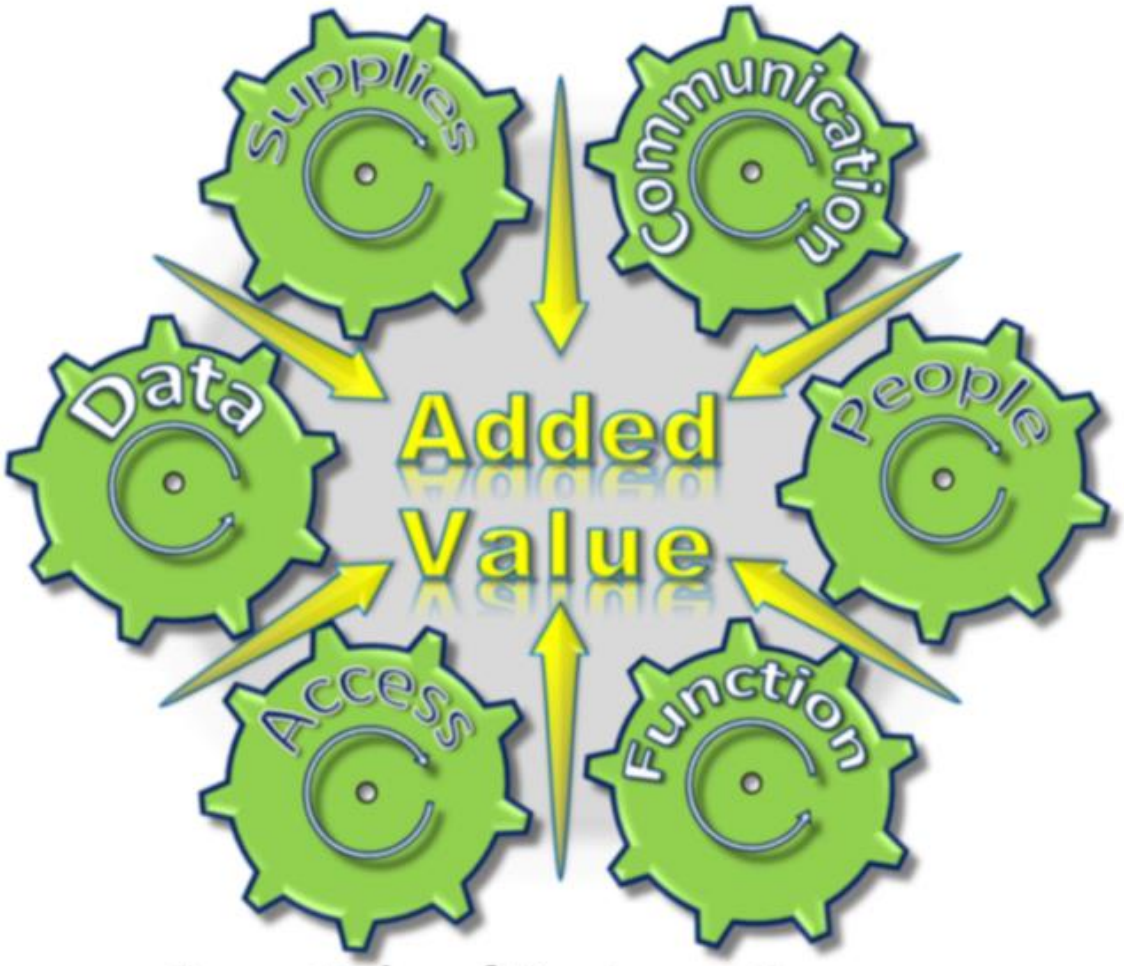
22301:2012



Essentials of Business Success

Business Disruption Scenarios

ΚΛΙΜΑΚΩΣΗ ΤΗΣ ΕΠΙΠΤΩΣΗΣ

- Ένα επαπειλούμενο στοιχείο συνιστά : **ΠΡΟΒΛΗΜΑ**
- Καθυστέρηση στην αντιμετώπιση πυροδοτεί : **ΔΙΑΤΑΡΑΧΗ**
- Αστοχία ενός στοιχείου δημιουργεί : **ΔΙΑΚΟΠΗ**
- Αστοχία δύο στοιχείων αποτελεί : **DISASTER**
- Αστοχία τριών στοιχείων αποτελεί **CATASTROPHE**

ΟΡΙΣΜΟΙ

Επιχειρησιακή Συνέχεια

Η ικανότητα ενός Οργανισμού να συνεχίσει να παρέχει προϊόντα ή υπηρεσίες σε αποδεκτά προκαθορισμένα επίπεδα μετά από ένα συμβάν διακοπής (ISO 22301)

Διαχείριση Επιχειρησιακής Συνέχειας

Ολιστική διεργασία διαχείρισης η οποία αναγνωρίζει τις πιθανές απειλές προς έναν Οργανισμό και τις επιπτώσεις στις επιχειρησιακές λειτουργίες, που μπορεί να προκαλέσουν αυτές οι απειλές, εάν υλοποιηθούν, και η οποία παρέχει ένα πλαίσιο δημιουργίας επιχειρησιακής αντοχής με την ικανότητα για μια αποτελεσματική απόκριση για τη διαφύλαξη των συμφερόντων των κυρίων ενδιαφερόμενων μερών, τη φήμη, το όνομα και τις δραστηριότητες που δημιουργούν αξία (ISO 22301)

ΔΟΜΙΚΑ ΣΤΟΙΧΕΙΑ ΣΥΣΤΗΜΑΤΟΣ

Η ανάπτυξη Συστήματος Διαχείρισης Επιχειρησιακής Συνέχειας σύμφωνα με τις απαιτήσεις του Προτύπου ISO 22301:2012 περιλαμβάνει:

- **Σύνταξη Μελέτης Ανάλυσης Επιχειρησιακών Επιπτώσεων (Business Impact Analysis), η οποία αναγνωρίζει το βαθμό κρισιμότητας της κάθε επιχειρησιακής λειτουργίας/δραστηριότητας**

- **Εφαρμογή της μεθοδολογίας Risk Management Process όπως αυτή περιγράφεται στο Πρότυπο ISO 31000 (Διαχείριση Διακινδύνευσης) προκειμένου να γίνει εκτίμηση των Κινδύνων και Απειλών (αναγνώριση, ανάλυση, αξιολόγηση), που μπορούν να διακόψουν τις κρίσιμες λειτουργίες που αναγνωρίστηκαν στην BIA**

- **Ακολουθηθούν τα βήματα της Διαχείρισης Κρίσεων και Εκτάκτων Καταστάσεων, ήτοι:**
  - **Ετοιμότητα (Readiness)**
  - **Αντίδραση / αντιμετώπιση (Response)**
  - **Ανάκαμψη (Recovery)**

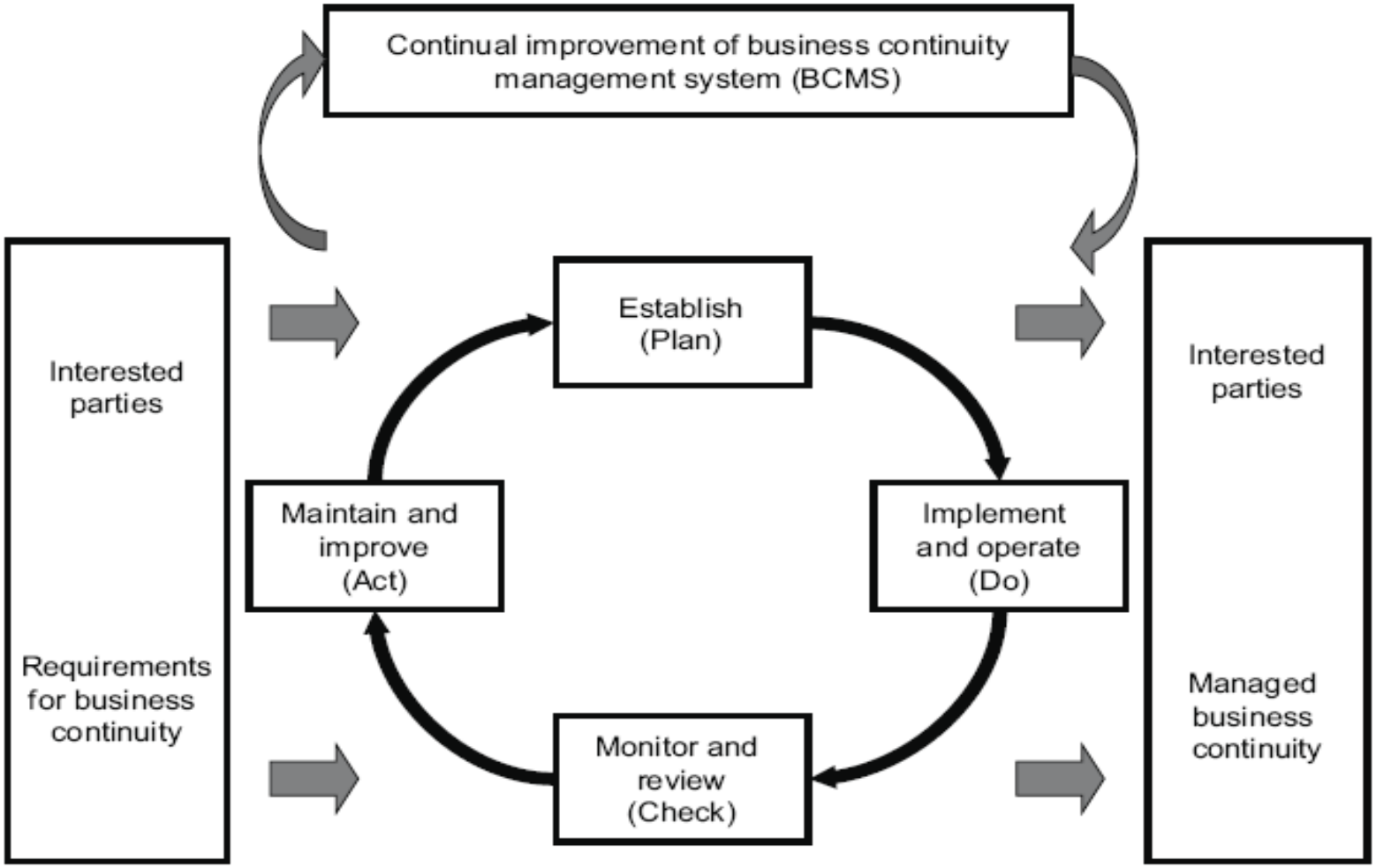
- **Σύνταξη Σχεδίου Επιχειρησιακής Συνέχειας (ΣΕΣ), το οποίο περιλαμβάνει Σχέδια Αντιμετώπισης και Σχέδια Ανάκαμψης μετά από περιστατικά διαταραχής**

- **Ανάπτυξη όλης της απαιτούμενης τεκμηρίωσης του Συστήματος Διαχείρισης (διαδικασίες, έντυπα, αρχεία)**

- **Ανάπτυξη πλαισίου Διαχείρισης Διακινδύνευσης (Risk Management framework) το οποίο θα περιλαμβάνει:**
  - **την Αρχιτεκτονική του Συστήματος (ρόλοι, υπευθυνότητες, επιτροπές και αρμοδιότητες αυτών και κανάλια επικοινωνίας)**
  - **τη Στρατηγική (πολιτική, τεχνικές εκτίμησης κινδύνων)**
  - **τα Πρωτόκολλα λειτουργίας του Συστήματος (τεκμηρίωση, τεχνικές, τρόποι αντιμετώπισης συμβάντων, κατευθυντήριες οδηγίες – guidelines, εκπαίδευση, επικοινωνία)**

ΔΟΜΗ ΤΟΥ ΠΡΟΤΥΠΟΥ

Στις διαδικασίες του BCMS εφαρμόζεται το μοντέλο PDCA



(ISO 22301/2012)

Σχεδιάζω (Plan)	Σχεδιασμός πολιτικής επιχειρησιακής συνέχειας, στόχων, ελέγχων και διαδικασιών σχετικών με τη βελτίωση της επιχειρησιακής συνέχειας
Εκτελώ (Do)	Εγκατάσταση και εφαρμογή πολιτικής, ελέγχων και διαδικασιών (υλοποίηση του σχεδιασμού)
Ελέγχω (Check)	Παρακολούθηση και ανασκόπηση της απόδοσης των διαδικασιών έναντι της πολιτικής και των στόχων, αναφορά αποτελεσμάτων στην ανασκόπηση από τη Διοίκηση και προσδιορισμός ενεργειών διόρθωσης και βελτίωσης
Ενεργώ (Act)	Διατήρηση και βελτίωση του ΣΔΕΣ με τη λήψη διορθωτικών ενεργειών βασισμένων στα αποτελέσματα της ανασκόπησης από τη Διοίκηση και επανεκτίμηση του σκοπού του ΣΔΕΣ, της πολιτικής και των στόχων

Plan

- Παράγραφος 4: Περιβάλλον του Οργανισμού
- Παράγραφος 5: Ηγεσία
- Παράγραφος 6: Σχεδιασμός
- Παράγραφος 7: Υποστήριξη

Do

- Παράγραφος 8: Λειτουργία

Check

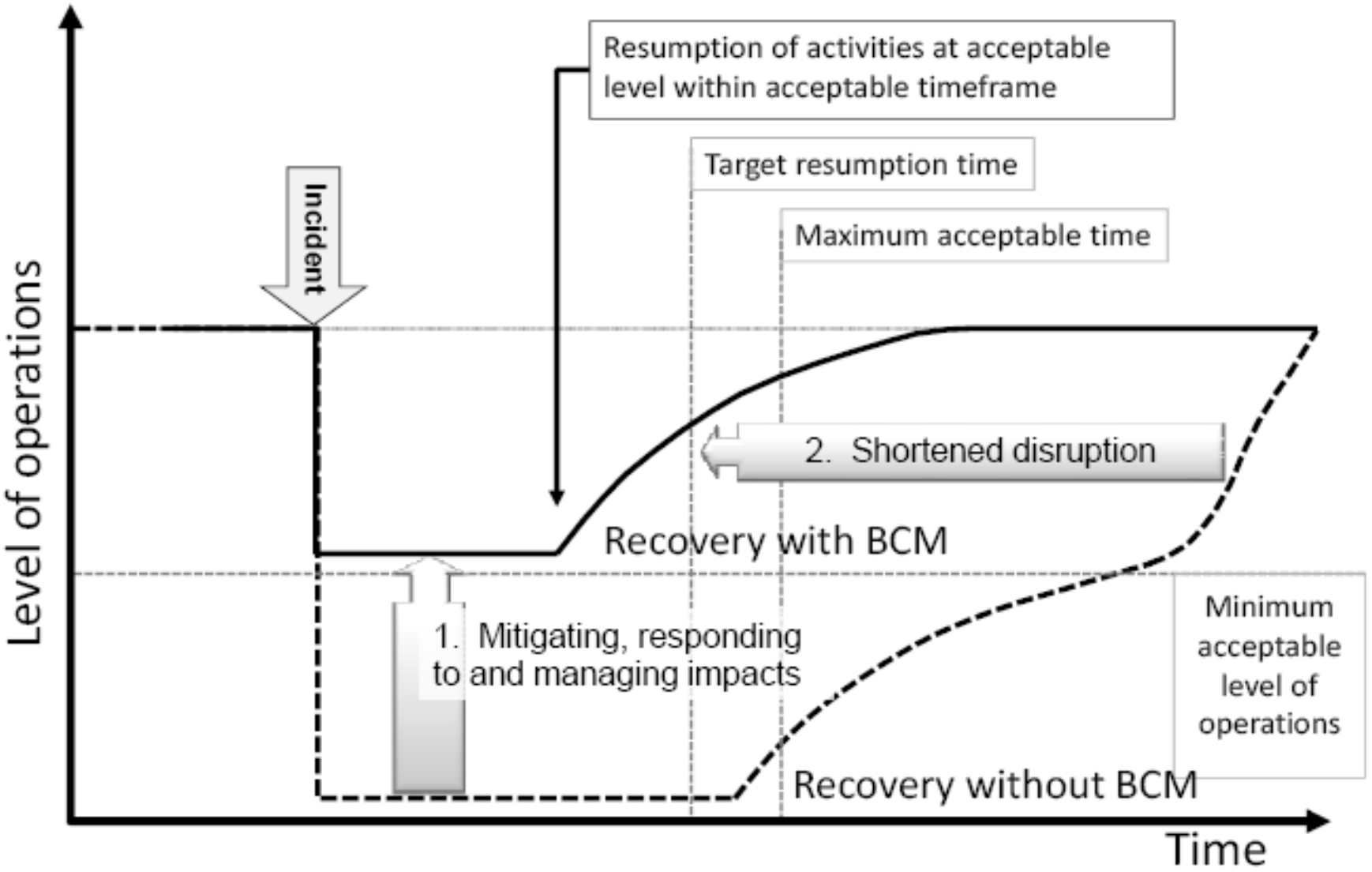
- Παράγραφος 9: Αξιολόγηση Απόδοσης

Act

- Παράγραφος 10: Βελτίωση

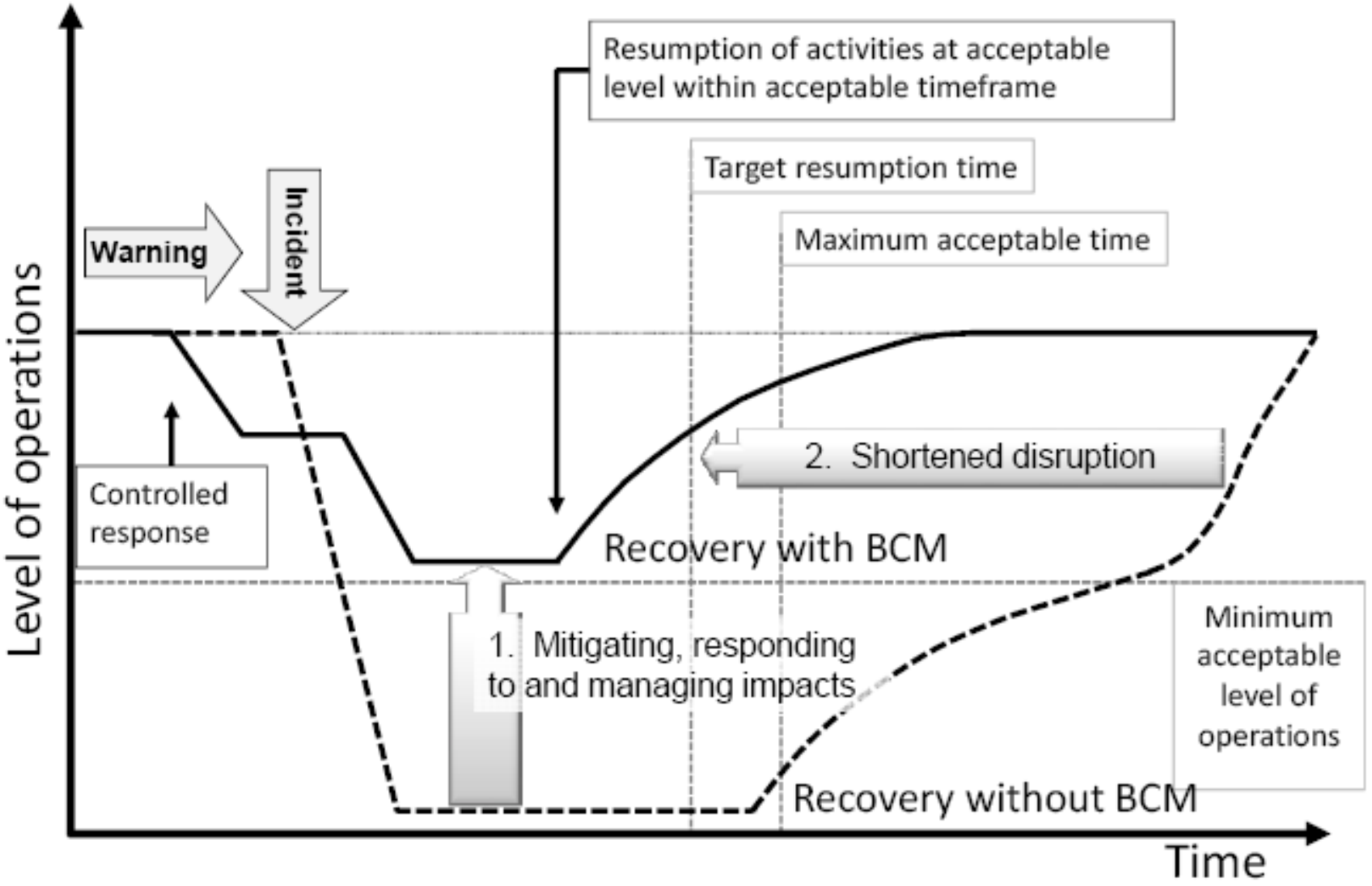
Μείωση των επιπτώσεων με την εφαρμογή ΣΔΕΣ

(αιφνίδια διακοπή)



Μείωση των επιπτώσεων με την εφαρμογή ΣΔΕΣ

(σταδιακή διακοπή)



4. Περιβάλλον του Οργανισμού

4.1 Κατανόηση του περιβάλλοντος του Οργανισμού

Εξωτερικό περιβάλλον: **PESTLE, ρυθμιστικό, εφοδιαστική αλυσίδα, σχέσεις με ενδιαφερόμενα μέρη εκτός Οργανισμού, τάσεις που μπορούν να επηρεάσουν τους σκοπούς και στόχους του Οργανισμού**

Εσωτερικό περιβάλλον: **προϊόντα και υπηρεσίες, δραστηριότητες, ενδιαφερόμενα μέρη εντός του Οργανισμού, αντιλήψεις, αξίες, κουλτούρα, δεξιότητες και πόροι (κεφάλαια, ανθρώπινο δυναμικό, διαδικασίες, συστήματα και τεχνολογίες), πληροφοριακά συστήματα, εφαρμοζόμενα πρότυπα και μοντέλα αναφοράς, δομές (σύστημα εταιρικής διακυβέρνησης, ρόλοι, υπευθυνότητες), στόχοι και στρατηγική διαχείρισης κινδύνου**

Επίπεδο Κινδύνου που ο Οργανισμός είναι πρόθυμος να αναλάβει (Risk Appetite) ***(ΔΕΝ ΑΠΑΙΤΕΙΤΑΙ ΣΤΟ ΝΕΟ ΠΡΟΤΥΠΟ)***

4.2 Κατανόηση αναγκών και προσδοκιών ενδιαφερόμενων μερών

4.2.1 Γενικά

Ο Οργανισμός θα πρέπει να προσδιορίσει:

α) τα ενδιαφερόμενα μέρη που είναι σχετικά με το ΣΔΕΣ

β) τις ανάγκες και προσδοκίες των ενδιαφερόμενων μερών

Ενδιαφερόμενα μέρη

Πελάτες, Προμηθευτές, Μέτοχοι, Εργαζόμενοι, Ρυθμιστικές Αρχές, Τοπική Κοινωνία κλπ

4.2.2 Νομικές και ρυθμιστικές απαιτήσεις

(documented information)

Αναγνώριση και καταγραφή του εφαρμοστέου δικαίου και των ρυθμιστικών απαιτήσεων σχετικών με τη συνέχιση των εργασιών/προϊόντων/υπηρεσιών

4.3 Προσδιορισμός πεδίου εφαρμογής

Ο Οργανισμός προκειμένου να προσδιορίσει το πεδίο εφαρμογής του ΣΔΕΣ πρέπει να προσδιορίσει τα όρια και τις συνθήκες εφαρμοσιμότητας του ΣΔΕΣ.

Προς τούτο θα πρέπει να λάβει υπόψη του το εσωτερικό και εξωτερικό περιβάλλον και τις απαιτήσεις των ενδιαφερόμενων μερών.

Ο προσδιορισμός του πεδίου εφαρμογής ενός ΣΔΕΣ είναι περισσότερο σύνθετος από ότι στα άλλα Διαχειριστικά Συστήματα, όπου περιλαμβάνονται μόνο οι δραστηριότητες του Οργανισμού. Στο ΣΔΕΣ το πεδίο εφαρμογής αναφέρει και τις περιπτώσεις και συνθήκες υπό τις οποίες μπορεί να εφαρμοσθεί το Σύστημα, από το επιθυμητό επίπεδο ασφαλείας, την τοποθεσία εφαρμογής, καθώς επίσης και προϊόντα/υπηρεσίες/δραστηριότητες.

5. Ηγεσία

5.2 Δέσμευση της Διοίκησης

Η Διοίκηση θα επιδείξει τη δέσμευσή της στο ΣΔΕΣ διασφαλίζοντας:

- **ότι έχουν δημιουργηθεί πολιτικές και στόχοι του ΣΔΕΣ και είναι συμβατοί με τη στρατηγική κατεύθυνση του Οργανισμού**
- **την ένταξη των απαιτήσεων του ΣΔΕΣ εντός των επιχειρησιακών διαδικασιών**
- **ότι είναι διαθέσιμοι οι απαιτούμενοι από το ΣΔΕΣ πόροι**
- **ότι το ΣΔΕΣ επιτυγχάνει τα προσδοκώμενα αποτελέσματα**
- **την επικοινωνία της σημαντικότητας της αποτελεσματικής επιχειρησιακής συνέχειας και συμμόρφωσης με τις απαιτήσεις του Προτύπου**
- **την υποστήριξη και την κατεύθυνση των ατόμων στο να συνεισφέρουν στην αποτελεσματικότητα το ΣΔΕΣ**

<u>Απόδειξη της Δέσμευσης της Διοίκησης είναι:</u>

- **η δημιουργία πολιτικής επιχειρησιακής συνέχειας**
- **η διασφάλιση ότι έχουν ορισθεί οι στόχοι και τα σχέδια εφαρμογής του ΣΔΕΣ**
- **η δημιουργία ρόλων, υπευθυνοτήτων και δεξιοτήτων σχετικών με το ΣΔΕΣ**
- **η ανάθεση σε ένα ή περισσότερα άτομα της ευθύνης του ΣΔΕΣ, με την απαιτούμενη εξουσιοδότηση και δεξιότητες έτσι ώστε να είναι υπεύθυνοι για την εφαρμογή και διατήρηση του Συστήματος**
- **ο ορισμός κριτηρίων αποδοχής κινδύνων και αποδεκτού επιπέδου κινδύνων**
- **η διοργάνωση ασκήσεων ετοιμότητας**

(documented information)

5.3 Πολιτική

Η Πολιτική Επιχειρησιακής Συνέχειας θα πρέπει να:

- **είναι κατάλληλη για τους σκοπούς του Οργανισμού**
- **παρέχει το πλαίσιο στοχοθέτησης της επιχειρησιακής συνέχειας**
- **περιέχει δέσμευση ικανοποίησης των σχετικών απαιτήσεων**
- **περιέχει δέσμευση για τη συνεχή βελτίωση του ΣΔΕΣ**

Θα πρέπει να:

- **είναι διαθέσιμη στα ενδιαφερόμενα μέρη**
- **έχει επικοινωνηθεί εντός του Οργανισμού**
- **ανασκοπείται ανά τακτά χρονικά διαστήματα και όταν συμβαίνουν σημαντικές αλλαγές**

(documented information)

5.4 Ρόλοι & Αρμοδιότητες

Η Διοίκηση θα πρέπει να διασφαλίσει την ανάθεση αρμοδιοτήτων και εξουσιοδοτήσεων για το ΣΔΕΣ.

Ένα μέλος της Διοίκησης θα πρέπει να έχει γενικές αρμοδιότητες και υπευθυνότητα για το Σύστημα.

Η Διοίκηση θα πρέπει να ορίσει ένα ή περισσότερους εκπροσώπους της οι οποίοι, ανεξαρτήτως των άλλων αρμοδιοτήτων τους, θα πρέπει να έχουν καθορισμένους ρόλους, αρμοδιότητες και εξουσιοδότηση για:

- **τη διασφάλιση της εφαρμογής και διατήρησης του ΣΔΕΣ σύμφωνα με την Πολιτική επιχειρησιακής συνέχειας**
- **την αναφορά στη Διοίκηση σχετικά με την απόδοση του ΣΔΕΣ**
- **την προώθηση της ευαισθητοποίησης σε όλο τον Οργανισμό σχετικά με την επιχειρησιακή συνέχεια**
- **τη διασφάλιση της αποτελεσματικότητας των διαδικασιών για την αντιμετώπιση συμβάντων, όχι όμως απαραίτητα και για την εφαρμογή τους κατά την εμφάνιση ενός συμβάντος *(Δομή Αντιμετώπισης)***

Ρόλοι & Αρμοδιότητες

Ρόλος	Υπεύθυνος	Αναπληρωτής
Συντονιστής ΣΕΣ	Ονομ/μο: …… Τηλ. επικοινωνίας: ……	Ονομ/νο: …… Τηλ.επικοινωνίας: ……

Αρμοδιότητες σε Έκτακτη Κατάσταση

- Ενεργοποιεί το ΣΕΣ
- Επιβλέπει την ομαλή εφαρμογή των Σχεδίων Αντίδρασης / Ανάκαμψη
- Προσδιορίζει την ανάγκη ενεργοποίησης εναλλακτικών δραστηριοτήτων επιχειρησιακής συνέχειας
- Επικοινωνεί με τα κύρια ενδιαφερόμενα μέρη όποτε απαιτείται
-
-

6. Σχεδιασμός

6.1 Ενέργειες για την αντιμετώπιση κινδύνων και ευκαιριών

Κατά το Σχεδιασμό του ΣΔΕΣ ο Οργανισμός θα πρέπει να λάβει υπόψη του θέματα σχετικά με το περιβάλλον του (§4.1) , τις ανάγκες και προσδοκίες των ενδιαφερομένων μερών (§ 4.2) και να προσδιορίσει τους Κινδύνους και τις Ευκαιρίες (Risk Identification) έτσι ώστε:

- **να διασφαλισθεί ότι το Σύστημα μπορεί να επιτύχει τους στόχους του**
- **να προληφθούν ή να μειωθούν ανεπιθύμητες επιδράσεις**
- **να επιτευχθεί συνεχής βελτίωση**

Ο Οργανισμός θα πρέπει να σχεδιάσει:

- **ενέργειες αντιμετώπισης/χειρισμού των Κινδύνων και Ευκαιριών (Risk Treatment)**
- **τον τρόπο εφαρμογής των ενεργειών αυτών και την ενσωμάτωσή τους στις διαδικασίες του ΣΔΕΣ**
- **τον τρόπο αξιολόγησης της αποτελεσματικότητας των ενεργειών αυτών**

ΣΤΟ ΝΕΟ ΠΡΟΤΥΠΟ ΟΙ ΚΙΝΔΥΝΟΙ ΤΗΣ παρ.6.1 ΑΦΟΡΟΥΝ ΤΗΝ ΑΠΟΤΕΛΕΣΜΑΤΙΚΟΤΗΤΑ ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ. ΚΙΝΔΥΝΟΙ ΠΟΥ ΑΠΕΙΛΟΥΝ ΤΗΝ ΕΠΙΧΕΙΡΗΣΙΑΚΗ ΣΥΝΕΧΕΙΑ ΑΝΤΙΜΕΤΩΠΙΖΟΝΤΑΙ ΣΤΗΝ παρ. 8.2

(documented information)

6.2 Στόχοι Επιχειρησιακής Συνέχειας και σχέδια υλοποίησής τους

Η Διοίκηση θα πρέπει να διασφαλίσει ότι έχουν ορισθεί και γίνει γνωστοί οι στόχοι επιχειρησιακής συνέχειας για τις σχετικές λειτουργίες και επίπεδα εντός του Οργανισμού.

Οι στόχοι επιχειρησιακής συνέχειας θα πρέπει:

- **να είναι συμβατοί με την πολιτική επιχειρησιακής συνέχειας**
- **να λαμβάνουν υπόψη τους το ελάχιστο επίπεδο προϊόντων και υπηρεσιών που είναι αποδεκτά από τον Οργανισμό για την ικανοποίηση των στόχων**
- **να είναι λογικοί**
- **να λαμβάνουν υπόψη τους τις σχετικές εφαρμόσιμες απαιτήσεις**
- **να παρακολουθούνται και ενημερώνονται κατάλληλα**

Για την επίτευξη των στόχων επιχειρησιακής συνέχειας ο Οργανισμός θα πρέπει να προσδιορίσει:

Ποιος είναι υπεύθυνος / Τι πρέπει να γίνει και πότε θα ολοκληρωθεί / Τι πόροι θα απαιτηθούν / Πώς θα αξιολογούνται τα αποτελέσματα

7. Υποστήριξη

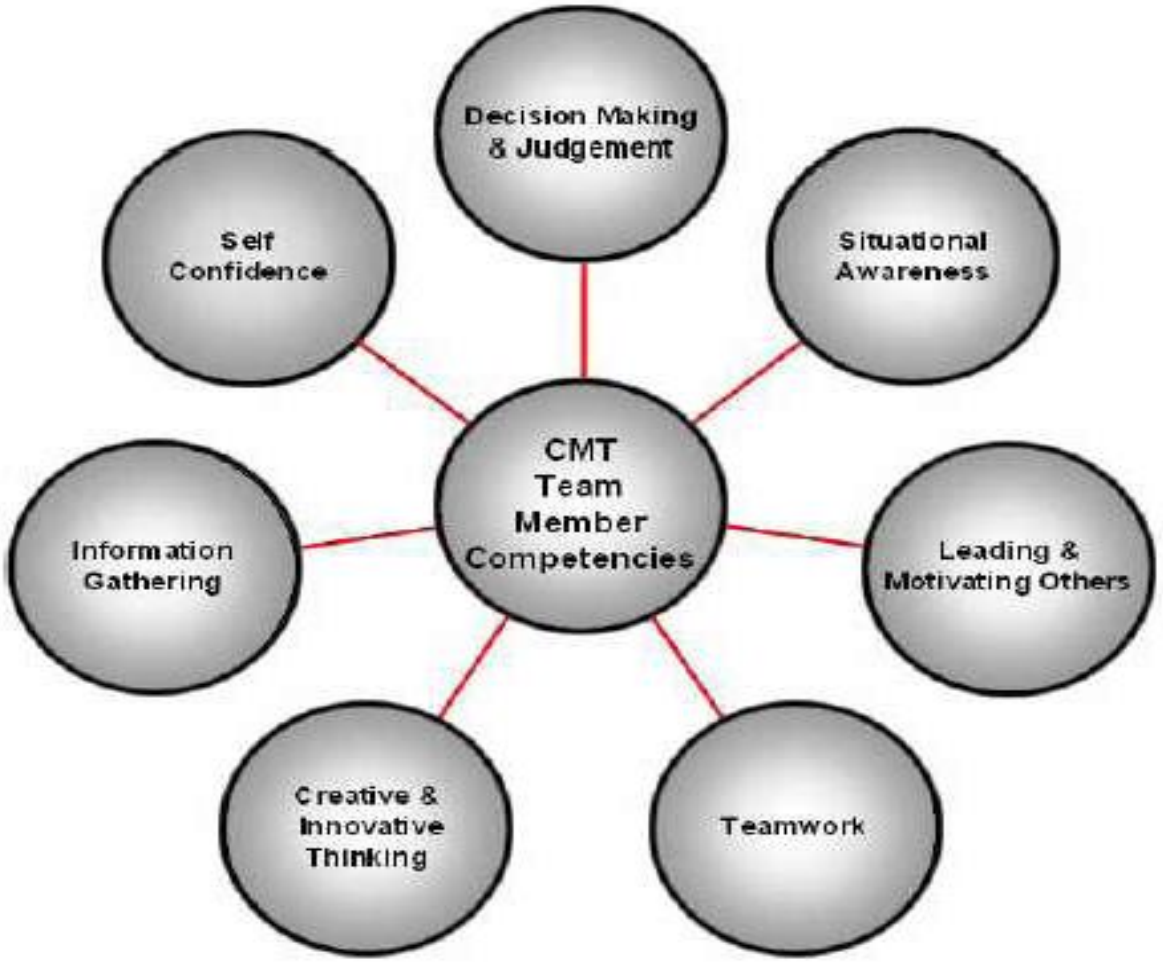
7.2 Ικανότητες

Ο Οργανισμός θα πρέπει να:

- **προσδιορίσει τις απαραίτητες ικανότητες των ανθρώπων που εκτελούν εργασίες υπό τον έλεγχό του που επηρεάζουν την απόδοσή του**
- **διασφαλίσει ότι τα άτομα αυτά είναι ικανά στη βάση κατάλληλης εκπαίδευσης, επιμόρφωσης και εμπειρίας**
- **να λάβει μέτρα για την απόκτηση των απαραίτητων ικανοτήτων και να αξιολογεί την αποτελεσματικότητα των ληφθέντων μέτρων**

Ικανότητα: είναι η μετρήσιμη ή παρατηρήσιμη γνώση (knowledge), δεξιότητες (skills), δυνατότητες (abilities) και συμπεριφορές (behaviors) κρίσιμες για την επιτυχή εργασιακή απόδοση (KSABs)

Βασικές μη τεχνικές ικανότητες που απαιτούνται να έχουν τα μέλη του Crisis Management Team (CMT)



'The Business Continuity Journal, Vol.2, Issue 1'

7.3 Ευαισθητοποίηση

Τα άτομα που εργάζονται υπό τον έλεγχο του Οργανισμού θα πρέπει να γνωρίζουν:

- **την πολιτική επιχειρησιακής συνέχειας**
- **τη συνεισφορά τους στην αποτελεσματικότητα του ΣΔΕΣ, περιλαμβανομένων των οφελών που από μια βελτιωμένη απόδοση της διαχείρισης επιχειρησιακής συνέχειας**
- **τις επιπτώσεις της μη συμμόρφωσης με τις απαιτήσεις του ΣΔΕΣ**
- **το ρόλο τους σε ένα περιστατικό διαταραχής (συμβάν)**

BEFORE a disruptive incident

DURING a disruptive incident

AFTER a disruptive incident

ΝΕΟ ΠΡΟΤΥΠΟ

(στα άτομα περιλαμβάνονται προσωπικό, προμηθευτές, εργολάβοι)

7.4 Επικοινωνία

Ο Οργανισμός πρέπει να αναπτύξει αποτελεσματικές διαδικασίες επικοινωνίας και διαβούλευσης με τα ενδιαφερόμενα μέρη, οι οποίες περιλαμβάνουν:

- **εσωτερική επικοινωνία μεταξύ των ενδιαφερόμενων μερών, συμπεριλαμβανομένων και των εργαζομένων**
- **εξωτερική επικοινωνία με πελάτες, τοπική κοινωνία, συνεργάτες και των ΜΜΕ**
- **την παραλαβή, τεκμηρίωση και ανταπόκριση στην επικοινωνία με όλα τα ενδιαφερόμενα μέρη**
- **την προσαρμογή και ενσωμάτωση εθνικού ή τοπικού συστήματος συμβουλών για απειλές *(π.χ Οδηγίες Γεν. Γραμματείας Πολιτικής Προστασίας)* στο σχεδιασμό και την επιχειρησιακή λειτουργία**
- **διασφάλιση διαθεσιμότητας μέσων επικοινωνίας κατά τη διάρκεια ενός περιστατικού διαταραχής (ασύρματοι κλπ)**

- **τη διευκόλυνση της δομημένης επικοινωνίας με τις κατάλληλες αρχές (πυροσβεστική, αστυνομία, ΕΚΑΒ κλπ) και διασφάλιση της διεπιχειρησιακής λειτουργίας των διαφόρων εμπλεκόμενων υπηρεσιών και προσωπικού**

- **τη λειτουργία και τον έλεγχο των επικοινωνιακών δυνατοτήτων που διατίθενται προς χρήση στην περίπτωση διακοπής των κανονικών επικοινωνιών**

Σε περίπτωση συμβάντος ο Οργανισμός πρέπει να παρέχει αποτελεσματική εξωτερική επικοινωνία (§ 8.4)

Λίστες επικοινωνίας

Εσωτερική

Εργαζόμενος	Τηλ. Επικοινωνίας	Email	Ρόλος

Εξωτερική

ΦΟΡΕΑΣ	Πρόσωπο επικοινωνίας	Τηλέφωνο/email

7.5 Τεκμηριωμένη Πληροφορία

Οι τεκμηριωμένες πληροφορίες (documented information) παρέχουν αποδείξεις αποτελεσματικής λειτουργίας και συμμόρφωσης στις απαιτήσεις του διαχειριστικού συστήματος.

Η τεκμηρίωση που προτείνεται για από το Πρότυπο περιλαμβάνει:

- **Πολιτική επιχειρησιακής συνέχειας**
- **Στόχους ΣΔΕΣ και διαχείρισης επιχειρησιακής συνέχειας**
- **Ανάλυση Επιχειρησιακών Επιπτώσεων (Business Impact Analysis)**
- **Risk assessment**
- **Options επιχειρησιακής συνέχειας**
- **Σχέδια Επιχειρησιακής Συνέχειας**
- **Διαδικασίες επιχειρησιακής συνέχειας**
- **Προγράμματα εκπαίδευσης και awareness**
- **Σχέδια και αναφορές ασκήσεων**

<u>Τεκμηριωμένη Πληροφορία</u> σχετική με το ΣΔΕΣ μπορεί να περιλαμβάνει:

- **Επιχειρησιακά και ατομικά προγράμματα εκπαίδευσης**
- **Αποδείξεις παρακολούθησης διεργασιών και απόδοσης**
- **Αποδείξεις επιθεωρήσεων, συντήρησης και διακρίβωσης**
- **Τεκμηρίωση εργολάβων και προμηθευτών, συμπεριλαμβανομένων και των γραπτών συμβάσεων**
- **Αναφορές διερεύνησης μετά από συμβάντα και παρ'ολίγον συμβάντα**
- **Αναφορές αποτελεσμάτων, αναλύσεων και συμπερασμάτων δοκιμών και ασκήσεων**
- **Αποτελέσματα επιθεωρήσεων**
- **Αποτελέσματα ανασκοπήσεων από τη Διοίκηση**
- **Τεκμηρίωση νομικών και ρυθμιστικών απαιτήσεων**
- **Πρακτικά συζητήσεων και συμπερασμάτων σχετικά με σημαντικούς κινδύνους**
- **Πρακτικά συσκέψεων σχετικών με διαχειριστικά συστήματα**
- **Newsletters και άλλες μορφές επικοινωνίας με ενδιαφερόμενα μέρη**

7.5.2 Δημιουργία & Επικαιροποίηση

Ο Οργανισμός πρέπει να συμμορφώνεται με όλες τις απαιτήσεις δημιουργίας ή/και ενημέρωσης των τεκμηριωμένων πληροφοριών.

Περιλαμβάνονται ο τίτλος, ημερομηνία, συντάκτης, εγκρίνων, κωδικός, αριθμός αναθεώρησης, η μορφοποίηση του εγγράφου – format και ο τρόπος διατήρησης (έγγραφος τύπος, ηλεκτρονική μορφή).

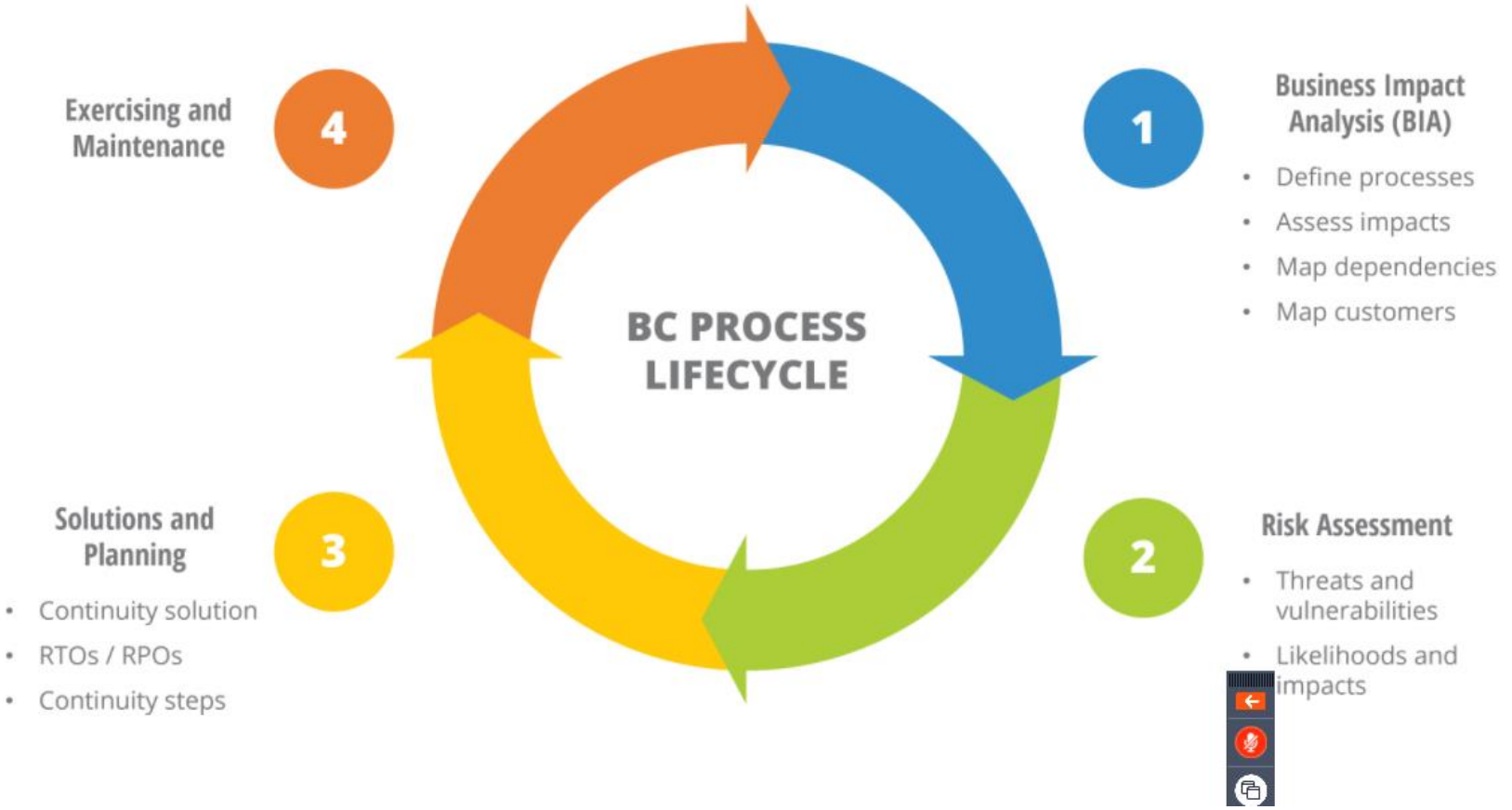
7.5.3 Έλεγχος τεκμηριωμένης πληροφορίας

Ο έλεγχος της τεκμηρίωσης αποσκοπεί στο να εξασφαλίσει ότι ο οργανισμός δημιουργεί, διατηρεί και προστατεύει έγγραφα με τρόπο που είναι κατάλληλος και επαρκής για την εφαρμογή και λειτουργία του ΣΔΕΣ.

Πρέπει να δημιουργηθεί μια τεκμηριωμένη διαδικασία (documented procedure) που να προσδιορίζει τους ελέγχους που απαιτούνται για:

- **τη διανομή, πρόσβαση της τρέχουσας έκδοσης των τεκμηριωμένων πληροφοριών στα σημεία χρήσης**
- **την έγκριση της καταλληλότητας των εγγράφων πριν τη διάθεσή τους**
- **την αναθεώρηση, επικαιροποίηση και επανέγκριση των εγγράφων**
- **την αποτροπή της χρήσης αποσυρθέντων εγγράφων και την εφαρμογή κατάλληλης αναγνώρισης αυτών**
- **τη διασφάλιση ότι οι αλλαγές είναι αναγνωρίσιμες (έλεγχος αλλαγών)**
- **τη διασφάλιση της ακεραιότητας των εγγράφων (back-up, προσβασιμότητα μόνο από εξουσιοδοτημένο προσωπικό, διαθεσιμότητα μόνο όταν χρειασθούν για αντιμετώπιση συμβάντων και επανάκαμψη**
- **τη διασφάλιση ότι εξωτερικά έγγραφα απαραίτητα για το σχεδιασμό και τη λειτουργία του ΣΔΕΣ αναγνωρίζονται και ελέγχεται η διανομή τους**

Elements of business continuity management (Source – ISO 22313)


BC PROCESS LIFECYCLE
1
Business Impact Analysis (BIA)
• Define processes
• Assess impacts
• Map dependencies
• Map customers
2
Risk Assessment
• Threats and vulnerabilities
• Likelihoods and impacts
3
Solutions and Planning
• Continuity solution
• RTOs / RPOs
• Continuity steps
4
Exercising and Maintenance

8. Λειτουργία

8.1 Επιχειρησιακός σχεδιασμός και έλεγχος

Ο οργανισμός θα πρέπει να σχεδιάζει, εφαρμόζει και ελέγχει τις απαιτούμενες διαδικασίες για την ικανοποίηση των απαιτήσεων και την εφαρμογή των ενεργειών που αναφέρονται στην παράγραφο 6.1, μέσω:

α) της δημιουργίας κριτηρίων για τις διαδικασίες

β) εφαρμογής ελέγχου των διαδικασιών σύμφωνα με τα κριτήρια

γ) διατήρησης τεκμηριωμένων πληροφοριών για τη διασφάλιση εφαρμογής των διαδικασιών σύμφωνα με το σχεδιασμό

Έλεγχος των εξωτερικά παρεχόμενων υπηρεσιών και της εφοδιαστικής αλυσίδας (ΝΕΟ ΠΡΟΤΥΠΟ)

(documented process)

8.2.2 Ανάλυση Επιχειρησιακών Επιπτώσεων

(Business Impact Analysis - BIA)

Η BIA αναγνωρίζει το βαθμό κρισιμότητας της κάθε επιχειρησιακής λειτουργίας, μέσω της αξιολόγησης της επίδρασης της διακοπής αυτής της λειτουργίας στην Επιχειρησιακή Συνέχεια. Η πληροφορία αυτή απαιτείται για την αναγνώριση της κατάλληλης στρατηγικής συνέχειας για την κάθε κρίσιμη λειτουργία. Η έμφαση που δίνεται σε μια BIA είναι η αναγνώριση της σχετικής σπουδαιότητας και κρισιμότητας της κάθε λειτουργίας, παρά στην αναγνώριση συμβάντων που μπορούν να επηρεάσουν τη συγκεκριμένη λειτουργία.

Το αποτέλεσμα μιας BIA είναι η αναγνώριση των κρίσιμων δραστηριοτήτων οι οποίες πρέπει να διατηρηθούν προκειμένου ο Οργανισμός να συνεχίσει τη λειτουργία του και τα χρονικά πλαίσια ανάκαμψής τους.

Η BIA πρέπει να περιλαμβάνει τα ακόλουθα:

α) αναγνώριση δραστηριοτήτων που υποστηρίζουν την παροχή προϊόντων και υπηρεσιών

β) αξιολόγηση της επίδρασης της μη εκτέλεσης των λειτουργιών αυτών

γ) ορισμός χρονικών πλαισίων ανάκτησης αυτών των δραστηριοτήτων σε προκαθορισμένα ελάχιστα αποδεκτά επίπεδα, λαμβάνοντας υπόψη το χρονικό διάστημα εντός του οποίου οι επιπτώσεις από τη συνεχιζόμενη διακοπή των δραστηριοτήτων θα είναι μη αποδεκτές

δ) την αναγνώριση των αλληλεξαρτήσεων και των υποστηρικτικών πόρων αυτών των δραστηριοτήτων, περιλαμβανομένων προμηθευτών, εξωτερικών συνεργατών και άλλων ενδιαφερομένων μερών

Χρονικά πλαίσια ανάκτησης δραστηριοτήτων

- **MAO / MTPD (Maximum Acceptable Outage / Maximum Tolerable Period of Disruption**

Το μέγιστο χρονικό διάστημα που είναι αποδεκτό μέχρι να επανέλθει η λειτουργία στο 100%, μετά από ένα περιστατικό διαταραχή

- **MBCO (Minimum Business Continuity Objective)**

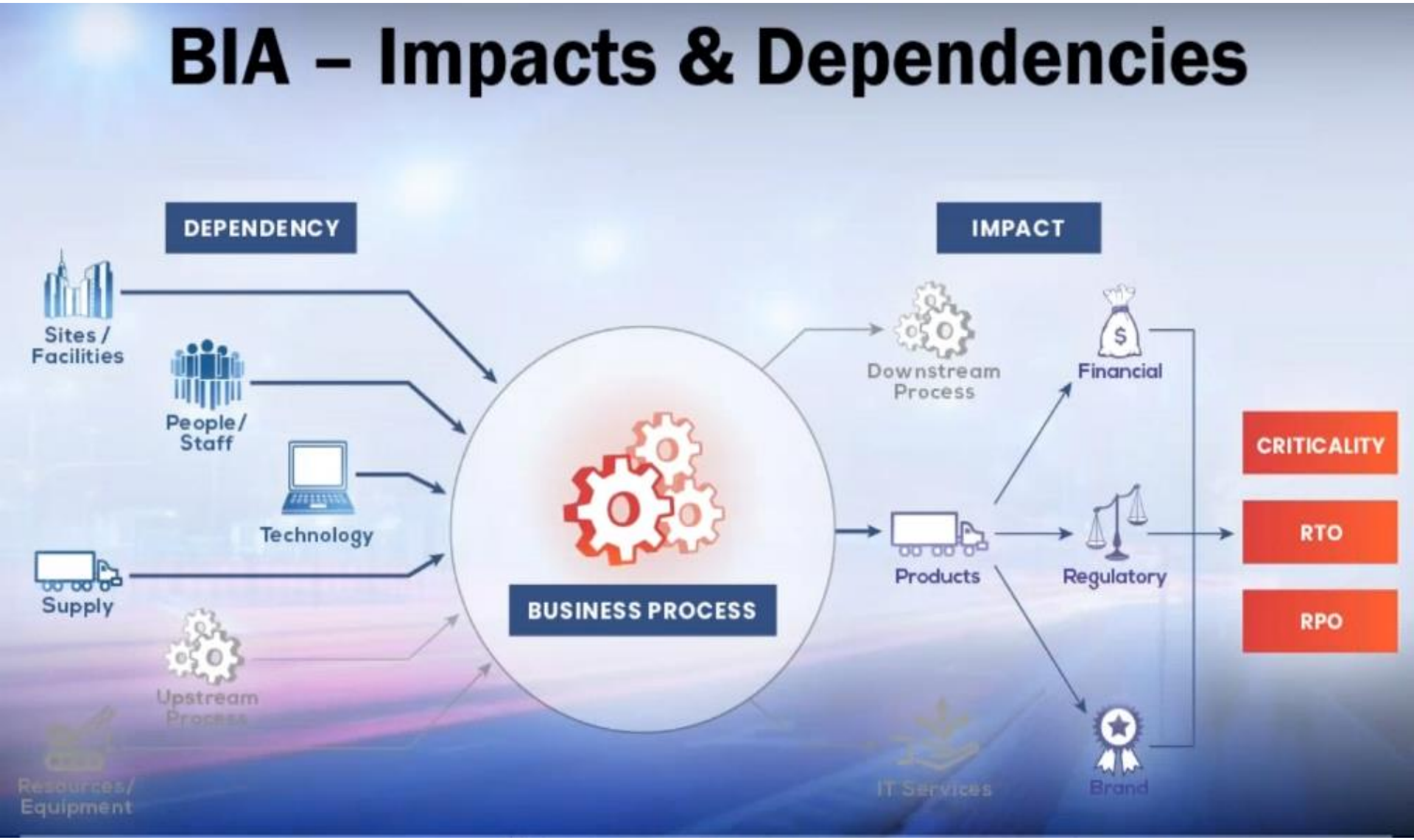
Το ελάχιστο επίπεδο υπηρεσιών ή/και προϊόντων (παραγωγής) που είναι αποδεκτό από τον Οργανισμό κατά τη διάρκεια ενός περιστατικού διαταραχής, προκειμένου να επιτύχει τους επιχειρησιακούς στόχους του

- **RTO (Recovery Time Objective)**

Χρονικό διάστημα μετά την εμφάνιση ενός περιστατικού διαταραχής εντός του οποίου θα ανακτηθεί η λειτουργία σε προκαθορισμένο ποσοστό σύμφωνα με το MBCO

- **RPO (Recovery Point Objective)**

Σημείο στο οποίο τα δεδομένα μιας δραστηριότητας πρέπει να αποθηκευθούν για να χρησιμοποιηθούν κατά την ανάκτηση (το τελευταίο back-up πριν τη διακοπή)


BIA – Impacts & Dependencies
DEPENDENCY
IMPACT
Sites / Facilities
People / Staff
Technology
Supply
Upstream Process
Resources/ Equipment
BUSINESS PROCESS
Downstream Process
Products
IT Services
Financial
Regulatory
Brand
CRITICALITY
RTO
RPO

ΑΛΛΗΛΕΞΑΡΤΗΣΕΙΣ

ΚΡΙΣΙΜΗ ΔΡΑΣΤΗΡΙΟΤΗΤΑ	ΕΞΑΡΤΑΤΑΙ ΑΠΟ	ΕΞΑΡΤΟΜΕΝΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ	ΠΑΡΑΤΗΡΗΣΕΙΣ

ΒΑΘΜΟΣ ΚΡΙΣΙΜΟΤΗΤΑΣ ΔΡΑΣΤΗΡΙΟΤΗΤΩΝ

ΔΡΑΣΤΗΡΙΟΤΗΤΑ	Επίπτωση	Προτεραιότητα Ανάκαμψης	Εναλλακτική	Βαθμός Κρισιμότητας

Βαθμός Κρισιμότητας = Επίπτωση * Προτεραιότητα * Εναλλακτική

Θ. Βλάχος, ΜΜΜ ΕΜΠ, MBA

Επίπτωση

1	Μη ζωτικής σημασίας
2	Χαμηλή
3	Μεσαία
4	Υψηλή
5	Ζωτικής σημασίας

Εναλλακτική

1	100%
2	75%
3	50%
4	25%
5	Καμία

Προτεραιότητα Ανάκαμψης

1	Μεγαλύτερη των 30 Ημερών
2	Εντός 20 Ημερών
3	Εντός 7 Ημερών
4	Εντός 3 Ημερών
5	Εντός 1 Ημέρας

ΣΥΝΟΠΤΙΚΟΣ ΠΙΝΑΚΑΣ ΕΠΙΠΤΩΣΕΩΝ ΑΠΟ ΤΗ ΔΙΑΚΟΠΗ ΤΩΝ ΚΡΙΣΙΜΩΝ ΔΡΑΣΤΗΡΙΟΤΗΤΩΝ

ΚΡΙΣΙΜΗ ΔΡΑΣΤΗΡΙΟΤΗΤΑ	ΕΠΙΠΤΩΣΗ

Θ. Βλάχος, ΜΜΜ ΕΜΠ, MBA

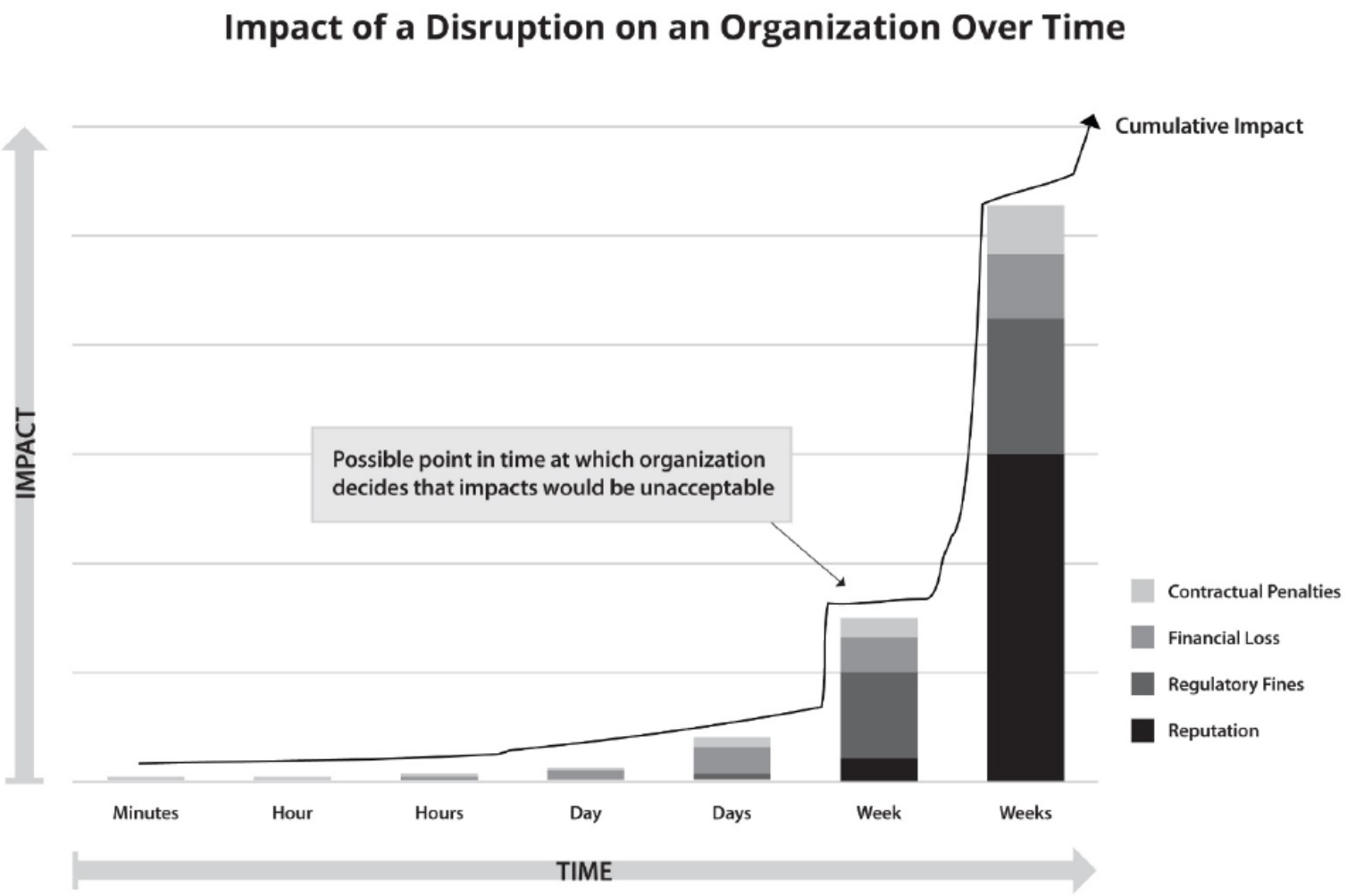
ΚΡΙΣΙΜΗ ΔΡΑΣΤΗΡΙΟΤΗΤΑ

	Διάρκεια διακοπής	Βαθμός Επίπτωσης				
		1	2	3	4	5
Χρηματοοικονομική						
	1 ημέρα		X			
	3 ημέρες			X		
	7 ημέρες				X	
	15 ημέρες					X
Συμβατικές Υποχρεώσεις						
	1 ημέρα	X				
	3 ημέρες		X			
	7 ημέρες			X		
	15 ημέρες					X
Φήμη						
	1 ημέρα	X				
	3 ημέρες	X				
	7 ημέρες	X				
	15 ημέρες					X
ΣΥΝΟΛΟ ΒΑΘΜΟΛΟΓΙΑΣ						
	1 ημέρα		X			
	3 ημέρες			X		
	7 ημέρες				X	
	15 ημέρες					X

Product and service level impact categories and examples

Impact Categories	Examples of impacts
Financial	Financial losses due to fines, penalties, lost profits, or diminished market share
Reputational	Negative opinion or brand damage
Legal and regulatory	Litigation liability and withdrawal of license to trade
Contractual	Breach of contracts or obligations between organizations
Business objectives	Failure to deliver on objectives or take advantage of opportunities

(Source: ISO 22317)



(Source: ISO 22317)

ΧΡΟΝΙΚΑ ΟΡΙΑ ΑΝΑΚΑΜΨΗΣ ΚΡΙΣΙΜΩΝ ΔΡΑΣΤΗΡΙΟΤΗΤΩΝ ΚΑΙ ΕΛΑΧΙΣΤΟ ΕΠΙΠΕΔΟ ΛΕΙΤΟΥΡΓΙΑΣ

α/α	ΔΡΑΣΤΗΡΙΟΤΗΤΑ	RTO	MAO	MBCO
1		2 ώρες	2 ώρες	100%
2		5 ημέρες	7 ημέρες	50%
3		2 ώρες	2 ώρες	100%
4		5 ημέρες	5 ημέρες	100%
6		5 ημέρες	7 ημέρες	50%
7		5 ημέρες	7 ημέρες	50%
8		5 ημέρες	7 ημέρες	50%

Θ. Βλάχος, ΜΜΜ ΕΜΠ, MBA

8.2.3 Αξιολόγηση Κινδύνων

(Risk assessment)

Ο οργανισμός θα πρέπει να δημιουργήσει, εφαρμόσει και διατηρήσει μια επίσημη τεκμηριωμένη διαδικασία αξιολόγησης κινδύνων, η οποία συστηματικά θα αναγνωρίζει, αναλύει και αξιολογεί τον κίνδυνο περιστατικών διαταραχής στον οργανισμό.

Ο οργανισμός θα πρέπει να:

α) αναγνωρίζει κινδύνους που μπορεί να προκαλέσουν διακοπή της λειτουργίας των κρίσιμων δραστηριοτήτων του
β) αναλύει συστηματικά τους κινδύνους
γ) εκτιμά ποιοι κίνδυνοι χρήζουν αντιμετώπισης
δ) αναγνωρίζει τρόπους αντιμετώπισης των κινδύνων συμβατούς με τους επιχειρησιακούς στόχους και σε συμφωνία με τη διάθεση ανάληψης κινδύνου (risk appetite)

ΔΡΑΣΤΗΡΙΟΤΗΤΑ	ΚΙΝΔΥΝΟΙ

ΕΚΤΙΜΗΣΗ ΚΙΝΔΥΝΩΝ ΑΝΑ ΚΡΙΣΙΜΗ ΔΡΑΣΤΗΡΙΟΤΗΤΑ				
(ΚΡΙΣΙΜΗ ΔΡΑΣΤΗΡΙΟΤΗΤΑ)				
α/α	Κίνδυνος	Πιθανότητα εμφάνισης	Επίπτωση	Βαθμός Κινδύνου
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				

Βαθμός Κινδύνου = Πιθανότητα * Επίπτωση

Αναγνώριση Κινδύνων

Παραδείγματα άμεσων περιστατικών διαταραχής

- Τρομοκρατική ενέργεια/ Απειλή βόμβας / Εγκληματική ενέργεια
- Πυρκαγιά
- Διακοπή ηλεκτροδότησης
- Πλημμύρα
- Πτώση IT Συστημάτων
- Διαφόρων μορφών Sabotage
- Μη συμμορφώσεις με τη νομοθεσία
- Αδυναμία προμηθευτή

Παραδείγματα έμμεσων περιστατικών διαταραχής

- Πανδημία / Σοβαρά περιστατικά υγείας
- Χρηματοοικονομική κρίση / Πολιτική αστάθεια
- Διακοπές λειτουργίας των Μέσων Μεταφοράς
- Αντίξοες καιρικές συνθήκες

Αναγνώριση κινδύνων

ΠΩΣ ???

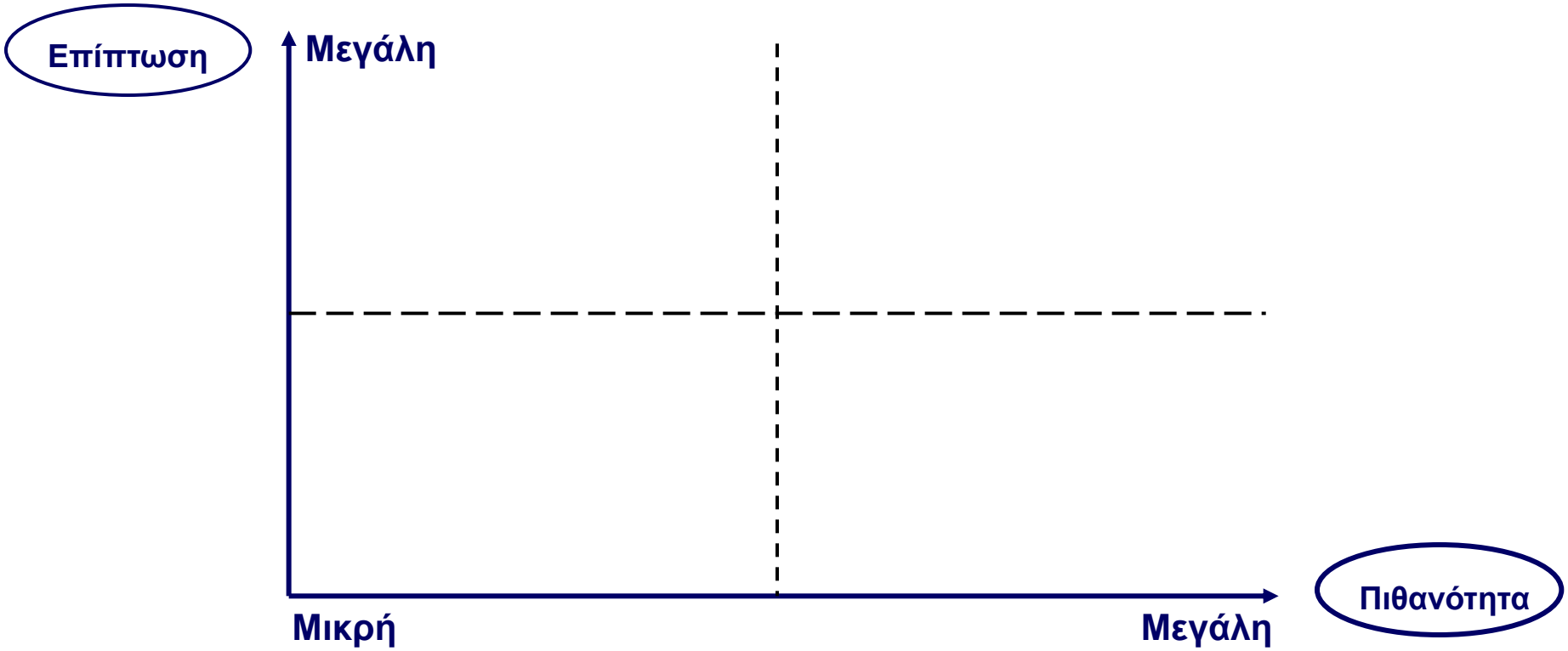
- Ερωτηματολόγια και checklists
- Workshops – brainstorming
- Επιθεωρήσεις εγκαταστάσεων / δραστηριοτήτων
- Αξιολογήσεις συμμόρφωσης
- Διαγράμματα ροής και ανάλυση αλληλεπιδράσεων
- HAZOP studies

Ανάλυση – Αξιολόγηση κινδύνων

ΠΟΙΟΤΙΚΟΣ ΠΡΟΣΔΙΟΡΙΣΜΟΣ

Risk Map

Πιθανότητα – Επίδραση



ΗΜΙΠΟΣΟΤΙΚΟΣ ΠΡΟΣΔΙΟΡΙΣΜΟΣ

ΕΠΙΔΡΑΣΗ / ΠΙΘΑΝΟΤΗΤΑ	Πολύ Μικρή 1	Μικρή 2	Μεγάλη 3	Πολύ Μεγάλη 4	Καταστροφική 5
Σχεδόν Απίθανη 1	1	2	3	4	5
Ελάχιστα Πιθανή 2	2	4	6	8	10
Πιθανή 3	3	6	9	12	15
Πολύ Πιθανή 4	4	8	12	16	20
Σχεδόν Βέβαιη 5	5	10	15	20	25

EMERGENCY MANAGEMENT MODEL EXAMPLE - NATURAL

(EXAMPLE ONLY – NOT CONDUCTED/PRIORITIZED

WEIGHT FACTOR	2 Points	5 Points	10 Points	7 Points	TOTAL
HAZARD	**HISTORY**	**VULNERABLILITY**	**MAXIMUM THREAT (Severity)**	**PROBABILITY**	
Intensity	**Events in last 100 years in which citizens affected**	**Percent of property or population affected**	**Percent of property or population affected in worse-case event**	**Likelihood of an occurrence within specified time period**	
High	4 or more events (7-10 Points)	More than 10% (7-10 Points)	More than 25% (7-10 Points)	1 incident in the next 10 years (7-10 Points)	
Moderate	2-3 events (4-6 Points)	From 1 to 10% (4-6 Points)	From 5% to 25% (4-6 Points)	1 incident in the next 50 years (4-6 Points)	
Low	1 or no event (1-3 Points)	Less than 1% (1-3 Points)	Less than 5% (1-3 Points)	1 incident in the next 100 years (1-3 Points)	
Weather Emergencies including Fire	**10 = 20**	**10 = 50**	**10 = 100**	**10 = 70**	**240**
Disease Outbreak	**5 = 10**	**10 = 50**	**9 = 90**	**10 = 100**	**250**
Earthquake	**5 = 10**	**9 = 45**	**10 = 100**	**9 = 63**	**223**
Flood	**10 = 20**	**10 = 50**	**8 = 80**	**10 = 70**	**220**
Hazardous Materials	**10 = 20**	**10 = 50**	**7 = 70**	**10 = 70**	**210**
Power Failure	**10 = 20**	**8 = 40**	**8 = 80**	**10 = 70**	**210**
Terror Attack - WMD	**2 = 4**	**10 = 50**	**10 = 100**	**8 = 56**	**210**
Pipe Line Disruption	**5 = 10**	**10 = 50**	**10 = 100**	**5 = 35**	**195**
Volcano/Fallout	**3 = 6**	**10 = 50**	**8 = 80**	**8 = 56**	**192**
Dam Failure	**2 = 4**	**10 = 50**	**10 = 100**	**4 = 28**	**182**
Landslide/Debris Flow	**10 = 20**	**1 = 5**	**2 = 20**	**10 = 70**	**115**