Παπαηλίας Άγγελος

Διπλωματική Εργασία υποβληθείσα στο Τμήμα MBA Total Quality Management του Πανεπιστημίου Πειραιώς

ΠΑΡΑΡΤΗΜΑ Δ : **ΥΠΕΥΘΥΝΗ ΔΗΛΩΣΗ** **ΕΚΠΟΝΗΣΗΣ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ**

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΟΡΓΑΝΩΣΗΣ ΚΑΙ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

Μεταπτυχιακό Πρόγραμμα Σπουδών

στη «Διοίκηση Επιχειρήσεων – Ολική Ποιότητα» με Διεθνή προσανατολισμό

ΒΕΒΑΙΩΣΗ ΕΚΠΟΝΗΣΗΣ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

(περιλαμβάνεται ως ξεχωριστή δεύτερη σελίδα στο σώμα της διπλωματικής εργασίας)

Δηλώνω υπεύθυνα ότι η διπλωματική εργασία για τη λήψη του μεταπτυχιακού τίτλου σπουδών, του Πανεπιστημίου Πειραιώς, στη Διοίκηση Επιχειρήσεων - Ολική Ποιότητα με διεθνή προσανατολισμό με τίτλο:

Ο ρόλος του risk management στα συστήματα διαχείρισης business case στον αγώνα εταιρειών παιχνιδομηχανών Α.Ε.

έχει συγγραφεί από εμένα αποκλειστικά και στο σύνολό της. Δεν έχει υποβληθεί ούτε έχει εγκριθεί στο πλαίσιο κάποιου άλλου μεταπτυχιακού προγράμματος ή προπτυχιακού τίτλου σπουδών, στην Ελλάδα ή στο εξωτερικό, ούτε είναι εργασία ή τμήμα εργασίας ακαδημαϊκού ή επαγγελματικού χαρακτήρα.

Δηλώνω επίσης υπεύθυνα ότι οι πηγές στις οποίες ανέτρεξα για την εκπόνηση της συγκεκριμένης εργασίας, αναφέρονται στο σύνολό τους, κάνοντας πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο.

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

Υπογραφή Μεταπτυχιακού Φοιτητή/τριας .....

Ονοματεπώνυμο Άγγελος Παπαηλίας

Ημερομηνία 11/11/2019

•Πρόγραμμα μεταπτυχιακών σπουδών Πανεπιστημίου Πειραιώς
•MBA-Total Quality Management
•Τίτλος Διπλωματικής Εργασίας: Ο ρόλος του Enterprise Risk Management στα Συστήματα Διαχείρισης, Business Case στον όμιλο εταιρειών ΠΑΠΑΔΟΠΟΥΛΟΣ Α.Ε.
•Ονοματεπώνυμο Συγγραφέα: Άγγελος Παπαηλίας
•Επιβλέπων καθηγητής : Μποχώρης Γεώργιος

Ευχαριστίες

Με την ολοκλήρωση της παρούσας εργασίας, αισθάνομαι την ανάγκη να ευχαριστήσω τον επιβλέποντα καθηγητή μου κύριο Μποχώρη Γεώργιο, ο οποίος μου έδωσε τη δυνατότητα να ασχοληθώ με αυτό το ενδιαφέρον θέμα καθώς και τη σημαντική του βοήθεια σε όλη τη διάρκεια της εργασίας μου.

Σημαντικοί Όροι: risk management , συστήματα διαχείρισης , απαιτήσεις προτύπων , International Organization for Standardization

ΠΕΡΙΛΗΨΗ

Η λέξη κίνδυνος προέρχεται από τη λατινική ρίζα "risicare" η οποία σημαίνει "τολμώ". Οι δράσεις που τολμούμε να αναλάβουμε, οι οποίες εξαρτώνται από την ελευθερία επιλογών που διαθέτουμε ,ουσιαστικά χαρακτηρίζουν την "ιστορία" της διαχείρισης κινδύνων αλλά και την κοινωνική εξέλιξη. Η διαχείριση κινδύνων ενσωματώνεται σε ένα πολύ μεγάλο φάσμα λήψης αποφάσεων. Σε κάθε περίπτωση κίνδυνος σημαίνει έκθεση στην αβεβαιότητα και αφορά εξίσου τις ανθρώπινες δραστηριότητες όσο και τις επιχειρήσεις.

Η νέα απαίτηση των συστημάτων (ISO) είναι η διαχείριση κινδύνου. Κάθε πρότυπο έχει τις δικές του απαιτήσεις .Σε αυτήν τη διπλωματική εργασία περιγράφεται η διαχείριση των εταιρικών ρίσκων μέσα από τον όμιλο ΠΑΠΑΔΟΠΟΥΛΟΣ Α.Ε , ο τρόπος που γίνεται η αξιολόγηση , η αναγνώριση , η ανάλυση και η αποτίμηση κινδύνων. Επίσης παρουσιάζεται ένα Flow Chart μέσα από το Aris BPMN Tool που δείχνει το πλάνο διεξαγωγής ενός Risk Assessment . Επιπλέον αναφέρονται τα εξής συστήματα (Pas 99) , (ISO 31000) , (ISO 90001) , (ISO 14001) ,(ISO 50000), (ISO 22301) , (ISO 19600) , (ISO 17025) , (ISO 45001 – OHSAS 18001) .Στη συνέχεια της εργασίας παρουσιάζεται ένα Case Study με βάση το πρότυπο επιχειρησιακής συνέχειας ISO 22301 όπου περιγράφεται η διαδικασία πραγματοποίησης ενός risk assessment , ύστερα από συνεργασία της εταιρείας ΠΑΠΑΔΟΠΟΥΛΟΣ Α.Ε και μιας εταιρείας ως multinatioal customer. Ο όμιλος για να ανταπεξέλθει στις απαιτήσεις του customer έπρεπε να ευθυγραμμίσει τις εσωτερικές του διαδικασίες και να έχει κοινή μεθοδολογία risk assessment.Στο case study περιγράφονται αναλυτικά όλες οι ενέργειες για να πραγματοποιηθεί αυτή η διαδικασία μέσα από τη διεξαγωγή workshops.Αναφέρονται αναλυτικά τα Requirements και Responsibilities ,οι αποκλίσεις μέσα από τη βοήθεια του εσωτερικού ελέγχου , η μεθοδολογία risk analysis όπως και η διαδικασία ενεργοποίησης και ρόλοι μέσα από απεικονίσεις. Τέλος στα πλαίσια του integrated management system παρουσιάζεται το κοινό risk matrix και όλες οι αλλαγές που χρειάστηκαν να γίνουν από τις εμπλεκόμενες επιχειρησιακές μονάδες για την ολοκλήρωση του έργου.

Περιεχόμενα

1.0 Διαχείριση εταιρικών ρίσκων ΠΑΠΑΔΟΠΟΥΛΟΣ Α.Ε.

1) Σκοπός

Η Αξιολόγηση Κινδύνων (Risk Assessment) είναι μια συνολική διεργασία για την αναγνώριση, την ανάλυση, την αποτίμηση και την αντιμετώπιση των επιχειρηματικών κινδύνων (ποιοτικά ή ποσοτικά) , οι οποίοι δύναται να απορρέουν από διάφορες δραστηριότητες, διαδικασίες ή καταστάσεις, εντός και εκτός εταιρείας. Πραγματοποιείται για να εξετάσει τις δυσμενείς επιπτώσεις που μπορεί να έχουν οι κίνδυνοι αυτοί στην επίτευξη των αντικειμενικών σκοπών της Εταιρείας, με στόχο τη λήψη από τα αρμόδια όργανα της Εταιρείας κατάλληλων μέτρων για τη διαχείριση και αντιμετώπισή των εν λόγω κινδύνων και την παρακολούθηση υλοποίησης των σχετικών μέτρων.
Σκοπός της παρούσας διαδικασίας είναι η δομημένη διαχείριση των επιμέρους αξιολογήσεων κινδύνων (risk assessments) που διενεργούνται στην Εταιρεία από τις αρμόδιες επιχειρησιακές μονάδες, δηλαδή η διαχείριση με βάση καθολικά κριτήρια εκτίμησης και αξιολόγησης, χρησιμοποιώντας μια κοινή μεθοδολογία, έτσι ώστε να υπάρχει ένας ενιαίος τρόπος διαχείρισης των εταιρικών κινδύνων, σύμφωνα με τις απαιτήσεις του προτύπου *ISO 31000:2009, Risk management – Principles and guidelines.*

2) Πεδίο Εφαρμογής

Η παρούσα διαδικασία ισχύει για όλον τον Όμιλο ΠΑΠΑΔΟΠΟΥΛΟΣ Α.Ε.
Αν κριθεί σκόπιμο από κάποια Εταιρεία του Ομίλου, μπορεί να την προσαρμόσει στα δικά της δεδομένα, με την προϋπόθεση ότι η τελική έγκριση θα δοθεί από τον Executive Director Κανονιστικής Συμμόρφωσης, Διαχείρισης Κινδύνων & Ασφάλισης Ομίλου ΠΑΠΑΔΟΠΟΥΛΟΣ Α.Ε..

3) Είδος Πρόσβασης

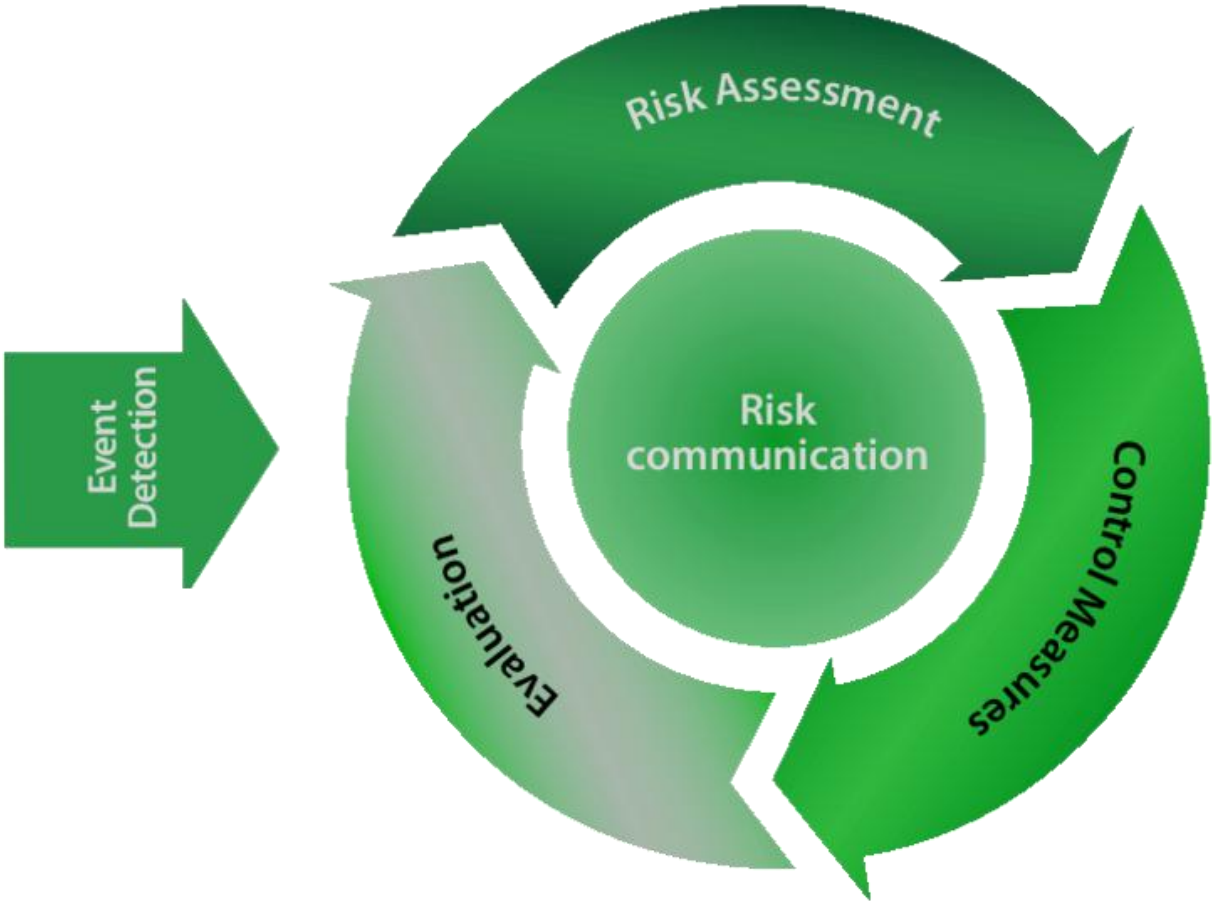
Η παρούσα διαδικασία είναι αναρτημένη στο Process του Ομίλου και ελεύθερα προσβάσιμη από όλο το απασχολούμενο προσωπικό της Εταιρείας είτε συνδέεται με σύμβαση εξαρτημένης εργασίας ή δανεισμού ή με άλλου είδους σχέση. Η αποστολή του εγγράφου εκτός Εταιρείας δεν είναι επιτρεπτή.

1.1 Αναγνώριση Κινδύνων Ομίλου ΠΑΠΑΔΟΠΟΥΛΟΣ Α.Ε.

Το πρώτο βήμα για τη διενέργεια Αξιολόγησης Κινδύνων είναι η αναγνώριση και αποτύπωση από την επιχειρησιακή μονάδα των κινδύνων, λαμβάνοντας υπόψη τις επιπτώσεις που ενδέχεται να έχουν στην επίτευξη των λειτουργικών στόχων αυτής και στην επίτευξη των επιχειρηματικών στόχων της Εταιρείας.
Για το λόγο αυτό οι κίνδυνοι κατατάσσονται ανάλογα με το είδος τους στις εξής κατηγορίες:

- **Στρατηγικοί**: μακροπρόθεσμες επιπτώσεις στο όνομα και τη φήμη της

Εταιρείας ή στην επίτευξη στρατηγικών εταιρικών στόχων.
- **Οικονομικοί**: οικονομικές επιπτώσεις επί των εσόδων (EBITDA/Cash), τα περιουσιακά στοιχεία και το μερίδιο αγοράς της Εταιρείας.
- **Λειτουργικοί**: κίνδυνοι που ενδέχεται να έχουν επιπτώσεις στους ανθρώπους (εργαζόμενοι, πελάτες, κλπ.), στο περιβάλλον, στην προμηθευτική αλυσίδα ή και στην διαθεσιμότητα των υπηρεσιών (Network, IT Systems).
- **Συμμόρφωσης**: επιπτώσεις που συνδέονται με τη μη συμμόρφωση της Εταιρείας με νόμους, κανονιστικές διατάξεις και ισχύοντα πρότυπα.



Πηγή 1* https://www.researchgate.net/figure/The-risk-management-cycle_fig1_294894575

1.2 Αξιολόγηση Κινδύνων Ομίλου ΠΑΠΑΔΟΠΟΥΛΟΣ Α.Ε.

Risk Assessment διενεργεί οποιαδήποτε επιχειρησιακή μονάδα της Εταιρείας πέραν της Υποδιεύθυνσης Enterprise Risk Management Ομίλου ΠΑΠΑΔΟΠΟΥΛΟΣ Α.Ε. είτε ad hoc είτε σε περιοδική βάση (κάθε μήνα, τρίμηνο, εξάμηνο, έτος, κτλ.), και ειδικότερα στις παρακάτω περιπτώσεις:

- Όταν αναγνωρίζει την ύπαρξη κινδύνων σε κάποια δραστηριότητα ή διαδικασία.
- Κατά τη διαδικασία ανάπτυξης και λανσαρίσματος νέων προϊόντων ή/και υπηρεσιών ή την βελτιστοποίηση υπαρχόντων.
- Κατά τη διαδικασία στρατηγικού σχεδιασμού και προγραμματισμού.
- Όταν αναγνωρίζει την ύπαρξη κινδύνων προερχόμενων από το εξωτερικό περιβάλλον.
- Αν προβλέπεται ρητά σε διάταξη νόμου.
- Αν υπάρχει σχετική απαίτηση από υφιστάμενη πιστοποίηση για την οποία η αρμόδια επιχειρησιακή μονάδα είναι υπεύθυνη (αρχές / κατευθυντήριες οδηγίες προτύπου).
- Αν ζητηθεί από τη Διοίκηση.

Όταν κριθεί αναγκαίο από κάποια επιχειρησιακή μονάδα να διενεργήσει Risk Assessment, η αρμόδια επιχειρησιακή μονάδα γνωστοποιεί την ανάγκη αυτή στην Υποδιεύθυνση Enterprise Risk Management Ομίλου ΠΑΠΑΔΟΠΟΥΛΟΣ Α.Ε.

Η Υποδιεύθυνση Enterprise Risk Management Ομίλου ΠΑΠΑΔΟΠΟΥΛΟΣ Α.Ε. έχει την αρμοδιότητα να επικοινωνήσει στις επιμέρους επιχειρησιακές μονάδες που διενεργούν αξιολόγηση κινδύνων την κοινή μεθοδολογία αξιολόγησης κινδύνων, όπως αυτή αποτυπώνεται στο ΠΑΠΑΔΟΠΟΥΛΟΣ Α.Ε Group Enterprise Risk Management System Manual".

Εφόσον η επιχειρησιακή μονάδα επιθυμεί τη χρήση διαφορετικής μεθοδολογίας αξιολόγησης κινδύνων, θα πρέπει να εκθέσει τους λόγους αυτούς στην Υποδιεύθυνση Enterprise Risk Management Ομίλου ΠΑΠΑΔΟΠΟΥΛΟΣ Α.Ε και να υπάρξει συμφωνία ως προς την ακολουθούμενη μεθοδολογία. Η Υποδιεύθυνση Enterprise Risk Management Ομίλου ΠΑΠΑΔΟΠΟΥΛΟΣ Α.Ε θα συνεργαστεί με την αρμόδια επιχειρησιακή μονάδα ή θα έχει συμβουλευτικό ρόλο στις επόμενες ενέργειες.

Σημείωση: Για τις επιχειρησιακές μονάδες που αναγνωρίζουν κινδύνους στο πλαίσιο ελέγχων που πραγματοποιούν ad-hoc ή περιοδικά, η παρούσα διαδικασία εφαρμόζεται σε συχνότητα που συμφωνείται με την Υποδιεύθυνση Enterprise Risk Management Ομίλου ΠΑΠΑΔΟΠΟΥΛΟΣ Α.Ε λαμβάνοντας υπόψη τους κινδύνους αυτούς.

1.3 Ανάλυση Κινδύνων Ομίλου ΠΑΠΑΔΟΠΟΥΛΟΣ Α.Ε.

Το δεύτερο βήμα μετά την αναγνώριση και κατάταξη του κινδύνου από την επιχειρησιακή μονάδα είναι ο υπολογισμός της ενδεχόμενης οικονομικής επίπτωσής του (financial impact) καθώς επίσης και της πιθανότητας εμφάνισής του (likelihood).

Α. Δυνητικές οικονομικές επιπτώσεις

Οι εταιρικοί κίνδυνοι θα πρέπει να υπολογίζονται ως προς την οικονομική τους επίπτωση.

Σε περίπτωση που δεν μπορεί να υπολογιστεί η οικονομική επίπτωση του κινδύνου, δύναται να κατατάσσεται σε μία από τις ακόλουθες τέσσερις κατηγορίες:

- Very Critical (financial impact >€20mn)
- Critical (financial impact >€12mn, <€20mn)
- Middle (financial impact >€5mn, <€12mn)
- Small (financial impact >€1mn, <€5mn)

Β. Πιθανότητα εμφάνισης κινδύνου

Ως πιθανότητα εμφάνισης ενός κινδύνου ορίζουμε την αναμενόμενη πιθανότητα να συμβεί ένα γεγονός μέσα σε ένα συγκεκριμένο χρονικό διάστημα. Δεδομένου ότι η πιθανότητα ως επί το πλείστον είναι δύσκολο να προσδιοριστεί, μπορούν να χρησιμοποιηθούν οι ακόλουθες τέσσερις κατηγορίες ταξινόμησης:

- **Very Low** (Unlikely to happen, Probability <5%, Likelihood of Occurrence: within 24 months)
- **Low** (Possible to happen, Probability 5%-25%, Likelihood of Occurrence: within12 months)
- **Medium** (Likely to happen, Probability 25%-50%, Likelihood of Occurrence: within 9 months)
- **High** (More than likely to happen, Probability 50%-100%, Likelihood of Occurrence: within 6 months).

Πληροφόρηση για τα κριτήρια αξιολόγησης που μπορούν να χρησιμοποιηθούν και το εργαλείο αξιολόγησης " ΠΑΠΑΔΟΠΟΥΛΟΣ Α.Ε GROUP Risk Evaluation Matrix” περιέχονται στο " ΠΑΠΑΔΟΠΟΥΛΟΣ Α.Ε Group Enterprise Risk Management System Manual".

1.4 Αποτίμηση Κινδύνων Ομίλου ΠΑΠΑΔΟΠΟΥΛΟΣ Α.Ε

Ο συνδυασμός της οικονομικής επίπτωσης και της πιθανότητας εμφάνισης ενός πιθανού κινδύνου αντιπροσωπεύει την τοποθέτησή του από την επιχειρησιακή μονάδα, ως προς τη σημαντικότητα (severity) και την προτεραιότητα (priority) αυτού σε ένα γράφημα (Heat Map) και συγκεκριμένα σε πίνακα 4x4, που έχει

την οικονομική επίπτωση επί του άξονα Υ και την πιθανότητα εμφάνισης του κινδύνου στον άξονα Χ.
Η κατάταξη του κινδύνου ως προς την προτεραιότητα και την σημαντικότητά του προσδιορίζεται και χρωματικά στον πίνακα, χρησιμοποιώντας 3 χρώματα (κόκκινο-κίτρινο-πράσινο) και δύναται να είναι:
- Σημαντικός (Significant, Red Color): Υψηλή προτεραιότητα, απαιτούνται άμεσες ενέργειες,
- Σπουδαίος (Important, Yellow Color): Μεσαία προτεραιότητα, απαιτείται βελτίωση με τη χρήση κατάλληλων αντισταθμιστικών μέτρων,
- Χαμηλός (Low, Green Color): Χαμηλή προτεραιότητα, ευαισθητοποίηση και συνεχής παρακολούθηση.

1.5 Καταγραφή πλάνου αποτίμησης ομίλου ΠΑΠΑΔΟΠΟΥΛΟΣ Α.Ε

Εφόσον ο κίνδυνος αναγνωριστεί και αποτιμηθεί θα πρέπει να ορισθεί από την αρμόδια επιχειρησιακή μονάδα ο υπεύθυνος ανάληψης κινδύνου (risk owner), ο οποίος είναι σε επίπεδο Διευθυντή και πρέπει να έχει βαθιά κατανόηση και γνώση της επιχειρησιακής μονάδας και κατά συνέπεια του κινδύνου και όλων των σχετικών πληροφοριών που σχετίζονται με την τρέχουσα κατάσταση του κινδύνου.
Στη συνέχεια, σχεδιάζονται από την αρμόδια επιχειρησιακή μονάδα σε συνεργασία με την Υποδιεύθυνση ERM Ομίλου ΠΑΠΑΔΟΠΟΥΛΟΣ Α.Ε, αν απαιτείται, τα κατάλληλα μέτρα αντιμετώπισης / διαχείρισης των κινδύνων, λαμβάνοντας υπόψη και την "Risk Appetite Policy" και εκπονείται πλάνο υλοποίησης αυτών που περιλαμβάνει τον υπεύθυνο υλοποίησης (mitigation owner) και την προβλεπόμενη ημερομηνία υλοποίησης το οποίο αποτυπώνεται στο αρχείο «Καταγραφή και Αποτίμηση Κινδύνων Επιχειρησιακής Μονάδας».

1.6 Έγκριση πλάνου αντιμετώπισης κινδύνων ομίλου ΠΑΠΑΔΟΠΟΥΛΟΣ Α.Ε

Το πλάνο αντιμετώπισης κινδύνων ελέγχεται από τον υπεύθυνο ανάληψης κινδύνου (risk owner). Αν υπάρχουν σχόλια επιστρέφεται για διορθώσεις.
Αν είναι σύμφωνος το εγκρίνει, αποδεχόμενος έτσι τα προτεινόμενα μέτρα για την αντιμετώπιση των κινδύνων, τον υπεύθυνο υλοποίησης (mitigation owner) και την ημερομηνία προβλεπόμενης υλοποίησης, τα οποία οφείλει να παρακολουθεί καθώς έχει την συνολική εποπτεία του κινδύνου .

1.7 Ενημέρωση αρμόδιων Ομίλου ΠΑΠΑΔΟΠΟΥΛΟΣ Α.Ε

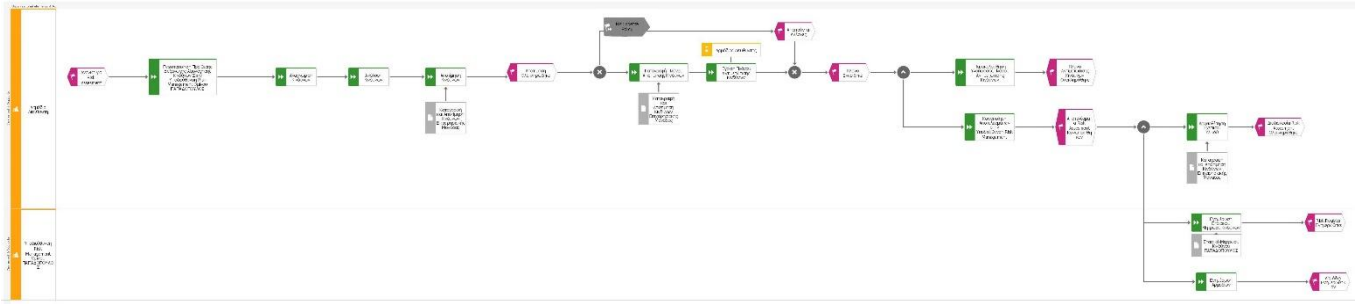
Η Υποδιεύθυνση Enterprise Risk Management Ομίλου ΠΑΠΑΔΟΠΟΥΛΟΣ Α.Ε. ενημερώνει σε τριμηνιαία βάση ή ad hoc όταν αυτό απαιτείται το GRC Committee για τις εξελίξεις των εταιρικών κινδύνων με σκοπό την λήψη περαιτέρω αντισταθμιστικών μέτρων και την περαιτέρω ενημέρωση της

Επιτροπής Ελέγχου και του Διοικητικού Συμβουλίου

1.8 Ενημέρωση εταιρικού Μητρώου Κινδύνων Ομίλου ΠΑΠΑΔΟΠΟΥΛΟΣ Α.Ε

Το Εταιρικό Μητρώο Κινδύνων Ομίλου ΠΑΠΑΔΟΠΟΥΛΟΣ Α.Ε (ΠΑΠΑΔΟΠΟΥΛΟΣ Α.Ε Group Corporate Risk Register) τηρείται, παρακολουθείται και επικαιροποιείται από την Υποδιεύθυνση Enterprise Risk Management. Η Υποδιεύθυνση Enterprise Risk Management του Ομίλου ενημερώνει το Εταιρικό Μητρώο Κινδύνων με τα αποτελέσματα της Αξιολόγησης Κινδύνων που έχει λάβει από τις λοιπές επιχειρησιακές μονάδες .

1.9 Διάγραμμα Ροής Risk Assessment



1.9.1Περιγραφή

Το διάγραμμα ροής γίνεται στο Aris Process Modeling Tool

1.Η αρμόδια Διεύθυνση εκφέρει την ανάγκη της για Risk Assessment.
2.Η πρώτη ενέργεια που κάνει είναι η γνωστοποίηση προώθησης διεξαγωγής αξιολόγησης.
3.Στη συνέχεια ακολουθεί η αναγνώριση κινδύνων.
4.Επόμενη ενέργεια ανάλυση κινδύνων
5.Αποτίμηση κινδύνων με ενσωμάτωση data object για καταγραφή και αποτίμηση κινδύνων επιχειρησιακής μονάδας.
6.Στη συνέχεια ή θα γίνουν αλλαγές εξαιτίας του Risk Apetite Policy ή θα γίνει καταγραφή κινδύνων και αποτίμηση με παράλληλη έγκριση ώστε να εγκριθεί το πλάνο και να προχωρήσει η διαδικασία.
7.Επιπλέον ταυτόχρονα πραγματοποιείται η ενέργεια παρακολούθησης υλοποίησης πλάνου όπως και η κοινοποίηση αποτελεσμάτων στην υποδιεύθυνση Risk Management.
8.Αφού ολοκληρωθούν οι ενέργειες ταυτόχρονα γίνεται η αρχειοθέτηση υλικού
9.Η υποδιεύθυνση Risk Management ενημερώνει το εταιρικό μητρώο κινδύνων .
10.Ενημερώνονται και οι αρμόδιοι που εμπλέκονται για να ολοκληρωθεί η διαδικασία.

1.9.2 Integrated Management System

Το κάθε πρότυπο δεν έχει ξεχωριστό risk management αλλά υπάρχει ένα ενιαίο (integrated) για την διαχείριση κινδύνων όλων των προτύπων το οποίο είναι πιστοποιημένο από το Pass 99.
Το μοντέλο του Ολοκληρωμένου Συστήματος Διαχείρισης (IMS), λαμβάνει υπόψη τις έξι κοινές απαιτήσεις για συστήματα διαχείρισης (ISO Guide 72)
1)Πολιτική
2)Σχεδίαση
3)Εφαρμογή & Λειτουργία
4)Αξιολόγησης της απόδοσης
5)Βελτίωση
6)Επισκόπηση διαχείρισης

Τα κοινά σημεία για το IMS είναι τα εξής

- iso-audits
- supplier-evaluation
- procurement-one certification body
- awareness culture-training/facilities
- common documentation-one set of processes fits all
- one integrated manual-scope, objectives, targets

Τα θετικά στοιχεία ενός ενοποιημένου συστήματος διαχείρισης είναι η 1) Συμμετοχή Οργανωτικών Μονάδων Διαλειτουργικά, 2) οι ώρες για την πιστοποίηση είναι μειωμένες και ταυτόχρονες και 3) παρατηρείται μείωση κόστους μέσω:
• Κεντρικής ανάπτυξης της τεκμηρίωσης.
• Κοινή εσωτερική αξιολόγηση και προετοιμασία με συναντήσεις και βίντεο.
• Κοινός οργανισμός πιστοποίησης και δραστηριότητες προμηθειών.
• Κοινή συμφωνία και Βελτίωση χειρισμού αλλά και άμεση ανταλλαγή γνώσεων και μεταφορά.

Στο **PAS 99** αναφέρεται η Διαχείριση κινδύνου στην παράγραφο 3.10 όπου είναι το ίδιο σημείο από το ISO 31000:2009 ,2.1 εκεί αναφέρεται το αποτέλεσμα της αβεβαιότητας σχετικά με τους στόχους.
Στην § 6.1 όπου αναφέρεται το planning πρέπει να ληφθούν (actions to address risks and opportunities)
Αυτό συμβαίνει γιατί κάθε οργανισμός αντιμετωπίζει σοβαρές προκλήσεις λόγω εσωτερικών και εξωτερικών παραγόντων που ενδέχεται να επηρεάσουν τους εταιρικούς στόχους. Επομένως, οι δραστηριότητές του υπόκεινται σε αβεβαιότητα. Οι επιπτώσεις αυτής της αβεβαιότητας στους στόχους της

εταιρείας είναι απόκλιση από το αναμενόμενο αποτέλεσμα και μπορεί να είναι θετικές (αναφερόμενες ως ευκαιρίες) ή αρνητικές (που αναφέρονται ως κίνδυνοι). Η Εταιρεία καθορίζει τις απαιτήσεις των ενδιαφερομένων (εσωτερικών και εξωτερικών) και υιοθετεί σημεία ελέγχου για την εκπλήρωση τους. Οι κίνδυνοι και τα αντίστοιχα σημεία ελέγχου που απεικονίζονται στις διαδικασίες IMS εντοπίζονται, αναλύονται και συμφωνούνται με τις αρμόδιες οργανωτικές μονάδες από τον οργανισμό. Ο οργανισμός, ενώ καθορίζει τους στόχους του IMS, λαμβάνει υπόψη τους προσδιορισμένους κινδύνους και ευκαιρίες και τις συναφείς απαιτήσεις, ευθυγραμμίζοντας παράλληλα τη σταθερή του δέσμευση για συνεχή βελτίωση.

Κατά την καθιέρωση των στόχων IMS, λαμβάνονται υπόψη οι ακόλουθοι παράγοντες: Συνέπεια με την Πολιτική IMS, τις μετρήσεις και τις ειδικές απαιτήσεις συστήματος διαχείρισης.

Η μεθοδολογία διαχείρισης κινδύνου του Ομίλου βασίζεται στις κατευθυντήριες γραμμές ISO 31000 που χρησιμοποιούνται για τον εντοπισμό, την ανάλυση, την αξιολόγηση και την αντιμετώπιση των προσδιορισθέντων κινδύνων

Πηγή 2* *Pas 99 (2012) σελ.16-20*

Παρακάτω παρουσιάζεται παράδειγμα εικόνας από risk matrix που απαιτεί το Pas 99

			Impact			
			0 Acceptable	1 Tolerable	2 Unacceptable	3 Intolerable
			Little or No Effect	Effects are Felt but Not Critical	Serious Impact to Course of Action and Outcome	Could Result in Disasters
Likelihood	Improbable	Risk Unlikely to Occur				
	Possible	Risk Will Likely Occur				
	Probable	Risk Will Occur				

Πηγή 3* * *https://www.business2community.com/strategy/how-to-develop-a-risk-matrix-02234010*

2.0 Βασικά στοιχεία του ISO 31000 (2018)

Ο ρόλος της ηγεσίας και η τεκμηριωμένη δέσμευση.Γίνεται ανανεωμένη εστίαση στον βασικό ηγετικό ρόλο της ανώτατης διοίκησης για την πλήρη ενσωμάτωση της διαχείρισης των κινδύνων σε όλα τα επίπεδα του οργανισμού (§5.2)
Η ευθύνη των οργάνων εποπτείας προστέθηκε.Οι ανώτεροι φορείς διαχείρισης και εποπτείας δεν πρέπει να αποδεικνύουν μόνο τη δέσμευσή τους για τη διαχείριση κινδύνου, αλλά και να εκφράζουν τη συνεχή δέσμευσή τους μέσω μιας πολιτικής / δήλωσης, η οποία πρέπει να κοινοποιείται .(§5.4.2)

2.1 Διαδικασία Διαχείρισης κινδύνων

Μεγαλύτερη προσοχή στον κυκλικό χαρακτήρα του πλαισίου διαχείρισης κινδύνων. Οι οργανισμοί πρέπει να αξιολογούν τη διαδικασία διαχείρισης των κινδύνων τους (ενδεικτική ενεργοποιούν νέες πληροφορίες, ανατροφοδότηση στην τρέχουσα διαδικασία κινδύνου ή / ελέγχους)
Μεγαλύτερη έμφαση στη διατήρηση ενός μοντέλου ανοιχτών συστημάτων που ανταλλάσσει τακτικά ανατροφοδότηση με το εξωτερικό του περιβάλλον.

2.2 Ενσωμάτωση

Σύμφωνα με το πρότυπο ISO 31000, ο κίνδυνος αντιμετωπίζεται σε κάθε τμήμα της δομής του οργανισμού. Ο καθένας έχει την ευθύνη για τη διαχείριση των κινδύνων. Η αποτελεσματικότητα της διαχείρισης κινδύνων θα εξαρτηθεί από την ενσωμάτωσή της στη διακυβέρνηση και όλες τις δραστηριότητες του οργανισμού, συμπεριλαμβανομένης της λήψης αποφάσεων (§5.3).

2.3 Αρχές Διαχείρισης κινδύνων

Η αρχή διαχείρισης κινδύνων αποτελεί τη βάση για τη διαχείριση του κινδύνου και πρέπει να επιτρέπει στον οργανισμό να διαχειρίζεται τις επιπτώσεις της αβεβαιότητας στους στόχους του.
Ο αριθμός των αρχών μειώθηκε από 11 σε 8. (§4). Ορισμένες αρχές έχουν ενσωματωθεί. Τα βασικά τους κριτήρια όσον αφορά τη δημιουργία αξίας και την προστασία έχουν διατηρηθεί.

2.4 Αναγνώριση κινδύνου

Διευρυμένη έμφαση στην αναγνώριση κινδύνου με τον καθορισμό ενός καταλόγου 11 αλληλένδετων παραγόντων που πρέπει να λαμβάνονται υπόψη κατά τον εντοπισμό πηγών κινδύνου εντός ενός οργανισμού (§6.4.2)

2.5 Αξιολόγηση κινδύνου

Λίστα με 5 επιλογές που υποστηρίζουν τη διαδικασία αξιολόγησης

2.6 Θεραπεία κινδύνου

Η επιλογή των επιλογών θεραπείας κινδύνου έχει απλοποιηθεί. Οι παράγραφοι §6.5.1 & §6.5.2 διευκρινίζουν τις επιλογές θεραπείας κινδύνου. Η αλλαγή φράσης, από τον "ανεκτό κίνδυνο" έως τον "αποδεκτό κίνδυνο", υποδεικνύει μια μετατόπιση από μια ανεκτή θεραπεία (αρνητικού) κινδύνου προς μία ευχάριστη (θετική) αντιμετώπιση κινδύνου.

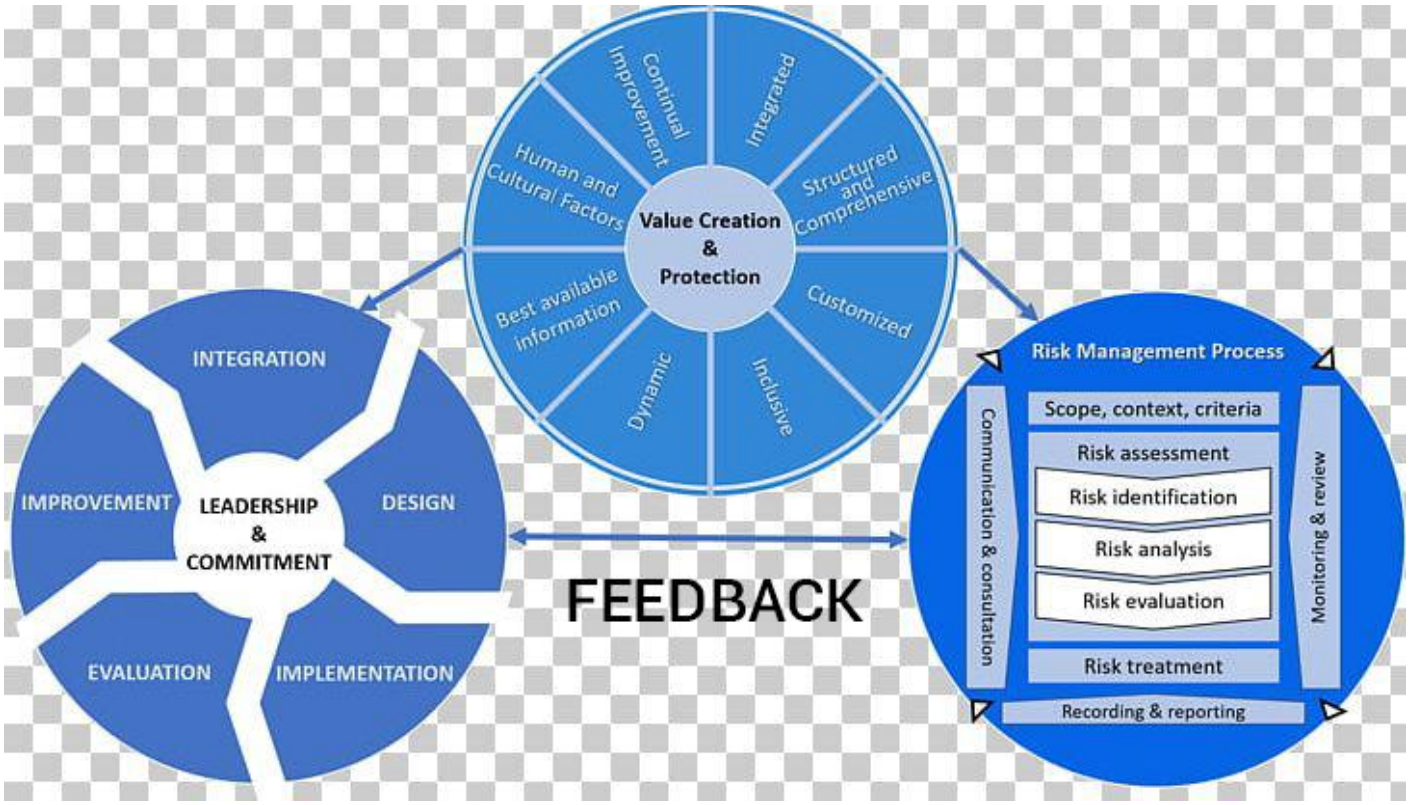
2.7 Καταγραφή και αναφορά

Προσθήκη ενός 8ου στοιχείου που σχετίζεται με τη διαδικασία κινδύνου, είναι η "Καταγραφή και αναφορά". (§6.7), προσθέτοντας το στοιχείο της επικοινωνίας των δραστηριοτήτων και των αποτελεσμάτων σε ολόκληρο τον οργανισμό.

2.8 Συνοπτικά

Σημασία ισχυρής ηγεσίας και δέσμευσης , Αρχή Διοίκησης Ευθύνης να εξετάσει τους κινδύνους κατά τη λήψη επιχειρηματικών αποφάσεων. Έμφαση στην ορθή εφαρμογή της διαδικασίας διαχείρισης κινδύνου, έτσι ώστε οι έλεγχοι να έχουν το επιδιωκόμενο αποτέλεσμα. Η διαχείριση του κινδύνου πρέπει να προσαρμόζεται, ειδικά στο προφίλ κινδύνου και στην όρεξη για κίνδυνο. Έμφαση στη διασφάλιση της ολοκληρωμένης διαχείρισης κινδύνων σε όλα τα επίπεδα του οργανισμού.
Έμφαση στην αξία της μέτρησης, αξιολόγησης και βελτίωσης του ίδιου του συστήματος διαχείρισης κινδύνων.

Πηγή 4 ISO 31000:2018| Risk Management - Guidelines| Main Changes vs 2009 edition σελ.2-8*



Πηγή 5* https://imgbin.com/png/sfXBEW77/iso-31000-risk-management-international-organization-for-standardization-png

3.0 Κοινά σημεία 31000 με τα υπόλοιπα πρότυπα.

3.1 ISO 31000(2018) κοινά σημεία με ISO 9001(2015)

Στο ISO 9001(2015) η αξιολόγηση της διακινδύνευσης είναι ιδιαιτέρως σημαντική για κάθε είδους οργανισμό. Για τον λόγο αυτό για πρώτη φορά εισάγεται η προσέγγιση διακινδύνευσης. Παρόλο που η διαχείριση της διακινδύνευσης δεν απαιτείται αυτή καθαυτή οι οργανισμοί θα πρέπει να εντοπίζουν τυχόν απειλές αλλά και ευκαιρίες και να τις λαμβάνουν υπόψη τους κατά το σχεδιασμό διαχείρισης ποιότητας. Σε αντάλλαγμα δεν προβλέπεται συγκεκριμένη απαίτηση για προληπτικές ενέργειες. Στην παράγραφο§ 6.1 αναφέρεται πως πρέπει να γίνουν ενέργειες για την αντιμετώπιση των κινδύνων και των ευκαιριών . Λαμβάνοντας υπόψη τα ζητήματα που τέθηκαν και τις απαιτήσεις των σχετικών ενδιαφερομένων μερών § (4.1 και 4.2), η εν λόγω παράγραφος απαιτεί τον προσδιορισμό των κινδύνων και των ευκαιριών που πρέπει να αντιμετωπιστούν, τις ενέργειες που πρέπει να αναληφθούν και την αξιολόγηση της αποτελεσματικότητας αυτών των δράσεων.

Ερμηνεία

Ο στόχος είναι ο σχεδιασμός του συστήματος Διαχείρισης ποιότητας κατά τρόπο, λαμβάνοντας υπόψη τα εσωτερικά και εξωτερικά θέματα, τις απαιτήσεις των ενδιαφερομένων μερών, να εντοπίζει τις απειλές και τις ευκαιρίες που πρέπει να αντιμετωπίζονται η να αξιοποιούνται ώστε το σύστημα διαχείρισης ποιότητας να επιτυγχάνει συνεχής βελτίωση. Παράδειγμα τεκμηρίωσης Κατάλογος απειλών, κατάλογος ευκαιριών, επενδυτικά σχέδια, στρατηγικά σχέδια.

Δείκτες μέτρησης και απόδοσης.

Δείκτες υλοποίησης επενδυτικών σχεδίων, δείκτες αστοχιών, ποσοστό υλοποίησης ενεργειών.

Αξιολόγηση ενεργειών για την αντιμετώπιση απειλών και ευκαιριών.

θα πρέπει να σχεδιασθούν, υλοποιηθούν και αξιολογηθούν ως προς την αποτελεσματικότητα τους μέτρα αντιμετώπισης των απειλών και αξιοποίησης των ευκαιριών. Ο προσδιορισμός των απειλών και των ευκαιριών σχετίζεται με την θέσπιση νέων πρακτικών την προώθηση νέων προϊόντων, το άνοιγμα νέων αγορών, την αναζήτηση νέων πελατών, την οικοδόμηση εταιρικών συνεργασιών

και την ανάπτυξη εταιρικής κουλτούρας.

Πηγή 6* *ISO 9001 :2015 σελ.17-19*

3.2 ISO 31000 (2018) κοινά σημεία με ISO 50001(2011) Σύστημα Διαχείρισης Ενέργειας (ΣΔΕ)

Το ISO 31000 ουσιαστικά επηρεάζει το πρότυπο διαχείρισης ενέργειας απαιτώντας ενεργειακό έλεγχο. Αυτό μπορούμε να το διακρίνουμε στην παράγραφο § 6.1 και § 6.1.2. Η ομάδα διαχείρισης ενέργειας είναι αρμόδια για την ενεργειακή ανασκόπηση τόσο μιας νέας εγκατάστασης η οποία μετά από απόφαση του Energy Committee, θα ενταχθεί στο πεδίο εφαρμογής του ΣΔΕ, όσο και για τις υφιστάμενες εγκαταστάσεις.

Αφού προσδιοριστούν τα φυσικά και λειτουργικά όρια της εγκατάστασης, διενεργείται ενεργειακή επιθεώρηση, όπου αναλύονται οι δραστηριότητες κάθε εγκατάστασης. Αναλύονται και αξιολογούνται οι ενεργειακές πλευρές αυτών των δραστηριοτήτων και προσδιορίζεται το Energy Baseline. Όλα τα παραπάνω εγκρίνονται από το Energy Committee και στη συνέχεια προσδιορίζονται οι κρίσιμοι παράγοντες ενεργειακής διαχείρισης, γύρω από τους οποίους θα αναπτυχθούν τα ενεργειακά προγράμματα.

Παρακολούθηση και μέτρηση επίδοσης συστήματος διαχείρισης ενέργειας

Αφού ολοκληρωθεί η ανάπτυξη του Συστήματος Διαχείρισης Ενέργειας (ΣΔΕ), ξεκινά η λειτουργία του συστήματος και ακολουθεί η παρακολούθηση και η

μέτρηση της επίδοσης του ΣΔΕ για την οποία υπεύθυνες είναι οι εμπλεκόμενες επιχειρησιακές μονάδες της Εταιρείας, όπως ορίζονται σε κάθε πρόγραμμα. Παρακολουθούνται και καταγράφονται οι καταναλώσεις ενέργειας και τα στοιχεία που αφορούν στην ενεργειακή διαχείριση των κτιρίων. Οι ενεργειακοί δείκτες επίδοσης συγκρίνονται με το Energy Baseline, ενημερώνεται ο Εκπρόσωπος της Διοίκησης για θέματα Διαχείρισης Ενέργειας ,συντάσσει απολογιστική αναφορά επίδοσης του ΣΔΕ και όπου απαιτείται προτείνονται διορθωτικές ενέργειες. Σε ετήσια βάση, ο συντονιστής διαχείρισης ενέργειας συντάσσει απολογιστική αναφορά επίδοσης του ΣΔΕ η οποία αποτελεί εισερχόμενο για την ανασκόπηση του, μέσω διαδικασίας.

3.3 Ανασκόπηση ενοποιημένων συστημάτων διαχείρισης

Μετά την ολοκλήρωση της παρακολούθησης και μέτρησης του συστήματος διαχείρισης ενέργειας και της αξιολόγησης διαδικασιών ενοποιημένων συστημάτων διαχείρισης, πραγματοποιείται η ανασκόπηση ενοποιημένων συστημάτων διαχείρισης. Κατά τη διάρκεια της ανασκόπησης συγκεντρώνονται παρουσιάζονται και συζητούνται ενώπιον της Management steering Committee όλα τα θέματα που μπορεί να έχουν προκύψει είτε από εσωτερικές αξιολογήσεις είτε από την παρακολούθηση και μέτρηση του συστήματος. Στη συνέχεια λαμβάνονται αποφάσεις που θα οδηγήσουν στη βελτίωση της αποτελεσματικότητας και της συνολικής επίδοσης σε όλα τα συστήματα διαχείρισης που εφαρμόζονται στον όμιλο ΠΑΠΑΔΟΠΟΥΛΟΣ Α.Ε.

πηγή 7* *ISO 50001:2018 Energy Management Systems σελ 10-12*

3.4 ISO 14001 κοινά σημεία με ISO 31000

ISO 14001(2015) environmental management system εκτίμηση κινδύνου
Το πρότυπο ISO 14001: 2004 στηρίζεται στην εκτίμηση κινδύνου μαζί με διορθωτικές και προληπτικές ενέργειες για την ελαχιστοποίηση των επιπτώσεων μιας επιχείρησης στο περιβάλλον. Ωστόσο, οι λόγοι στους οποίους αναμένεται να εκτελεστούν τα παραπάνω δεν προσδιορίζονται. Το πρότυπο 14001: 2015 θα επιδιώξει να αντικαταστήσει την "προληπτική δράση" με την "αυξημένη διαχείριση κινδύνου". Ως εκ τούτου, η εστίαση θα προχωρήσει από προληπτικές ενέργειες, οι οποίες μπορεί να είναι λιγότερο αποτελεσματικές επειδή μπορούν να πραγματοποιηθούν μόνο από ορισμένα άτομα εντός ενός οργανισμού, στη διαχείριση κινδύνων, η οποία θα πρέπει να είναι μια διεξοδικότερη διαδικασία λόγω της εισόδου και της δέσμευσης από πολλούς ενδιαφερόμενους, με αυξημένη αίσθηση σπουδαιότητας λόγω της αλλαγής του προτύπου. Επίσης, εάν πρέπει να δώσετε μια διορθωτική

ενέργεια, αντιδράτε σε ένα γεγονός που έχει ήδη συμβεί. Το νέο πρότυπο αποβλέπει στην πρόληψη αυτών των περιστατικών που περιγράφονται με τη χρήση διαχείρισης κινδύνου και προληπτικής αξιολόγησης κινδύνου.
Στόχος της «στρατηγικής διαχείρισης κινδύνου» είναι να επικεντρωθεί η ανώτατη διοίκηση και η ομάδα του οργανισμού τόσο στο να αξιοποιήσουν περισσότερο χρόνο, να ερευνήσουν και να κατανοήσουν πτυχές που ενδέχεται να παρουσιάσουν κίνδυνο για το περιβάλλον ,όσο και να εκτελέσουν αυτές τις ενέργειες πριν δημιουργηθεί κάποια περιβαλλοντική επίπτωση.
Σύμφωνα με την § 6.1.1 Ο οργανισμός πρέπει να καθιερώνει να εφαρμόζει, να ελέγχει και να διατηρεί ενήμερες τις διεργασίες που χρειάζονται για την ικανοποίηση των απαιτήσεων του συστήματος περιβαλλοντικής διαχείρισης. Άρα πρέπει να γίνεται καθιέρωση κριτηρίων λειτουργίας για τις διεργασίες και εφαρμογή ελέγχου των διεργασιών σύμφωνα με τα κριτήρια λειτουργίας.
Σε συμφωνία με τη προσέγγιση του κύκλου ζωής ο Οργανισμός πρέπει να καθιερώνει ελέγχους, όπως ενδείκνυται, ώστε να διασφαλίζεται ότι οι περιβαλλοντικές του απαιτήσεις λαμβάνονται υπόψη κατά τη διεργασία σχεδιασμού και ανάπτυξης προϊόντων και υπηρεσιών εξετάζοντας όλα τα στάδια του κύκλου ζωής τους. Καθορίζει τις περιβαλλοντικές του απαιτήσεις για την προμήθεια προϊόντων και υπηρεσιών όπως ενδείκνυται, γνωστοποιεί τις σχετικές περιβαλλοντικές απαιτήσεις στους εξωτερικούς παρόχους συμπεριλαμβανομένων των υπεργολάβων και εξετάζει την αναγκαιότητα παροχής πληροφόρησης σχετικά με τις δυνητικές σημαντικές περιβαλλοντικές επιπτώσεις που συνδέονται με την μεταφορά ή παράδοση, τη χρήση, την επεξεργασία στο τέλος του κύκλου ζωής και την τελική διάθεση προϊόντων και υπηρεσιών. Ο οργανισμός πρέπει να διατηρεί ενήμερες τεκμηριωμένες πληροφορίες στο βαθμό που είναι αναγκαίος για τη δημιουργία εμπιστοσύνης ότι οι διεργασίες υλοποιούνται σύμφωνα με τα προβλεπόμενα.

Ετοιμότητα και ανταπόκριση σε καταστάσεις έκτακτης ανάγκης.
Ο οργανισμός πρέπει να:

- Προετοιμάζεται ώστε να ανταποκρίνεται μέσω του σχεδιασμού ενεργειών πρόληψης ή περιορισμού των δυσμενών περιβαλλοντικών από καταστάσεις έκτακτης ανάγκης.
- Ανταποκρίνεται σε πραγματικές καταστάσεις έκτακτης ανάγκης
- Αναλαμβάνει ενέργειες πρόληψης ή περιορισμού των συνεπειών από καταστάσεις έκτακτης ανάγκης ανάλογα με τη σοβαρότητα των καταστάσεων καθώς και των δυνητικών περιβαλλοντικών επιπτώσεων.
- Δοκιμάζει περιοδικά τις προβλεπόμενες ενέργειες ανταπόκρισης, όπου είναι εφικτό

- Ανασκοπεί περιοδικά και αναθεωρεί τις διεργασίες και τις προβλεπόμενες ενέργειες ανταπόκρισης ιδιαίτερα μετά από περιστατικά ή δοκιμές .
- Παρέχει όπως ενδείκνυται σχετική πληροφόρηση και κατάρτιση για την ετοιμότητα και ανταπόκριση σε καταστάσεις έκτακτης ανάγκης στα σχετικά ενδιαφερόμενα μέρη, συμπεριλαμβανομένων των προσώπων που εργάζονται υπό τον έλεγχό του.

Αποτελεί υπευθυνότητα του κάθε Οργανισμού να είναι προετοιμασμένος και να ανταποκρίνεται στις καταστάσεις έκτακτης ανάγκης με τρόπο που αρμόζει στις ιδιαίτερες ανάγκες του.
Κατά το σχεδιασμό διεργασίας ετοιμότητας και ανταπόκρισης σε καταστάσεις έκτακτης ανάγκης ο οργανισμός πρέπει να εξετάζει:
1) Την πλέον κατάλληλη μέθοδο ανταπόκρισης σε καταστάσεις έκτακτης ανάγκης.
2) Τη διεργασία εσωτερικής και εξωτερικής επικοινωνίας .
3) Τις απαιτούμενες ενέργειες για την πρόληψη ή τον περιορισμό των περιβαλλοντικών επιπτώσεων .
4) Τις ενέργειες περιορισμού και ανταπόκρισης που αναλαμβάνονται για διαφορετικά είδη καταστάσεων έκτακτης ανάγκης.
5) Την ανάγκη για εκ των υστέρων αξιολόγηση της κατάστασης έκτακτης ανάγκης ώστε να καθορίζονται και να υλοποιούνται διορθωτικές ενέργειες.
6) Την περιοδική δοκιμή των σχεδιασμένων ενεργειών ανταπόκρισης σε καταστάσεις έκτακτης ανάγκης.
7) Την κατάρτιση του προσωπικού ανταπόκρισης σε καταστάσεις έκτακτης ανάγκης.
8) Τον κατάλογο βασικού προσωπικού και υπηρεσιών αρωγής συμπεριλαμβανομένων των στοιχείων επικοινωνίας.
9) Τις οδού διαφυγής και τα σημεία συγκέντρωσης και τη δυνατότητα αμοιβαίας βοήθειας από γειτονικούς οργανισμούς.

3.5 Διαχείριση Κινδύνων: Τα βασικά περιβαλλοντικά οφέλη

Είναι σαφές ότι οι αλλαγές στο Σχέδιο Διεθνούς Προτύπου αποσκοπούν στην εξασφάλιση μιας προληπτικής, μετρούμενης και στρατηγικής προοπτικής για τις περιβαλλοντικές ανησυχίες. Τα βασικά οφέλη για το περιβάλλον πρέπει να προέρχονται από μια μεγάλη προκατάληψη για τον εντοπισμό και την πρόληψη των περιστατικών, και όχι με τις αντιδράσεις στα γεγονότα. Αυτή η εστίαση θα έχει τεράστια θετική επίδραση στο περιβάλλον και την κληρονομιά που αφήνουμε για τις επόμενες γενιές. Με τις συλλογικές βελτιώσεις του ISO 14001, διαπιστευμένοι και συμμορφούμενοι οργανισμοί σε όλο τον κόσμο θα

επηρεάσουν θετικά τον πλανήτη στον οποίο ζούμε και τους πόρους που αφήνουμε για τους άλλους.

3.6 Διαχείριση κινδύνων: Τα οφέλη για τον οργανισμό

Η διαδικασία αναθεώρησης της διαχείρισής πρέπει να κατευθύνει την πορεία σε γενικούς στόχους αλλά η ομάδα μπορεί να πραγματοποιήσει τη συντριπτική πλειοψηφία της καθημερινής εργασίας του σχεδίου, να ελέγχει και να ενεργεί. Η ταλάντευση του στρατηγικού σχεδιασμού του τρόπου με τον οποίο αξιολογείτε τις περιβαλλοντικές πτυχές, με τη συμμετοχή της ομάδας διαχείρισης, θα δημιουργήσει μια θεμελιώδη αλλαγή στις περιβαλλοντικές επιδόσεις. Σκεφτείτε ότι τώρα θα είναι φυσιολογικό ολόκληρη η ομάδα διαχείρισης να σκεφτεί για οποιεσδήποτε πτυχές που μπορεί να επηρεάσουν την επιχείρησή και να συζητήσουν πώς θα διαχειρίζονται, θα μετριάζονται και θα καταργούνται αυτοί οι κίνδυνοι. Πολλές περιβαλλοντικές "πτυχές", οι οποίες με την πάροδο του χρόνου γίνονται "περιστατικά", είναι δαπανηρές όχι μόνο για το περιβάλλον αλλά και για την επιχείρησή . Θα πρέπει τώρα να παρατηρηθεί μια οριστική βελτίωση σε αυτόν τον τομέα των κριτηρίων απόδοσης και να βελτιώσετε τους βασικούς περιβαλλοντικούς δείκτες απόδοσης. Η συνεχής αναθεώρηση, η προσαρμογή και η συνεχής βελτίωση θα διασφαλίσουν ότι αυτός ο κύκλος θα συνεχιστεί. Η πρόληψη, με τη βοήθεια του μελλοντικού σχεδιασμού και της διαχείρισης κινδύνου, είναι πολύ καλύτερη από μια θεραπεία.

Συνοπτικά, μια αυξημένη στροφή προς τη στρατηγική διαχείριση κινδύνων θα έχει ως αποτέλεσμα οφέλη τόσο για τον πλανήτη όσο και για την οικονομική απόδοση του οργανισμού.

πηγή 8*: ISO 14001:2015 – Environmental Management System σελ.19-20

4.0 ISO 22301 κοινά σημεία με ISO 31000

Το πρότυπο για το σύστημα επιχειρησιακής συνέχειας ουσιαστικά δέχεται input από το intergrated management system του ομίλου ΠΑΠΑΔΟΠΟΥΛΟΣ Α.Ε με αυτό τον τρόπο εντοπίζονται όλα τα ρίσκα από όλους τους τομείς και βγαίνει ένα συνολικό αποτέλεσμα.

4.1 Λειτουργικός σχεδιασμός και έλεγχος

Ο οργανισμός πρέπει να σχεδιάζει, να εφαρμόζει και να ελέγχει τις διεργασίες που απαιτούνται για την ικανοποίηση των απαιτήσεων καθώς και την υλοποίηση των ενεργειών που προσδιορίζονται μέσω του καθορισμού κριτηρίων για τις διεργασίες, της διενέργειας ελέγχου των διεργασιών

σύμφωνα με τα κριτήρια και της διατήρησης των αρχείων ως αποδεικτικών στοιχείων στο βαθμό που απαιτείται ώστε να υπάρχει εμπιστοσύνη. Επιπλέον ο οργανισμός θα πρέπει να ελέγχει τις προβλεπόμενες αλλαγές και να ανασκοπεί τις συνέπειες των ακούσιων αλλαγών, αναλαμβάνοντας ενέργειες για τον περιορισμό των δυσμενών συνεπειών όπως απαιτείται. Ο οργανισμός πρέπει να διασφαλίζει ότι ελέγχονται οι εξωτερικές αναθέσεις

4.2 Επιχειρησιακές επιπτώσεις και αξιολόγηση διακινδύνευσης

Ο οργανισμός πρέπει να καθιερώνει, εφαρμόζει και διατηρεί μια επίσημη και τεκμηριωμένη διεργασία για την ανάλυση της διακινδύνευσης και των επιπτώσεων.

1) Πρέπει να καθιερώνει το πλαίσιο της αξιολόγησης, να καθορίζει τα κριτήρια και να αποτιμά την ενδεχόμενη επίδραση ενός αποδιοργανωτικού περιστατικού.
2) Να λαμβάνει υπόψη νομικές και άλλες απαιτήσεις τις οποίες ο οργανισμός έχει αποδεχτεί.
3) Να περιλαμβάνει συστηματική ανάλυση, επεξεργασία της προτεραιότητας των διακινδυνεύσεων και τα συναφή κόστη.
4) Να ορίζει το απαιτούμενο αποτέλεσμα από την ανάλυση των επιχειρησιακών επιπτώσεων και την αξιολόγηση της διακινδύνευσης.
5) Να προδιαγράφει τις απαιτήσεις για αυτές τις πληροφορίες ώστε να διατηρούνται ενημερωμένες και εμπιστευτικές.

4.3 Ανάλυση επιχειρησιακών επιπτώσεων

Ο οργανισμός πρέπει να καθιερώνει και να εφαρμόζει μια επίσημη και τεκμηριωμένη διεργασία αποτίμησης για τον προσδιορισμό των προτεραιοτήτων συνέχεια και επαναφοράς, στόχων και σκοπών. Η διεργασία αυτή πρέπει να περιλαμβάνει την αξιολόγηση επιπτώσεων αποδιοργανωτικών περιστατικών η οποία υποστηρίζει τα προϊόντα και τις υπηρεσίες του Οργανισμού.

Η ανάλυση επιχειρησιακών επιπτώσεων περιλαμβάνει τα ακόλουθα.

1) Τον προσδιορισμό των δραστηριοτήτων που υποστηρίζουν την παροχή προϊόντων και υπηρεσιών.
2) Την αξιολόγηση των επιπτώσεων με την πάροδο του χρόνου της μη διενέργειας των δραστηριοτήτων αυτών.
3) Τον καθορισμό χρονοδιαγραμμάτων προτεραιότητας για τη συνέχιση των δραστηριοτήτων αυτών σε καθορισμένο ελάχιστο αποδεκτό επίπεδο, λαμβάνοντας υπόψη το χρόνο εντός του οποίου οι επιπτώσεις της μη επαναφοράς τους θα γινόταν μη αποδεκτές.

4) Τον προσδιορισμό των αναγκών και υποστηρικτικών πόρων για τις συγκεκριμένες δραστηριότητες που θα συμπεριλαμβάνουν προμηθευτές εξωτερικούς συνεργάτες και άλλα ενδιαφερόμενα μέρη.

4.4 Αξιολόγηση διακινδύνευσης

Η αξιολόγηση γίνεται με βάση το ISO 31000 οπότε βλέποντας την παράγραφο 6.1 του προτύπου.

1) Εντοπίζει της διακινδυνεύσεις στις πλέον σημαντικές δραστηριότητες και διεργασίες του οργανισμού, συστήματα, πληροφορίες, πρόσωπα, περιουσιακά στοιχεία, εξωτερικούς συνεργάτες και στους άλλους πόρους που υποστηρίζουν τις δραστηριότητες τους.
2) Αναλύει σημαντικά τη διακινδύνευση.
3) Αποτιμά ποια συνδεόμενη με αποδιοργάνωση διακινδύνευση απαιτεί αντιμετώπιση.
4) Προσδιορίζει αντιμετώπιση σύμφωνα με τους στόχους της επιχειρησιακής συνέχειας σύμφωνα με την εύθετη διακινδύνευση του Οργανισμού.

Πηγή 9* *ΕΛΟΤ ISO 22301:2014 σελ. 21*

5 . OHSAS 18001 και ISO 45001 βασισμένα στο ρίσκο

Κατά τον σχεδιασμό του συστήματος διαχείρισης OHSAS, ο οργανισμός εξετάζει τα θέματα που αναφέρονται στο πλαίσιο, τις απαιτήσεις και το πεδίο εφαρμογής και προσδιορίζει τους κινδύνους και τις ευκαιρίες. Στην παράγραφο 3.1 του προτύπου OHSAS 18001 (2018) απαιτείται να γίνει αναγνώριση του κινδύνου, στην παράγραφο 3.2 αναφέρεται σε ανεκτή επικινδυνότητα, στην παράγραφο 3.10 απαιτείται αξιολόγηση της διακινδύνευσης και στο 3.15 συνδυασμός της πιθανότητας εμφάνισης ενός επικίνδυνου συμβάντος ή έκθεσης σε κίνδυνο και της σοβαρότητας τραυματισμού ή της επαγγελματικής ασθένειας που μπορεί να προκληθεί. Στόχο έχουν:

α) Να εξασφαλίσουν ότι το σύστημα διαχείρισης OHSAS μπορεί να επιτύχει τα επιδιωκόμενα αποτελέσματά του.
β) Να προλαμβάνει ή να μειώνει ανεπιθύμητα αποτελέσματα.
γ) Επίτευξη συνεχούς βελτίωσης.

Κατά τον προσδιορισμό των κινδύνων και των ευκαιριών, ο οργανισμός λαμβάνει υπόψη:

- τους κινδύνους
- ευκαιρίες
- νομικές απαιτήσεις και άλλες απαιτήσεις

Ο οργανισμός διατηρεί τεκμηριωμένες πληροφορίες σχετικά με τους κινδύνους και τις ευκαιρίες και τις ενέργειες που απαιτούνται για τον προσδιορισμό και την αντιμετώπιση των κινδύνων και των ευκαιριών του

Δράσεις για την αντιμετώπιση των κινδύνων και των ευκαιριών
Πρόκειται για μια εντελώς νέα απαίτηση σε σύγκριση με το προηγούμενο OHSAS 18001. Κατά τον σχεδιασμό του ο οργανισμός θα πρέπει να καθορίσει τους κινδύνους και τις ευκαιρίες που επηρεάζουν τον οργανισμό.
Οι κίνδυνοι που σχετίζονται με το σύστημα διαχείρισης OHSAS είναι μια νέα απαίτηση σε σύγκριση με το προηγούμενο, αυτή η απαίτηση καλύπτει όχι μόνο τους κινδύνους που σχετίζονται αλλά και τους κινδύνους σχετικά με τις νομικές και άλλες απαιτήσεις και το γενικό πλαίσιο του οργανισμού.

Ο οργανισμός καταρτίζει, εφαρμόζει και διατηρεί μια διαδικασία για τον εντοπισμό των κινδύνων, η οποία είναι συνεχής και προορατική. Η διαδικασία λαμβάνει υπόψη:
τον τρόπο οργάνωσης της εργασίας, τους κοινωνικούς παράγοντες (συμπεριλαμβανομένου του φόρτου εργασίας, των ωρών εργασίας, της θυματοποίησης, της παρενόχλησης και του εκφοβισμού), της ηγεσίας και του πολιτισμού στον οργανισμό. Συνήθεις και μη συνήθεις δραστηριότητες και καταστάσεις, συμπεριλαμβανομένων όλων των κινδύνων,
παρελθόντα σχετικά περιστατικά, εσωτερικά ή εξωτερικά του οργανισμού, συμπεριλαμβανομένων των καταστάσεων έκτακτης ανάγκης, και των αιτιών τους ,πιθανές καταστάσεις έκτακτης ανάγκης,ανθρώπων,
συμπεριλαμβανομένης της πρόσβασης στην εργασία, των εργολάβων, των επισκεπτών κ.λπ.Αλλα θέματα, συμπεριλαμβανομένης της εξέτασης χώρων εργασίας, διαδικασιών, εγκαταστάσεων, διαδικασιών λειτουργίας ,πραγματικές ή προτεινόμενες αλλαγές στην οργάνωση, τις λειτουργίες, τις διαδικασίες, τις δραστηριότητες και το σύστημα διαχείρισης OHSAS, αλλαγές στις γνώσεις και πληροφορίες σχετικά με τους κινδύνους.

Πηγή 10* *OHSAS 18001 σελ. 8-10 & ISO 4 5001:2018 σελ. 11*

6. ISO 17025 risk based approach

Προσέγγιση με βάση τους κινδύνους
Ένα νέο κεφάλαιο έχει προστεθεί στη σκέψη που βασίζεται στον κίνδυνο

Προσέγγιση διαδικασιών

Η προσέγγιση της διαδικασίας ταιριάζει με τα νεότερα πρότυπα όπως το ISO 9001: 2015. Μεγαλύτερη ευελιξία στις κατευθυντήριες γραμμές για τις διαδικασίες, τις διεργασίες, τις τεκμηριωμένες πληροφορίες και τις οργανωτικές ευθύνες.

Τεχνολογίες πληροφορικής

Το πρότυπο έχει μεγαλύτερη έμφαση στις τεχνολογίες της πληροφορίας. Σε αναγνώριση αυτού, τα εγχειρίδια και τα αρχεία των σκληρών αντιγράφων εγκαταλείπονται σιγά σιγά υπέρ των ηλεκτρονικών εκδόσεων.

Πεδίο εφαρμογής

Το πεδίο εφαρμογής έχει αναθεωρηθεί ώστε να καλύπτει όλες τις εργαστηριακές δραστηριότητες. Αυτό περιλαμβάνει τη δοκιμή, τη βαθμονόμηση και τη δειγματοληψία που συνδέεται με επακόλουθη βαθμονόμηση και δοκιμή.

Ορολογία

Η ορολογία έχει ενημερωθεί. Για παράδειγμα, έχει προστεθεί ορισμός για "εργαστήριο"

Θέματα προς αξιολόγηση

Ενδεικτικά Θέματα προς αξιολόγηση
Εξοπλισμός (Διακρίβωση –Συντήρηση Εξοπλισμού- Κατάλογος Παρακολούθηση εξοπλισμού)
Διαχείριση Παραπόνων (Πόσα παράπονα, διορθωτικές ενέργειες, ερωτηματολόγιο ικανοποίησης κλπ.)
Εκπαίδευση προσωπικού για την διενέργεια των συγκεκριμένων μετρήσεων και την χρήση αυτού του εξοπλισμού (κάθετες επιθεωρήσεις)
Κάθετες επιθεωρήσεις σχετικά με την ορθή τήρηση της μεθόδου δοκιμής για κάθε εργαζόμενο
Σύμβαση πρόσληψης προσωπικού (δεσμεύονται σχετικά με την αμεροληψία και ακεραιότητάς τους)
Προμηθευτές (Κατάλογος Προμηθευτών – Αξιολόγηση)
Μετρήσεις: Η/Μ σε σταθερή, Δειγματοληπτικός έλεγχος μετρήσεων Η/Μ (1 μέτρηση που έγινε εσωτερικά, 1 μέτρηση που έγινε από προμηθευτή και αφορούσε παράπονο), Επαλήθευση μέτρησης Η/Μ από εξωτερικό φορέα (Πανεπιστήμιο κλπ.) & Αξιολόγηση των αποτελεσμάτων από το εργαστήριο & Ενημέρωση Πελάτη για την διενέργεια των μετρήσεων από εξωτερικό υπεργολάβο.
Νομοθεσία (Φάκελο με τις τελευταίες εκδόσεις των νομοθετικών εγγράφων από τον τεχνικό υπεύθυνο του εργαστηρίου)
Ασφαλή αποθήκευση των αρχείων του εργαστηρίου- ύπαρξη back up.
Αξιολόγηση Κινδύνων | Risk Assessment Approach.
Αξιολόγηση των στόχων του όπως αυτοί περιλαμβάνονται στην ανασκόπηση του ΣΔ.
Έλεγχος άρσης αποκλίσεων ευρημάτων εσωτερικής αξιολόγησης & εξωτερικής επιθεώρησης.

Πηγή 11 ISO 17025:2017 σελ.32*

7. ISO 19600 compliance management systems κοινά σημεία με το ISO 31000

Οι οργανισμοί διεξάγουν εκτιμήσεις για τον εντοπισμό διαφόρων τύπων οργανωτικού κινδύνου. Για παράδειγμα, μπορούν να διεξάγουν εκτιμήσεις κινδύνου για επιχειρήσεις προκειμένου να προσδιορίσουν τους στρατηγικούς, λειτουργικούς, χρηματοοικονομικούς κινδύνους και τους κινδύνους συμμόρφωσης στους οποίους εκτίθεται ο οργανισμός. Στις περισσότερες περιπτώσεις, η διαδικασία εκτίμησης κινδύνων για τις επιχειρήσεις επικεντρώνεται στην αναγνώριση των κινδύνων εκείνων που θα μπορούσαν να επηρεάσουν την ικανότητα του οργανισμού να επιτύχει τους στρατηγικούς του στόχους. Οι περισσότερες οργανώσεις διεξάγουν εκτιμήσεις κινδύνου εσωτερικού ελέγχου για να βοηθήσουν στην ανάπτυξη του σχεδίου εσωτερικού ελέγχου. Μια παραδοσιακή αξιολόγηση του κινδύνου εσωτερικού ελέγχου είναι πιθανό να εξετάσει τους κινδύνους της χρηματοοικονομικής κατάστασης και άλλους κινδύνους λειτουργίας και συμμόρφωσης.
Ενώ και οι δύο αυτές εκτιμήσεις κινδύνου αποσκοπούν συνήθως στον εντοπισμό σημαντικών κινδύνων που σχετίζονται με τη συμμόρφωση, δεν έχει σχεδιαστεί ειδικά για τον προσδιορισμό των νομικών ή κανονιστικών κινδύνων συμμόρφωσης . Επομένως, ενώ οι αξιολογήσεις κινδύνου συμμόρφωσης πρέπει ασφαλώς να συνδέονται με τις διαδικασίες του επιχειρηματικού κινδύνου ή του κινδύνου εσωτερικού ελέγχου, απαιτούν γενικά μια πιο εστιασμένη προσέγγιση. Αυτό δεν σημαίνει ότι δεν μπορούν να ολοκληρωθούν ταυτόχρονα ή ότι πρέπει να καταβληθούν προσπάθειες. Πάραυτα οι περισσότεροι οργανισμοί μπορεί να είναι σε θέση να συνδυάσουν τις δραστηριότητες που υποστηρίζουν διάφορες αξιολογήσεις κινδύνου, ίσως μετά από μια αρχική διαδικασία ταυτοποίησης και αξιολόγησης του κινδύνου συμμόρφωσης.

Πηγή 12* *ΕΛΟΤ ISO 19600 :2014 σελ.13-14*

8.0 Business Case Study
Σκοπός της Μελέτης

Η μελέτη καταγράφει την συμμόρφωση εσωτερικών μονάδων του ομίλου ΠΑΠΑΔΟΠΟΥΛΟΣ Α.Ε στο πρότυπο ISO 22301 και συγκεκριμένα στην διεξαγωγή κοινής μεθοδολογίας Risk Assessments και κοινών ρόλων (Organization roles, responsibilities and authorities) όπως απαιτούν τα πρότυπα ISO 31000 (Annex B: integration into organizational processes) και ISO 22301 αντίστοιχα.

Η αναγκαιότητα στο να υπάρξει ενοποίηση με τις ίδιες κατηγορίες κινδύνων και αντίκτυπων (impact types) προήλθε και από απαιτήσεις multinational Company- Πελάτη όπου αιτήθηκε υπηρεσίες Πληροφορικής. Οι απαιτήσεις του Πελάτη για πιθανή διακοπή των μελλοντικών προσφερόμενων υπηρεσιών Πληροφορικής, λόγω σημαντικών απειλών (risks) εσωτερικών ή εξωτερικών, δημιούργησε την ευκαιρία στην Διεύθυνση Διαδικασιών και Ποιότητας (Process Improvement του Ομίλου ΠΑΠΑΔΟΠΟΥΛΟΣ Α.Ε) και με την ¨στρατηγική¨ βοήθεια του τμήματος Διαχείρισης Κινδύνων (Enterprise Risk Management) να αναλάβει τον συντονισμό, μέσα από διαδικασία Project Plan. Αναλύθηκαν και συμφωνήθηκαν κατά τη διάρκεια του Project μια σειρά προγραμματισμένων συναντήσεων με όλους τους βασικούς συντελεστές των υπευθύνων μονάδων ώστε να συμμορφωθούν στις αποκλίσεις που υπήρχαν.

Η μελέτη καταγράφει την συμμόρφωση κοινής μεθοδολογίας Risk Assessment καθώς και καταγραφής κοινής ονομασίας των ρόλων και της αρμοδιότητας αυτών.

8.1 Εισαγωγή

Ένα εταιρικό περιβάλλον που χρησιμοποιεί βασικά εργαλεία και εφαρμογές Πληροφορικής (IT) θα μπορούσε να εκτεθεί σε αρκετές πηγές πιθανών απειλών και συμβάντων διακοπής των υπηρεσιών που παρέχουν σε εσωτερικούς η εξωτερικούς πελάτες.

Παρακάτω περιγράφονται γενικές απειλές που προέρχονται από τις μελέτες των εσωτερικών μονάδων του ομίλου ΠΑΠΑΔΟΠΟΥΛΟΣ Α.Ε.

1. Έλλειψη εφεδρικού Data Center, για τις σημαντικές υποδομές της Πληροφορικής, η εγκατάσταση μιας και μόνο μονάδας μπαταριών

(UPS) ή η μοναδική παροχή ηλεκτρικής ισχύος, αποτελούν κινδύνους διακοπής των υπηρεσιών.

2. Γεωγραφικές απειλές που σχετίζονται με την υποδομή του Πληροφοριακού κέντρου όπου το σύνολο της εγκατάστασης μπορεί να είναι το μοναδικό σημείο αποτυχίας αν επηρεάζεται από ένα κίνδυνο όπως σεισμό.
3. Διαδικασία δημιουργίας αντιγράφων ασφαλείας με ασυνεπή δεδομένα. Αποτυχία συχνών αντίγραφων ασφαλείας, κακή καταγραφή ή παρακολούθηση, Ασυνεπή μεταφορά σε διαφορετικό χώρο των αντιγράφων ασφαλείας. Ασυνεπή αποθήκευση των αντιγράφων ασφαλείας, εν γένει απουσία Safe Boxes για τα αντίγραφα ασφαλείας.
4. Ανεπαρκή διαδικασία διαχείρισης αλλαγών. Η απουσία διασφάλισης ελέγχου των αλλαγών με προστασία των δεδομένων είναι μια συχνή αιτία των διακοπών και απώλεια δεδομένων λόγω ανθρώπινου λάθους, λάθη κώδικα, έλλειψη προγραμματισμού ή ανεπαρκείς δοκιμές, κλπ.
5. Απουσία ρύθμισης παραμέτρων των πληροφοριακών συστημάτων. Εξάρτηση από τη διαθεσιμότητα του καταρτισμένου προσωπικού είναι ένας κίνδυνος όταν δεν υπάρχει για βασικά συστήματα η τεκμηρίωση και οι οδηγίες.

Ο όμιλος ΠΑΠΑΔΟΠΟΥΛΟΣ Α.Ε μέσα από διενέργειες μελετών αξιολόγησε και δημιούργησε εφεδρικές εγκαταστάσεις σε δίκτυα, συστήματα Πληροφορικής και επένδυσε σε υποδομές ώστε να καλύψει τους πιθανούς κινδύνους. Δημιούργησε εσωτερικά οργανωτικές μονάδες υποστήριξης διαδικασιών και ελέγχων ώστε να εξασφαλίσει την ανθεκτικότητα των εσωτερικών του δραστηριοτήτων και την επιχειρησιακή συνέχεια.

Ο όμιλος ΠΑΠΑΔΟΠΟΥΛΟΣ Α.Ε είναι πιστοποιημένος στα περισσότερα ISO. Ένα από αυτά είναι το ISO 22301. Στο ISO 22301

εμπλέκονται μονάδες Πληροφορικής IT Service Continuity, Δικτύου Network, Επιχειρησιακής συνέχειας Business Continuity και Διαχείρισης Εταιρικών Κινδύνων Enterprise Risk Management. Στον οργανισμό διεξάγονται συστηματικά audits, re-certifications από εξωτερικούς ελεγκτές καθώς επίσης έλεγχος διαδικασιών από την εσωτερική μονάδα Process Improvement. Επίσης τρέχουν audits και από την μονάδα Εσωτερικού Ελέγχου σε συνεργασία και με εξωτερικούς φορείς.

Στους ελέγχους βασικός στόχος είναι να μη υπάρχουν αποκλίσεις από τα πρότυπα αλλά και τις επιμέρους μεθοδολογίες και διενέργειες που ακολουθούνται από τα assessments.

Business case

8.2 Project for a Multinational Company

Μια εταιρεία με δραστηριότητες σε αρκετές ευρωπαϊκές χώρες ζήτησε υπηρεσίες από τον όμιλο ΠΑΠΑΔΟΠΟΥΛΟΣ Α.Ε στα πλαίσια ενός outsourcing Project της. Βασική προϋπόθεση ήταν ο ΠΑΠΑΔΟΠΟΥΛΟΣ Α.Ε να είναι πιστοποιημένος στο ISO 22301 καθώς και σε 14000, 9000 κ.λπ.

8.2.1 Σημαντική Απαίτηση:

Σε περίπτωση εταιρικού κινδύνου του ομίλου ΠΑΠΑΔΟΠΟΥΛΟΣ Α.Ε από κυρίως εξωγενείς παράγοντες να μετακινηθούν όλες οι παρεχόμενες υπηρεσίες (συμπεριλαμβανομένου του εξοπλισμού των συστημάτων IT) ώστε να μπορούν να λειτουργήσουν οι IT εφαρμογές από άλλο χώρο από άλλη ευρωπαϊκή χώρα, για χάρη συντομίας, Run from Other Country (ROC).

8.3 Βασικές Απαιτήσεις

Παρατίθεται παρακάτω μέρος των απαιτήσεων του πελάτη σχετικά με το Business Continuity management & Service Continuity.

Business Service Continuity and Disaster Recovery Requirements and Responsibilities	PAPADOPOULOS A.E Group	Multinational Customer
1. Define Business Service Continuity and Disaster Recovery Services strategy, requirements and policies		
2. Recommend best practices for Business Service Continuity and Disaster Recovery Services strategies, policies, process and procedures		
3. Document Business Service Continuity and Disaster Recovery Services process and procedures that adhere to Multinational Customer requirements and policies		
4. Review and approve Business Service Continuity and Disaster Recovery Services procedures		
5. As needed, assist Customer in other Business continuity and emergency management activities		
6. Develop and maintain a detailed BC-DR plan to meet Business Service Continuity and Disaster Recovery requirements. Plan shall include plans for data, replication, backups, storage management and contingency operations that provide for recovering Customer's systems within established recovery requirement time frames after a disaster affects Customer's use of the Services.		
7. Define data (file system, database, flat files, etc.) replication, backup and retention requirements		
8. Realize the BC-DR Service, according to Technology Requirements (Schedule C11). Ensure the data replication is configured and on-going, as well as the necessary hardware and OS instances, Storage and LAN configuration are provisioned in the respective status to cover the BC-DR SLRs.		
9. Ensure that BC-DR setup and on-going support will always cover the respective SLRs (RTO and RPO)		
10. Establish processes to ensure BC-DR plans are kept up to date and reflect Changes in Customer environment		

11. Establish processes to ensure that BC-DR setup and realization is updated accordingly to the changes happening in the primary DC environment		
12. Establish procedures to ensure the impact to the BC-DR plans are reviewed by the Change Management process.		
13. Review and approve BC-DR plans		
14. Establish BC-DR test requirements		
15. Perform scheduled BC-DR tests per Customer policies		

Στις απαιτήσεις του Πελάτη υπήρχε και η επιμέρους απαίτηση να παρέχονται από τον όμιλο ΠΑΠΑΔΟΠΟΥΛΟΣ Α.Ε και οι αναφορές SOC1, SOC2.

8.4 Situation

Η κατάσταση ήταν η ακόλουθη:
Στις απαιτήσεις του πελάτη ο Όμιλος έπρεπε να ευθυγραμμίσει αρκετές εσωτερικές διαδικασίες καθώς επίσης και κοινή μεθοδολογία Risk Assessment. Να ορίσει ποια μονάδα χρειάζεται να εμπλακεί με την αρμοδιότητα του να παρέχει τα SOC reports και έπειτα να είναι σε θέση να προσφέρει τις υπηρεσίες IT στον πολυεθνικό Πελάτη.

Η μελέτη παρακάτω είναι για την συμμόρφωση της απόκλισης στα Risk Assessment που διεξάγονται από διαφορετικές μονάδες η οποία ήταν γνωστή λόγω audit του εσωτερικού ελέγχου.

Παραθέτω τις παρακάτω 2 εικόνες από έλεγχο της μονάδας Εσωτερικού Ελέγχου του ομίλου.

Priority	VERY HIGH

Απόκλιση 01	**Κίνδυνοι (Ρίσκα) / Ποσοτικοποίηση Επίδρασης Ευρημάτων**
Risk Assessments – Δεν ακολουθείται κοινή μεθοδολογία κατά τη διενέργεια Risk Assessments από εκπροσώπους των αρμόδιων επιχειρησιακών μονάδων *(Security, BCM, NT DR, IT DR) με βάση την πολιτική Enterprise Risk Management τμήματος*	
	Πρόταση (Recommendation Action)
	Να διαμορφωθεί από τις άμεσα εμπλεκόμενες επιχειρησιακές μονάδες νέα, κοινή μεθοδολογία διενέργειας Risk Assessments.

Πίνακας 1

Priority	VERY HIGH

Διερεύνηση Αιτιών (Root Cause Analysis)

Management Response/ Απάντηση - Σχέδιο Δράσης:
Έχει συμφωνηθεί από τις άμεσα εμπλεκόμενες επιχειρησιακές μονάδες να δημιουργηθεί κοινή μεθοδολογία διενέργειας Risk Assessments και εγκρίθηκε στο Board of Directors Q3 του έτους.

Αρμόδιος Υλοποίησης:	**Ημερομηνία Υλοποίησης**
Υποδιεύθυνση Enterprise Risk Management (Στρατηγική-καθοδήγηση)	Q3

Πίνακας 2

8.5 Actions

Συμφωνήθηκε σε βάθος χρόνου από τις μονάδες Επιχειρησιακής συνέχειας, It Disaster Recovery και με την καθοδήγηση της Enterprise Risk Management μονάδας να δημιουργηθεί κοινή μεθοδολογία που να εγκριθεί και να υλοποιηθεί από την μονάδα Διαδικασιών. Η ανάθεση των SOC reports ζητήθηκε να τρέχει από το τμήμα των Διαδικασιών και Ποιότητας (Process Improvement).

Παράλληλα ο Πελάτης είχε απαιτήσεις, με βάση τις αρχές του προτύπου ISO 22301, όπου έπρεπε να:

Α) Να υπάρχουν διακριτοί ρόλοι, ρόλοι και ευθύνες με μορφή RACI (Responsible Accountable Consulted Information) Model, να έχει RTO (Recovery Point Objective) 6 ώρες και RPO (Recovery Point Objective) 1 ώρα αντίστοιχα.

Β) Για τη συνέχιση των υπηρεσιών πληροφορικής να δημιουργηθεί Risk Assessment, με πιθανούς εταιρικούς, επιχειρησιακούς κινδύνους ώστε να καταγραφούν και να αναλυθούν, με πιθανότητα εμφάνισης, σε εργαλείο του IT για να μπορούν να αξιολογηθούν από τον πελάτη.

9.0 Δημιουργία Έργου (BCM Lifecycle)

9.1 Φάση 1 Σκοπός του Έργου

Για το έργο ζητήθηκε να αναπτυχθεί μια συνεπής δομή (framework), η οποία να καθιστά εύκολη την οργάνωση και τη διεξαγωγή των μελλοντικών Risk Assessments.
Ανατέθηκε στο IT να τρέξει τη μελέτη για το Risk Assessment σε συνεργασία με τις άλλες εσωτερικές μονάδες, καθώς και να δημιουργηθούν ρόλοι βάση του προτύπου. Το IT είχε πιστοποιηθεί με το πρότυπο του ISO 22301 και με βάση το BCM Lifecycle ανέπτυξε, εκτός του BIA, την μεθοδολογία του Risk Analysis μόνο για IT κινδύνους.

Ακολουθεί εικόνα του Business Continuity Lifecycle

Πηγή *13 https://stmaartennews.com/business/ready-part-two/

BCM Lifecycle

Το έργο είχε ανατεθεί για συντονισμό στην Υποδιεύθυνση Διαχείρισης Συστημάτων Ποιότητας Ομίλου ΠΑΠΑΔΟΠΟΥΛΟΣ Α.Ε για να υλοποιηθεί επίσημη διαδικασία στο Process Tool.
Σε αυτές τις απαιτήσεις οι μονάδες που αναφέρονται στον πίνακα 1 έπρεπε να συμμετάσχουν σε μια σειρά ενεργειών όπως η εκτίμηση πιθανότητας, επικινδυνότητας εταιρικών κινδύνων/γεγονότων, για την συνέχιση/μεταφοράς των υπηρεσιών των συστημάτων του πελάτη.

9.2 Φάση 2 Κοινή Μεθοδολογία

Αρχικά παρουσιάζονται τα συγκεκριμένα βήματα, όπως περιγράφονται παρακάτω

9.3 Πρώτο Βήμα:

Η μεθοδολογία που επιλέχθηκε για να εκτελέσει την αξιολόγηση κινδύνου πρέπει να έχει κοινά χαρακτηριστικά δηλαδή κοινή ονομασία και μεθοδολογία (Risk Terminology & Framework).

9.4 Δεύτερο Βήμα:

9.4.1 The risk assessment areas

Στο IT disaster recovery, συνήθως εστιάζουμε σε ένα ή περισσότερα από τα ακόλουθα τέσσερα σενάρια κινδύνου, η απώλεια των οποίων θα είχε αρνητικό αντίκτυπο στην ικανότητα του οργανισμού να συνεχίσει τις επιχειρηματικές δραστηριότητες του:

- Loss of data
- Loss of IT function
- Loss of skills
- Loss of Access to premises

Τα Risk assessments επικεντρώνονται στους IT κινδύνους που μπορούν να οδηγήσουν σε αυτά τα αποτελέσματα.

Μεθοδολογία που το IT έτρεχε risk assessment εικονογραφείται στον παρακάτω πίνακα 2.1

Βασικοί κίνδυνοι διακοπής λειτουργίας με πιθανότητα εμφάνισης ενός συμβάντος καθώς και τη σοβαρότητα του συμβάντος (π.χ. ζημιά στην επιθυμητή διαδικασία), εκτιμούσαν την ευπάθεια μιας επίπτωσης και κατάσταση δυσλειτουργίας της επιχείρησης.

9.5 Τρίτο βήμα:

Δημιουργείται πίνακας τιμών και υπολογίζεται το πιθανό risk.

Το εργαλείο του IT είχε forms για το risk evaluation του business continuity όπως το παρακάτω:

Risk = Likelihood x Severity x Vulnerability

Situation	Likelihood	Severity	Vulnerability	Calculated Risk
Fire	0.3	0.7	0.2	0.042
Hurricane	0.7	0.9	0.4	0.25
Theft	0.5	0.3	0.6	0.09

Virus attack	0.6	0.8	0.4	0.19
Data Loss	0.2	0.7	0.3	0.042

Πίνακας 2.1

Likelihood: 0 = Not likely to 1 = 100% likely to occur

Severity: 0 = No impact to 1 = Total destruction

Vulnerability: 0 = None to 1 =Totally vulnerable

Για παράδειγμα ο αριθμός 0.042 κινδύνου στο παράδειγμα "Fire" είναι ότι υπάρχει μια πιθανότητα 0.3 στο έτος να συμβεί πυρκαγιά που προκαλεί σημαντική ζημιά με βαθμό 0.7 και αντίκτυπο 0.2 με βάση την υπάρχουσα εκτίμηση.

Ακολούθως, αναφέρεται ο αντίκτυπος (με scorecard) στις λειτουργίες του ΠΑΠΑΔΟΠΟΥΛΟΣ Α.Ε με την πιθανότητα εμφάνισής των συμβάντων για τα επόμενα 5 χρόνια, όσο θα ήταν η συμβατική υποχρέωση με το πελάτη. Στο τέλος αυτού του εγγράφου, παρέχονται οθόνες υπολογισμού της μελέτης εκτίμησης κινδύνου.

Επίσης για τους ρόλους (μοντέλο RACI), συμφωνήθηκε με τον πελάτη και απαντήθηκε (Annex A) μόνο για RA.

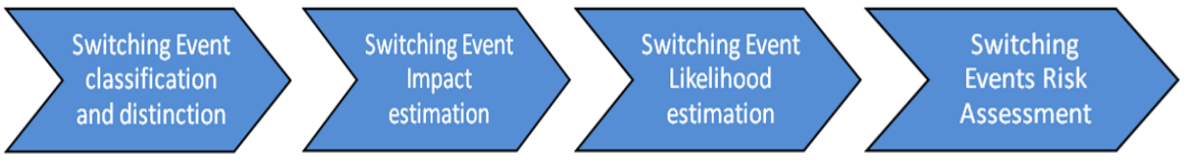
9.6 Φάση 3 Διεξαγωγή Workshops

9.7 Workshop 1

Συμφωνήθηκαν να αποτυπώνονται ανά workshop συγκεκριμένα βήματα όπως

Situation (Υπάρχουσα κατάσταση), Actions (Ενέργειες), Results (Αποτελέσματα)

Η ακολουθούμενη προσέγγιση ανά περιοχή συμφωνήθηκε και απεικονίζεται στο παρακάτω διάγραμμα ροής.



Στην μελέτη του Risk Assessment για την πιθανή μεταφορά των συστημάτων δημιουργήθηκαν κάποιες παραδοχές (assumptions)

Η διάρκεια του χρόνου απόφασης για μεταφορά των συστημάτων σε άλλη χώρα παρέμεινε στην ευθύνη του πελάτη όπου μετά το τέλος 7 ημερών θα μπορούσε να εγείρει την ενεργοποίηση του πλάνου μεταφοράς.

Ως "εναλλαγή" (Switching) νοείται η διαδικασία αλλαγής του Primary Data Center (PDC στην Ελλάδα) στο Secondary Data Center (SDC ευρωπαϊκής χώρας) και του SDC είτε στο PDC στην Ελλάδα είτε σε μια εναλλακτική τοποθεσία, σύμφωνα με τις απαιτήσεις αρχικές απαιτήσεις.

Τα γεγονότα της ενεργοποίησης του προγράμματος Switching για την μεταφορά συστημάτων, παρατίθενται παρακάτω, να είναι συμφωνηθέντα από κοινού μεταξύ του Multinational Customer και του ΠΑΠΑΔΟΠΟΥΛΟΣ Α.Ε. (Mutual agreement)

9.8 Workshop 2

Κατάσταση: Για το παραπάνω χαρακτηρισμό δεν υπήρχαν στρατηγικοί κίνδυνοι (event names).

Ενέργεια: Η επιχειρησιακή μονάδα Enterprise risk management πρότεινε τα πιθανά Στρατηγικά σενάρια κινδύνου/events και που παρουσιάζεται παρακάτω.

Αποτέλεσμα: Να είναι μετρήσιμοι κίνδυνοι που υπάρχει πιθανότητα να συμβούν.

Switching Event Id	Switching Event Name	Description
SE1	**Nationalization**	The Nationalization of the Supplier
SE2	**Material Service Level Failure**	A Material Service Level Failure caused in whole or in part (whether directly or indirectly) by instability resulting in actual or threatened disruption in Greece.
SE3	**Civil commotion**	Civil commotion and/or disruption in business critical utilities and other services (including telecommunications and power services) caused in whole or in part (whether directly or indirectly) by instability resulting in actual or threatened imminent disruption to the provision of the Services or degradation in Service Levels.
SE4	**Fuel shortage**	Fuel shortage(s) for one week during which time the Supplier is unable to re-fill the generator fuel tanks from its own fuel inventories.
SE5	**Power outages**	Country-wide power outages for an aggregate period of ten (10) days within any period of thirty (30) days
SE6	**Telco black-out**	Country-wide telecommunication lines black-out for an aggregate period of seven (7) days within any period (30) days
SE7	**Europe exit**	Exit of Greece from the European Union.
SE8	**Eurozone exit**	Exit of Greece's currency from the Eurozone area.
SE9	**Access to Customer**	The unauthorized access by a Greek Government Body to customer assets and/or the services provided by Customer to its End Users

Πίνακας 3

1. SE1- Εθνικοποίηση
2. SE2- Επίπεδο αποτυχίας υλικού
3. SE4- Αστική αναταραχή
4. SE4- 'Ελλειψη καυσίμων
5. SE5 Διακοπές ρεύματος
6. SE6 Διακοπές Τηλεπικοινωνιών
7. SE7 Έξοδος από την Ευρώπη
8. SE8 Έξοδος από την Ευρωπαϊκή Ένωση

9. SE9 Πρόσβαση στον πελάτη

9.9 Workshop 3

Κατάσταση: Για το παραπάνω χαρακτηρισμό δεν υπήρχε εκτίμηση κινδύνου (impact estimation).

Ενέργεια: Δημιουργήθηκαν περιοχές που μπορεί να είχαν αντίκτυπο στον πελάτη

Software Assets - Επιπτώσεις στα περιουσιακά στοιχεία λογισμικού
Operation Impact-Επιπτώσεις στην λειτουργία
Impact on PAPADOPOYLOS A.E Service-επιπτώσεις στις υπηρεσίες ΠΑΠΑΔΟΠΟΥΛΟΣ Α.Ε.
Data Center / Infrastructure Assets - Επιπτώσεις στο PDC / Περιουσιακά Στοιχεία Υποδομής
Replacement Value Range-Εύρος τιμής αντικατάστασης
Impact on PAPADOPOYLOS A.E Service- επιπτώσεις στις υπηρεσίες ΠΑΠΑΔΟΠΟΥΛΟΣ Α.Ε
Operation Impact- Επιπτώσεις στην λειτουργία
Service Assets - Αντίκτυπος σε στοιχεία παρεχόμενων υπηρεσιών
Impact on PAPADOPOYLOS A.E Service- επιπτώσεις στις υπηρεσίες ΠΑΠΑΔΟΠΟΥΛΟΣ Α.Ε.

Αποτέλεσμα: Να είναι κίνδυνοι τέτοιοι ώστε να υπάρχει πιθανός αντίκτυπος.

10.0 Workshop 4

Κατάσταση: Για το παραπάνω δεν υπήρχε πιθανότητα σε 5 έτη.

Ενέργεια: Το IT πρότεινε μια κλίμακα βαθμολόγησης που παρουσιάζεται παρακάτω.

Αποτέλεσμα: Να οδηγεί σε scorecard ώστε να μπορεί να αξιολογηθεί.

Η περίοδος πιθανότητας εκτείνεται σε 5 χρόνια. Η ανάλυση για τον υπολογισμό της πιθανότητας ήταν καθοδηγούμενη από τις εμπειρίες, με αρκετά ιστορικά δεδομένα, που θα μπορούσαν να οδηγήσουν στην ενεργοποίηση ¨ROC¨ στα τα επόμενα 5 χρόνια. Ως εκ τούτου, χρησιμοποιήθηκε κλίμακα 5 επιπέδων για τον προσδιορισμό της πιθανότητας και απεικονίζεται στον παρακάτω πίνακα. Κάθε τιμή πιθανότητας συνδέθηκε με ένα σκορ, που κυμαίνεται έως 5 με πολύ μεγάλη πιθανότητα, έως 1 με πολύ χαμηλή πιθανότητα.

Switching Event Likelihood for the next 5 years	Score
Very High	**5**
High	**4**
Medium	**3**
Low	**2**
Very Low	**1**

Αποτέλεσμα: Να είναι κίνδυνοι τέτοιοι ώστε να υπάρχει πιθανός αντίκτυπος.

10.1 Workshop 5

Κατάσταση: Για το παραπάνω υπήρχε εργαλείο και reporting από το IT.

Ενέργεια: Καμία αλλαγή.

Αποτέλεσμα: Το scorecard να δοθεί στον Πελάτη για να μπορεί να βαθμολογήσει τις περιοχές με επιπλέον κατάλογο των πιθανών IT συμβάντων που κατανεμήθηκε σε 2 μέχρι 3 κατηγορίες που επηρεάζουν τις παρεχόμενες υπηρεσίες του πελάτη.

10 .2 Workshop 6

Να τρέξει πιλοτικά από όλες τις εμπλεκόμενες μονάδες και έπειτα να δοθεί στον πελάτη.

Τα αποτελέσματα δίνονται παρακάτω από τους πίνακες

Likelihood	
Category	Score
Very High	5
High	4
Medium	3
Low	2
Very Low	1

Impact Scoring	
Score	Category
18	Very High
17	Very High
16	Very High
15	High
14	High
13	High
12	Medium
11	Medium
10	Medium
9	Low
8	Low
7	Very Low
6	Very Low

Και σε workshop που έγινε από όλες τις εμπλεκόμενες μονάδες δημιουργήθηκε το παρακάτω scorecard.

	Switching Event	PAPADOPOULOS A.E Nationalization	Material Service Level Failure	Civil commotion	Fuel shortage	Power outages	Telco black-out	Europe exit	Euro zone exit	Access to Multinational Customer
Score	Impact (out of 18)	6	14	17	17	18	18	7	7	8
	Likelihood (out of 5)	2	2	2	1	1	1	1	2	1

10 .3 Φάση 4 Alignment Workshops

Ο ΠΑΠΑΔΟΠΟΥΛΟΣ Α.Ε έπρεπε να αποδείξει βάσει των προτύπων ότι θα ανταποκρίνεται με συνέπεια ή θα ικανοποιεί τις απαιτήσεις του Multinational Ccustomer για τη συνέχιση των υπηρεσιών μετά από πιθανή αιτία δυσλειτουργίας.

Επίσης ο όμιλος έπρεπε να παραδώσει στον πελάτη τις μεθοδολογίες αλλά και τις πιστοποιήσεις για την επιβεβαίωση ότι έχει πολιτικές, στρατηγικές και συγκεκριμένα πλαίσια εργασίας (frameworks).

Το αποτέλεσμα του risk assessment συζητήθηκε με τις μονάδες και εμφανίσθηκε η απόκλιση σε σχέση με το ERM Strategy.

10.4 Alignment Workshop 1

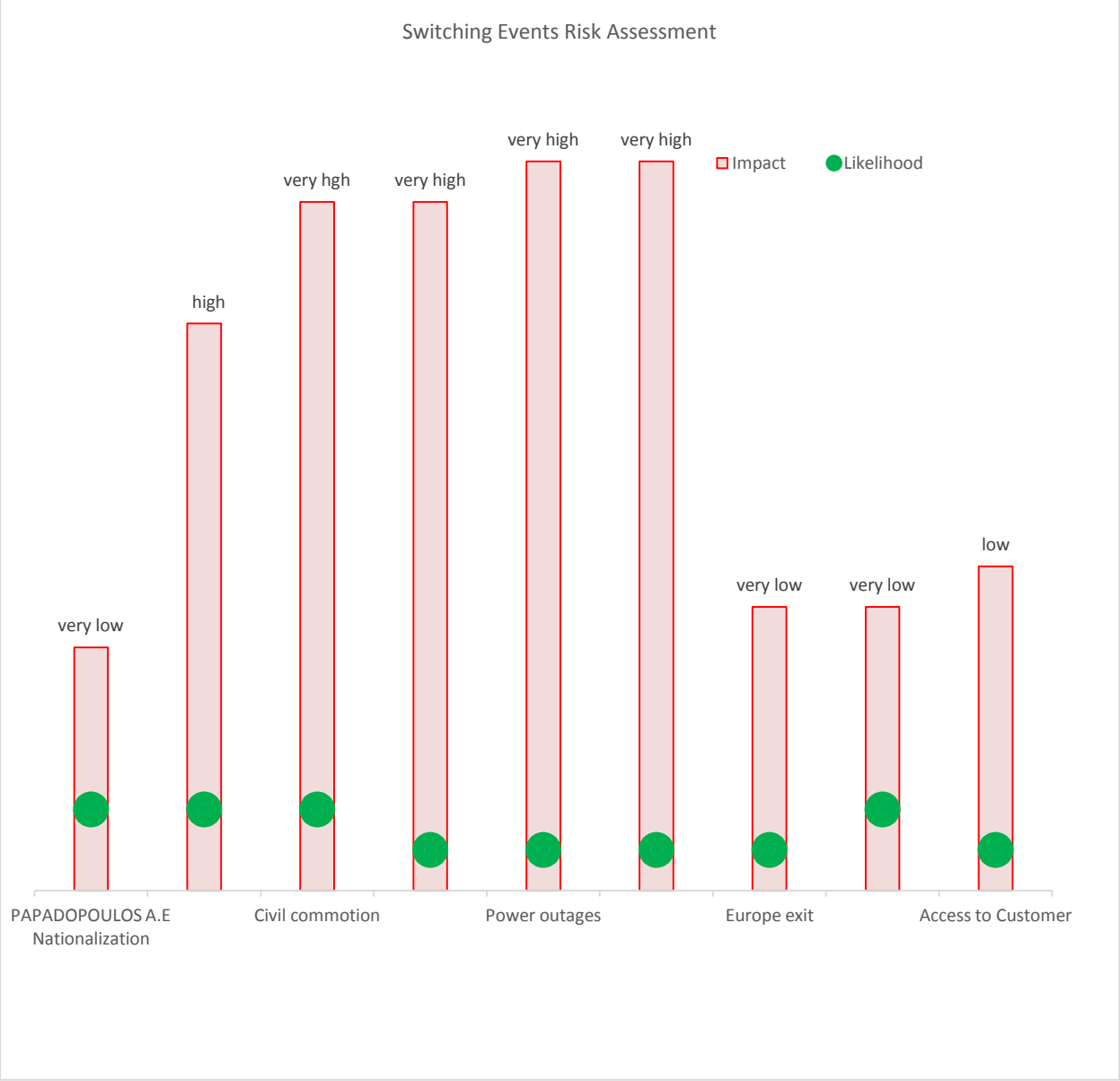
Οι βαθμίδες βαθμολόγησης δεν ήταν οι ίδιες σύμφωνα με την κλίμακα του ERM.

Switching Event Likelihood for the next 5 years	Score
Very High	5
High	4
Medium	3
Low	2
Very Low	1

Σε σχέση με το ERM όπου οι βαθμίδες έπρεπε να είναι 4 και έπρεπε να προσαρμοσθούν

Switching Event Likelihood for the next 5 years	Score
High	**4**
Medium	**3**
Low	**2**
Very Low	**1**

Επίσης η απόκλιση με την περιγραφή στα impact types ήταν διαφορετική όπως φαίνεται στον παρακάτω πίνακα



10.5 Alignment Workshop 2

Οι κατηγορίες θα έπρεπε να έχουν την ERM περιγραφή

Likelihood	
Category	**Score**
Very Critical	4
Critical	3
Middle	2
Small	1

Impact Scoring	
Score	**Category**
18	Very Critical
17	Very Critical
16	Very Critical
15	Critical
14	Critical
13	Critical
12	Middle
11	Middle
10	Middle
9	Small
8	Small
7	Small
6	Small

10. 6 Alignment Workshop 3

Συγκέντρωση όλων των μονάδων, re-define και αποδοχή των παραμέτρων και των βαθμίδων των εργαλείων της πληροφορικής. Δημιουργήθηκαν και έτρεξαν με την παρακάτω προτεραιότητα.

1) Υλοποίηση των 4 βαθμίδων στο Toolkit και δημιουργία νέου risk assessment workbook

Switching Event Id	Switching Event Description	Impact	Impact	Likelihood of Switching Event	Likelihood
SE1	PAPADOPOULOS A.E Nationalization	6	small	Low	2
SE2	Material Service Level Failure	14	critical	Low	2
SE3	Civil commotion	17	Very critical	Low	2
SE4	Fuel shortage	17	Very critical	Very Low	1
SE5	Power outages	18	Very critical	Very Low	1
SE6	Telco black-out	18	Very critical	Very Low	1
SE7	Europe exit	7	small	Very Low	1
SE8	Eurozone exit	7	small	Low	2
SE9	Access to Customer	8	small	Very Low	1

2) Προσδιορισμός του impact analysis με προσδιορισμό των impact κατηγοριών με πίνακα likelihood όπου συμφωνήθηκε και παρέμεινε ο ίδιος πίνακας

	Switching Event	PAPADOPOULOS A.E Nationalization	Material Service Level Failure	Civil commotion	Fuel shortage	Power outages	Telco black-out	Europe exit	Eurozone exit	Access to Ccustomer
Score	Impact									
	Likelihood									

3) Έτρεξε η βαθμολόγηση στο εργαλείο σε κάθε μία από τις κατηγορίες. Επιπλέον, χρησιμοποιήθηκε βαθμολογία 3 επιπέδων σε κάθε υποκατηγορία, από low (score = 1) έως high (score = 3). Για κάθε τιμή σκορ, δόθηκε μια εξήγηση στις εμπλεκόμενες ομάδες ώστε να κατανοήσει καλύτερα τα 3 διαφορετικά επίπεδα αντίκτυπου (low, medium, high). Οι κατηγορίες και οι

υποκατηγορίες, καθώς και τα χαρακτηριστικά βαθμολόγησης που χρησιμοποιήθηκαν στην ανάλυση επιπτώσεων αλλαγής συμβάντων παρουσιάζονται στον παρακάτω πίνακα:

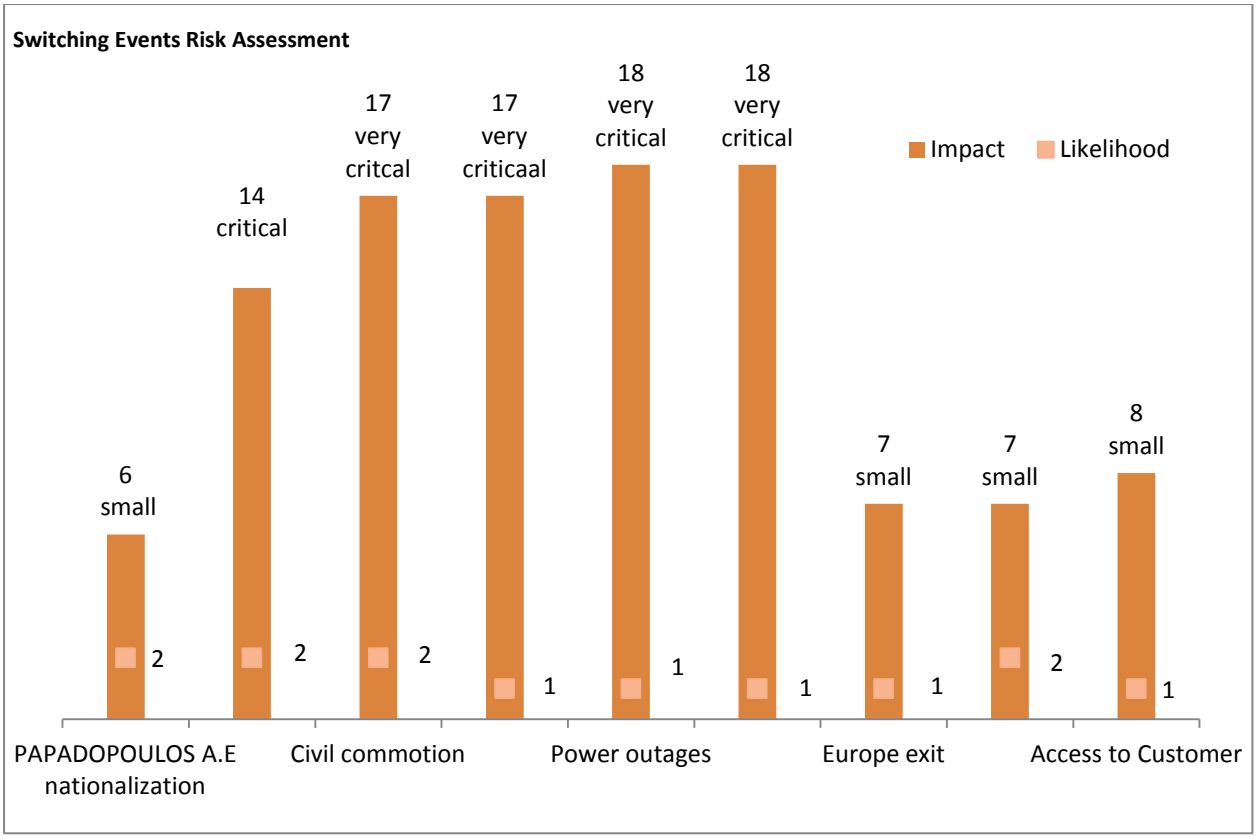
Impact Category	Impact Sub-category	Reason for No/ Low Impact (score=1)	Reason for Medium Impact (Score=2)	Reason for High Impact (Score=3)
Software Assets				
Software Assets	**Operation Impact**	Unavailability of the asset has no / minimal impact on internal operations	Unavailability of the asset has a moderate impact on internal operations	Unavailability of the asset has a severe impact on internal operations
Software Assets	**Impact on PAPADOPOULOS A.E Service**	Unavailability of the asset has No / minimal Impact on PAPADOPOYLOS A.E Services	Unavailability of the asset has moderate Impact on PAPADOPOULOS A.E Services	Unavailability of the asset has severe Impact on PAPADOPOULOS A.E Services
Data Center / Infrastructure Assets				
Data Center / Infrastructure Assets	**Replacement Value Range**	Replacement Value range in case of Asset's unavailability is Low	Replacement Value range in case of Asset's unavailability is Medium	Replacement Value range in case of Asset's unavailability is High
Data Center / Infrastructure Assets	**Impact on PAPADOPOULOS A.E Service**	Unavailability of the asset has No / minimal Impact on PAPADOPOULOS A.E Services	Unavailability of the asset has moderate Impact on PAPADOPOULOS A.E Services	Unavailability of the asset has severe Impact on PAPADOPOULOS A.E Services
Data Center / Infrastructure Assets	**Operation Impact**	Unavailability of the asset has no / minimal impact on internal operations	Unavailability of the asset has a moderate impact on internal operations	Unavailability of the asset has a severe impact on internal operations
Service type Assets				
Service type Assets	**Impact on PAPADOPOULOS A.E Service**	No / Minimal Impact	Limited impact on Operations (within the SLAs/ contracts/ regulatory requirements)	Significant impact on Operations (failing to meet SLAs/ regulatory requirements)

10.7 Alignment Workshop 4

Προσαρμόσθηκε το εργαλείο, σε σχέση με την πολιτική του Enterprise risk management, όπου αλλάχθηκαν οι βαθμίδες impact να είναι 4 που έχει το παρακάτω risk matrix.

Risk Matrix – Heat Map (Customer Computing Services)					
Switching Event Impact					
Very Critical (16-18)	**SE4 SE5 SE6**	**SE3**			
Critical (13-15)		**SE2**			
Middle (9-12)					
Small (6-8)	**SE7 SE9**	**SE1 SE8**			
	Very Low 0-5%	**Low 5-25%**	**Medium 25-50%**	**High 50-100%**	**Switching Event Likelihood (for the next 5 years)**

Με την ολοκλήρωση των αλλαγών παράχθηκε το παρακάτω γράφημα.



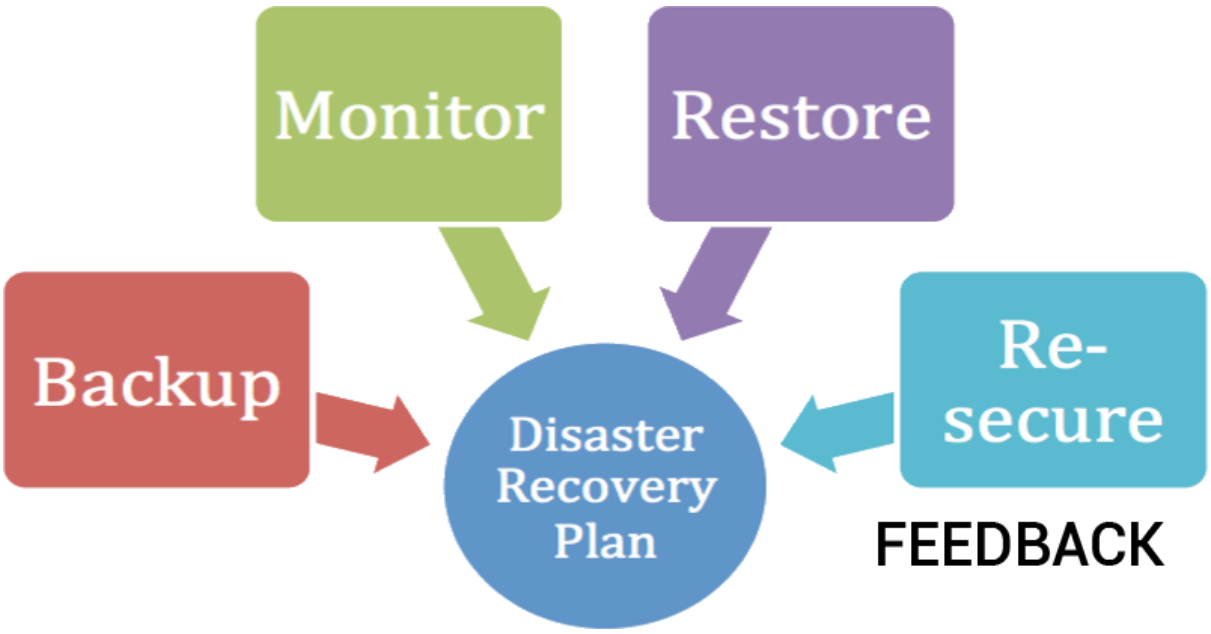
10.8 Alignment Workshop 5

Διαδικασία ενεργοποίησης και Ρόλοι

Το παρακάτω **διάγραμμα ροής** δίνει την επισκόπηση της διαδικασίας συμβάντων και παρουσιάζει τις ομάδες / άτομα που συμμετέχουν σε κάθε φάση.

• **Φάση ανίχνευσης και γνωστοποίησης συμβάντων** (ή διαχείρισης έκτακτων περιστατικών και κρίσεων) που ξεκινάει από την ανίχνευση και την ειδοποίηση συναγερμού και τελειώνει με την αξιολόγηση και κλιμάκωση

• **Φάση δήλωσης DR (Disaster Recovery)**: Ξεκίνησε η δυνατότητα αλλαγής των λεπτομερειών και έρχεται στη διαδικασία διαχείρισης κρίσεων από τον πελάτη και τον ΠΑΠΑΔΟΠΟΥΛΟΣ Α.Ε σχετικά με την ενεργοποίηση μερικής ή ολικής καταστροφής ή την επίτευξη κανονικής επίλυσης περιστατικών.

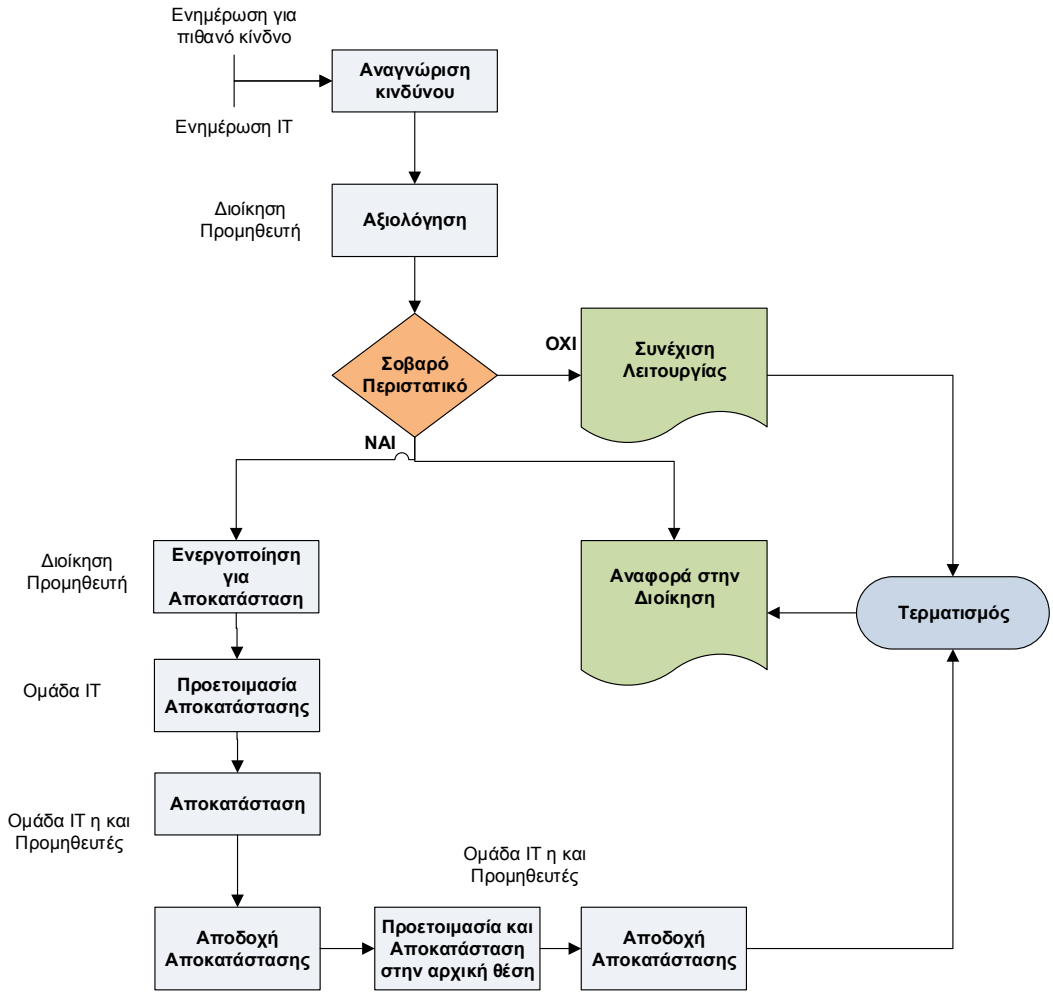


Πηγή14 * https://www.robicomp.com/alasan-mengapa-perusahaan-wajib-mengimplementasikan-disaster-recovery.html

• **Φάση προετοιμασίας και ενεργοποίησης DR** που μετά τη δήλωσή τους για καταστροφή οι Ομάδες DR (PAPADOPOULOS A.E και Multinational Customer ξεκινούν την προετοιμασία για ανάκτηση του συστήματος συγκεντρώνοντας και εκτελώντας όλες τις αντίστοιχες δραστηριότητες από το DRP)

• **Αποδοχή της Φάσης Ανάκτησης** όπου ελέγχονται οι Επιχειρηματικές Κρίσιμες Υπηρεσίες στο Κέντρο Ανάκτησης του ΠΑΠΑΔΟΠΟΥΛΟΣ Α.Ε για να διασφαλιστεί η σωστή λειτουργικότητα και απόδοση.

• **Επιστροφή και Αποδοχή Φάσης Επιστροφής** όπου η επιστροφή (αποτυχία) στον Χώρο Παραγωγής εκτελείται και γίνεται δεκτή



11.0 Team roles and responsibilities

11.1 Recovery Management Committee

Η Στρατηγική ανάκαμψης σε περίπτωση καταστροφών του Ομίλου υπαγορεύει ότι η Επιτροπή Διαχείρισης Ανάκτησης θα αποτελείται από τους Διευθυντές της Εταιρείας και τα αντίστοιχα στελέχη αντίστοιχα. Η επιτροπή θα περιλαμβάνει τους παρακάτω ρόλους

- Chief PAPADOPOULOS A.E and PAPADOPOULOS A.E IT Officer
- Multinational Customer Continuity Manager

- Multinational Customer Directors
- PAPADOPOULOS A.E IT Infrastructure Director
- Multinational Customer Security Policy & Business Continuity Director
- PAPADOPOULOS A.E IT Continuity Management Units

  Η Επιτροπή έχει την κυριότητα και την ευθύνη των αποφάσεων και είναι υπεύθυνη για:
  Αξιολόγηση της βαρύτητας ενός περιστατικού.
  Δήλωση της καταστροφής.
  Ενεργοποίηση του σχεδίου.
  Παροχή συγκατάθεσης για την επιστροφή των δραστηριοτήτων στον κύριο χώρο.
  Εξασφάλιση της υιοθέτησης της στρατηγικής.
  Προτεραιότητα και έγκριση των Σχεδίων και δαπανών DR.

11.2 PAPADOPOULOS A.E DR Team

Η Ομάδα Επιχειρήσεων αποτελείται από μηχανικούς που είναι υπεύθυνοι για τη διεξαγωγή διαδικασιών έκτακτης ανάγκης για κρίσιμα συστήματα, εξασφαλίζουν ότι οι οδηγίες υποδομής και λειτουργίας είναι σωστές και δίνουν συμβουλές για την κατάσταση παραγωγής και για τυχόν ασυνήθιστα προβλήματα που απαιτούν βοήθεια. Τα μέλη αυτής της ομάδας θα συμβάλλουν από την άποψη της υποδομής, του δικτύου και της αποθήκευσης. Οι διαφορετικοί ρόλοι στο πλαίσιο αυτού του συστήματος περιλαμβάνουν τα εξής:

- **Infrastructure responsible**

  Συμμετέχει στο σχεδιασμό / υλοποίηση όλων των συνιστωσών του συστήματος ανάκαμψης από δυσλειτουργία βάσει των απαιτήσεων του Πελάτη και των διαδικασιών επαναφοράς στο αρχικό στάδιο, καθώς και μελλοντικών αλλαγών / ενημερώσεων ή αναβαθμίσεων του συστήματος. Στα καθήκοντα του ρόλου συμπεριλαμβάνεται η δημιουργία πλάνου διαθεσιμότητας του συστήματος. Συμμετοχή έχουν επίσης οι εξής.1) Multinational customer Account Manager,2) Multinational Customer Service Delivery Manager, 3) Multinational customer service Delivery Manager.

11.3 Προμηθευτές

Οι προμηθευτές είναι οι εξωτερικές εταιρείες που παρέχουν υποστήριξη για την υποδομή του multinational Customer. Ανάλογα με την έκταση της καταστροφής και την ικανότητα των εσωτερικών ομάδων να επιλύσουν το ζήτημα, μπορεί να τους ζητηθεί να παράσχουν βοήθεια βάση της συμφωνίας που έχει υπογραφεί μεταξύ του ΠΑΠΑΔΟΠΟΥΛΟΣ Α.Ε και των προμηθευτών.

Πόρισμα

Σκοπός είναι στις εταιρείες η κυρίως αναγνώριση και η ανάδειξη των βασικών προϋποθέσεων για την μελλοντική δημιουργία των παρακάτω περιοχών:

- Στρατηγική αντιμετώπιση των πιθανών εταιρικών κινδύνων.
- Δημιουργία συμφωνιών/ασφαλίσεων ώστε να μετριάζονται οι πιθανοί κίνδυνοι.

Υπάρχουν βασικές κατηγορίες για την αντιμετώπιση των κινδύνων που οι εταιρείες πρέπει να λάβουν υπόψη

1. Κοινοποίηση: Τον εντοπισμό και προς άλλη οντότητα ώστε να απορροφήσει ένα μέρος του κινδύνου. Π.χ. χρησιμοποιώντας ασφάλιση των συστημάτων (SLA, IAAS) όπου συχνά θεωρείται χρήσιμη επιλογή.
2. Διατήρηση: Προθυμία να αποδεχθεί τον κίνδυνο και τα πιθανά αποτελέσματα.

Αυτές οι επιλογές μπορεί να ληφθούν υπόψη της επιχειρηματικής συνέχειας/αποκατάστασης από καταστροφή για σχεδιασμό στρατηγικών. Όσον αφορά στην αντιμετώπιση των κινδύνων, μπορεί να χρησιμοποιηθεί και η ακόλουθη κατηγοριοποίηση:

- Πρόληψης: υψηλής-πιθανότητας/υψηλού-αντίκτυπου γεγονότα (λειτουργούν ενεργά για να μετριάσουν των κίνδυνο).
- Αποδοχή: χαμηλής-πιθανότητας/χαμηλού-αντίκτυπου γεγονότα (διατήρηση και παρακολούθηση).
- Περιορισμός: υψηλής πιθανότητας /χαμηλού-αντίκτυπου γεγονότα (ελαχιστοποίηση της πιθανότητας εμφάνισης).

- Προσχεδιασμός: χαμηλής-πιθανότητας/υψηλού-αντίκτυπου γεγονότα (σχεδιασμένα βήματα για να μετριάσουν τον κίνδυνο, εάν αυτό συμβεί).

Annex A

Business Service Continuity and Disaster Recovery απαιτήσεις και ευθύνες μεταξύ του PAPADOPOULOS A.E GROUP και του Multinational Customer

Business Service Continuity and Disaster Recovery Requirements and Responsibilities	PAPADOPOULOS A.E Group	Customer
1. Define Business Service Continuity and Disaster Recovery Services strategy, requirements and policies		X
2. Recommend best practices for Business Service Continuity and Disaster Recovery Services strategies, policies, process and procedures	X	
3. Document Business Service Continuity and Disaster Recovery Services process and procedures that adhere to Customer requirements and policies	X	
4. Review and approve Business Service Continuity and Disaster Recovery Services procedures		X
5. As needed, assist Customer in other Business continuity and emergency management activities	X	
6. Develop and maintain a detailed BC-DR plan to meet Business Service Continuity and Disaster Recovery requirements. Plan shall include plans for data, replication, backups, storage management and contingency operations that provide for recovering Customer's systems within established recovery requirement time frames after a disaster affects Customer's use of the Services.	X	
7. Define data (file system, database, flat files, etc.) replication, backup and retention requirements		X

8. Realize the BC-DR Service, according to Technology Requirements (Schedule C11). Ensure the data replication is configured and on-going, as well as the necessary hardware and OS instances, Storage and LAN configuration are provisioned in the respective status to cover the BC-DR SLRs.	X	
9. Ensure that BC-DR setup and on-going support will always cover the respective SLRs (RTO and RPO)	X	
10. Establish processes to ensure BC-DR plans are kept up to date and reflect Changes in Customer environment	X	
11. Establish processes to ensure that BC-DR setup and realization is updated accordingly to the changes happening in the primary DC environment	X	
12. Establish procedures to ensure the impact to the BC-DR plans are reviewed by the Change Management process.	X	
13. Review and approve BC-DR plans		X
14. Establish BC-DR test requirements		X
15. Perform scheduled BC-DR tests per Customer policies	X	
16. Ensure that the test systems (in live status), which run permanently in the BC-DR site, are not affected by the annual BC-DR test	X	
17. Coordinate involvement of Customer end users for BC-DR testing		X
18. Coordinate involvement of all other parties for BC-DR testing	X	
19. Participate in BC-DR tests	X	X
20. Track and report BC-DR test results to Multinational customer	X	
21. Review and approve BC-DR testing results		X
22. Develop action plan to address BC-DR testing results	X	
23. Review and approve BC-DR testing action plan		X
24. Implement action plan and provide ongoing status until completion	X	

25. Initiate the BC-DR plan in the event of a Customer BC-DR situation per the BC-DR policies and procedures		X
26. Initiate the BC-DR plan in the event of a Provider BC-DR situation and notify Customer per BC-DR policies and procedures	X	
27. Coordinate with Customer during a Provider BC-DR situation per BC-DR policies and procedures	X	
28. Provide Customer access to Business Service Continuity and BC-DR reporting and monitoring systems and data	X	

Annex B

Παρακάτω περιγράφονται οι παράγραφοι του προτύπου που αναφέρουν τις απαιτήσεις που ήταν απαραίτητο να γίνουν ώστε να πραγματοποιηθούν οι ενέργειες.

2.14 Risk assessment
Overall process of risk identification (2.15), risk analysis (2.21) and risk evaluation (2.24)
[ISO Guide 73:2009, definition 3.4.1]
2.15 Risk identification
Process of finding, recognizing and describing risks (2.1)
NOTE 1 Risk identification involves the identification of risk sources (2.16), events (2.17), their causes and their
Potential consequences (2.18)
NOTE 2 Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and
Stakeholder's needs (2.13).
[ISO Guide 73:2009, definition 3.5.1]

Annex C

Ο ΠΑΠΑΔΟΠΟΥΛΟΣ Α.Ε είναι επίσης πιστοποιημένος σε ISO 31000 και έχει αναπτύξει ισχυρούς μηχανισμούς παρακολούθησης.

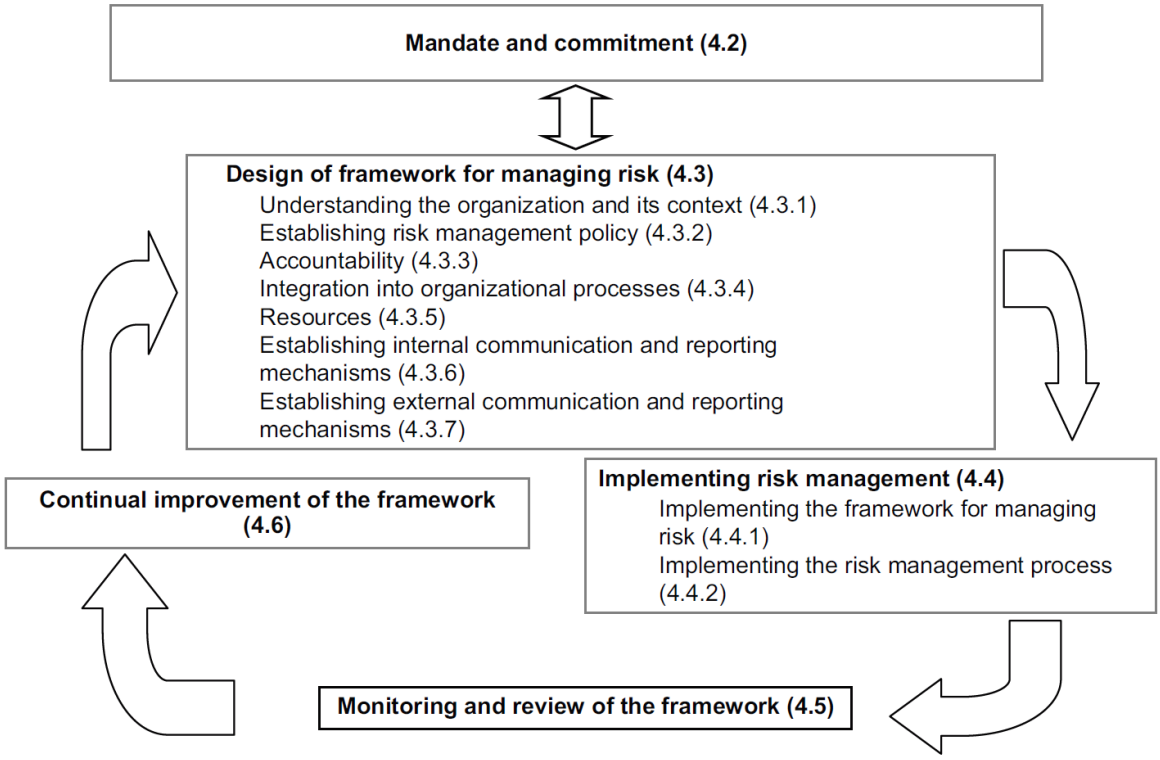


Figure 2 — Relationship between the components of the framework for managing risk

This framework is not intended to prescribe a management system, but rather to assist the organization to integrate risk management into its overall management system. Therefore, organizations should adapt the components of the framework to their specific needs.

If an organization's existing management practices and processes include components of risk management or if the organization has already adopted a formal risk management process for particular types of risk or situations, then these should be critically reviewed and assessed against this International Standard, including the attributes contained in Annex A, in order to determine their adequacy and effectiveness.

Πηγή 15 *https://www.researchgate.net/figure/Relationships-between-the-components-of-the-ISO-31000-framework-for-managing-risk_fig1_266318528

Βιβλιογραφία

Πηγές

2*: *Pas 99 (2012) σελ.16-20*

4*: *ISO 31000:2018*| *Risk Management - Guidelines*| *Main Changes vs 2009 edition σελ.2-8*

6* *ISO 9001:2015 σελ.17-19*

7*: *ISO 50001:2018 Energy Management Systems σελ. 10-12*

8*: ISO 14001:2015 – Environmental Management System σελ.19-20

9*: *ΕΛΟΤ ISO 22301:2014 σελ. 21*

10*: *OHSAS 18001 σελ. 8-10 & ISO 4 5001:2018 σελ. 11*

11 ISO 17025:2017 σελ.32*

12*: *ΕΛΟΤ ISO 19600:2014 σελ.13-14*

Διαδικτυακοί τόποι

1* https://www.researchgate.net/figure/The-risk-management-cycle_fig1_294894575

*3 * https://www.business2community.com/strategy/how-to-develop-a-risk-matrix-02234010*

5* https://imgbin.com/png/sfXBEW77/iso-31000-risk-management-international-organization-for-standardization-png

13* https://stmaartennews.com/business/ready-part-two/

14 * https://www.robicomp.com/alasan-mengapa-perusahaan-wajib-mengimplementasikan-disaster-recovery.html

15 *https://www.researchgate.net/figure/Relationships-between-the-components-of-the-ISO-31000-framework-for-managing-risk_fig1_266318528