

8.3 Στρατηγικές και Λύσεις Επιχειρησιακής Συνέχειας

8.3.1 Προσδιορισμός και επιλογή (8.3.2 ΝΕΟ ΠΡΟΤΥΠΟ)

Ο προσδιορισμός και η επιλογή των στρατηγικών βασίζεται στα συμπεράσματα της Ανάλυσης Επιχειρησιακών Επιπτώσεων (BIA) και της Αξιολόγησης Κινδύνων.

Ο οργανισμός πρέπει να προσδιορίσει κατάλληλες στρατηγικές επιχειρησιακής συνέχειας για:

α) την προστασία των κρίσιμων δραστηριοτήτων

β) τη σταθεροποίηση, τη συνέχιση και την ανάκαμψη των κρίσιμων δραστηριοτήτων των αλληλεξαρτήσεών τους και των υποστηρικτικών πόρων τους

γ) την εξάλειψη και διαχείριση των επιπτώσεων

- τη μείωση της πιθανότητας εμφάνισης
- τη μείωση του χρόνου διακοπής
- τον περιορισμό των επιπτώσεων της διακοπής στα προϊόντα και υπηρεσίες του Οργανισμού

(ΝΕΟ ΠΡΟΤΥΠΟ)

8.3.3 Επιλογή στρατηγικών και λύσεων

Η επιλογή μπορεί να βασισθεί στην έκταση που οι στρατηγικές και οι λύσεις:

α) ικανοποιούν τις απαιτήσεις συνέχισης και ανάκαμψης των ιεραρχημένων δραστηριοτήτων εντός των προκαθορισμένων χρονικών ορίων και του συμφωνημένου επιπέδου λειτουργίας

β) λαμβάνουν υπόψη το μέγεθος και τον τύπο της επικινδυνότητας που ο Οργανισμός επιθυμεί να αναλάβει

γ) λαμβάνουν υπόψη του σχετικού κόστους-οφέλους

ΣΤΡΑΤΗΓΙΚΕΣ ΕΠΙΧΕΙΡΗΣΙΑΚΗΣ ΣΥΝΕΧΕΙΑΣ

ΠΕΡΙΟΧΗ ΣΤΡΑΤΗΓΙΚΗΣ	ΕΙΔΟΣ ΣΤΡΑΤΗΓΙΚΗΣ	ΕΝΕΡΓΕΙΕΣ ΥΛΟΠΟΙΗΣΗΣ
Πωλήσεις	Διατήρηση αποθεμάτων ασφαλείας	
Εξοπλισμός	Stand-by εξοπλισμός	
Εγκαταστάσεις	Χρήση εναλλακτικών εγκαταστάσεων (cold sites)	
Ανθρώπινο Δυναμικό	Εκπαίδευση	

8.3.2 Απαιτούμενοι Πόροι (8.3.4 ΝΕΟ ΠΡΟΤΥΠΟ)

Ο Οργανισμός πρέπει να προσδιορίσει τις απαιτήσεις σε πόρους προκειμένου να εφαρμόσει τις επιλεχθείσες στρατηγικές.

α) Προσωπικό

β) Πληροφορίες και Δεδομένα

γ) Κτίρια

δ) Εξοπλισμός και αναλώσιμα

ε) Πληροφοριακά & Τηλεπικοινωνιακά Συστήματα

στ) Μεταφορές

ζ) Χρηματοοικονομικοί πόροι

η) Προμηθευτές και συνεργάτες

8.3.3 Προστασία και εξάλειψη

Για τους αναγνωρισθέντες κινδύνους που απαιτούν χειρισμό, ο οργανισμός θα πρέπει να λάβει προληπτικά μέτρα που θα:

α) μειώνουν την πιθανότητα της εμφάνισης συμβάντος

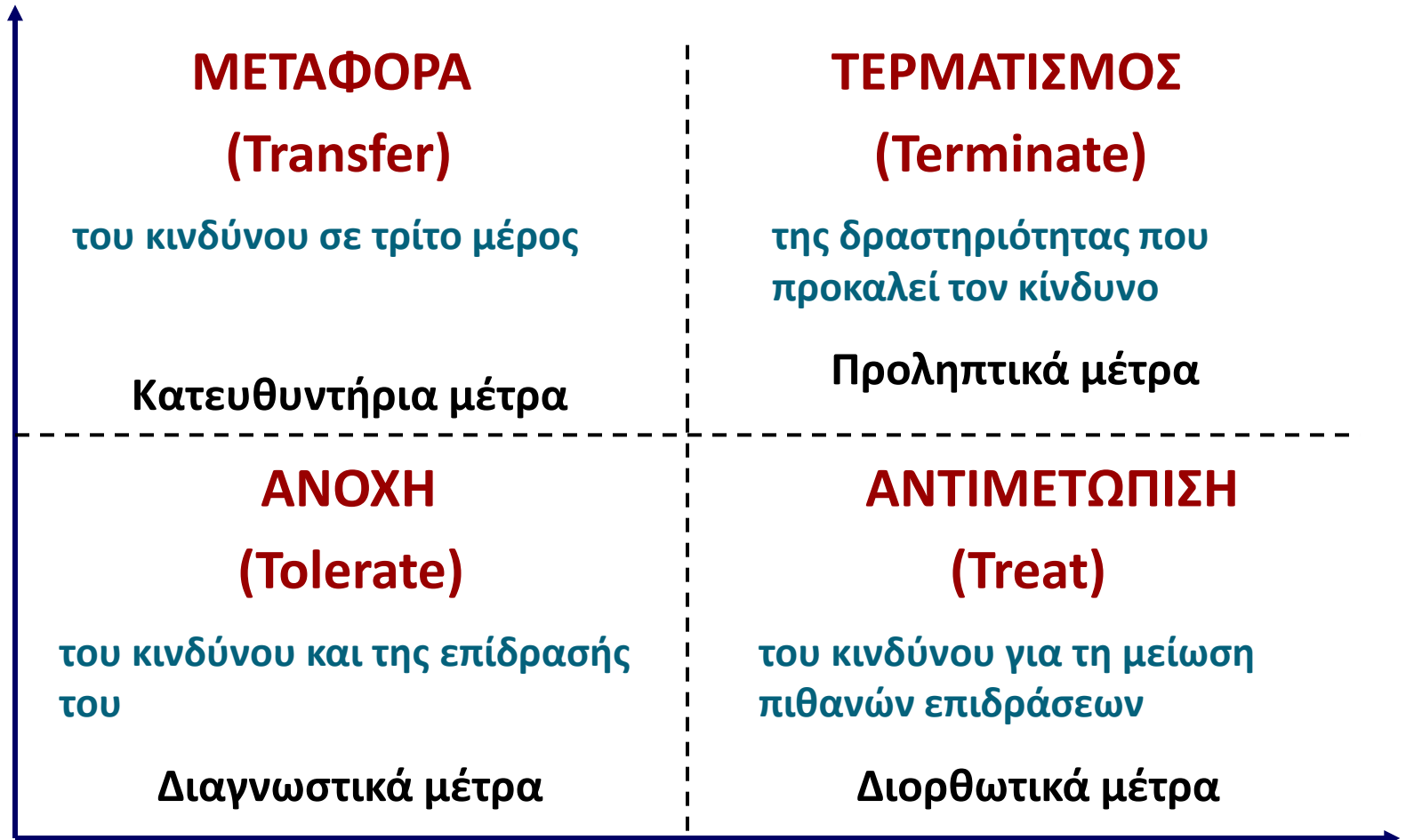
β) ελαττώνουν το χρονικό διάστημα της διακοπής

γ) περιορίζουν την επίπτωση της διακοπής της λειτουργίας στα κρίσιμα προϊόντα και υπηρεσίες του οργανισμού

Ο οργανισμός θα πρέπει να επιλέξει και να εφαρμόσει κατάλληλους χειρισμούς των κινδύνων, σύμφωνα με τη διάθεση ανάληψης κινδύνων (risk appetite).

Χειρισμός Κινδύνων

Επίπτωση



Πιθανότητα

8.4.2 Δομή αντιμετώπισης περιστατικού

Ο Οργανισμός θα πρέπει να δημιουργήσει διαδικασίες και διοικητική δομή (management structure) για αντίδραση σε περιστατικά διακοπής χρησιμοποιώντας προσωπικό με την κατάλληλη αρμοδιότητα, εξουσία και ικανότητα για τη διαχείριση περιστατικών διακοπής.

Η δομή της αντίδρασης θα πρέπει να:

- α) αναγνωρίζει το κατώφλι της επίδρασης που ενεργοποιεί την εκκίνηση της επίσημης αντίδρασης
- β) αξιολογεί τη φύση και την έκταση του περιστατικού διαταραχής και τις πιθανές επιπτώσεις του
- γ) ενεργοποιεί μια κατάλληλη αντίδραση επιχειρησιακής συνέχειας
- δ) έχει διαδικασίες και διεργασίες για την ενεργοποίηση, λειτουργία, συντονισμό και επικοινωνία της αντίδρασης
- ε) έχει πόρους διαθέσιμους για την υποστήριξη των διαδικασιών και των διεργασιών διαχείρισης περιστατικών διαταραχής για την ελαχιστοποίηση των επιπτώσεων
- στ) επικοινωνεί με τα ενδιαφερόμενα μέρη, τις αρχές και τα ΜΜΕ

8.4.2.1 Ο Οργανισμός εφαρμόζει και διατηρεί δομή αντιμετώπισης περιστατικών (Ομάδες Δράσης)

8.4.2.2 Οι ρόλοι και οι αρμοδιότητες της κάθε Ομάδας και οι μεταξύ τους σχέσεις θα πρέπει να είναι ευκρινώς καθορισμένες

8.4.2.3 Οι Ομάδες θα πρέπει να είναι ικανές:

- α) να αξιολογούν την έκταση και τη φύση της διακοπής και τις επιπτώσεις της
- β) να αξιολογούν τις επιπτώσεις έναντι προκαθορισμένων ορίων ενεργοποίησης επίσημης αντιμετώπισης
- γ) να ενεργοποιούν μια κατάλληλη αντιμετώπιση επιχειρησιακής συνέχειας
- δ) να σχεδιάζουν ενέργειες που πρέπει να αναληφθούν
- ε) να λειτουργούν βάσει προτεραιοτήτων (πρώτη προτεραιότητα η Διασφάλισης της Ανθρώπινης Ζωής)
- στ) να παρακολουθούν τα αποτελέσματα της διακοπής και της αντιμετώπισης του Οργανισμού
- ζ) να ενεργοποιούν τις λύσεις επιχειρησιακής συνέχειας
- η) να επικοινωνούν με σχετιζόμενα ενδιαφερόμενα μέρη, Αρχές και ΜΜΕ

8.4.2.4 Για κάθε Ομάδα θα πρέπει να :

- α) έχουν ορισθεί μέλη και αναπληρωματικά μέλη με τις απαραίτητες αρμοδιότητες και ικανότητες εκτέλεσης των ρόλων τους
- β) έχουν ορισθεί τεκμηριωμένες διαδικασίες ενεργειών

8.4.3 Αναγγελία περιστατικού και επικοινωνία

Ο οργανισμός θα πρέπει να καθιερώνει, εφαρμόσει και διατηρήσει διαδικασίες για:

α) την ανίχνευση συμβάντων

β) την παρακολούθηση συμβάντων

γ) την εσωτερική επικοινωνία εντός του οργανισμού και την επικοινωνία με τα ενδιαφερόμενα μέρη

δ) τη λήψη, τεκμηρίωση και απάντηση σε κάθε εθνικό ή τοπικό σύστημα διαχείρισης κινδύνων

ε) τη διασφάλιση των μέσων επικοινωνίας κατά τη διάρκεια του συμβάντος

στ) καταγραφή ζωτικής πληροφόρησης σχετικά με το συμβάν, ληφθεισών ενεργειών και αποφάσεων

Οι διαδικασίες αυτές θα πρέπει να δοκιμάζονται τακτικά μέσω ασκήσεων ετοιμότητας

NOTIFICATION AND ACTIVATION

- Defining:

- Tier Levels
- Impacts
- Thresholds

- Results In:

- Notification and Activation Protocols that marshal the appropriate resources in time for it to matter

DEFINED STATUS or ESCALATION	NOTIFICATION ACTIVATION	THRESHOLD	QUANTIFIERS + ANALYSIS = TRIGGERS
LEVEL 1	CATASTROPHIC	FULL SYSTEM DEPLOYED	<ul style="list-style-type: none"> MUTUAL ASSISTANCE MULTI-AGENCY COORDINATION GROUP (MACG)
LEVEL 2	FULL	WARNING	<ul style="list-style-type: none"> INCIDENT MANAGEMENT TEAM (IMT) INCIDENT ACTION PLAN (IAP)
LEVEL 3	PARTIAL	WATCH	<ul style="list-style-type: none"> VIRTUAL OR PHYSICAL EOC OPERATIONAL PERIODS DEFINED COMMUNICATIONS IN PLACE
LEVEL 4	STANDBY	ALERT	<ul style="list-style-type: none"> COMMON OPERATING PICTURE SITUATIONAL AWARENESS
LEVEL 5	INFORMATIONAL MONITORING	INFORMATIONAL SHARING	LOSS OF: <ul style="list-style-type: none"> PEOPLE FACILITIES SYSTEMS INFRASTRUCTURE

8.4.4 Σχέδια Επιχειρησιακής Συνέχειας

Για τις αναγνωρισθέντες από την ΒΙΑ κρίσιμες λειτουργίες και σύμφωνα με την Εκτίμηση των Κινδύνων που αφορούν τις κρίσιμες λειτουργίες, θα εκπονηθούν Σχέδια Επιχειρησιακής Συνέχειας (ανά κρίσιμη λειτουργία και ανά κίνδυνο) που θα περιλαμβάνουν:

- Αξιολόγηση Κινδύνων Κρίσιμων Λειτουργιών
- Σχέδια Αντιμετώπισης
- Σχέδια Ανάκαμψης
- Ρόλους & Υπευθυνότητες
- Λίστες εσωτερικής και εξωτερικής επικοινωνίας
- Στρατηγική επικοινωνίας με τα ΜΜΕ μετά από περιστατικό διαταραχής

Response Plans in BCM

Threats

Assets & Downstream Impacts

Response Plan Types

Denial of Access to **Building**



Emergency Plans
Storm Response Plans
Site Incident Response Plans

Lack of **People** Resources



Pandemic Plans
Alternate Work Areas
Work From Home Plans

IT Service Unavailable



Data Centre Fail-Over Plans
Infrastructure Recovery Plans
Application Validation Plans

Business Disruption



Business Processes

Business Continuity Plans
Process Resumption Plans
Continuity of Operations

Supply Chain Disruption



Vendor Management Plans
Alternate Supplier Management Plan
Product Recall Plan

Σχέδιο Αντιμετώπισης

ΠΕΡΙΣΤΑΤΙΚΟ	ΣΕΙΣΜΟΣ
ΑΜΕΣΗ ΑΝΤΙΔΡΑΣΗ	ΑΥΤΟΠΡΟΣΤΑΣΙΑ ΑΝΑΛΟΓΑ ΜΕ ΤΟ ΠΟΥ ΕΙΜΑΣΤΕ ΣΤΟ ΧΩΡΟ ΕΡΓΑΣΙΑΣ ΜΕ ΤΟ ΜΕΓΕΘΟΣ ΚΑΙ ΤΗ ΔΙΑΡΚΕΙΑ. ΔΕΝ ΜΕΤΑΚΙΝΟΥΜΑΙ ΟΣΟ ΔΙΑΡΚΗ Ο ΣΕΙΣΜΟΣ: 1. ΠΕΦΤΩ – ΚΑΛΥΠΤΟΜΑΙ – ΚΡΑΤΙΕΜΑΙ 2. ΕΑΝ ΥΠΑΡΧΕΙ ΚΑΤΑΡΡΕΥΣΗ ΤΟΥ ΧΩΡΟΥ ΠΟΥ ΕΙΜΑΣΤΕ ΨΑΧΝΩ ΤΟ ΤΡΙΓΩΝΟ ΤΗΣ ΖΩΗΣ. 3. ΣΕ ΠΕΡΙΠΤΩΣΗ ΕΓΚΛΩΒΙΣΜΟΥ ΚΑΤΩ ΑΠΟ ΕΡΕΙΠΙΑ ΔΕΝ ΧΑΝΩ ΤΗΝ ΨΥΧΡΑΙΜΙΑ ΜΟΥ ΚΑΙ ΠΡΟΣΠΑΘΩ ΝΑ ΔΩΣΩ ΤΗ ΘΕΣΗ ΜΟΥ
ΕΝΕΡΓΟΠΟΙΗΣΗ ΣΑΕΚ	Ο ΣΥΝΤΟΝΙΣΤΗΣ ΜΕ ΤΟ ΠΕΡΑΣ ΤΟΥ ΦΑΙΝΟΜΕΝΟΥ ΔΙΑΤΑΣΣΕΙ ΤΗΝ ΑΜΕΣΗ ΕΚΚΕΝΩΣΗ ΤΟΥ ΧΩΡΟΥ ΕΡΓΑΣΙΑΣ ΠΛΗΝ ΚΡΙΣΙΜΩΝ ΛΕΙΤΟΥΡΓΙΩΝ.
Α΄ ΦΑΣΗ	ΕΚΚΕΝΩΣΗ ΧΩΡΩΝ – ΑΜΕΣΗ ΔΙΑΚΟΠΗ ΠΑΡΟΧΩΝ (ΦΥΣ. ΑΕΡΙΟΥ/ΥΔΡΟΓΟΝΟΥ/ΡΕΥΜΑΤΟΣ ΚΛΠ) ΣΥΓΚΕΝΤΡΩΣΗ ΣΤΟΥΣ ΧΩΡΟΥΣ ΚΑΤΑΦΥΓΗΣ – ΚΑΤΑΜΕΤΡΗΣΗ ΠΡΟΣΩΠΙΚΟΥ – ΕΛΕΓΧΟΣ ΠΙΘΑΝΩΝ ΑΠΩΛΕΙΩΝ – ΕΛΕΓΧΟΣ ΕΓΚΑΤΑΣΤΑΣΕΩΝ - ΕΝΗΜΕΡΩΣΗ ΣΥΝΤΟΝΙΣΤΗ ΣΧΕΔΙΟΥ – ΣΥΓΚΕΝΤΡΩΣΗ ΟΜΑΔΩΝ ΔΡΑΣΗΣ ΤΟΥ ΣΑΕΚ ΣΤΑ ΠΡΟΚΑΘΟΡΙΣΜΕΝΑ ΣΗΜΕΙΑ ΚΑΙ ΕΞΟΠΛΙΣΜΟΣ ΤΟΥΣ
Β΄ ΦΑΣΗ	ΑΣΦΑΛΙΣΗ ΧΩΡΩΝ ΠΟΥ ΕΧΟΥΝ ΥΠΟΣΤΕΙ ΖΗΜΙΕΣ Ή ΕΧΟΥΝ ΑΝΑΦΕΡΘΕΙ ΑΠΩΛΕΙΕΣ – ΕΠΕΜΒΑΣΗ ΟΜΑΔΩΝ ΔΡΑΣΗΣ – ΠΥΡΟΣΒΕΣΗ ΕΣΤΙΩΝ ΠΥΡΚΑΓΙΑΣ – ΕΝΤΟΠΙΣΜΟΣ ΕΓΚΛΩΒΙΣΜΕΝΩΝ – ΔΗΜΙΟΥΡΓΙΑ ΧΩΡΟΥ TRIAGE (ΔΙΑΛΟΓΗΣ ΤΡΑΥΜΑΤΙΩΝ) – ΤΟΠΟΘΕΤΗΣΗ ΦΡΑΓΜΩΝ ΣΕ ΠΕΡΙΠΤΩΣΕΙΣ ΔΙΑΡΡΟΗΣ ΧΗΜΙΚΩΝ – ΚΛΗΣΗ ΕΞΩΤΕΡΙΚΗΣ ΒΟΗΘΕΙΑΣ – ΕΝΗΜΕΡΩΣΗ ΚΕΝΤΡΙΚΩΝ ΕΤΑΙΡΕΙΑΣ
Γ΄ ΦΑΣΗ	ΑΠΕΓΚΛΩΒΙΣΜΟΣ ΕΡΓΑΖΟΜΕΝΩΝ – ΜΕΤΑΦΟΡΑ ΤΡΑΥΜΑΤΙΩΝ ΣΤΟ ΧΩΡΟ ΔΙΑΛΟΓΗΣ – ΠΑΡΟΧΗ ΠΡΩΤΩΝ ΒΟΗΘΕΙΩΝ – ΜΕΤΑΦΟΡΑ ΤΡΑΥΜΑΤΙΩΝ ΣΕ ΝΟΣΟΚΟΜΕΙΑ – ΠΡΟΣΠΑΘΕΙΑ ΠΕΡΙΟΡΙΣΜΟΥ ΧΗΜΙΚΗΣ ΡΥΠΑΝΣΗΣ - ΕΝΗΜΕΡΩΣΗ ΤΟΠΙΚΩΝ ΑΡΧΩΝ & ΜΜΕ
Δ΄ ΦΑΣΗ	ΑΠΟΚΑΤΑΣΤΑΣΗ ΠΙΘΑΝΩΝ ΦΘΟΡΩΝ ΣΤΑ ΔΙΚΤΥΑ ΚΟΙΝΗΣ ΩΦΕΛΕΙΑΣ ΠΟΥ ΤΡΟΦΟΔΟΤΟΥΝ ΤΗΝ ΕΓΚΑΤΑΣΤΑΣΗ ΜΑΣ – ΚΑΘΑΡΙΣΜΟΣ ΑΠΟΡΡΥΠΑΝΣΗ ΜΟΛΥΣΜΕΝΩΝ ΕΠΙΦΑΝΕΙΩΝ ΑΠΟ ΚΑΠΝΑΕΡΙΑ Ή ΧΗΜΙΚΕΣ ΟΥΣΙΕΣ – ΕΛΕΓΧΟΣ ΣΤΑΤΙΚΟΤΗΤΑΣ ΚΤΙΡΙΩΝ – ΑΡΣΗ ΑΠΟΚΛΕΙΣΜΟΥ – ΕΠΑΝΑΛΕΙΤΟΥΡΓΙΑ ΕΓΚΑΤΑΣΤΑΣΗΣ –

Σχέδιο Ανάκαμψης

ΚΡΙΣΙΜΗ ΔΡΑΣΤΗΡΙΟΤΗΤΑ	
Υλοποιηθείς Κίνδυνος	
Επιπτώσεις	
Χρόνοι & Επίπεδα Ανάκαμψης	RTO: (Recovery Time Objective) MBCO: (Minimum Business Continuity Objective)
Υπεύθυνος	Τομεάρχης Εκμετάλλευσης
Ενέργειες Ανάκαμψης	<ul style="list-style-type: none">●●●
	ΠΟΡΟΙ
Προσωπικό	
Εξοπλισμός	
Εγκαταστάσεις	
Εργολάβοι / Προμηθευτές	

8.4.5 Ανάκαμψη (Recovery)

Ο Οργανισμός θα πρέπει να έχει καταγεγραμμένες διαδικασίες για την αποκατάσταση και την επιστροφή στις επιχειρησιακές δραστηριότητες από τα προσωρινά μέτρα που υιοθετήθηκαν για την υποστήριξη των επιχειρησιακών απαιτήσεων μετά από ένα περιστατικό.

ΕΠΙΣΤΡΟΦΗ ΣΤΗΝ ΚΑΝΟΝΙΚΟΤΗΤΑ

8.5 Ασκήσεις ετοιμότητας

Ο Οργανισμός πρέπει να διενεργεί ασκήσεις και δοκιμές οι οποίες:

- α) θα είναι σύμφωνες με το score και τους στόχους του ΣΔΕΣ
- β) θα βασίζονται σε καλά σχεδιασμένα σενάρια με σαφώς καθορισμένους σκοπούς και στόχους
- γ) θα επικυρώνουν τις ρυθμίσεις επιχειρησιακής συνέχειας
- δ) θα ελαχιστοποιούν τον κίνδυνο διακοπής της λειτουργίας
- ε) θα παράγουν αναφορές συμπερασμάτων οι οποίες θα περιέχουν αποτελέσματα, προτάσεις και ενέργειες για την εφαρμογή βελτιώσεων
- στ) θα αναθεωρούνται στο πλαίσιο της συνεχούς βελτίωσης
- ζ) θα πραγματοποιούνται σε προγραμματισμένα διαστήματα καθώς επίσης και όταν υπάρχουν σημαντικές αλλαγές στο εσωτερικό του Οργανισμού ή στο περιβάλλον εντός του οποίου δραστηριοποιείται

Οι ασκήσεις για την εφαρμογή του ΣΕΣ περιλαμβάνουν τις παρακάτω μορφές :

- **Σχεδιασμός στο γραφείο**
- **Λειτουργικές Ασκήσεις**
- **Άσκηση προετοιμασίας**
- **Άσκηση πλήρους κλίμακας**

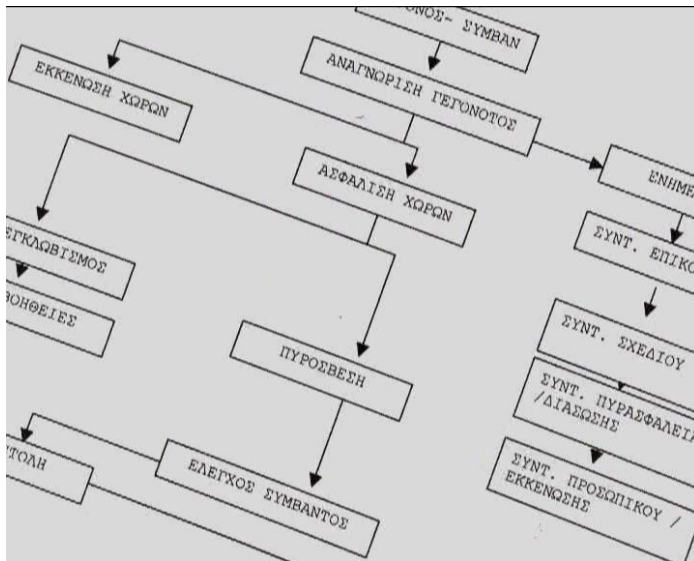
Σχεδιασμός στο γραφείο

Οι συντονιστές των ομάδων του ΣΕΣ, συγκεντρώνονται στο γραφείο συσκέψεων και ενημερώνονται:

- **για τις αρμοδιότητές τους**
- **για το σχέδιο αντίδρασής τους σε διάφορα επείγοντα περιστατικά**
- **για τη μεταξύ τους επικοινωνία και συνεργασία**

Λειτουργικές Ασκήσεις

Οι συντονιστές του ΣΕΣ δοκιμάζουν ειδικές λειτουργίες (όπως επείγουσες ανακοινώσεις, διαδικασίες επικοινωνιών, ειδοποίησης και ελέγχου του εξοπλισμού).



Ασκήσεις προετοιμασίας

Οι ομάδες του ΣΕΣ εκπαιδεύονται σε σχετικές ασκήσεις στους χώρους εργασίας τους.



Άσκηση πλήρους κλίμακας

Ενεργοποίηση του ΣΕΣ σε μία, σχεδόν πραγματική, επείγουσα κατάσταση. Αυτή η άσκηση εμπλέκει όλες τις Ομάδες του ΣΕΣ, καθώς και εξωτερικούς φορείς (Π.Υ. , ΕΚΑΒ , Ε.Α. , ΓΓΠΠ, κ.ά.).



8.6 Αξιολόγηση των διαδικασιών και των δυνατοτήτων επιχειρησιακής συνέχειας

Ο Οργανισμός θα πρέπει να:

α) αξιολογήσει την επάρκεια, καταλληλότητα και αποτελεσματικότητα της ΒΙΑ, της RA, των στρατηγικών, των λύσεων και των διαδικασιών

β) διενεργεί τις αξιολογήσεις μέσω ανασκοπήσεων, αναλύσεων, ασκήσεων, δοκιμών, αναφορών μετά από περιστατικά

γ) διενεργεί αξιολογήσεις των ικανοτήτων επιχειρησιακής συνέχειας συνεργατών και προμηθευτών

δ) αξιολογεί τη συμμόρφωση με νομικές και ρυθμιστικές απαιτήσεις και την πολιτική και τους στόχους του

ε) ανανεώνει την τεκμηρίωση και τις διαδικασίες

Οι αξιολογήσεις αυτές θα πρέπει να διενεργούνται σε προγραμματισμένα χρονικά διαστήματα, μετά από περιστατικά και όταν συμβαίνουν σημαντικές αλλαγές.

9. Αξιολόγηση της Απόδοσης

9.1 Παρακολούθηση, Μετρήσεις, Ανάλυση και Αξιολόγηση

(documented information)
of results

Ο Οργανισμός θα πρέπει να προσδιορίσει :

- τί χρειάζεται να μετρηθεί
- τις μεθόδους παρακολούθησης, μέτρησης, ανάλυσης και αξιολόγησης
- πότε θα πραγματοποιείται η παρακολούθηση και μέτρηση και πότε θα αναλύονται και αξιολογούνται τα αποτελέσματα

Ο Οργανισμός θα πρέπει να αξιολογεί την απόδοση και την αποτελεσματικότητα του ΣΔΕΣ.

Οι διαδικασίες παρακολούθησης της απόδοσης θα πρέπει να προβλέπουν:

- τον ορισμό δεικτών απόδοσης κατάλληλων για τις ανάγκες του Οργανισμού**
- την παρακολούθηση του βαθμού υλοποίησης της πολιτικής επιχειρησιακής συνέχειας, των σκοπών και στόχων**
- την απόδοση των διαδικασιών, διεργασιών και λειτουργιών που προστατεύουν τις προτεραιοποιημένες δραστηριότητες**
- παρακολούθηση της συμμόρφωσης με το Πρότυπο και τους σκοπούς της επιχειρησιακής συνέχειας**
- παρακολούθηση ιστορικών στοιχείων ελλειπούς απόδοσης του ΣΔΕΣ**
- καταγραφή δεδομένων και αποτελεσμάτων για την εφαρμογή διορθωτικών ενεργειών**

Αξιολογήσεις των διαδικασιών επιχειρησιακής συνέχειας θα πρέπει να γίνονται μέσω:

- **περιοδικών ανασκοπήσεων**
- **ασκήσεων**
- **αναφορών μετά από συμβάν (post-incident ανασκόπηση)**

Επίσης θα πρέπει να αξιολογείται περιοδικά η συμμόρφωση με τις νομοθετικές και ρυθμιστικές απαιτήσεις.

9.2 Εσωτερικές Επιθεωρήσεις

Προγράμματα Εσωτερικών Επιθεωρήσεων, συχνότητα, επιλογή Εσωτερικών Επιθεωρητών (αντικειμενικότητα, ανεξαρτησία, ικανότητες), follow-up για επιβεβαίωση λήψης διορθωτικών ενεργειών κλπ (ISO 19011).

Τα προγράμματα εσωτερικών επιθεωρήσεων πρέπει να βασίζονται στα αποτελέσματα της Αξιολόγησης Κινδύνων (Risk assessment) των δραστηριοτήτων του Οργανισμού, στην Ανάλυση Επιχειρησιακών Επιπτώσεων (BIA) και στα αποτελέσματα των προηγούμενων εσωτερικών επιθεωρήσεων

9.3 Ανασκόπηση από τη Διοίκηση

Εισερχόμενα

- Ενέργειες που είχαν αποφασισθεί σε προηγούμενες ανασκοπήσεις
- αλλαγές στο εξωτερικό και εσωτερικό περιβάλλον σχετικές με το ΣΔΕΣ
- πληροφορίες σχετικά με την απόδοση της επιχειρησιακής συνέχειας, συμπεριλαμβανομένων:
 - ✓ μη συμμορφώσεων και διορθωτικών ενεργειών
 - ✓ αποτελεσμάτων παρακολούθησης και μετρήσεων
 - ✓ αποτελεσμάτων εσωτερικών επιθεωρήσεων
- ευκαιρίες βελτίωσης
- αποτελέσματα ασκήσεων
- κίνδυνοι μη επαρκώς προβλεφθέντες σε προηγούμενα risk assessments
- συμπεράσματα από προηγούμενα περιστατικά διαταραχής

Εξερχόμενα

- αλλαγές στο σκοπό του Συστήματος και
- βελτιώσεις της αποτελεσματικότητας του Συστήματος
- επικαιροποίηση της Ανάλυσης Κινδύνων, της Ανάλυσης Επιχειρησιακών Επιπτώσεων, Σχεδίων Επιχειρησιακής Συνέχειας και σχετικών διαδικασιών
- τροποποιήσεις των διαδικασιών και μέτρων ελέγχου λόγω αλλαγών:
 - ✓ στις επιχειρησιακές και λειτουργικές απαιτήσεις
 - ✓ στις απαιτήσεις ασφάλειας (security requirements)
 - ✓ στις νομικές και ρυθμιστικές απαιτήσεις
 - ✓ στις συμβατικές υποχρεώσεις
 - ✓ στα επίπεδα κινδύνου και στα κριτήρια αποδοχής κινδύνων (Risk Appetite)
 - ✓ στις απαιτήσεις χρηματοδοτήσεις και προϋπολογισμού
- αποφάσεις σχετικά με τον τρόπο μέτρησης της αποτελεσματικότητας των μέτρων ελέγχου

10. Βελτίωση

(documented information)

10.1 Μη Συμμόρφωση και Διορθωτικές Ενέργειες

- αναγνώριση της μη-συμμόρφωσης
- διόρθωση μη-συμμόρφωσης και αντιμετώπιση συνεπειών
- ανασκόπηση αποτελεσματικότητας διορθωτικών ενεργειών
- ενέργειες εξάλειψης των αιτιών της μη-συμμόρφωσης μέσω:
 - προσδιορισμού των αιτιών της μη-συμμόρφωσης
 - λήψης διορθωτικής ενέργειας (επί των αιτιών) έτσι ώστε να διασφαλιστεί ότι δεν θα ξαναεμφανιστεί η μη-συμμόρφωση
 - ανασκόπησης της αποτελεσματικότητας των διορθωτικών ενεργειών
 - αλλαγών στο ΣΔΕΣ, εάν απαιτούνται

Τεκμηριωμένη πληροφορία καταγραφής μη-συμμορφώσεων, διορθωτικών ενεργειών και αποτελεσμάτων αυτών.

10.2 Συνεχής Βελτίωση

Ο Οργανισμός θα πρέπει να βελτιώνει συνεχώς την καταλληλότητα, την επάρκεια και την αποτελεσματικότητα του ΣΔΕΣ.

Μέσω των διαδικασιών :

- ❖ της Αξιολόγησης της Απόδοσης
- ❖ του Σχεδιασμού
- ❖ της Ηγεσίας

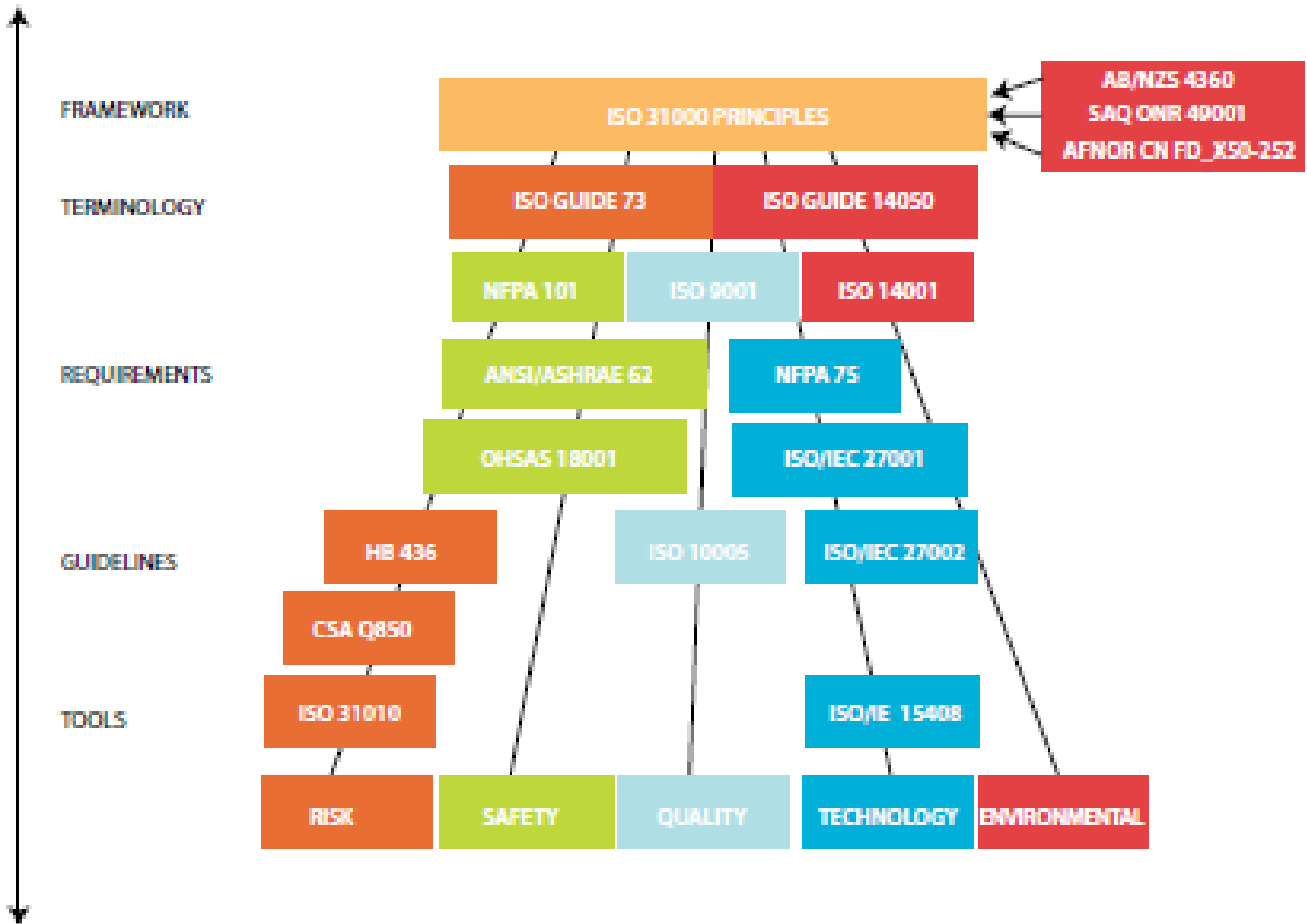
ΣΥΝΟΔΑ ΠΡΟΤΥΠΑ

- **ISO 22313 : Guidance**
- **ISO 22317: Business Impact Analysis**
- **ISO 22318: Guidelines for supply chain continuity**
- **ISO 22325: Emergency Management Capability Assessment**
- **ISO 22331: Guidelines for business continuity strategy**
- **ISO 22390: Guidelines for exercises and testing**

**ΠΛΑΤΦΟΡΜΑ
ΔΙΑΧΕΙΡΙΣΤΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
ΓΙΑ ΤΗΝ ΑΝΑΠΤΥΞΗ ΤΗΣ
ΔΙΑΧΕΙΡΙΣΗΣ ΔΙΑΚΙΝΔΥΝΕΥΣΗΣ**

ΠΙΣΤΟΠΟΙΗΣΙΜΑ ΔΙΑΧΕΙΡΙΣΤΙΚΑ ΣΥΣΤΗΜΑΤΑ ΜΕ ΑΠΑΙΤΗΣΕΙΣ ΔΙΑΧΕΙΡΙΣΗΣ ΔΙΑΚΙΝΔΥΝΕΥΣΗΣ

- **ISO 22301** (Κίνδυνοι διακοπής της Επιχειρησιακής Συνέχειας)
- **ISO 45001** (Κίνδυνοι για την Υγεία & Ασφάλεια στην Εργασία)
- **ISO 14001** (Περιβαλλοντικοί Κίνδυνοι)
- **ISO 27001** (Κίνδυνοι Πληροφοριακών Συστημάτων)
- **ISO 9001** (Κίνδυνοι Ποιότητας)
- **ISO 28000** (Κίνδυνοι Εφοδιαστικής Αλυσίδας)
- **ISO 39001** (Οδική ασφάλεια)
- **ISO 37001** (Κίνδυνοι δωροδοκίας)
- **ISO 22000** (Κίνδυνοι για την ασφάλεια τροφίμων)
- **ISO 20121** (Κίνδυνοι κατά τη διοργάνωση εκδηλώσεων)



ΟΛΟΚΛΗΡΩΣΗ ΤΩΝ ΚΟΙΝΩΝ ΑΠΑΙΤΗΣΕΩΝ ΤΩΝ ΔΙΑΧΕΙΡΙΣΤΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ



Source: BSI PAS 99:2012

ΚΟΙΝΕΣ ΑΠΑΙΤΗΣΕΙΣ ΔΙΑΧΕΙΡΙΣΤΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΔΙΑΧΕΙΡΙΣΗΣ ΔΙΑΚΙΝΔΥΝΕΥΣΗΣ

(πλατφόρμα Διαχείρισης Διακινδύνευσης)

- Αναγνώριση περιβάλλοντος
- Ετοιμότητα αντίδρασης & Σχέδια Αντιμετώπισης
- Αναγνώριση & Αξιολόγηση Κινδύνων
- Μέτρα Ελέγχου
- Ασκήσεις & Δοκιμές
- Παρακολούθηση & Μετρήσεις
- Διαδικασία Εσωτερικών Επιθεωρήσεων
- Επικοινωνία (εσωτερική & εξωτερική)
- Ανασκόπηση από τη Διοίκηση

ΣΥΝΔΕΣΗ ΣΥΣΤΗΜΑΤΩΝ ΜΕ ΤΗ ΔΙΑΧΕΙΡΙΣΗ ΔΙΑΚΙΝΔΥΝΕΥΣΗΣ



ΕΝΕΡΓΕΙΕΣ ΙΚΑΝΟΠΟΙΗΣΗΣ ΤΩΝ ΚΟΙΝΩΝ ΑΠΑΙΤΗΣΕΩΝ ΔΙΑΧΕΙΡΙΣΗΣ ΔΙΑΚΙΝΔΥΝΕΥΣΗΣ

- Αξιολόγηση Κινδύνων για επιχειρησιακή συνέχεια, υγεία & ασφάλεια, περιβάλλον, πληροφοριακά συστήματα, εφοδιαστική αλυσίδα
- Σχέδια Αντιμετώπισης Εκτάκτων Καταστάσεων
- Σχέδια Ανάκαμψης
- Μέτρα μείωσης κινδύνων
- Δείκτες μέτρησης
- Ρόλοι & αρμοδιότητες
- Διαδικασίες (διερεύνησης & καταγραφής περιστατικών και παρ' ολίγον συμβάντων, διαχείρισης εγγράφων, εσωτερικών επιθεωρήσεων κλπ)
- Ασκήσεις ετοιμότητας