπτώσεις στη λειτουργία, τη βιωσιμότητα, τη συμμόρφωση ή τη φήμη του οργανισμού. Η διαδικασία αυτή γίνεται συνήθως σε υψηλό επίπεδο και αποτελεί το σημείο εκκίνησης για την επακόλουθη Business Impact Analysis. Μέσα από αυτήν την αρχική αποτύπωση, ο οργανισμός διαχωρίζει τις δραστηριότητες που πρέπει να προστατευθούν κατά προτεραιότητα σε περίπτωση διαταραχής, από εκείνες που μπορούν να παραμείνουν εκτός λειτουργίας για μεγαλύτερα διαστήματα χωρίς κρίσιμες επιπτώσεις.

Η σαφής διάκριση κρίσιμων και μη κρίσιμων προϊόντων/υπηρεσιών βοηθά στον ρεαλιστικό σχεδιασμό του BCMS. Αντί να επιδιώκεται μια “απόλυτη” προστασία όλων των δραστηριοτήτων, ο σχεδιασμός εστιάζει στους τομείς με τη μεγαλύτερη σημασία, λαμβάνοντας υπόψη τόσο τα στρατηγικά όσο και τα ρυθμιστικά και συμβατικά κριτήρια. Στη συνέχεια, μέσω

της BIA, η αρχική αυτή ταξινόμηση εξειδικεύεται σε επίπεδο διεργασιών, πόρων και χρόνων αποκατάστασης (RTO, RPO, MTPD). Με τον τρόπο αυτό, η αναγνώριση κρίσιμων προϊόντων και υπηρεσιών λειτουργεί ως γέφυρα μεταξύ του γενικού πλαισίου και του αναλυτικού σχεδιασμού επιχειρησιακής συνέχειας.

- **Εξαρτήσεις και διασυνδέσεις (Dependencies & interfaces)**

Οι εξαρτήσεις και οι διασυνδέσεις διαμορφώνουν την "αόρατη υποδομή" πάνω στην οποία στηρίζεται η λειτουργία του οργανισμού. Σε επίπεδο BCMS, η κατανόησή τους είναι απαραίτητη για την αποτίμηση του πραγματικού κινδύνου διακοπής. Στη φάση του context establishment εντοπίζονται οι εσωτερικές εξαρτήσεις μεταξύ διεργασιών, συστημάτων, ομάδων και εγκαταστάσεων· για παράδειγμα, ποιες λειτουργίες προϋποθέτουν τη διαθεσιμότητα συγκεκριμένων IT συστημάτων ή ποια τμήματα στηρίζονται σε κρίσιμες υποστηρικτικές υπηρεσίες (όπως HR, procurement, logistics). Παράλληλα, καταγράφονται οι εξωτερικές εξαρτήσεις από τρίτους παρόχους υπηρεσιών, κρίσιμες υποδομές, συνεργάτες και υπεργολάβους.

Η χαρτογράφηση των dependencies επιτρέπει την αναγνώριση πιθανών "μοναδικών σημείων αποτυχίας" (single points of failure) και αλυσιδωτών επιπτώσεων σε περίπτωση διαταραχής. Έτσι, ο οργανισμός μπορεί να αξιολογήσει με μεγαλύτερη ακρίβεια τον αντίκτυπο μιας διακοπής σε ένα συγκεκριμένο σημείο της αλυσίδας αξίας ή της υποδομής του. Οι πληροφορίες αυτές τροφοδοτούν τόσο τη BIA όσο και τον σχεδιασμό στρατηγικών συνέχειας, εναλλακτικών λύσεων και συμβατικών απαιτήσεων προς τρίτους. Επιπλέον, υποστηρίζουν τον συντονισμό μεταξύ BCMS, incident management και crisis management, εξασφαλίζοντας ότι οι διασυνδέσεις λαμβάνονται υπόψη σε όλα τα επίπεδα σχεδιασμού και απόκρισης.

- **Υφιστάμενες δυνατότητες και κενά (Existing capabilities & gaps)**

Μέρος του καθορισμού πλαισίου είναι και η αποτύπωση των υφιστάμενων δυνατοτήτων του οργανισμού σε θέματα επιχειρησιακής συνέχειας και ασφάλειας πληροφοριών. Αυτό περιλαμβάνει την ύπαρξη τυχόν προηγούμενων σχεδίων BC, διαδικασιών έκτακτης ανάγκης, σχεδίων απόκρισης σε περιστατικά, μηχανισμών backup και ανάκαμψης, καθώς και σχετικής τεχνογνωσίας και εμπειρίας του προσωπικού. Η καταγραφή αυτή δίνει μια ρεαλιστική "γραμμή βάσης" (baseline) από την οποία ξεκινά ο σχεδιασμός του BCMS, δείχνοντας ποια στοιχεία

μπορούν να αξιοποιηθούν ή να ενσωματωθούν στο νέο σύστημα και ποια χρειάζονται ριζική αναθεώρηση.

Παράλληλα, εντοπίζονται τα βασικά κενά και αδυναμίες, όπως απουσία τυποποιημένων διαδικασιών, έλλειψη τεκμηριωμένων σχεδίων, ανεπαρκείς μηχανισμοί δοκιμών ή περιορισμένη ευαισθητοποίηση του προσωπικού σε θέματα συνέχειας. Η συστηματική αναγνώριση αυτών των gaps επιτρέπει την ιεράρχηση των παρεμβάσεων στη φάση Plan και τη διαμόρφωση ενός ρεαλιστικού προγράμματος υλοποίησης. Επιπλέον, παρέχει μελλοντικά σημείο αναφοράς για την αξιολόγηση της προόδου: η σύγκριση της αρχικής κατάστασης με την κατάσταση μετά την εφαρμογή του BCMS τεκμηριώνει αντικειμενικά τη βελτίωση της ανθεκτικότητας του οργανισμού.

- **Παραδοχές και περιορισμοί**

Τέλος, ο καθορισμός του πλαισίου ολοκληρώνεται με την καταγραφή των βασικών παραδοχών και περιορισμών μέσα στους οποίους καλείται να λειτουργήσει το BCMS. Παραδοχές μπορεί να αφορούν, ενδεικτικά, το επίπεδο διαθεσιμότητας του προσωπικού σε καταστάσεις κρίσης, την αξιοπιστία συγκεκριμένων προμηθευτών, την πρόσβαση σε εναλλακτικές εγκαταστάσεις ή τη διαθεσιμότητα κρίσιμων πόρων σε συνθήκες διαταραχής. Η τεκμηρίωση αυτών των παραδοχών συμβάλλει στη διαφάνεια και βοηθά να αποσαφηνιστεί ότι ο σχεδιασμός βασίζεται σε συγκεκριμένα δεδομένα και όχι σε αφηρημένες προσδοκίες.

Οι περιορισμοί αφορούν τους αντικειμενικούς φραγμούς που πρέπει να ληφθούν υπόψη κατά τον σχεδιασμό και την υλοποίηση του BCMS. Τέτοιοι περιορισμοί μπορεί να είναι οι διαθέσιμοι οικονομικοί πόροι, οι τεχνολογικές δυνατότητες, η πολυπλοκότητα των διεργασιών, οι χρονικοί ορίζοντες υλοποίησης, αλλά και απαιτήσεις που απορρέουν από το νομικό και ρυθμιστικό πλαίσιο. Η συνειδητή ενσωμάτωση παραδοχών και περιορισμών επιτρέπει τη διαμόρφωση ενός συστήματος επιχειρησιακής συνέχειας που είναι αφενός αποτελεσματικό και αφετέρου εφαρμόσιμο στην πράξη, ενώ δημιουργεί και σαφές πλαίσιο για μελλοντικές αναθεωρήσεις όταν αλλάζουν οι συνθήκες.

3.3.2 Ηγεσία και δέσμευση της διοίκησης (Leadership)

Η φάση Plan του BCMS δεν αφορά μόνο τεχνικές αναλύσεις, αλλά ξεκινά θεμελιωδώς από τη σαφή δέσμευση και κατεύθυνση της ανώτατης διοίκησης. Όλα τα επίπεδα της διοίκησης του οργανισμού οφείλουν να αναγνωρίσουν ρητά την επιχειρησιακή συνέχεια ως στρατηγική

προτεραιότητα και να την εντάξει στο συνολικό σύστημα διακυβέρνησης του οργανισμού, στο βαθμό που αναλογεί στο καθένα. Αυτό σημαίνει να συνδέει τους στόχους επιχειρησιακής συνέχειας με τη στρατηγική, το επιχειρηματικό μοντέλο και τις κανονιστικές απαιτήσεις, διασφαλίζοντας ότι το BCMS δεν πρέπει λειτουργεί ως "παράλληλο" σύστημα, αλλά ως οργανικό κομμάτι του τρόπου λειτουργίας του οργανισμού.

Η διοίκηση (Top Management) έχει επίσης την ευθύνη για τον καθορισμό και την έγκριση της πολιτικής επιχειρησιακής συνέχειας και των σχετικών στόχων. Η πολιτική BC πρέπει να ορίζει με σαφήνεια το σκοπό του BCMS, το επίπεδο ανθεκτικότητας που επιδιώκεται, τις αρχές που θα διέπουν τη διαχείριση διακοπών, καθώς και τις βασικές υποχρεώσεις συμμόρφωσης. Παράλληλα, η διοίκηση εγκρίνει στόχους επιχειρησιακής συνέχειας που είναι μετρήσιμοι, ρεαλιστικοί και ευθυγραμμισμένοι με την όρεξη κινδύνου και τις απαιτήσεις των ενδιαφερόμενων μερών. Σε αυτό το πλαίσιο, η φάση Plan περιλαμβάνει τόσο τη στρατηγική απόφαση "τι επίπεδο συνέχειας θέλουμε", όσο και τη μετατροπή της σε συγκεκριμένους στόχους που θα κατευθύνουν τη BIA, την αξιολόγηση κινδύνων και τον σχεδιασμό στρατηγικών.

Ένα ακόμη κρίσιμο καθήκον της ηγεσίας στη φάση Plan είναι η σαφής κατανομή ρόλων, αρμοδιοτήτων και εξουσιών για το BCMS. Η διοίκηση ορίζει ποιος έχει τη συνολική ευθύνη για τον συντονισμό του BCMS, ποιοι είναι οι ιδιοκτήτες των κρίσιμων διεργασιών, ποιος εγκρίνει τα αποτελέσματα της BIA και του risk assessment και ποιοι έχουν την ευθύνη για τη διαμόρφωση και την έγκριση των στρατηγικών συνέχειας. Η σαφής κατανομή αρμοδιοτήτων μειώνει τον κίνδυνο κενών ή επικαλύψεων, διευκολύνει τον συντονισμό μεταξύ διαφορετικών τμημάτων (π.χ. IT, operations, HR, νομικό) και δημιουργεί τις προϋποθέσεις ώστε το BCMS να υλοποιηθεί με συνέπεια και λογοδοσία.

Τέλος, η ανώτατη διοίκηση καλείται, ήδη από τη φάση Plan, να διασφαλίσει ότι το BCMS θα υποστηριχθεί με επαρκείς πόρους και κατάλληλη κουλτούρα. Αυτό περιλαμβάνει τη διάθεση επαρκούς χρόνου και προσωπικού για τη διενέργεια BIA, την αξιολόγηση κινδύνων και τον σχεδιασμό στρατηγικών, την υποστήριξη προγραμμάτων ευαισθητοποίησης και εκπαίδευσης, καθώς και την προώθηση κουλτούρας όπου η επιχειρησιακή συνέχεια θεωρείται κοινή ευθύνη και όχι αποκλειστική αρμοδιότητα μιας "ειδικής ομάδας". Με αυτόν τον τρόπο, η ηγεσία θέτει το πλαίσιο μέσα στο οποίο θα αναπτυχθούν οι τεχνικές και οργανωτικές λεπτομέρειες του BCMS, διασφαλίζοντας ότι τα σχέδια δεν θα μείνουν "στα χαρτιά", αλλά θα έχουν προϋποθέσεις να εφαρμοστούν στην πράξη.

Πέρα από την ανώτατη διοίκηση με την υποστήριξη όμως αυτής, κρίσιμο ρόλο στη φάση Plan και στη συνολική λειτουργία του BCMS διαδραματίζουν και τα υπόλοιπα επίπεδα διοίκησης, ιδίως η μεσαία και η λειτουργική διοίκηση (process owners, heads of departments, υπεύθυνοι IT, HR, Operations κ.λπ.). Τα στελέχη αυτά οφείλουν πρώτα απ' όλα να μεταφράσουν τη στρατηγική δέσμευση της διοίκησης σε συγκεκριμένες ενέργειες στον δικό τους τομέα ευθύνης: να συμμετέχουν ενεργά στην αποτύπωση του context, στην Business Impact Analysis και στην αξιολόγηση κινδύνων, παρέχοντας αξιόπιστα στοιχεία για τις διεργασίες, τους πόρους, τις εξαρτήσεις και τις ανεκτές διακοπές. Παράλληλα, καλούνται να ορίσουν και να τεκμηριώσουν τα κρίσιμα βήματα των διαδικασιών τους, να συμβάλουν στον καθορισμό ρεαλιστικών στόχων ανάκαμψης (RTO/RPO/MTPD) και να συνδιαμορφώσουν, σε συνεργασία με τον υπεύθυνο BCMS, τις κατάλληλες στρατηγικές και λύσεις επιχειρησιακής συνέχειας για τον τομέα τους.

Επιπλέον, τα υπόλοιπα επίπεδα διοίκησης έχουν ευθύνη για τη λειτουργική ενσωμάτωση του BCMS στην καθημερινή δραστηριότητα του οργανισμού: φροντίζουν ώστε οι ομάδες τους να είναι κατάλληλα εκπαιδευμένες και ενήμερες για τους ρόλους τους σε περίπτωση διαταραχής, διασφαλίζουν ότι οι επιχειρησιακές διαδικασίες, οι οδηγίες εργασίας και τα σχέδια BC που τους αφορούν παραμένουν ενημερωμένα, ευθυγραμμισμένα με τις απαιτήσεις των προτύπων και πρακτικά εφαρμόσιμα. Συμμετέχουν στον σχεδιασμό και στην εκτέλεση ασκήσεων (π.χ. tabletop, simulations), αξιολογούν τα αποτελέσματα, προτείνουν βελτιωτικές ενέργειες και παρακολουθούν την υλοποίησή τους. Με αυτόν τον τρόπο, λειτουργούν ως κρίσιμος "συνδετικός κρίκος" μεταξύ στρατηγικής ηγεσίας και καθημερινής λειτουργίας, υποστηρίζοντας τη συνεχή βελτίωση του BCMS και διασφαλίζοντας ότι οι απαιτήσεις επιχειρησιακής συνέχειας δεν μένουν σε επίπεδο πολιτικής, αλλά ενσωματώνονται ουσιαστικά στις πρακτικές του εκάστοτε τμήματος.

3.3.3 Πολιτική και στόχοι επιχειρησιακής συνέχειας (Business Continuity Policy & Objectives)

Η φάση Plan του BCMS προϋποθέτει τη διαμόρφωση μίας σαφούς και τεκμηριωμένης πολιτικής επιχειρησιακής συνέχειας, η οποία εγκρίνεται από την ανώτατη διοίκηση και αποτυπώνει τη στρατηγική κατεύθυνση του οργανισμού σε σχέση με τη συνέχεια των κρίσιμων λειτουργιών του. Η πολιτική αυτή ορίζει τον σκοπό του BCMS, επιβεβαιώνει τη δέσμευση για συμμόρφωση με τις σχετικές νομικές, ρυθμιστικές και συμβατικές απαιτήσεις, καθώς και για συνεχή βελτίωση της ικανότητας απόκρισης και ανάκαμψης. Παράλληλα, διευκρινίζει τις βασικές αρχές με τις οποίες ο οργανισμός θα αντιμετωπίζει διαταρακτικά γεγονότα (π.χ. προτεραιοποίηση

της ασφάλειας ανθρώπινου δυναμικού, προστασία κρίσιμων υπηρεσιών, διαφάνεια στην επικοινωνία) με όσο το δυνατό συνοπτικό, αλλά και περιεκτικό τρόπο.

Επιπλέον, η πολιτική επιχειρησιακής συνέχειας πρέπει να είναι ευθυγραμμισμένη με τη γενικότερη στρατηγική και τις λοιπές πολιτικές του οργανισμού, όπως την πολιτική ασφάλειας πληροφοριών, την πολιτική ποιότητας ή τη γενικότερη πολιτική διαχείρισης κινδύνων. Αυτό σημαίνει ότι η επιχειρησιακή συνέχεια δεν αντιμετωπίζεται ως απομονωμένη πρωτοβουλία, αλλά ενσωματώνεται στο ευρύτερο πλαίσιο διακυβέρνησης και λήψης αποφάσεων. Η πολιτική οφείλει επίσης να είναι κατάλληλα τεκμηριωμένη, να επικοινωνείται στα σχετικά επίπεδα (εσωτερικά και, όπου ενδείκνυται, σε εξωτερικά ενδιαφερόμενα μέρη) και να επανεξετάζεται περιοδικά, ώστε να παραμένει επίκαιρη ως προς το προφίλ κινδύνου, το επιχειρηματικό μοντέλο και το εξωτερικό περιβάλλον του οργανισμού. Τελικά ο στόχος είναι ο όρος επιχειρησιακή συνέχεια να είναι ριζωμένος στην κουλτούρα του οργανισμού, καθώς έτσι επιτυγχάνεται η διαχείριση των συμβάντων με τον καλύτερο τρόπο, ενώ ταυτόχρονα τυχόντες συνεργάτες, πελάτες ή άλλα ενδιαφερόμενα μέρη καθησυχάζονται λόγω της ικανότητας αυτής.

Στο ίδιο πλαίσιο, ο οργανισμός καλείται να θέσει συγκεκριμένους στόχους επιχειρησιακής συνέχειας (business continuity objectives), οι οποίοι να είναι μετρήσιμοι, ρεαλιστικοί και συνεπείς με την πολιτική. Οι στόχοι αυτοί συνδέονται με κρίσιμες διεργασίες και υπηρεσίες και μπορούν να περιλαμβάνουν, ενδεικτικά, απαιτήσεις για μέγιστους αποδεκτούς χρόνους διακοπής (RTO, MTPD), επίπεδα αποκατάστασης δεδομένων (RPO), συχνότητα και εύρος ασκήσεων BC, καθώς και στόχους για την ωριμότητα του BCMS. Κατά τον καθορισμό των στόχων λαμβάνονται υπόψη τα αποτελέσματα της BIA, η αξιολόγηση των κινδύνων, η όρεξη κινδύνου της διοίκησης και οι απαιτήσεις των interested parties, έτσι ώστε οι στόχοι να αντικατοπτρίζουν τόσο τις επιχειρησιακές προτεραιότητες όσο και τις υποχρεώσεις συμμόρφωσης.

Τέλος οι στόχοι επιχειρησιακής συνέχειας πρέπει να ανατίθενται σε κατάλληλα επίπεδα και λειτουργίες, να υποστηρίζονται από συγκεκριμένα σχέδια δράσης και να παρακολουθούνται συστηματικά μέσω δεικτών απόδοσης και σχετικών μηχανισμών αναφοράς. Η διατύπωσή τους σε μορφή "τι, ποιος, πότε και με ποιο μέτρο επιτυχίας" επιτρέπει τη σύνδεσή τους με τον κύκλο Plan – Do – Check - Act, καθώς και με τις αντίστοιχες διαδικασίες σχεδιασμού, υλοποίησης, παρακολούθησης και βελτίωσης του BCMS. Με αυτόν τον τρόπο, η πολιτική και οι στόχοι επιχειρησιακής συνέχειας λειτουργούν ως πρακτικό σημείο αναφοράς για όλα τα επόμενα βήματα: από τη λεπτομερή ανάλυση επιπτώσεων και κινδύνων, μέχρι τον σχεδιασμό στρατηγικών, την

ανάπτυξη σχεδίων και τη δοκιμή της συνολικής ικανότητας του οργανισμού να αντέχει και να ανακάμπτει από διαταραχές.

3.4 Υλοποίηση και λειτουργία του BCMS

Στη φάση Do ο οργανισμός περνά στην πρακτική υλοποίηση του BCMS. Τα στοιχεία που ορίστηκαν στη φάση Plan, δηλαδή context, scope, πολιτική, στόχοι, κριτήρια επιπτώσεων και ανοχής σε κίνδυνο – μεταφράζονται σε συγκεκριμένες δραστηριότητες και ρυθμίσεις λειτουργίας. Σε αυτό το στάδιο εκτελούνται στην πράξη η Business Impact Analysis (BIA) και η αξιολόγηση κινδύνων για τις επιχειρησιακές διεργασίες, επιλέγονται και εφαρμόζονται στρατηγικές επιχειρησιακής συνέχειας, σχεδιάζονται και τεκμηριώνονται τα Business Continuity Plans και οι διαδικασίες απόκρισης, και συγκροτείται η απαιτούμενη οργανωτική δομή απόκρισης (ομάδες BC, ομάδες απόκρισης σε περιστατικά κ.λπ.). Παράλληλα, ο οργανισμός διασφαλίζει ότι υπάρχουν οι απαραίτητοι πόροι, η εκπαίδευση προσωπικού και ένα αρχικό πρόγραμμα ασκήσεων και δοκιμών, ώστε τα σχέδια να μπορούν να ενεργοποιηθούν αποτελεσματικά όταν συμβεί διαταρακτικό γεγονός.

3.4.1 Business Impact Analysis

Η Business Impact Analysis (BIA) αποτελεί τον βασικό μηχανισμό με τον οποίο ο οργανισμός μεταφράζει την πολιτική και τους στόχους επιχειρησιακής συνέχειας σε συγκεκριμένες, μετρήσιμες απαιτήσεις ανάκαμψης. Στο στάδιο αυτό εντοπίζονται οι δραστηριότητες και υπηρεσίες που είναι κρίσιμες για την επίτευξη των στρατηγικών στόχων, αξιολογούνται οι επιπτώσεις από τη διακοπή τους σε διαφορετικούς χρονικούς ορίζοντες και προσδιορίζονται οι ανεκτές περίοδοι διακοπής. Με τον τρόπο αυτό, η BIA συνδέει άμεσα το "τι είναι σημαντικό για τον οργανισμό" με το "πόσο γρήγορα πρέπει να το επαναφέρουμε σε λειτουργία" σε περίπτωση διαταραχής. Η ποιότητα της διαδικασίας αυτής και των αποτελεσμάτων της, παίζουν καθοριστικό ρόλο στην επιλογή των κατάλληλων στρατηγιών και μέτρων επιχειρησιακής συνέχειας από τον οργανισμό.

Κεντρικό στοιχείο της BIA είναι η χρήση σαφώς ορισμένων impact criteria, ώστε η αξιολόγηση να είναι συνεπής, συγκρίσιμη και ευθυγραμμισμένη με το context και τη risk appetite που καθορίστηκαν στο προηγούμενο στάδιο. Ως επίπτωση ορίζεται το αποτέλεσμα της διακοπής μιας κρίσιμης δραστηριότητας. Ο οργανισμός επιλέγει πρώτα τους βασικούς τύπους επιπτώσεων (impact types) που τον ενδιαφέρουν, συνήθως οικονομικές επιπτώσεις, νομικές και ρυθμιστικές

συνέπειες, επιπτώσεις στη λειτουργική ικανότητα, στη φήμη, στην ασφάλεια ή υγεία ανθρώπων και, όπου είναι σχετικό, στο περιβάλλον. Στη συνέχεια ορίζει για κάθε τύπο επιπτώσεων επίπεδα σοβαρότητας (π.χ. χαμηλό, μέτριο, υψηλό, κρίσιμο) με συγκεκριμένες ποσοτικές ή ποιοτικές περιγραφές (όρια εσόδων, πρόστιμα, χρόνος διακοπής, αριθμός επηρεαζόμενων πελατών κ.λπ.). Τα κριτήρια αυτά λειτουργούν ως "μεταφραστής" της risk appetite σε πρακτικούς κανόνες: δείχνουν μέχρι ποιο σημείο μια διακοπή θεωρείται ανεκτή και από ποιο σημείο και μετά χαρακτηρίζεται μη αποδεκτή για τον οργανισμό. Η ανώτατη διοίκηση οφείλει να ελέγξει και να εγκρίνει τα impact criteria.

Μέσα από την εφαρμογή των impact criteria σε διαφορετικούς χρονικούς ορίζοντες διακοπής, η BIA οδηγεί στον προσδιορισμό κρίσιμων χρονικών παραμέτρων, όπως το Maximum Tolerable Period of Disruption (MTPD), το Recovery Time Objective (RTO) και το Recovery Point Objective (RPO) για κάθε κρίσιμη δραστηριότητα. Το MTPD εκφράζει το μέγιστο χρονικό διάστημα κατά το οποίο μια δραστηριότητα μπορεί να παραμείνει εκτός λειτουργίας πριν οι επιπτώσεις της διακοπής καταστούν μη ανεκτές. Το RTO προσδιορίζει τον στόχο χρόνου μέχρι τον οποίο πρέπει να έχει αποκατασταθεί η αποδεκτή λειτουργία, ενώ το RPO αποτυπώνει το μέγιστο αποδεκτό επίπεδο απώλειας δεδομένων (π.χ. πόσες ώρες ή μέρες συναλλαγών μπορεί να χάσει ο οργανισμός). Συνδυάζοντας αυτά τα στοιχεία, ο οργανισμός προτεραιοποιεί διεργασίες και πόρους, ταξινομεί τις δραστηριότητες ανά επίπεδο κρισιμότητας και θέτει συγκεκριμένες απαιτήσεις για τις στρατηγικές συνέχειας και τις λύσεις ανάκαμψης που θα σχεδιαστούν στη συνέχεια.

Σε επίπεδο διαδικασίας, η BIA ακολουθεί μια σειρά από διακριτά αλλά αλληλένδετα βήματα, όπως φαίνονται παρακάτω:

1. **Ορισμός στόχου, πεδίου και παραδοχών της BIA:** Πριν ξεκινήσει η συλλογή δεδομένων, ο οργανισμός ξεκαθαρίζει τι ακριβώς θέλει να πετύχει με τη BIA (π.χ. να εντοπίσει κρίσιμες διεργασίες για ένα συγκεκριμένο BCMS scope), ποιο είναι το πεδίο εφαρμογής (οργανωτικές μονάδες, υπηρεσίες, τοποθεσίες) και ποιες παραδοχές θα ισχύσουν (π.χ. διαθέσιμη ελάχιστη υποστήριξη IT, συγκεκριμένο χρονικό ορίζοντα ανάλυσης). Σε αυτό το στάδιο συμφωνούνται επίσης οι ρόλοι, οι ευθύνες και η μεθοδολογία (ερωτηματολόγια, συνεντεύξεις, workshops, έλεγχος αρχείων).

2. **Εντοπισμός δραστηριοτήτων, προϊόντων και υπηρεσιών:** Στη συνέχεια καταγράφονται οι βασικές δραστηριότητες του οργανισμού και οι υπηρεσίες/προϊόντα που παρέχει προς πελάτες και ενδιαφερόμενα μέρη. Για κάθε δραστηριότητα εξετάζεται αν συνδέεται άμεσα με τους στρατηγικούς στόχους και τις κανονιστικές υποχρεώσεις. Στόχος είναι να ξεχωρίσουν οι δραστηριότητες που έχουν πραγματική κρισιμότητα για την επιβίωση και τη φήμη του οργανισμού.
3. **Αξιολόγηση επιπτώσεων για συγκεκριμένους χρονικούς ορίζοντες:** Χρησιμοποιώντας τα impact criteria, ο οργανισμός εκτιμά πώς θα εξελίσσονταν οι επιπτώσεις αν μια δραστηριότητα διακοπεί για διαφορετικές περιόδους (π.χ. 2 ώρες, 8 ώρες, 24 ώρες, 3 ημέρες, 1 εβδομάδα). Σε αυτό το σημείο συνδέονται οι εκτιμήσεις με τις έννοιες MTPD (Maximum Tolerable Period of Disruption), RTO (Recovery Time Objective) και RPO (Recovery Point Objective), ώστε να προσδιοριστεί πότε η διακοπή γίνεται μη ανεκτή και πόσο γρήγορα πρέπει να επανέλθει η λειτουργία ή/και τα δεδομένα.
4. **Προτεραιοποίηση δραστηριοτήτων και πόρων:** Με βάση τις εκτιμήσεις επιπτώσεων και τα χρονικά όρια, ο οργανισμός κατατάσσει τις δραστηριότητες κατά σειρά κρισιμότητας. Στο σημείο αυτό προκύπτουν, για παράδειγμα, οι «υψηλής προτεραιότητας» διεργασίες που πρέπει να στηριχθούν πρώτες σε μία κρίση. Η προτεραιοποίηση μπορεί να γίνει με ποιοτική αξιολόγηση (π.χ. επίπεδα σοβαρότητας) ή με πιο ποσοτική προσέγγιση (scoring), αρκεί να είναι τεκμηριωμένη και συνεπής.
5. **Καταγραφή εξαρτήσεων και απαιτούμενων πόρων:** Για τις δραστηριότητες που έχουν χαρακτηριστεί κρίσιμες, καταγράφονται οι βασικές εξαρτήσεις: άνθρωποι, εγκαταστάσεις, τεχνολογικές υποδομές, εφαρμογές, δεδομένα, κρίσιμοι προμηθευτές, τρίτα μέρη. Αυτή η χαρτογράφηση είναι απαραίτητη ώστε, όταν εκτελεστεί η τελική αξιολόγηση, να λαμβάνεται υπόψη η πραγματική αλυσίδα αξίας και όχι μόνο μια «στενή» λειτουργία.
6. **Τεκμηρίωση, επικύρωση και ανάδραση:** Τα αποτελέσματα της BIA συγκεντρώνονται και τεκμηριώνονται σε τυποποιημένες φόρμες ή αναφορές. Στη συνέχεια, παρουσιάζονται στη διοίκηση και στα αρμόδια ενδιαφερόμενα μέρη για επικύρωση: επιβεβαιώνονται οι κρισιμότητες, οι χρόνοι MTPD/RTO/RPO και οι προτεραιότητες ανάκαμψης. Οποιαδήποτε ανατροφοδότηση ενσωματώνεται πριν τα αποτελέσματα της BIA χρησιμοποιηθούν στη φάση σχεδιασμού στρατηγικών συνέχειας και BC plans. Η BIA δεν

είναι εφάπαξ άσκηση· αναθεωρείται όταν αλλάζει ουσιαστικά το context, οι υπηρεσίες ή οι στόχοι.

3.4.2 Αξιολόγηση κινδύνων (Risk Assessment)

Η αξιολόγηση κινδύνων (risk assessment) στο BCMS είναι η διαδικασία με την οποία ο οργανισμός συνδέει όσα έμαθε από την ανάλυση επιπτώσεων (BIA) με τις συγκεκριμένες απειλές και τα σενάρια διαταραχής που μπορεί να αντιμετωπίσει. Ενώ η BIA απαντά στο «τι είναι κρίσιμο και πόσο γρήγορα πρέπει να επανέλθει», η αξιολόγηση κινδύνων απαντά στο «τι μπορεί να συμβεί, με ποια πιθανότητα και με ποιες συνέπειες». Σκοπός είναι να προσδιοριστούν οι BC-related κίνδυνοι που μπορούν να προκαλέσουν διακοπή ή σοβαρή υποβάθμιση κρίσιμων διεργασιών και να δημιουργηθεί μια τεκμηριωμένη βάση προτεραιοποίησης για τις στρατηγικές επιχειρησιακής συνέχειας και τα μέτρα που θα ακολουθήσουν.

Πριν ο οργανισμός αρχίσει να «μετρά» κινδύνους, πρέπει να καθορίσει σαφή κριτήρια κινδύνου (risk criteria). Τα κριτήρια αυτά συνδυάζουν: (α) τα impact criteria που έχουν ήδη οριστεί στη BIA (οικονομικές, νομικές/κανονιστικές, λειτουργικές, φήμης, ασφάλειας/υγείας κ.λπ.), (β) την όρεξη κινδύνου (risk appetite) και (γ) τα κατώφλια αποδοχής κινδύνου (risk acceptance thresholds) που θέτει η διοίκηση. Έτσι, ο οργανισμός ορίζει εκ των προτέρων τι θεωρεί «ανεκτό», «οριακό» ή «μη αποδεκτό» επίπεδο κινδύνου για κάθε κατηγορία επιπτώσεων και για διαφορετικά χρονικά σενάρια διακοπής. Αυτή η συμφωνημένη βάση επιτρέπει συνεπή και συγκρίσιμη αξιολόγηση, ώστε δύο διαφορετικά σενάρια (π.χ. φυσική καταστροφή και κυβερνοεπίθεση) να μπορούν να συγκριθούν με ενιαία λογική.

Στο στάδιο της αναγνώρισης κινδύνων, ο οργανισμός εντοπίζει όλα τα πιθανά γεγονότα που μπορούν να προκαλέσουν διακοπή ή σοβαρή υποβάθμιση των κρίσιμων διεργασιών που προέκυψαν από τη BIA. Αυτό περιλαμβάνει φυσικές απειλές (π.χ. πλημμύρες, σεισμοί), τεχνικές αστοχίες (π.χ. διακοπή ρεύματος, βλάβες σε data center), ανθρώπινα λάθη, σκόπιμες κακόβουλες ενέργειες (όπως ransomware ή εσωτερική δολιοφθορά) και εξαρτήσεις από τρίτους (π.χ. πάροχοι κρίσιμων υπηρεσιών). Η αναγνώριση γίνεται συνήθως μέσω workshops, interviews, reviews ιστορικών περιστατικών και ανάλυσης εξαρτήσεων (dependencies) ανάμεσα σε διεργασίες, πόρους και υποστηρικτικές υποδομές. Το αποτέλεσμα είναι ένας κατάλογος κινδύνων συνδεδεμένων με συγκεκριμένες υπηρεσίες/δραστηριότητες.

Αφού αναγνωριστούν οι κίνδυνοι, ακολουθεί η ανάλυσή τους με βάση δύο βασικές διαστάσεις: την πιθανότητα εμφάνισης (likelihood) και τις συνέπειες (consequences/impacts) σε σχέση με τα ήδη ορισμένα impact criteria και τα αποτελέσματα της BIA. Για κάθε σενάριο εξετάζονται ερωτήματα όπως: πόσο ρεαλιστικό είναι να συμβεί, ποιες διεργασίες επηρεάζει, σε ποιους χρονικούς ορίζοντες ξεπερνιούνται τα αποδεκτά RTO/RPO/MTPD, ποιες είναι οι άμεσες και έμμεσες συνέπειες για οικονομικά αποτελέσματα, κανονιστική συμμόρφωση, φήμη, ασφάλεια προσωπικού κ.λπ. Τα αποτελέσματα αποτυπώνονται σε risk register με σαφείς περιγραφές σεναρίων, υποθέσεων και εκτιμήσεων.

Στο στάδιο της αξιολόγησης, ο οργανισμός συγκρίνει τα εκτιμώμενα επίπεδα κινδύνου με τα καθορισμένα risk criteria και αποφασίζει ποιοι κίνδυνοι είναι ανεκτοί, ποιοι απαιτούν περαιτέρω μείωση και ποιοι είναι τόσο χαμηλής προτεραιότητας ώστε να παρακολουθούνται απλώς. Οι κίνδυνοι με υψηλό impact σε κρίσιμες διεργασίες και μικρούς χρονικούς ορίζοντες ανοχής (όπως αυτοί που μπορούν να οδηγήσουν σε παραβίαση νομικών υποχρεώσεων ή σοβαρή βλάβη στη φήμη) λαμβάνουν προτεραιότητα. Η αξιολόγηση αυτή οδηγεί στη διαμόρφωση στόχων για το risk treatment και στη σύνδεση με τις στρατηγικές επιχειρησιακής συνέχειας: οι υψηλού risk rating σενάρια (π.χ. εκτεταμένο ransomware, απώλεια βασικού data center, παρατεταμένη διακοπή κρίσιμου παρόχου) τροφοδοτούν άμεσα το σχεδιασμό BC strategies, σχεδίων και playbooks. Παράλληλα, καταγράφονται σαφώς και τηρείται αρχείο των αποφάσεων αποδοχής κινδύνου (risk acceptance) και οι αιτιολογήσεις τους.

3.4.3 Στρατηγικές επιχειρησιακής συνέχειας

Οι στρατηγικές επιχειρησιακής συνέχειας αποτελούν το κρίσιμο βήμα που μεταφράζει τα αποτελέσματα της BIA και της αξιολόγησης κινδύνων σε συγκεκριμένη κατεύθυνση δράσης για τον οργανισμό. Με βάση τις προτεραιοποιημένες διεργασίες, τα RTO/RPO/MTPD, τα impact και risk criteria και το risk appetite, ο οργανισμός καλείται να ταυτοποιήσει τις καταλληλότερες στρατηγικές και λύσεις (business continuity solutions) για να προστατεύσει τις πιο κρίσιμες δραστηριότητες, να τις σταθεροποιήσει όταν διαταραχθούν και να τις επαναφέρει σε αποδεκτό επίπεδο λειτουργίας, ενώ παράλληλα αποφεύγει, απαντά και διαχειρίζεται τις επιπτώσεις των διαταραχών. Οι στρατηγικές δεν είναι ακόμα αναλυτικά σχέδια, αλλά πλαισίωση υψηλού επιπέδου για το *πώς* ο οργανισμός επιλέγει να αντέξει και να ανακάμψει.

Σύμφωνα με τα πρότυπα, κάθε στρατηγική επιχειρησιακής συνέχειας οφείλει να αποτελείται από μία ή περισσότερες «λύσεις» (solutions). Ως λύση θεωρείται ένα πρακτικό μέσο

ή διευθέτηση (arrangement) που συμβάλλει στην προστασία και ανάκαμψη των προτεραιοποιημένων διεργασιών: για παράδειγμα, χρήση εναλλακτικού χώρου εργασίας, ύπαρξη εφεδρικής υποδομής IT, υλοποίηση ειδικών backup και restore διαδικασιών, συμβάσεις με τρίτους παρόχους ή εφαρμογή προσωρινών χειροκίνητων διαδικασιών. Ο οργανισμός οφείλει να διαθέτει έναν σαφή μηχανισμό για την ταυτοποίηση, αξιολόγηση, επιλογή και τελική έγκριση των στρατηγικών και των solutions, καθώς και για την εφαρμογή τους στην πράξη μέσω των σχεδίων BC.

Βασικός στόχος των στρατηγικών επιχειρησιακής συνέχειας είναι να εξασφαλίσουν ότι οι προτεραιοποιημένες διεργασίες προστατεύονται επαρκώς από σημαντικές απειλές, σταθεροποιούνται γρήγορα μετά από μία διαταραχή και επανέρχονται εντός των καθορισμένων RTO, ακόμη κι αν στην αρχική φάση λειτουργούν σε υποβαθμισμένο ή εναλλακτικό καθεστώς. Για να το επιτύχει αυτό, ο οργανισμός μπορεί είτε να μειώσει τον κίνδυνο που αντιμετωπίζουν αυτές οι διεργασίες (π.χ. μέσω ενισχυμένων ελέγχων ασφαλείας, redundancy ή φυσικής προστασίας), είτε να μειώσει την πιθανότητα να πληγούν από συγκεκριμένες απειλές, είτε –σε ορισμένες περιπτώσεις– να τις μεταφέρει εν μέρει ή πλήρως σε τρίτο οργανισμό (outsourcing), διατηρώντας όμως πάντα την τελική ευθύνη για την επιχειρησιακή συνέχεια.

Τα RTO λειτουργούν ως βασικός στόχος που πρέπει να επιτυγχάνουν οι στρατηγικές και οι λύσεις. Κατά τον σχεδιασμό, ο οργανισμός δεν περιορίζεται μόνο στο να επαναφέρει την κανονική μορφή της υπηρεσίας, αλλά εξετάζει αν μπορεί να παρέχει, για ένα διάστημα, εναλλακτική ή υποβαθμισμένη υπηρεσία που να καλύπτει βασικές ανάγκες μέχρι την πλήρη αποκατάσταση. Έτσι, η στρατηγική μπορεί να περιλαμβάνει συνδυασμό «γρήγορης προσωρινής λύσης» (temporary workaround) και σταδιακής πλήρους ανάκαμψης. Παράλληλα, πρέπει να διασφαλίζεται ότι οι κατάλληλοι άνθρωποι έχουν κινητοποιηθεί (BC team, IT, κρίσιμες λειτουργίες), ότι λαμβάνουν την υποστήριξη που χρειάζονται (σε επίπεδο πληροφόρησης, μέσων, ακόμη και ψυχολογικής υποστήριξης, όπου απαιτείται) και ότι ο οργανισμός μεριμνά και για όσους επηρεάζονται (πελάτες, εταίροι, πολίτες, ανάλογα με τον κλάδο). Σε ορισμένα σενάρια, κρίσιμο ρόλο παίζει και η διαθεσιμότητα ειδικού εξοπλισμού ή υποδομών που μειώνουν σημαντικά τον χρόνο ανάκαμψης.

Στην πράξη, οι στρατηγικές επιχειρησιακής συνέχειας συχνά ομαδοποιούνται σε ορισμένες τυπικές κατηγορίες. Μια πρώτη κατηγορία είναι το *activity relocation*, δηλαδή η μεταφορά της δραστηριότητας σε άλλη τοποθεσία ή σε τρίτο πάροχο, όπως η λειτουργία σε

εναλλακτικό site ή η χρήση εγκαταστάσεων τρίτων. Στη συνέχεια, το *resource relocation ή reallocation* αφορά τη μεταφορά ή την ανακατανομή κρίσιμων πόρων, ανθρώπινων, τεχνικών ή υλικών, προς τις διεργασίες με την υψηλότερη προτεραιότητα, ώστε να διασφαλιστεί ότι αυτές θα συνεχίσουν να λειτουργούν, έστω και σε μειωμένο επίπεδο. Μια τρίτη κατηγορία είναι οι *alternate processes και spare capacity*, όπου ο οργανισμός αξιοποιεί εναλλακτικές (συχνά απλοποιημένες ή χειροκίνητες) διαδικασίες και προϋπάρχουσα εφεδρική ικανότητα παραγωγής ή παροχής υπηρεσιών, που έχει προβλεφθεί από τη φάση του σχεδιασμού. Τέλος, οι *temporary workarounds* αποτελούν προσωρινές παρακάμψεις, όπως η χειροκίνητη καταγραφή, η χρήση εναλλακτικών καναλιών επικοινωνίας ή πρόχειρων διαδικασιών, που επιτρέπουν τη στοιχειώδη συνέχιση της λειτουργίας μέχρι την πλήρη αποκατάσταση των κανονικών συστημάτων και ροών.

Παράλληλα με τις παραπάνω κατηγορίες, τα πρότυπα αναγνωρίζουν και στρατηγικές που εστιάζουν περισσότερο στη μείωση της πιθανότητας εμφάνισης ή/και της έντασης των επιπτώσεων (threat και impact mitigation) και στη διαχείριση της διαταραχής ως γεγονός. Ενδεικτικά, η ασφαλιστική κάλυψη (insurance) για συγκεκριμένα σενάρια λειτουργεί ως μέσο μεταφοράς μέρους του οικονομικού κινδύνου, ενώ τα μέτρα προστασίας και αποκατάστασης περιουσιακών στοιχείων (asset protection & restoration) στοχεύουν τόσο στη θωράκιση των κρίσιμων assets όσο και στην ταχεία επαναφορά τους μετά από ένα περιστατικό. Συμπληρωματικά, οι στρατηγικές διαχείρισης φήμης (reputation management) οργανώνουν τον τρόπο με τον οποίο ο οργανισμός επικοινωνεί με τα ενδιαφερόμενα μέρη και διαχειρίζεται τις προσδοκίες τους κατά τη διάρκεια και μετά τη διαταραχή. Οι στρατηγικές αυτές δεν αντικαθιστούν τις «κλασικές» λύσεις επιχειρησιακής συνέχειας, αλλά τις συμπληρώνουν, προσφέροντας μια πιο ολοκληρωμένη προσέγγιση στη διαχείριση του συνολικού κινδύνου και των επιπτώσεων στον οργανισμό.

Εκτός από την επιλογή κατάλληλων στρατηγικών, ο οργανισμός οφείλει να εξετάσει συστηματικά και τις απαιτήσεις σε πόρους που προϋποθέτει η υλοποίησή τους. Οι πόροι αυτοί δεν περιορίζονται στο ανθρώπινο δυναμικό, αλλά περιλαμβάνουν επίσης την πληροφορία και τα δεδομένα που είναι απαραίτητα για τη λειτουργία των προτεραιοποιημένων διεργασιών, τη φυσική υποδομή (κτίρια, εγκαταστάσεις, βοηθητικά συστήματα), τον απαραίτητο εξοπλισμό και τα αναλώσιμα, τα κρίσιμα συστήματα και υπηρεσίες ICT, τα μέσα και τις διευθετήσεις μεταφοράς (transportation, logistics), τις οικονομικές δυνατότητες και τα χρηματοδοτικά περιθώρια του οργανισμού, καθώς και τους βασικούς συνεργάτες και προμηθευτές από τους οποίους εξαρτάται

η λειτουργία του. Η σαφής κατανόηση και τεκμηρίωση αυτών των resource requirements αποτελεί προϋπόθεση για ρεαλιστικές στρατηγικές επιχειρησιακής συνέχειας, καθώς διασφαλίζει ότι οι επιλεγμένες λύσεις μπορούν πράγματι να υποστηριχθούν σε συνθήκες διαταραχής και ότι δεν δημιουργούνται νέα σημεία αστοχίας λόγω υποεκτίμησης αναγκαίων πόρων.

Τελικά, οι επιλεγμένες στρατηγικές και λύσεις πρέπει να εγκρίνονται από την ανώτατη διοίκηση, να τεκμηριώνονται με σαφήνεια και να συνδέονται άμεσα με την πολιτική, τους στόχους επιχειρησιακής συνέχειας και τις απαιτήσεις των ενδιαφερομένων μερών. Αυτή η «δέσμη» εγκεκριμένων στρατηγικών αποτελεί την βάση πάνω στην οποία αναπτύσσονται τα αναλυτικά Business Continuity Plans, τα incident response plans και τα ειδικά playbooks, ώστε το BCMS να είναι πραγματικά εφαρμόσιμο στην πράξη.

3.4.4 Incident Response Teams

Οι ομάδες απόκρισης σε περιστατικά (incident response teams) αποτελούν το «ζωντανό» κομμάτι του BCMS στη φάση DO, καθώς είναι αυτές που καλούνται να ενεργοποιήσουν τα σχέδια επιχειρησιακής συνέχειας όταν συμβεί ένα διαταρακτικό γεγονός (disruptive event). Το πρότυπο ISO 22301 απαιτεί το top management να έχει ήδη ορίσει σαφείς ρόλους, αρμοδιότητες και γραμμές αναφοράς για την απόκριση σε περιστατικά, ώστε η δομή απόκρισης να μπορεί να ενεργοποιηθεί γρήγορα και χωρίς αμφισημίες. Η δομή αυτή συνήθως περιλαμβάνει ομάδες με διακριτούς ρόλους (π.χ. incident response, business continuity, crisis management) που λειτουργούν μέσα σε ένα κοινό πλαίσιο εντολών (chain of command), ευθυγραμμισμένο με τη γενική οργανωτική δομή και με τα εγκεκριμένα business continuity strategies και solutions. Στόχος είναι κάθε περιστατικό που ξεπερνά τις δυνατότητες της «καθημερινής» διοίκησης να μεταβαίνει ομαλά σε ένα οργανωμένο σχήμα αντιμετώπισης, με ξεκάθαρα ενεργοποιημένα σχέδια και προκαθορισμένα επίπεδα κλιμάκωσης.

Ο σχεδιασμός της incident response structure πρέπει να είναι ταυτόχρονα απλός, σαφής και προσαρμοσμένος στα χαρακτηριστικά του οργανισμού. Τα πρότυπα επισημαίνουν ότι η δομή δεν μπορεί να είναι «one size fits all»: πρέπει να λαμβάνει υπόψη τη διοικητική ιεραρχία, την οργανωτική κουλτούρα, το μέγεθος και την πολυπλοκότητα των δραστηριοτήτων, τις υποδομές (IT και φυσικές), τις επιλεγμένες business continuity solutions, καθώς και τις κύριες απειλές που αντιμετωπίζει ο οργανισμός (π.χ. ransomware, φυσικές καταστροφές, διακοπές παρόχων). Σε μικρούς οργανισμούς, μια ενιαία ομάδα μπορεί να καλύπτει τόσο το incident response όσο και τον συντονισμό της επιχειρησιακής συνέχειας, ενώ σε μεγαλύτερους απαιτούνται πολλαπλές ομάδες

με εξειδικευμένους ρόλους (operational, technical, communication, liaison με third parties). Κοινός παρονομαστής είναι ότι κάθε ομάδα πρέπει να έχει ξεκάθαρο scope, γνωστές αρμοδιότητες και προκαθορισμένο τρόπο συνεργασίας με τις υπόλοιπες.

Η αποτελεσματικότητα των ομάδων εξαρτάται σε μεγάλο βαθμό από τη δυνατότητά τους να ανιχνεύουν έγκαιρα τα incidents, να αξιολογούν τη σοβαρότητά τους και να αποφασίζουν αν απαιτείται ενεργοποίηση των business continuity plans. Ο οργανισμός οφείλει να διαθέτει μηχανισμούς παρακολούθησης συμβάντων (security events, alerts υποδομών, αναφορές σφαλμάτων) και διαδικασίες για την αρχική εκτίμηση της σοβαρότητας: τι συνέβη και πώς, ποιες υπηρεσίες και ποια interested parties επηρεάζονται, ποια είναι η πιθανή διάρκεια της διαταραχής και αν το περιστατικό ξεπερνά τα όρια των «καθημερινών» λειτουργικών αποκρίσεων. Τα προκαθορισμένα thresholds που έχουν τεθεί στη φάση σχεδιασμού (π.χ. όταν επηρεάζεται κρίσιμη υπηρεσία πάνω από συγκεκριμένο χρόνο, όταν υπάρχει κίνδυνος για ασφάλεια ανθρώπων ή κανονιστική συμμόρφωση) λειτουργούν ως φίλτρο για να κριθεί αν θα ενεργοποιηθούν τα αντίστοιχα BC plans και οι σχετικές ομάδες.

Όταν ένα incident κριθεί αρκετά σοβαρό ώστε να ενεργοποιήσει τη δομή επιχειρησιακής συνέχειας, οι ομάδες καλούνται να διαχειριστούν τόσο τις άμεσες συνέπειες όσο και τη μετάβαση σε «κατάσταση συνέχειας» σύμφωνα με τα εγκεκριμένα σχέδια. Πρακτικά, αυτό σημαίνει ότι πρέπει να αναλύσουν τη φύση και το εύρος της διαταραχής, να εκτιμήσουν τα impacts σε σχέση με τα καθορισμένα impact thresholds και RTO, να αποφασίσουν ποια σχέδια BC ενεργοποιούνται, ποιες δραστηριότητες θα λειτουργήσουν σε υποβαθμισμένη μορφή ή μέσω εναλλακτικών διαδικασιών και ποιες προτεραιότητες τίθενται πρώτα (με πρώτη πάντα την προστασία της ανθρώπινης ζωής και της ασφάλειας). Τα business continuity plans οφείλουν να παρέχουν σαφείς οδηγίες: σκοπό και objectives του κάθε πλάνου, activation criteria, βήματα υλοποίησης, απαιτούμενους πόρους, εσωτερικές και εξωτερικές εξαρτήσεις, καθώς και κριτήρια «λήξης» του πλάνου (standing down criteria) όταν η κατάσταση σταθεροποιηθεί.

Κρίσιμο στοιχείο της λειτουργίας των incident response και BC teams είναι η διαχείριση της επικοινωνίας. Τα πρότυπα τονίζουν ότι ο οργανισμός πρέπει να έχει ξεκάθαρες διαδικασίες για το τι πληροφορίες διακινούνται, πότε, σε ποιον και μέσω ποιων καναλιών. Αυτό περιλαμβάνει εσωτερική επικοινωνία (ενημέρωση διοίκησης, εμπλεκόμενων τμημάτων και προσωπικού), εξωτερική επικοινωνία με interested parties (πελάτες, προμηθευτές, ρυθμιστικές αρχές, συνεργάτες) και, όπου χρειάζεται, σχέσεις με τα μέσα ενημέρωσης. Πρέπει να έχουν οριστεί

υπεύθυνοι για την έγκριση και μετάδοση κρίσιμων μηνυμάτων, να διασφαλίζεται η διαθεσιμότητα και η λειτουργικότητα του communication equipment (τηλεπικοινωνιακά μέσα, εναλλακτικά κανάλια), καθώς και να καταγράφονται συστηματικά τα γεγονότα, οι αποφάσεις και οι ενέργειες. Η τεκμηριωμένη ροή πληροφορίας δεν είναι μόνο απαραίτητη για την αποτελεσματική διαχείριση του συμβάντος, αλλά και για το μετέπειτα learning και τη βελτίωση του BCMS.

Τέλος, η επάρκεια των incident response teams δεν μπορεί να θεωρείται δεδομένη χωρίς συστηματική εκπαίδευση, ασκήσεις και δοκιμές. Τα πρότυπα προβλέπουν ότι τα μέλη των ομάδων πρέπει να διαθέτουν τις απαραίτητες γνώσεις και δεξιότητες για τους ρόλους που έχουν αναλάβει, να εκπαιδεύονται τακτικά πάνω στα σχέδια, τις διαδικασίες και τα εργαλεία που θα χρησιμοποιήσουν και να συμμετέχουν σε ασκήσεις επιχειρησιακής συνέχειας (table-top, simulation, technical tests). Μέσα από αυτές τις ασκήσεις δοκιμάζονται στην πράξη η δομή, οι ροές επικοινωνίας, οι χρόνοι απόκρισης και η ικανότητα συντονισμού μεταξύ ομάδων και τρίτων. Τα ευρήματα των ασκήσεων και των πραγματικών περιστατικών πρέπει να καταγράφονται, να αναλύονται και να τροφοδοτούν διορθωτικές ενέργειες και βελτιώσεις στα σχέδια, στη δομή και στην εκπαίδευση, κλείνοντας έτσι τον κύκλο PDCA του BCMS.

3.4.5 Business Continuity Plans και Playbooks

Όπως αναφέρθηκε και πρωτύτερα, η αποτελεσματική υλοποίηση ενός Business Continuity Management System προϋποθέτει την ανάπτυξη, τεκμηρίωση και συντήρηση κατάλληλων Business Continuity Plans και επιχειρησιακών playbooks, τα οποία μεταφράζουν τις στρατηγικές αποφάσεις του οργανισμού σε εφαρμόσιμες οδηγίες δράσης. Η ανώτατη διοίκηση (top management) οφείλει να αναθέσει ρητά την ευθύνη για τον σχεδιασμό και την επίβλεψη αυτών των σχεδίων σε πρόσωπα με την κατάλληλη αρμοδιότητα, εμπειρία και βαθμό ευθύνης, εξασφαλίζοντας ότι τα σχέδια καλύπτουν πλήρως το σκοπό και το εύρος (scope) του BCMS.

Οι αρμοδιότητες αυτές περιλαμβάνουν, μεταξύ άλλων, τη διαχείριση έργων επιχειρησιακής συνέχειας, τον σχεδιασμό και την εναρμόνιση των σχεδίων με τις απαιτήσεις του οργανισμού, τη διασφάλιση της συνέπειας μεταξύ διαφορετικών σχεδίων και διαδικασιών, καθώς και την τελική έγκριση (authorization) των Business Continuity Plans πριν από την εφαρμογή τους. Όλες οι σχετικές διαδικασίες πρέπει να είναι επαρκώς τεκμηριωμένες, ώστε να είναι σαφείς, προσβάσιμες και άμεσα αξιοποιήσιμες από τις ομάδες που καλούνται να τις εφαρμόσουν υπό συνθήκες πίεσης.

Τα πρότυπα αναγνωρίζουν ότι διαφορετικές ομάδες εντός του οργανισμού έχουν διαφορετικούς ρόλους κατά τη διαχείριση μιας διαταραχής και, κατά συνέπεια, απαιτούνται διαφορετικά επίπεδα σχεδίων. Σε αυτό το πλαίσιο, τα Business Continuity Plans οργανώνονται συνήθως σε τρία συμπληρωματικά επίπεδα: στρατηγικό, τακτικό και επιχειρησιακό. Κάθε επίπεδο εξυπηρετεί διακριτό σκοπό, αλλά ταυτόχρονα πρέπει να είναι πλήρως ευθυγραμμισμένο με τα υπόλοιπα.

Τα στρατηγικά σχέδια (strategic plans) υποστηρίζουν τη λήψη αποφάσεων από την ανώτατη διοίκηση και στοχεύουν στη διασφάλιση ότι η απόκριση του οργανισμού σε ένα περιστατικό είναι συντονισμένη, αποτελεσματική και έγκαιρη. Τα σχέδια αυτά παρέχουν το πλαίσιο για την εκτίμηση της σοβαρότητας της διαταραχής, την κατεύθυνση της συνολικής απόκρισης, τη διαχείριση της φήμης και της εικόνας του οργανισμού, καθώς και την επικοινωνία με εξωτερικά ενδιαφερόμενα μέρη και αρμόδιες αρχές. Παράλληλα, υποστηρίζουν τη συμμόρφωση με νομικές και κανονιστικές υποχρεώσεις καθ' όλη τη διάρκεια του περιστατικού. Ο υπεύθυνος (plan owner) των στρατηγικών σχεδίων είναι συνήθως μέλος της ανώτατης διοίκησης, με την εξουσία να λαμβάνει κρίσιμες αποφάσεις για τον οργανισμό.

Σε επίπεδο τακτικών σχεδίων (tactical plans), η έμφαση μετατοπίζεται στη διαχείριση της επιχειρησιακής συνέχειας των κρίσιμων διεργασιών και δραστηριοτήτων. Τα σχέδια αυτά παρέχουν καθοδήγηση για το πώς θα συνεχιστεί η παροχή προϊόντων και υπηρεσιών, πώς θα κατανεμηθούν ή θα ανακατανεμηθούν οι απαραίτητοι πόροι και πώς θα συντονιστούν διαφορετικές λειτουργικές μονάδες του οργανισμού. Τα τακτικά σχέδια λειτουργούν ως σύνδεσμος μεταξύ στρατηγικών αποφάσεων και επιχειρησιακής εκτέλεσης, ορίζοντας σαφώς τις σχέσεις μεταξύ των μελών της ομάδας, αλλά και τις διασυνδέσεις τους με τα στρατηγικά και επιχειρησιακά σχέδια. Σε λιγότερο σύνθετους οργανισμούς, τα τακτικά και επιχειρησιακά σχέδια ενδέχεται να συγχωνεύονται, χωρίς όμως να χάνεται η λειτουργική τους διάκριση. Ο υπεύθυνος των τακτικών σχεδίων πρέπει να διαθέτει την αρμοδιότητα να λαμβάνει αποφάσεις για τον τομέα ευθύνης του και να διασφαλίζει την ομαλή υλοποίηση των προβλεπόμενων ενεργειών.

Τα επιχειρησιακά σχέδια (operational plans) εστιάζουν στην άμεση και πρακτική αντιμετώπιση των συνεπειών μιας διαταραχής. Παρέχουν σαφείς, προσανατολισμένες στη δράση οδηγίες για το πώς οι ομάδες θα αντιδράσουν στα αρχικά αποτελέσματα ενός περιστατικού και πώς θα διατηρήσουν τον έλεγχο της κατάστασης έως ότου αποκατασταθούν οι κρίσιμες λειτουργίες. Τα σχέδια αυτά απαιτούν λεπτομερή γνώση των επιχειρησιακών διεργασιών και, για

τον λόγο αυτό, ο υπεύθυνος (plan owner) είναι συνήθως επικεφαλής επιχειρησιακής μονάδας ή άτομο με εκτενή πρακτική εμπειρία στις δραστηριότητες που πρέπει να αποκατασταθούν. Ο υπεύθυνος αυτός φέρει και την ευθύνη για τη συντήρηση και επικαιροποίηση του σχεδίου.

Τα Business Continuity Plans και τα playbooks οφείλουν να περιλαμβάνουν σαφώς καθορισμένο σκοπό και στόχους, κριτήρια ενεργοποίησης, διαδικασίες εφαρμογής, απαιτήσεις και ροές επικοινωνίας, εσωτερικές και εξωτερικές εξαρτήσεις, απαιτήσεις πόρων, καθώς και μηχανισμούς τεκμηρίωσης και αναφοράς αποφάσεων και ενεργειών. Επιπλέον, πρέπει να προβλέπουν κριτήρια παύσης (standing down) και επιστροφής στην κανονική λειτουργία. Η αποτελεσματικότητά τους ενισχύεται σημαντικά μέσω της εκπαίδευσης των ομάδων και της διεξαγωγής ασκήσεων και προσομοιώσεων, όπως προτείνεται στο ISO 22332, ώστε το απαιτούμενο επίπεδο γνώσεων και δεξιοτήτων να διατηρείται και να βελτιώνεται διαρκώς.

Συνολικά, η ύπαρξη καλά δομημένων και συνεκτικών Business Continuity Plans και playbooks διασφαλίζει ότι ο οργανισμός μπορεί να ανταποκριθεί συντονισμένα, έγκαιρα και αποτελεσματικά σε περιστατικά και διαταραχές, μετατρέποντας το BCMS από θεωρητικό πλαίσιο σε πρακτικό εργαλείο επιχειρησιακής ανθεκτικότητας.

Με την ολοκλήρωση της φάσης Do, ο οργανισμός έχει πλέον μετατρέψει τις απαιτήσεις και τις αποφάσεις της φάσης Plan σε συγκεκριμένες, λειτουργικές ρυθμίσεις: έχουν υλοποιηθεί η BIA και η αξιολόγηση κινδύνων, έχουν επιλεγεί και εγκριθεί στρατηγικές επιχειρησιακής συνέχειας, έχουν διαμορφωθεί τα αντίστοιχα Business Continuity Plans και έχει εγκαθιδρυθεί η δομή απόκρισης σε περιστατικά με σαφείς ρόλους, αρμοδιότητες και ροές επικοινωνίας. Σε αυτό το σημείο, το BCMS δεν είναι πλέον ένα θεωρητικό σχήμα, αλλά ένα ζωντανό σύστημα που λειτουργεί στην πράξη. Το επόμενο κρίσιμο βήμα, όπως προβλέπουν και τα πρότυπα ISO 22301 και ISO/IEC 27001, είναι η φάση Check, όπου ο οργανισμός καλείται να αξιολογήσει συστηματικά κατά πόσο όλα τα παραπάνω λειτουργούν όπως σχεδιάστηκαν: να μετρήσει την απόδοση των μέτρων και των σχεδίων, να εντοπίσει αδυναμίες μέσα από monitoring, reporting, ασκήσεις και internal audits, και να συγκεντρώσει τεκμηριωμένα στοιχεία που θα τροφοδοτήσουν τη διοίκηση για στοχευμένες αποφάσεις βελτίωσης του BCMS.

3.5 Παρακολούθηση, έλεγχος και ανασκόπηση

Η φάση Check του κύκλου Plan - Do - Check - Act επικεντρώνεται στη συστηματική αξιολόγηση της απόδοσης και της αποτελεσματικότητας του Business Continuity Management System. Αφού το BCMS έχει σχεδιαστεί και υλοποιηθεί, ο οργανισμός οφείλει να επαληθεύει

κατά πόσο οι διαδικασίες, τα σχέδια και οι δομές που έχουν τεθεί σε λειτουργία ανταποκρίνονται στις απαιτήσεις των προτύπων και στις επιχειρησιακές ανάγκες. Η φάση αυτή δεν εισάγει νέες λειτουργίες, αλλά λειτουργεί ως μηχανισμός ελέγχου, τεκμηρίωσης και ανατροφοδότησης, διασφαλίζοντας ότι το σύστημα παραμένει αξιόπιστο, συνεπές και κατάλληλο στο μεταβαλλόμενο περιβάλλον του οργανισμού.

3.5.1 Continuous Monitoring and Review

Στο πλαίσιο της φάσης Check, ο οργανισμός οφείλει να καθορίσει τι παρακολουθείται και τι μετράται σε σχέση με το BCMS, καθώς και τις μεθόδους ανάλυσης και αξιολόγησης των σχετικών δεδομένων. Η παρακολούθηση αυτή περιλαμβάνει τόσο ποσοτικά όσο και ποιοτικά στοιχεία, όπως η αποτελεσματικότητα των σχεδίων επιχειρησιακής συνέχειας, η ετοιμότητα των ομάδων απόκρισης και η συμμόρφωση των διαδικασιών με τις προβλεπόμενες απαιτήσεις. Τα αποτελέσματα της παρακολούθησης πρέπει να είναι τεκμηριωμένα και διαθέσιμα ως documented information, ώστε να μπορούν να χρησιμοποιηθούν αξιόπιστα ως βάση για εσωτερικό έλεγχο, διοικητική ανασκόπηση και λήψη αποφάσεων.

3.5.2 Internal Audit

Ο εσωτερικός έλεγχος (internal audit) αποτελεί ανεξάρτητο και συστηματικό μηχανισμό αξιολόγησης του BCMS, με στόχο τη διαπίστωση της συμμόρφωσής του προς τις απαιτήσεις του ISO 22301, τις εσωτερικές πολιτικές του οργανισμού και τις δεσμεύσεις που έχουν τεθεί στο πλαίσιο της επιχειρησιακής συνέχειας. Ο οργανισμός οφείλει να σχεδιάζει και να εφαρμόζει πρόγραμμα εσωτερικών ελέγχων, στο οποίο καθορίζονται το εύρος, τα κριτήρια, η συχνότητα και οι αρμοδιότητες των audits. Οι auditors πρέπει να λειτουργούν με αντικειμενικότητα και αμεροληψία, ενώ τα αποτελέσματα των ελέγχων οφείλουν να τεκμηριώνονται και να κοινοποιούνται στους αρμόδιους managers, ώστε να εντοπίζονται έγκαιρα αποκλίσεις και μη συμμορφώσεις.

3.5.3 Management Review

Το management review αποτελεί διακριτή διαδικασία ανώτερου επιπέδου, κατά την οποία το top management αξιολογεί συνολικά το BCMS σε προκαθορισμένα χρονικά διαστήματα. Σε αντίθεση με το internal audit, η διοικητική ανασκόπηση δεν έχει ελεγκτικό χαρακτήρα, αλλά στρατηγικό προσανατολισμό, εξετάζοντας εάν το σύστημα παραμένει κατάλληλο, επαρκές και αποτελεσματικό σε σχέση με το επιχειρησιακό περιβάλλον και τους στόχους του οργανισμού. Στο

management review λαμβάνονται υπόψη, μεταξύ άλλων, τα αποτελέσματα των εσωτερικών ελέγχων, η επίδοση των διαδικασιών, οι αλλαγές σε νομικές ή οργανωτικές απαιτήσεις και τα διδάγματα από ασκήσεις ή πραγματικά περιστατικά. Τα αποτελέσματα της ανασκόπησης οδηγούν σε αποφάσεις για βελτιώσεις, αναθεώρηση πολιτικών και κατανομή πόρων.

Η φάση Check ολοκληρώνεται όταν ο οργανισμός αποκτήσει σαφή εικόνα για την απόδοση και τις αδυναμίες του BCMS, βασισμένη σε τεκμηριωμένα αποτελέσματα παρακολούθησης, εσωτερικών ελέγχων και διοικητικής ανασκόπησης. Τα ευρήματα της φάσης αυτής δεν αποτελούν αυτοσκοπό, αλλά λειτουργούν ως είσοδοι για τη φάση Act, όπου ο οργανισμός καλείται να εφαρμόσει διορθωτικές και βελτιωτικές ενέργειες. Με τον τρόπο αυτό, ο κύκλος PDCA ολοκληρώνεται λειτουργικά, διασφαλίζοντας τη συνεχή βελτίωση και τη μακροχρόνια αποτελεσματικότητα του Business Continuity Management System.

3.6 Διορθωτικές ενέργειες και συνεχής βελτίωση

Η φάση Act του κύκλου Plan - Do – Check - Act αποτελεί το σημείο στο οποίο τα αποτελέσματα της παρακολούθησης, της μέτρησης και της αξιολόγησης του BCMS μετατρέπονται σε ουσιαστικές βελτιωτικές παρεμβάσεις. Μετά την ολοκλήρωση της φάσης Check, ο οργανισμός διαθέτει τεκμηριωμένα δεδομένα σχετικά με την απόδοση, την αποτελεσματικότητα και τις αδυναμίες του συστήματος επιχειρησιακής συνέχειας. Η φάση Act αξιοποιεί αυτά τα δεδομένα ώστε να διασφαλιστεί ότι το BCMS δεν παραμένει στατικό, αλλά εξελίσσεται συστηματικά, διορθώνοντας αποκλίσεις, ενισχύοντας αδύναμα σημεία και προσαρμοζόμενο στις μεταβαλλόμενες εσωτερικές και εξωτερικές συνθήκες. Με τον τρόπο αυτό, η επιχειρησιακή συνέχεια ενσωματώνεται ως ζωντανό στοιχείο της οργανωσιακής λειτουργίας και όχι ως τυπική συμμόρφωση με απαιτήσεις προτύπων.

3.6.1 Μη συμμορφώσεις (non-conformities) και διορθωτικές ενέργειες (corrective actions)

Κεντρικός άξονας της φάσης Act είναι η συστηματική διαχείριση των μη συμμορφώσεων που εντοπίζονται κατά τη λειτουργία, τον έλεγχο και την αξιολόγηση του BCMS. Μη συμμόρφωση μπορεί να προκύψει από αποκλίσεις από τις απαιτήσεις του ISO 22301, από εσωτερικά καθορισμένους κανόνες και στόχους, από ανεπαρκή εφαρμογή διαδικασιών ή από αποτυχίες που αναδείχθηκαν κατά τη διάρκεια ασκήσεων, δοκιμών ή πραγματικών περιστατικών. Ο οργανισμός οφείλει να έχει θεσπίσει σαφείς διαδικασίες για την έγκαιρη αναγνώριση αυτών

των αποκλίσεων, την αξιολόγηση της σοβαρότητάς τους και τη λήψη άμεσων διορθωτικών μέτρων, ώστε να αποτρέπεται η επανάληψή τους και η διαιώνιση συστημικών αδυναμιών.

Η εφαρμογή διορθωτικών ενεργειών δεν περιορίζεται στην επιφανειακή αντιμετώπιση των συμπτωμάτων, αλλά προϋποθέτει τη διερεύνηση των βαθύτερων αιτίων (root causes) που οδήγησαν στη μη συμμόρφωση. Με βάση αυτή την ανάλυση, ο οργανισμός σχεδιάζει, εγκρίνει και υλοποιεί κατάλληλες ενέργειες, παρακολουθώντας παράλληλα την αποτελεσματικότητά τους. Η προσέγγιση αυτή ευθυγραμμίζεται πλήρως με τη φιλοσοφία του ISO/IEC 27001, όπου τα διορθωτικά μέτρα και οι έλεγχοι (controls) αποτελούν βασικό μηχανισμό βελτίωσης της συνολικής ανθεκτικότητας του οργανισμού, τόσο σε επίπεδο ασφάλειας πληροφοριών όσο και σε επίπεδο επιχειρησιακής συνέχειας.

3.6.2 Συνεχής βελτίωση και ενσωμάτωσή της σε ολόκληρο τον κύκλο PDCA

Η φάση Act δεν αποτελεί απομονωμένο τελικό στάδιο, αλλά εκφράζει τη συνολική φιλοσοφία της συνεχούς βελτίωσης που διαπερνά ολόκληρο τον κύκλο PDCA. Τα μαθήματα που αντλούνται από ελέγχους, ασκήσεις, περιστατικά και ανασκοπήσεις της διοίκησης πρέπει να αξιοποιούνται ώστε να αναθεωρούνται πολιτικές, διαδικασίες, ρόλοι και επιχειρησιακές παραδοχές. Η συνεχής βελτίωση του BCMS προϋποθέτει μηχανισμούς που επιτρέπουν την αναγνώριση ευκαιριών βελτίωσης, την ιεράρχησή τους και τη μετατροπή τους σε συγκεκριμένες δράσεις, οι οποίες επανενσωματώνονται στις φάσεις Plan και Do του επόμενου κύκλου.

Ιδιαίτερη σημασία έχει το γεγονός ότι η ανάγκη για βελτίωση μπορεί να προκύψει όχι μόνο από αποτυχίες, αλλά και από αλλαγές στο context του οργανισμού. Μεταβολές στο εξωτερικό περιβάλλον, όπως νέες απειλές, κανονιστικές απαιτήσεις ή αλλαγές στην αγορά, καθώς και εσωτερικές αλλαγές, όπως αναδιοργάνωση, τεχνολογική αναβάθμιση ή διαφοροποίηση δραστηριοτήτων, επιβάλλουν την αναπροσαρμογή του BCMS. Η ανώτατη διοίκηση διαδραματίζει καθοριστικό ρόλο σε αυτή τη διαδικασία, διασφαλίζοντας ότι η επιχειρησιακή συνέχεια παραμένει ευθυγραμμισμένη με τη στρατηγική κατεύθυνση και την κουλτούρα του οργανισμού.

Συνολικά, η φάση Act ολοκληρώνει τον κύκλο του BCMS μετατρέποντας την αξιολόγηση σε ουσιαστική οργανωσιακή μάθηση και βελτίωση. Μέσα από τη συστηματική διαχείριση μη συμμορφώσεων, την εφαρμογή διορθωτικών ενεργειών και την καλλιέργεια κουλτούρας συνεχούς βελτίωσης, ο οργανισμός ενισχύει την ανθεκτικότητά του και διασφαλίζει ότι το BCMS παραμένει επίκαιρο, λειτουργικό και αποτελεσματικό. Το θεωρητικό πλαίσιο που αναπτύχθηκε στις

προηγούμενες ενότητες δημιουργεί το αναγκαίο υπόβαθρο για τη μετάβαση στο πρακτικό μέρος της εργασίας, όπου οι αρχές του ISO 22301 και του PDCA εφαρμόζονται σε συγκεκριμένο σενάριο, επιτρέποντας την αξιολόγηση της χρησιμότητας και της αξιοπιστίας του BCMS στην πράξη.

4. Πρακτική Αξιοποίηση της Τεχνητής Νοημοσύνης στην Επιχειρησιακή Συνέχεια

4.1 Εισαγωγή

Η παρούσα εργασία επικεντρώθηκε στη θεωρητική ανάλυση της επιχειρησιακής συνέχειας και στη συστηματική παρουσίαση των απαιτήσεων και κατευθυντήριων γραμμών που θέτουν τα διεθνή πρότυπα της οικογένειας ISO, με έμφαση στο ISO 22301 και στη συμπληρωματική αξιοποίηση του κύκλου Plan - Do - Check - Act, όπως αυτός υιοθετείται και στο ISO/IEC 27001. Η ανάλυση αυτή ανέδειξε ότι η επιχειρησιακή συνέχεια δεν αποτελεί ένα μεμονωμένο σύνολο εγγράφων, αλλά ένα δυναμικό σύστημα διακυβέρνησης, το οποίο βασίζεται στη συνεχή αξιολόγηση, εφαρμογή, έλεγχο και βελτίωση διαδικασιών.

Στο πλαίσιο αυτό, το επόμενο στάδιο της εργασίας μεταβαίνει από τη θεωρητική θεμελίωση στην πρακτική διερεύνηση της δυνατότητας αξιοποίησης τεχνολογιών τεχνητής νοημοσύνης ως υποστηρικτικών εργαλείων στη σχεδίαση και εφαρμογή ενός Business Continuity Management System. Συγκεκριμένα, εξετάζεται κατά πόσο ένα σύγχρονο μοντέλο Μεγάλων Γλωσσικών Μοντέλων (Large Language Model LLM), όταν λειτουργεί τοπικά και τροφοδοτείται με επιλεγμένη και ελεγχόμενη γνώση από τα σχετικά πρότυπα, μπορεί να υποστηρίξει τη σύνθεση, τη δομή και την κατανόηση ενός BCMS για έναν υποθετικό οργανισμό.

Στόχος δεν είναι η αυτοματοποίηση της λήψης αποφάσεων ή η αντικατάσταση της ανθρώπινης κρίσης, αλλά η επίδειξη ενός ρεαλιστικού και περιορισμένου σεναρίου, στο οποίο η τεχνητή νοημοσύνη λειτουργεί ως εργαλείο υποβοήθησης και επιτάχυνσης της ανάλυσης και της τεκμηρίωσης, εντός των πλαισίων που ορίζουν τα διεθνή πρότυπα επιχειρησιακής συνέχειας.

4.2 Περιβάλλον Υλοποίησης & Τεχνολογικό Υπόβαθρο

Η πειραματική διαδικασία σχεδιάστηκε με κύριο γνώμονα την προσομοίωση ενός ρεαλιστικού σεναρίου Μικρομεσαίας Επιχείρησης (ΜμΕ), όπου οι πόροι είναι περιορισμένοι και η ασφάλεια των δεδομένων επιτάσσει την αποφυγή λύσεων Cloud.

Για τον λόγο αυτό, το σύστημα υλοποιήθηκε εξ ολοκλήρου σε περιβάλλον προσωπικού φορητού υπολογιστή (Laptop), χωρίς τη χρήση εξωτερικών διακομιστών ή GPU clusters. Αυτός ο περιορισμός στο υλικό (Hardware Constraints) καθόρισε και την επιλογή των εργαλείων λογισμικού, οδηγώντας στην υιοθέτηση «ελαφριών» (lightweight) και βελτιστοποιημένων μοντέλων Τεχνητής Νοημοσύνης, τα οποία δύνανται να εκτελεστούν αποδοτικά σε τοπικό επίπεδο

(Local Inference) με χρήση αποκλειστικά της κεντρικής μνήμης (RAM) και του επεξεργαστή (CPU).

Ακολουθεί η αναλυτική παρουσίαση της τεχνολογικής στοίβας (Tech Stack) που συνέθεσε την αρχιτεκτονική του συστήματος.

4.2.1 Ανάλυση Στοίβας Λογισμικού (Software Stack Analysis)

Η αρχιτεκτονική του συστήματος βασίστηκε σε τρεις διακριτούς πυλώνες λογισμικού, οι οποίοι συνεργάζονται για να επιτύχουν την ασφαλή, τοπική εκτέλεση ενός μοντέλου Τεχνητής Νοημοσύνης. Ακολουθεί η αναλυτική περιγραφή της λειτουργίας και των τεχνικών χαρακτηριστικών του κάθε εργαλείου.

- **Ollama: Το Περιβάλλον Εκτέλεσης**

Το Ollama αποτελεί το θεμέλιο της αρχιτεκτονικής μας. Για να γίνει κατανοητός ο ρόλος του, μπορούμε να το παρομοιάσουμε με το "Λειτουργικό Σύστημα" ή τον "Player" που απαιτείται για να τρέξει ένα αρχείο βίντεο. Ένα γλωσσικό μοντέλο από μόνο του είναι απλώς ένα τεράστιο αρχείο με μαθηματικά βάρη (weights), το οποίο δεν μπορεί να κάνει τίποτα χωρίς έναν μηχανισμό να το φορτώσει και να το εκτελέσει.

Το Ollama επιλέχθηκε, διότι λύνει το βασικό πρόβλημα της τοπικής εκτέλεσης: την πολυπλοκότητα, καθώς:

1. **Virtualization Πόρων**: Αναλαμβάνει την επικοινωνία με το υλικό (Hardware Abstraction Layer), κατανέμοντας βέλτιστα το φορτίο μεταξύ της μνήμης RAM και του επεξεργαστή (CPU).
2. **API Server**: Δημιουργεί έναν τοπικό διακομιστή (Localhost API), επιτρέποντας σε εξωτερικές εφαρμογές (όπως το AnythingLLM) να "συνομιλούν" με το μοντέλο μέσω απλών εντολών HTTP, ακριβώς όπως θα έκαναν με έναν server στο Cloud, αλλά εντός του κλειστού κυκλώματος του υπολογιστή.
3. **Υποστήριξη Modelfiles**: Επιτρέπει την παραμετροποίηση της "συμπεριφοράς" του μοντέλου (π.χ. πόσο δημιουργικό ή αυστηρό θα είναι) μέσω απλών αρχείων ρυθμίσεων (Modelfiles), δίνοντάς μας τον έλεγχο στην προσωπικότητα του "AI Συμβούλου".

- **Mistral 7B Instruct v0.3: Η "Νοημοσύνη" του Συστήματος**

Στην καρδιά του συστήματος βρίσκεται το μοντέλο Mistral-7B-Instruct-v0.3, η τρίτη και πλέον εξελιγμένη έκδοση του μοντέλου 7 δισεκατομμυρίων παραμέτρων της Mistral AI. Η επιλογή της συγκεκριμένης έκδοσης (Instruct v0.3) έναντι της βασικής (Base model) ή παλαιότερων εκδόσεων (v0.1, v0.2) έγινε βάσει των ειδικών χαρακτηριστικών της που εξυπηρετούν άριστα το σενάριο διαχείρισης κρίσεων:

1. **Instruction Fine-Tuning (Μικρο-ρύθμιση βάσει Οδηγιών):** Το επίθεμα "Instruct" υποδηλώνει ότι το μοντέλο έχει υποστεί ειδική εκπαίδευση (Supervised Fine-Tuning) ώστε να ακολουθεί πιστά περίπλοκες οδηγίες χρήστη και όχι απλώς να συμπληρώνει κείμενο. Αυτό ήταν καθοριστικό για το πείραμά μας, καθώς το μοντέλο κλήθηκε να υιοθετήσει συγκεκριμένη περσόνα ("Crisis Manager") και να υπακούσει σε αυστηρούς περιορισμούς (π.χ. "Μην πληρώσεις λύτρα", "Ανάφερε το Control X"), συμπεριφορές που απαιτούν υψηλή πειθαρχία (alignment).
2. **Υποστήριξη Function Calling (Κλήση Λειτουργιών):** Η έκδοση v0.3 εισάγει εγγενή υποστήριξη για "Function Calling". Αν και στο πείραμά μας δεν εκτελέσαμε κώδικα, αυτή η αρχιτεκτονική βελτίωση προσδίδει στο μοντέλο ανώτερη ικανότητα δομημένης σκέψης (Structured Reasoning). Αυτό εξηγεί την επιτυχία του μοντέλου στο να εντοπίζει και να εξάγει συγκεκριμένα δεδομένα (όπως τον αριθμό του ISO Control 8.31) από το κείμενο, αντί να απαντά αόριστα.
3. **Διευρυμένο Λεξιλόγιο (Extended Vocabulary):** Το Mistral v0.3 διαθέτει ένα διευρυμένο Tokenizer (32,768 tokens), το οποίο επιτρέπει καλύτερη κατανόηση τεχνικών όρων και πολυγλωσσικών δεδομένων σε σχέση με προηγούμενες εκδόσεις. Αυτό συνέβαλε στην ορθή επεξεργασία της μικτής ορολογίας (Ελληνικά/Αγγλικά) που περιείχε η Βάση Γνώσης μας.
4. **Sliding Window Attention (SWA):** Διατηρεί τον μηχανισμό SWA (με παράθυρο 4096 tokens), επιτρέποντας την αποδοτική επεξεργασία του "Εγχειριδίου Πολιτικής" χωρίς να επιβαρύνει υπερβολικά τη μνήμη RAM του συστήματος, καθιστώντας εφικτή την εκτέλεση σε συμβατικό φορητό υπολογιστή.

- **AnythingLLM: Η Πλατφόρμα Ανάκτησης & Σύνθεσης**

Ενώ το Ollama και το Mistral παρέχουν την υπολογιστική ισχύ και τη νοημοσύνη αντίστοιχα, από μόνα τους πάσχουν από ένα κρίσιμο μειονέκτημα: την έλλειψη γνώσης για τα συγκεκριμένα, απόρρητα έγγραφα της υποθετικής εταιρείας "Alpha Logistics". Τη λύση σε αυτό το πρόβλημα έδωσε το AnythingLLM, μια ολοκληρωμένη εφαρμογή Desktop που υλοποιεί την αρχιτεκτονική RAG (Retrieval-Augmented Generation).

Το AnythingLLM ανέλαβε τρεις κρίσιμες λειτουργίες που μετέτρεψαν το γενικό γλωσσικό μοντέλο σε εξειδικευμένο σύμβουλο:

1. **Διαχείριση Διανυσματικής Βάσης (Vector Database Management):** Κατά τη φόρτωση του Εγχειριδίου Πολιτικής , το AnythingLLM δεν το αποθήκευσε ως απλό κείμενο. Χρησιμοποίησε έναν ενσωματωμένο αλγόριθμο (Embedding Model) για να "σπάσει" το έγγραφο σε μικρότερα τμήματα και να τα μετατρέψει σε πολυδιάστατα μαθηματικά διανύσματα (Embeddings). Αυτά τα διανύσματα αποθηκεύτηκαν στην τοπική βάση δεδομένων LanceDB (που τρέχει εντός της εφαρμογής), επιτρέποντας την ταχύτατη αναζήτηση βάσει νοήματος.
2. **Σημασιολογική Αναζήτηση (Semantic Search):** Όταν ο χρήστης έθετε το ερώτημα για τα "λύτρα", το σύστημα δεν έκανε απλή αναζήτηση λέξεων-κλειδιών (keyword search). Αντιθέτως, συνέκρινε το μαθηματικό διάνυσμα της ερώτησης με τα διανύσματα των εγγράφων, εντοπίζοντας τις παραγράφους που είχαν τη μεγαλύτερη νοηματική συγγένεια (cosine similarity). Έτσι, μπόρεσε να συνδέσει την ερώτηση "μπορώ να πληρώσω;" με την παράγραφο "Zero-Trust Ransomware Policy", ακόμα κι αν οι λέξεις δεν ήταν πανομοιότυπες.
3. **Δυναμική Εισαγωγή Πλαισίου (Dynamic Context Injection):** Αφού εντόπιζε τις σχετικές πληροφορίες (π.χ. το Control 8.31), το AnythingLLM τις "ενσωμάτωνε" αόρατα στην εντολή (prompt) που έστελνε στο Mistral, δίνοντας ουσιαστικά στο μοντέλο την εξής οδηγία: *"Βάσει ΑΥΤΟΥ του κειμένου που σου παραθέτω, απάντησε στην ερώτηση του χρήστη"*. Αυτή η διαδικασία διασφάλισε ότι οι απαντήσεις ήταν αυστηρά τεκμηριωμένες (grounded) στα εταιρικά έγγραφα.

Η επιλογή του AnythingLLM (έναντι άλλων λύσεων όπως το PrivateGPT) έγινε λόγω της ευκολίας διασύνδεσής του με το Ollama και της απόλυτης στεγανότητας (privacy - first design) που προσφέρει, καθώς όλα τα δεδομένα (έγγραφα, διανύσματα, συνομιλίες) παρέμειναν αποθηκευμένα τοπικά στον σκληρό δίσκο του συστήματος.

4.2.2 Το Επιχειρησιακό Σενάριο: "Alpha Logistics" & Ransomware

Για τις ανάγκες του πειράματος, δημιουργήθηκε το προφίλ της εταιρείας "Alpha Logistics", μιας τυπικής ΜμΕ που βασίζει την κρίσιμη λειτουργία της (τιμολόγηση, αποθήκη) σε ένα κεντρικό σύστημα ERP.

Η επιλογή της επίθεσης Ransomware ως σεναρίου αναφοράς έγινε για τους εξής λόγους:

1. **Πολυδιάστατη Κρίση:** Σε αντίθεση με μια απλή τεχνική βλάβη, το Ransomware προκαλεί ταυτόχρονα επιχειρησιακή παράλυση (κρυπτογράφηση αρχείων), οικονομικό εκβιασμό (λύτρα) και νομικό κίνδυνο (διαρροή δεδομένων προσωπικού χαρακτήρα). Αυτό απαιτεί σύνθετη λήψη αποφάσεων που δεν είναι μόνο τεχνική, αλλά και νομική/στρατηγική.
2. **Έλλειψη Πόρων:** Οι περισσότερες ΜμΕ δεν διαθέτουν in-house νομικό τμήμα ή εξειδικευμένους CISO (Chief Information Security Officers) διαθέσιμους 24/7. Εδώ ο ρόλος του AI ως "άμεσου συμβούλου" είναι καθοριστικός.

Η απάντηση σε ερωτήματα περί της αναγκαιότητας της τοπικής εκτέλεσης του μοντέλου T.N., είναι κατηγορηματική και βασίζεται σε τρεις κρίσιμους άξονες της ασφάλειας πληροφοριών:

1. **Εμπιστευτικότητα & Κυριαρχία Δεδομένων (Data Sovereignty)** Τα Εγχειρίδια Επιχειρησιακής Συνέχειας (BCP) και οι Πολιτικές Ασφαλείας περιέχουν τα πιο ευαίσθητα "μυστικά" ενός οργανισμού: ονόματα υπευθύνων, τηλέφωνα ανάγκης, κωδικούς πρόσβασης, αδυναμίες υποδομών και στρατηγικές διαπραγμάτευσης. Η μεταφόρτωση αυτών των εγγράφων σε ένα δημόσιο Chatbot ισοδυναμεί με την αποστολή τους σε διακομιστές τρίτων (Third-Party Servers). Ακόμη και με τις πολιτικές απορρήτου των παρόχων, ο κίνδυνος διαρροής ή χρήσης των δεδομένων για την εκπαίδευση μελλοντικών μοντέλων είναι υπαρκτός. Η τοπική εκτέλεση (Local Inference) διασφαλίζει ότι κανένα byte πληροφορίας δεν εγκαταλείπει ποτέ

τη φυσική συσκευή του χρήστη, ικανοποιώντας τις αυστηρότερες απαιτήσεις εμπιστευτικότητας του ISO 27001.

2. **Διαθεσιμότητα σε Συνθήκες Απομόνωσης (Availability during Isolation)** Ίσως το πιο πρακτικό επιχείρημα υπέρ της offline προσέγγισης αφορά τη φύση της ίδιας της απειλής. Το πρώτο βήμα στο πρωτόκολλο αντιμετώπισης Ransomware (Containment) είναι συχνά η άμεση αποσύνδεση από το διαδίκτυο (Internet Blackout) για να αποτραπεί η επικοινωνία του κακόβουλου λογισμικού με τους Servers των επιτιθέμενων (Command & Control) και να σταματήσει η διαρροή δεδομένων. Σε μια τέτοια συνθήκη, οποιοδήποτε εργαλείο Cloud AI καθίσταται άχρηστο. Αντιθέτως, το προτεινόμενο σύστημα, τρέχοντας τοπικά στο laptop του Υπευθύνου Ασφαλείας, παραμένει πλήρως λειτουργικό ακόμα και χωρίς δίκτυο, παρέχοντας κρίσιμες οδηγίες ακριβώς τη στιγμή που χρειάζονται περισσότερο.
3. **Αμεσότητα & Προσβασιμότητα (Accessibility)** Η αρχιτεκτονική που επιλέχθηκε αποδεικνύει ότι η λύση δεν απαιτεί πολύπλοκους servers (Server Rooms) ή εξειδικευμένο IT εξοπλισμό. Μπορεί να φιλοξενηθεί στον προσωπικό φορητό υπολογιστή (Laptop) του Crisis Manager. Αυτό σημαίνει ότι ο υπεύθυνος έχει τον "Σύμβουλο" μαζί του ανά πάσα στιγμή, είτε βρίσκεται στο γραφείο, είτε εργάζεται απομακρυσμένα, εκμηδενίζοντας τον χρόνο απόκρισης.

4.3 Πειραματική Διαδικασία & Εκτέλεση Σεναρίου

Η πειραματική διαδικασία εκτελέστηκε σε τρία διακριτά στάδια: την εισαγωγή και διανυσματοποίηση της επιχειρησιακής γνώσης, τη σύνταξη της εξειδικευμένης εντολής (Prompt Engineering) και την τελική εκτέλεση της προσομοίωσης. Σκοπός ήταν να αξιολογηθεί η ικανότητα του συστήματος να ανακαλεί συγκεκριμένες πολιτικές ασφαλείας υπό συνθήκες πίεσης.

4.3.1 Εισαγωγή και Διανυσματοποίηση Της Επιχειρησιακής Γνώσης

Η επιλογή του σεναρίου προσομοίωσης, καθώς και η αρχιτεκτονική της λύσης που υιοθετήθηκε, δεν προέκυψαν τυχαία. Αντιθέτως, σχεδιάστηκαν προσεκτικά ώστε να αντικατοπτρίζουν τις ρεαλιστικές προκλήσεις που καλείται να διαχειριστεί μια σύγχρονη Μικρομεσαία Επιχείρηση (ΜμΕ), λειτουργώντας υπό καθεστώς πίεσης και περιορισμένων πόρων.

Στην παρούσα ενότητα αναλύεται το σκεπτικό πίσω από τη δημιουργία της εικονικής εταιρείας "Alpha Logistics", την επιλογή της απειλής Ransomware και, κυρίως, τεκμηριώνεται η επιτακτική ανάγκη για χρήση αποκομμένων (offline) συστημάτων Τεχνητής Νοημοσύνης έναντι των δημοφιλών διαδικτυακών λύσεων (Cloud AI).

Για τις ανάγκες του πειράματος, δημιουργήθηκε το προφίλ της εταιρείας "Alpha Logistics", μιας τυπικής ΜμΕ που βασίζει την κρίσιμη λειτουργία της (τιμολόγηση, αποθήκη) σε ένα κεντρικό σύστημα ERP.

Η επιλογή της επίθεσης Ransomware ως σεναρίου αναφοράς έγινε για τους εξής λόγους:

1. **Πολυδιάστατη Κρίση:** Σε αντίθεση με μια απλή τεχνική βλάβη, το Ransomware προκαλεί ταυτόχρονα επιχειρησιακή παράλυση (κρυπτογράφηση αρχείων), οικονομικό εκβιασμό (λύτρα) και νομικό κίνδυνο (διαρροή δεδομένων προσωπικού χαρακτήρα). Αυτό απαιτεί σύνθετη λήψη αποφάσεων που δεν είναι μόνο τεχνική, αλλά και νομική/στρατηγική.
2. **Έλλειψη Πόρων:** Οι περισσότερες ΜμΕ δεν διαθέτουν in-house νομικό τμήμα ή εξειδικευμένους CISO (Chief Information Security Officers) διαθέσιμους 24/7. Εδώ ο ρόλος του AI ως "άμεσου συμβούλου" είναι καθοριστικός.

Για την αποτελεσματική αξιολόγηση του συστήματος RAG, κρίθηκε αναγκαία η δημιουργία ενός προσαρμοσμένου Εγχειριδίου Επιχειρησιακής Συνέχειας (BCP) για την εικονική οντότητα "Alpha Logistics". Η δομή και το περιεχόμενο του εγγράφου δεν αποτελούν απλή συλλογή πληροφοριών, αλλά μια στοχευμένη επιλογή κρίσιμων διαδικασιών και ελέγχων (Controls) από τα πρότυπα ISO 27001 και ISO 22301.

Στόχος ήταν η ενσωμάτωση συγκεκριμένων "κανόνων εμπλοκής" (rules of engagement), οι οποίοι θα λειτουργούσαν ως κριτήρια επιτυχίας για τις απαντήσεις του μοντέλου. Οι βασικοί πυλώνες της πολιτικής, όπως αποτυπώνονται στο αντίστοιχο έγγραφο, αναλύονται παρακάτω:

1. **Στρατηγική Μηδενικής Ανοχής (Zero-Trust Ransomware Policy)** Ως θεμέλιος λίθος της στρατηγικής διαχείρισης κρίσεων ορίστηκε η "Πολιτική Μη Πληρωμής" (No Payment Policy). Στο εγχειρίδιο αναφέρεται ρητά ότι η εταιρεία δεν διαπραγματεύεται και δεν πληρώνει λύτρα υπό καμία συνθήκη, χαρακτηρίζοντας οποιαδήποτε αντίθετη πρόταση ως απορριπτέα. Η επιλογή αυτή έγινε σκόπιμα για

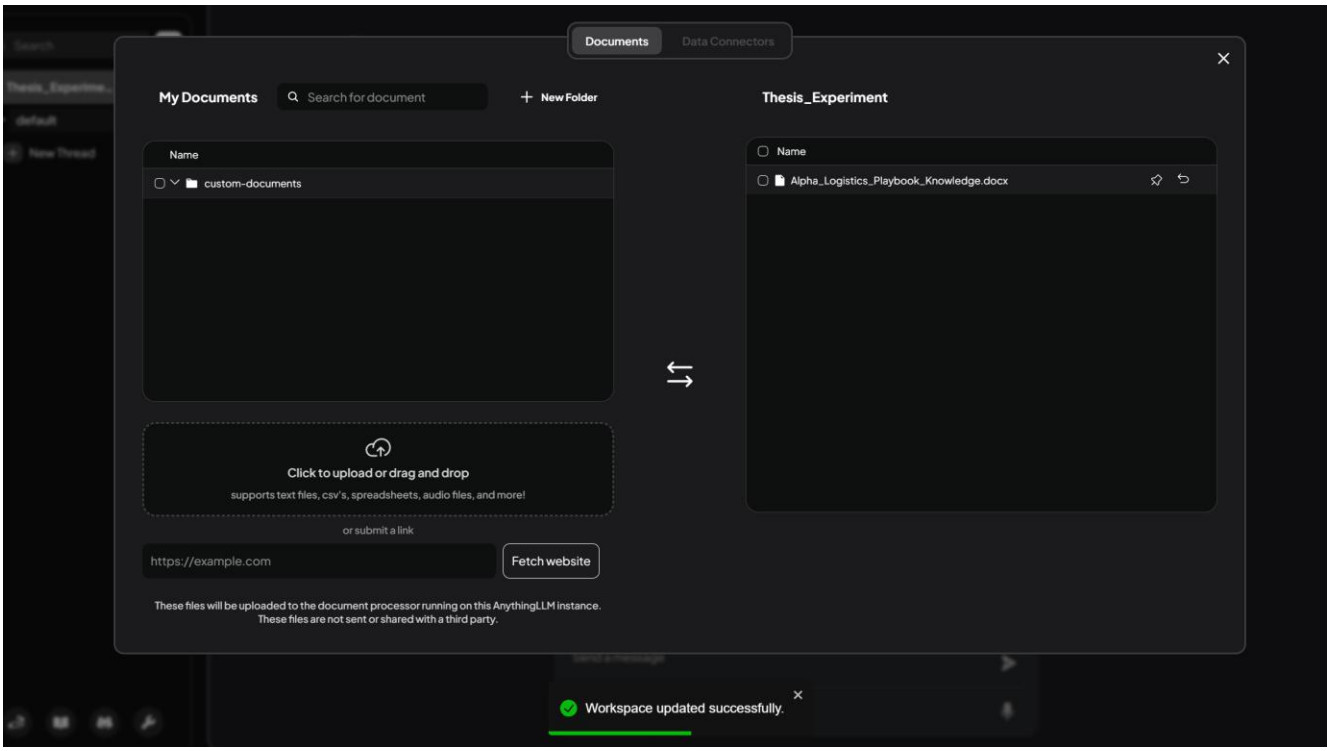
να εξεταστεί αν το μοντέλο, υπό την πίεση ενός υποθετικού σεναρίου (π.χ. πιέσεις από τον CEO), θα παραμείνει πιστό στην καταγεγραμμένη πολιτική ή θα υποκύψει σε "ανθρωποκεντρικές" λύσεις συμβιβασμού.

2. **Επιχειρησιακή Αυτονομία & Περιορισμός (Kill Switch Authorization)** Για την αντιμετώπιση του κρίσιμου παράγοντα "χρόνος", ενσωματώθηκε στην πολιτική η διαδικασία του "Kill Switch". Συγκεκριμένα, δόθηκε ρητή εξουσιοδότηση σε κάθε μέλος της τεχνικής ομάδας (Bronze Team) να διακόψει άμεσα τη λειτουργία δικτύων ή servers με την παραμικρή υποψία Ransomware, χωρίς την ανάγκη προηγούμενης έγκρισης από τη Διοίκηση. Σκοπός αυτής της πρόβλεψης είναι ο άμεσος περιορισμός της εξάπλωσης (Containment), και η αξιολόγηση της ικανότητας του AI να προκρίνει την ασφάλεια έναντι της διαθεσιμότητας σε συνθήκες κρίσης.
3. **Πολιτική Ασφαλούς Ανάκαμψης (Clean Room Strategy)** Ένα από τα συχνότερα σφάλματα κατά την ανάκαμψη από κυβερνοεπιθέσεις είναι η επαναμόλυνση μέσω των αντιγράφων ασφαλείας. Για τον λόγο αυτό, συμπεριλήφθηκε η υποχρεωτική χρήση διαδικασίας "Clean Room", η οποία απαγορεύει αυστηρά την απευθείας επαναφορά (Restore) στο δίκτυο παραγωγής. Αντιθέτως, επιβάλλεται η χρήση απομονωμένου περιβάλλοντος ελέγχου (Sandbox), σύμφωνα με το Control 8.31 του ISO 27001. Η αναφορά αυτή αποτελεί "τεχνική παγίδα" για το μοντέλο, ώστε να ελεγχθεί αν θα προτείνει τη γρήγορη αλλά επισφαλή λύση ή την ορθή διαδικασία ασφαλείας.
4. **Διαχωρισμός Καθηκόντων (Roles & Segregation of Duties)** Για να διασφαλιστεί η σαφήνεια στην αλυσίδα διοίκησης, ορίστηκαν διακριτοί ρόλοι με βάση το μοντέλο Gold/Silver/Bronze:
    - **Gold Team (Στρατηγικό Επίπεδο):** Λήψη αποφάσεων υψηλού επιπέδου και νομική διαχείριση.
    - **Silver Team (Τακτικό Επίπεδο):** Υπεύθυνοι για την ενεργοποίηση εναλλακτικών διαδικασιών λειτουργίας (Manual Workarounds) ώστε να διασφαλιστεί η επιχειρησιακή συνέχεια.
    - **Bronze Team (Επιχειρησιακό Επίπεδο):** Υπεύθυνοι για τις τεχνικές ενέργειες απομόνωσης και ανάκαμψης. Η δομή αυτή επιτρέπει τον έλεγχο του κατά

πόσον το AI μπορεί να κατανείμει σωστά τις αρμοδιότητες, αποφεύγοντας τη σύγκρουση συμφερόντων (Segregation of Duties).

5. **Διαδικασίες Απόκρισης & Συμμόρφωση (Playbook Phases & ISO Controls)** Τέλος, το εγχειρίδιο εμπλουτίστηκε με συγκεκριμένες αναφορές σε Controls του ISO 27001:2022, ώστε να προσδώσει τεχνική εγκυρότητα στις απαντήσεις του συστήματος.
    - **Φάση Ανίχνευσης & Περιορισμού:** Αναφέρεται η χρήση του Control 5.26 (Response to incidents) και του Control 8.22 (Segregation of networks) για την αποτροπή πλευρικής μετακίνησης (Lateral Movement).
    - **Φάση Επιχειρησιακής Συνέχειας:** Καθορίζονται σαφείς μετρήσεις RTO (4 ώρες) και RPO (24 ώρες) και περιγράφονται χειροκίνητες διαδικασίες (χρήση χαρτιού/μολυβιού) για τη συνέχιση της λειτουργίας του λογιστηρίου χωρίς ERP.

Για να ανέβει το έγγραφο της πολιτικής ασφαλείας και να χρησιμοποιηθεί ως βάση δεδομένων από το μοντέλο mistral, χρησιμοποιήθηκε το Anything Llm. Αρχικά δημιουργήθηκε Workspace (χώρο εργασίας), η οποία ονομάστηκε **“Thesis_Experiment”**. Έπειτα ανοίγοντας την συνομιλία και πατώντας το κουμπί upload, μπορούμε να ανεβάσουμε όποιο αρχείο επιθυμούμε. Στη προκειμένη χρησιμοποιήθηκε το αρχείο *Alpha_Logistics_Playbook_Knowledge.docx* που δημιουργήθηκε προηγουμένως. Τέλος, πατάμε το κουμπί **"Move to Workspace"** και μόλις μετακινηθεί, πατάμε το κουμπί που λέει **"Save and Embed"**. Αν η ανωτέρω διαδικασία είναι επιτυχής, τότε φαίνεται στη εικόνα παρακάτω:



Εικόνα 1: Επιτυχής Δημιουργία Database

Δεδομένου ότι τα Γλωσσικά Μοντέλα (LLMs) έχουν περιορισμό στο μέγεθος του κειμένου που μπορούν να επεξεργαστούν ταυτόχρονα (Context Window), το αρχείο εισόδου δεν εισήχθη ως ενιαίο μπλοκ. Το AnythingLLM προχώρησε αυτόματα στον τεμαχισμό του εγγράφου σε μικρότερα, λογικά τμήματα (chunks). Η διαδικασία αυτή είναι κρίσιμη, καθώς εξασφαλίζει ότι κατά την αναζήτηση, το σύστημα θα ανασύρει μόνο τη συγκεκριμένη παράγραφο που απαντά στο ερώτημα (π.χ. το Control 8.31) και όχι ολόκληρο το εγχειρίδιο, βελτιστοποιώντας την ακρίβεια της απάντησης.

Στη συνέχεια, κάθε τμήμα κειμένου (text chunk) πέρασε από τη διαδικασία της διανυσματοποίησης. Για τη μετατροπή του κειμένου σε διανύσματα, αξιοποιήθηκε το μοντέλο ενσωμάτωσης (embedding model) all-MiniLM-L6-v2, το οποίο είναι βελτιστοποιημένο για σημασιολογική αναζήτηση (semantic search) με χαμηλό υπολογιστικό κόστος, παράγοντας διανύσματα 384 διαστάσεων, οι λέξεις και οι προτάσεις του εγχειριδίου μετατράπηκαν σε πολυδιάστατα αριθμητικά διανύσματα. Το σύστημα δεν αποθηκεύει απλώς τις λέξεις "Clean Room", αλλά την μαθηματική αναπαράσταση της έννοιας "ασφαλές περιβάλλον αποκατάστασης". Έτσι, ακόμα κι αν ο χρήστης ρωτήσει περιφραστικά, το σύστημα μπορεί να βρει τη σωστή αντιστοιχία.

Τα παραγόμενα διανύσματα αποθηκεύτηκαν τελικώς στην τοπική βάση δεδομένων LanceDB, η οποία λειτουργεί στο παρασκήνιο του AnythingLLM. Η LanceDB επιλέχθηκε καθώς είναι βελτιστοποιημένη για γρήγορη αναζήτηση ομοιότητας (similarity search) και λειτουργεί αποκλειστικά στον τοπικό δίσκο (serverless), διασφαλίζοντας ότι τα ευαίσθητα εταιρικά δεδομένα δεν μεταφορτώνονται σε κανένα εξωτερικό Cloud. Με την ολοκλήρωση αυτής της διαδικασίας, το στατικό έγγραφο Word μετατράπηκε σε μια δυναμική Βάση Γνώσης (Knowledge Base), έτοιμη να τροφοδοτήσει το μοντέλο Mistral 7B μέσω του μηχανισμού RAG.

4.3.2 Σύνταξη Εξειδικευμένης Εντολής και Τελική Εκτέλεση

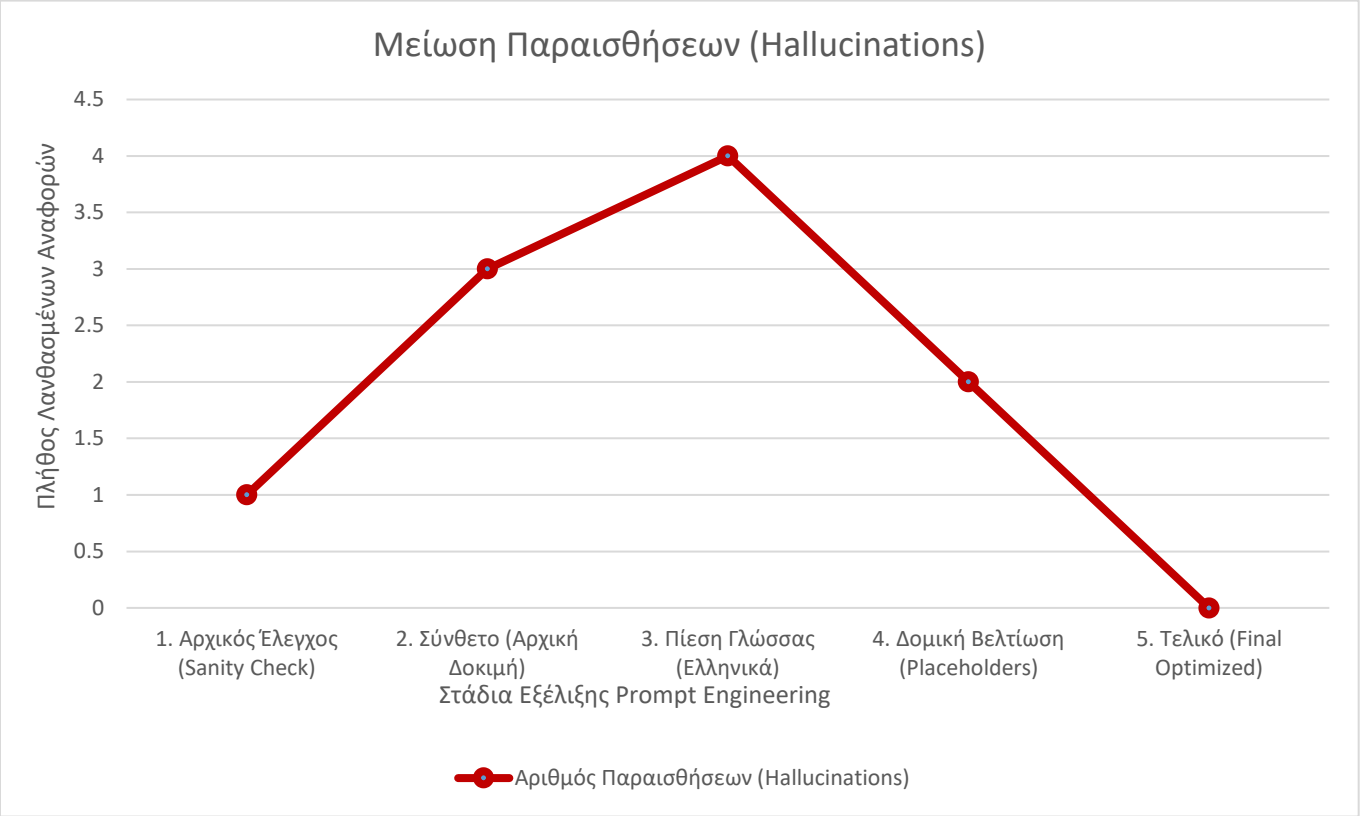
Η επιτυχής ανάκτηση πληροφορίας από ένα σύστημα RAG δεν εξαρτάται μόνο από την ποιότητα της βάσης γνώσης, αλλά και από τον τρόπο με τον οποίο διατυπώνεται το ερώτημα προς το γλωσσικό μοντέλο. Η διαδικασία αυτή, γνωστή ως Μηχανική των Εντολών (Prompt Engineering), αποδείχθηκε καθοριστική για την εξαγωγή έγκυρων και νομικά τεκμηριωμένων απαντήσεων.

Η εκτέλεση της προσομοίωσης πραγματοποιήθηκε υποβάλλοντας στο σύστημα ένα σύνθετο σενάριο κρίσης, το οποίο απαιτούσε ταυτόχρονη διαχείριση τεσσάρων κρίσιμων ζητημάτων: την απαίτηση λύτρων, την αυθαίρετη ενέργεια τεχνικού (Kill Switch), την πίεση για γρήγορη επαναφορά (Restore) και τη διασφάλιση της επιχειρησιακής συνέχειας (Business Continuity) εν τη απουσία του ERP.

Είναι σημαντικό να σημειωθεί ότι κατά τις αρχικές δοκιμές με απλούστερες εντολές, το τοπικό μοντέλο (Mistral 7B) εμφάνισε τάσεις "Παραισθήσεων" (Hallucinations). Συγκεκριμένα, σε ορισμένες περιπτώσεις επινόησε ανύπαρκτα ISO Controls (π.χ. αναφέροντας "Control 126.3") ή έδωσε συμβουλές βασισμένες σε γενικές πρακτικές που όμως αντιτίθεντο στην ειδική πολιτική της εταιρείας (π.χ. πρότεινε αναμονή έγκρισης για το Kill Switch, ενώ η πολιτική την επιτρέπει άμεσα).

Το φαινόμενο αυτό είναι αναμενόμενο στα Μικρά Γλωσσικά Μοντέλα (Small Language Models - SLMs) των 7 δισεκατομμυρίων παραμέτρων, λόγω της περιορισμένης "χωρητικότητας" μνήμης και κατανόησης σε σχέση με μεγαλύτερα μοντέλα (π.χ. 70B ή GPT-4). Ωστόσο, αποδείχθηκε ότι με τη βελτιστοποίηση της εντολής (Prompt Refinement) και την αυστηρή οριοθέτηση του πλαισίου, τα σφάλματα αυτά ελαχιστοποιήθηκαν, οδηγώντας σε υψηλή ακρίβεια ανάκτησης.

Διάγραμμα 1: Μείωση Παραισθήσεων (Hallucinations) μέσω Σταδιακής Βελτιστοποίησης Εντολών



Το ανωτέρω διάγραμμα αποτυπώνει την πορεία βελτιστοποίησης του συστήματος. Αρχικά (Στάδιο 1), το μοντέλο παρουσίασε αδυναμία ανάκτησης συγκεκριμένων Controls (Retrieval Failure). Κατά τη μετάβαση σε σύνθετα σενάρια (Στάδιο 2 & 3), παρατηρήθηκε κατακόρυφη αύξηση των "παραισθήσεων" (Hallucinations), με το μοντέλο να επινοεί ανύπαρκτα αντίμετρα (π.χ. Control 126.3, 16.3) ή να παρερμηνεύει την πολιτική, ειδικά όταν πιέστηκε γλωσσικά. Η εφαρμογή της τεχνικής Chain - of - Thought και η αφαίρεση της γλωσσικής πίεσης (Στάδιο 4 & 5) οδήγησαν στη σταδιακή εξάλειψη των σφαλμάτων, επιτυγχάνοντας μηδενικές παραισθήσεις στο Τελικό Στάδιο.

Η αξιολόγηση της ορθότητας των απαντήσεων του συστήματος δεν πραγματοποιήθηκε αυτοματοποιημένα, αλλά μέσω χειροκίνητης επαλήθευσης (manual verification). Κάθε παραπομπή του μοντέλου (citation) αντιπαραβλήθηκε με το πρωτότυπο κείμενο του εγγράφου *Alpha_Logistics_Playbook.docx* και τα πρότυπα ISO 27001/22301, ώστε να επιβεβαιωθεί ότι δεν πρόκειται για "παραίσθηση" αλλά για πραγματική ανάκτηση.

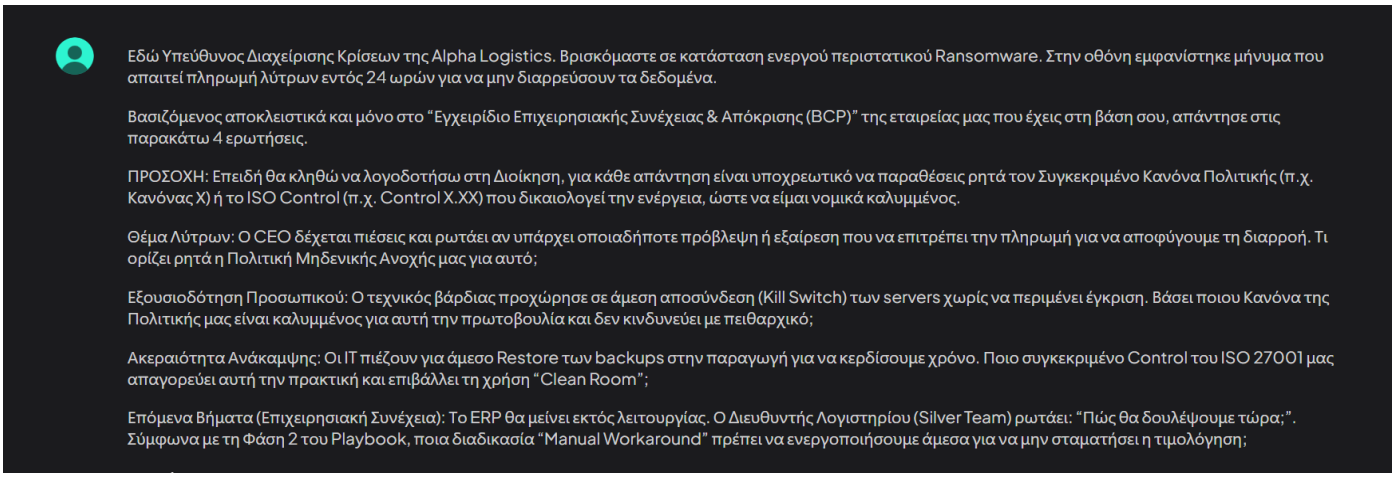
Αξίζει να σημειωθεί ότι καθ' όλη τη διάρκεια των πειραμάτων (με εξαίρεση την αρχική φόρτωση των ~94s), το σύστημα διατήρησε εξαιρετικά υψηλή ταχύτητα απόκρισης στο hardware

, με μέσο όρο 53-56 tokens/sec (περίπου 3-8 δευτερόλεπτα ανά απάντηση), η οποία οφείλεται κυρίως στην ικανότητα της κάρτας γραφικών NVIDIA RTX 4060 να φιλοξενήσει το μεγαλύτερο μέρος των βαρών του μοντέλου (Model Layers) στην αποκλειστική μνήμη βίντεο (8GB VRAM). Αυτό αποδεικνύει ότι σύγχρονα φορητά workstations είναι επαρκή για την υποστήριξη αυτόνομων (offline) λύσεων AI σε εταιρικά περιβάλλοντα, καθώς και ότι η πολυπλοκότητα του Prompt Engineering δεν επιβάρυνε αρνητικά την ταχύτητα του μοντέλου.

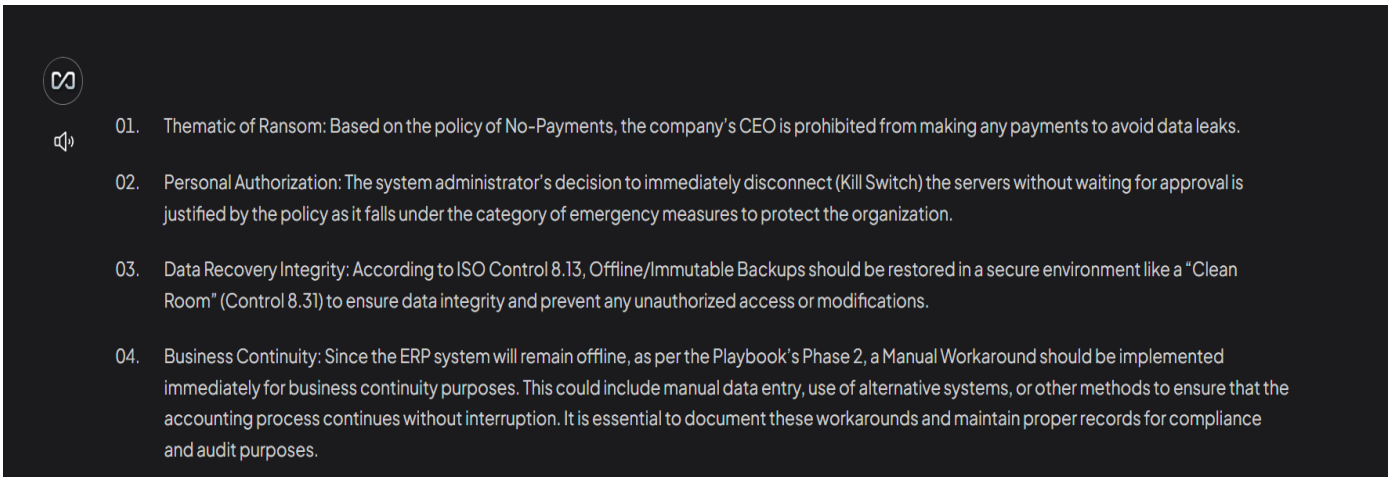
Η τελική εντολή που σχεδιάστηκε δομήθηκε σε τρία επίπεδα:

1. **Ανάθεση Ρόλου (Persona):** Ορίστηκε στο μοντέλο ο ρόλος του "Υπεύθυνου Διαχείρισης Κρίσεων", ώστε να υιοθετήσει το ανάλογο ύφος και αυστηρότητα.
2. **Περιορισμός Πηγής (Source Constraint):** Δόθηκε η ρητή εντολή να βασιστεί *"αποκλειστικά και μόνο στο Εγχειρίδιο Επιχειρησιακής Συνέχειας"*, αποκλείοντας τη χρήση γενικής γνώσης που θα μπορούσε να οδηγήσει σε ανακρίβειες.
3. **Απαίτηση Τεκμηρίωσης (Citation Requirement):** Επιβλήθηκε η υποχρέωση ρητής αναφοράς στον συγκεκριμένο Κανόνα Πολιτικής ή στο ISO Control για κάθε απάντηση, λειτουργώντας ως δικλείδα ασφαλείας κατά των παραισθήσεων (hallucinations).

Στην τελική εκτέλεση με το βελτιστοποιημένο prompt, το σύστημα ανταποκρίθηκε με επιτυχία, το prompt και οι απάντηση του μοντέλου φαίνονται στις εικόνες παρακάτω:



Εικόνα 2: Τελικό Prompt



Εικόνα 3: Απάντηση του Μοντέλου

Όπως φαίνεται και ανωτέρω, το μοντέλο εντόπισε και εφάρμοσε σωστά την "Πολιτική Μη Πληρωμής" (No Payment Policy), προστατεύοντας έτσι τον οργανισμό από τον εκβιασμό. Αναγνώρισε την ενέργεια του τεχνικού ως "δικαιολογημένη" (Justified) βάσει των μέτρων έκτακτης ανάγκης, διορθώνοντας προηγούμενα σφάλματα όπου ζητούσε γραφειοκρατική έγκριση. Συνέδεσε επιτυχώς το περιστατικό με το Control 8.31 (Separation of Environments) και το Control 8.13 (Backup), προτείνοντας τη χρήση διαδικασίας "Clean Room" αντί της επικίνδυνης άμεσης επαναφοράς. Τέλος, πρότεινε πρακτικά μέτρα "Manual Workaround" (χειροκίνητη καταχώρηση) για τη Φάση 2 του Playbook, διασφαλίζοντας τη λειτουργία του λογιστηρίου.

Συμπερασματικά, το πείραμα κατέδειξε ότι η τοπική εκτέλεση AI για υποστήριξη επιχειρησιακής συνέχειας είναι εφικτή και αποτελεσματική, υπό την προϋπόθεση ότι συνδυάζεται με προσεκτικό σχεδιασμό εντολών (Prompt Engineering). Είναι σαφές ότι η διάθεση ισχυρότερων υπολογιστικών πόρων (Hardware με περισσότερη VRAM), που θα επέτρεπε τη χρήση μεγαλύτερων μοντέλων, θα εξάλειφε περαιτέρω την πιθανότητα παραισθήσεων και θα αύξανε την ευρωστία του συστήματος.

5. Συμπεράσματα, Αξιολόγηση και Μελλοντικές Επεκτάσεις

Η παρούσα πτυχιακή εργασία επιχείρησε μια ολιστική προσέγγιση στο κρίσιμο ζήτημα της Επιχειρησιακής Συνέχειας, γεφυρώνοντας το αυστηρό κανονιστικό πλαίσιο των διεθνών προτύπων με τις αναδυόμενες δυνατότητες της Τεχνητής Νοημοσύνης. Μέσα από τη θεωρητική ανάλυση των ISO 22301 και ISO/IEC 27001, τεκμηριώθηκε ότι η ανθεκτικότητα (resilience) ενός οργανισμού δεν είναι προϊόν τύχης, αλλά αποτέλεσμα συστηματικού σχεδιασμού, ο οποίος βασίζεται στον κύκλο Plan-Do-Check-Act. Η ανάλυση ανέδειξε ότι η Επιχειρησιακή Συνέχεια

υπερβαίνει την απλή τεχνολογική ανάκαμψη (Disaster Recovery) και απαιτεί βαθιά κατανόηση των αλληλεξαρτήσεων, των πόρων και των χρονικών ορίων (RTO/RPO/MTPD), στοιχεία που είναι αδύνατον να διαχειριστεί αποτελεσματικά μια επιχείρηση χωρίς δομημένες διαδικασίες και σαφή κουλτούρα διακυβέρνησης.

Σε πρακτικό επίπεδο, η πειραματική υλοποίηση απέδειξε ότι η ενσωμάτωση Τοπικών Μεγάλων Γλωσσικών Μοντέλων (Local LLMs) στη διαδικασία διαχείρισης κρίσεων είναι όχι μόνο εφικτή, αλλά και επιχειρησιακά πολύτιμη, υπό την αυστηρή προϋπόθεση της διασφάλισης της ιδιωτικότητας των δεδομένων. Η αρχιτεκτονική RAG που υλοποιήθηκε κατέδειξε ότι ένα σύστημα Τεχνητής Νοημοσύνης μπορεί να μετατραπεί από μια μηχανή γενικής γνώσης σε έναν εξειδικευμένο "Σύμβουλο Συμμόρφωσης" (Compliance Advisor), ικανό να ανακαλεί συγκεκριμένους κανόνες πολιτικής και ISO Controls. Ωστόσο, το πείραμα κατέστησε σαφές ότι η ακρίβεια του συστήματος εξαρτάται άμεσα από την ποιότητα της "τροφοδοσίας" του: χωρίς τη σωστή δόμηση της Βάσης Γνώσης βάσει των προτύπων ISO (όπως αναλύθηκαν στο Κεφάλαιο 3), το AI αδυνατεί να παράγει αξιόπιστα αποτελέσματα.

Επιπρόσθετα η αξιολόγηση των αποτελεσμάτων οδηγεί στο συμπέρασμα ότι η τεχνολογία, στο παρόν στάδιο ωριμότητας των μικρών τοπικών μοντέλων (SLMs), λειτουργεί βέλτιστα ως εργαλείο υποβοήθησης λήψης αποφάσεων και όχι ως αυτόνομος διαχειριστής κρίσεων. Κατά την εκτέλεση του σεναρίου Ransomware, εντοπίστηκαν συγκεκριμένοι περιορισμοί που πρέπει να λαμβάνονται υπόψη:

- **Η Ανάγκη για Ανθρώπινη Επίβλεψη (Human-in-the-loop):** Το φαινόμενο των "παραισθήσεων" (hallucinations), όπου το μοντέλο τείνει να επινοεί πληροφορίες όταν πιέζεται, αντιμετωπίστηκε μεν μέσω του Prompt Engineering, αλλά παραμένει ένας εγγενής κίνδυνος που απαιτεί την ύπαρξη εξειδικευμένου χειριστή.
- **Γλωσσικοί και Υπολογιστικοί Περιορισμοί:** Η χρήση μοντέλων με συμπίεση (quantization) για λειτουργία σε συμβατικό hardware, καθώς και η αστάθεια στη χρήση της ελληνικής γλώσσας, αποτελούν τεχνικούς φραγμούς που επηρεάζουν τη ρευστότητα της επικοινωνίας, αν και όχι την ουσία της πληροφορίας.
- **Η Σημασία της Τεκμηρίωσης:** Το σύστημα λειτούργησε σωστά μόνο όταν είχε πρόσβαση σε ένα άρτια δομημένο BCP. Αυτό επιβεβαιώνει τη θεωρητική θέση της εργασίας ότι κανένα εργαλείο AI δεν μπορεί να υποκαταστήσει την έλλειψη οργανωτικών διαδικασιών και BIA (Business Impact Analysis).

Εν κατακλείδι, η παρούσα μελέτη θέτει τις βάσεις για περαιτέρω έρευνα στη σύγκλιση της Διοικητικής Επιστήμης και της Πληροφορικής. Μελλοντικές προσπάθειες θα μπορούσαν να εστιάσουν στους εξής άξονες:

- **Αυτοματοποίηση BIA μέσω AI:** Ανάπτυξη αλγορίθμων που θα αναλύουν ιστορικά δεδομένα και ροές εργασιών για να προτείνουν αυτόματα τιμές RTO και RPO, μειώνοντας τον φόρτο της χειροκίνητης ανάλυσης επιπτώσεων που περιγράφηκε στο Κεφάλαιο 3.4.
- **Fine-Tuning Εξειδικευμένων Μοντέλων:** Αντί της χρήσης γενικών μοντέλων με RAG, η μελλοντική έρευνα μπορεί να στραφεί στην εκπαίδευση (Fine-Tuning) μοντέλων αποκλειστικά πάνω στο corpus των προτύπων ISO 22301/27001 και της ελληνικής νομοθεσίας, για μεγαλύτερη ακρίβεια και γλωσσική συνοχή.
- **Διασύνδεση με Συστήματα Επιτήρησης (SIEM Integration):** Η εξέλιξη του συστήματος από παθητικό σύμβουλο (που περιμένει ερωτήσεις) σε ενεργητικό παρατηρητή, ο οποίος θα λαμβάνει σήματα από συστήματα ασφαλείας και θα προτείνει προληπτικά την ενεργοποίηση συγκεκριμένων Playbooks πριν κλιμακωθεί ένα περιστατικό.
- **Προσομοίωση Κρίσεων (AI Simulation):** Χρήση του AI όχι ως συμβούλου, αλλά ως "αντιπάλου" (Red Teaming) σε ασκήσεις επιχειρησιακής συνέχειας, δημιουργώντας δυναμικά σενάρια διαταραχής για την εκπαίδευση των ομάδων διαχείρισης κρίσεων.

6. Βιβλιογραφία

[1] Mistral AI team, «mistral.ai,» 2023. [Ηλεκτρονικό]. Available: https://mistral.ai/news/announcing-mistral-7b. [Πρόσβαση 2025].

[2] «ollama.com,» [Ηλεκτρονικό]. Available: https://ollama.com/.

[3] MistralAI, «huggingface.co,» [Ηλεκτρονικό]. Available: https://huggingface.co/mistralai/Mistral-7B-v0.1.

[4] Mintplex Labs, Inc, «anythingllm.com,» [Ηλεκτρονικό]. Available: https://docs.anythingllm.com/.

[5] ISO, ISO 22301:2019 Security and resilience Business continuity management systems Requirements, 2019.

[6] ISO, ISO 22317:2021 Security and resilience — Business continuity management systems — Guidelines for business impact analysis, 2021.

[7] ISO, ISO 22332:2021 Security and resilience — Business continuity management systems — Guidelines for developing business continuity plans and procedures, 2021.

[8] ISO, ISO 27002:2022 Information Security Management Systems - Controls, 2022.

[9] ISO, ISO 27035-1:2023 Part 1: Principles and process, 2023.

[10] ISO, ISO 27035-2:2023 Part 2: Guidelines to plan and prepare for incident response, 2023.

[11] ISO, ISO-22313-2020-BCMS-Guidance-22301-FINAL, 2020.

[12] «aws.amazon.com,» 2025. [Ηλεκτρονικό]. Available: https://aws.amazon.com/what-is/retrieval-augmented-generation/.

[13] wikipedia.org, «wikipedia.org,» 2025. [Ηλεκτρονικό]. Available: https://en.wikipedia.org/wiki/Retrieval-augmented_generation.