Διαχείριση Ρίσκου σε Επιχειρήσεις

ISO 31000:2009

STAVROS IOAKIM

MSc Security & Risk Management
MSc Electrical Electronics Eng.
BSc Electrical Eng.
Business Continuity Institute Diploma

9 ΜΑΙΟΥ 2017

Η Αξία εφαρμογής Συστήματος Διαχείρισης Ρίσκων

ISO 31000: 2009

Η κάθε επιχείρηση, ανεξάρτητα από το μέγεθος της, πρέπει να διαχειρίζεται το κάθε ρίσκο.

Όταν γίνεται αντιληπτή η ύπαρξη ρίσκου, αυτό από μόνο του μπορεί να έχει θετικό αντίκτυπο στην Επιχείρηση.

Αντίληψη ύπαρξης ρίσκου – κουλτούρα.

Η Αξία εφαρμογής Συστήματος Διαχείρισης Ρίσκων

ISO 31000: 2009

Η διαχείριση του ρίσκου πρέπει να είναι μια ουσιαστική δραστηριότητα σε κάθε επιχείρηση.

Οι επιχειρήσεις που διαχειρίζονται τα ρίσκα τους αποτελεσματικά, ευημερούν, παράγουν προϊόντα και παρέχουν υπηρεσίες ψηλής ποιότητας.

Η εφαρμογή διαχείρισης ρίσκων σε μια επιχείρηση, πρέπει να να είναι αντιληπτή σε όλα τα επίπεδα της επιχείρηση.

ΡΙΣΚΟ

Για να αντιληφτούμε το πρότυπο είναι σημαντικό να αντιληφτούμε τον ορισμό του ρίσκου.

“ the effect of uncertainty on objectives”

Το αποτέλεσμα της αβεβαιότητας όσον αφορά την επίτευξη των στόχων της επιχείρησης (βραχυπρόθεσμων και μακροπρόθεσμων)

Effect – απόκλιση (θετικά ή/και αρνητικά) από το αναμενόμενο

Uncertainty – ανεπάρκεια να αντιληφτούμε ένα γεγονός (την πιθανότητα να συμβεί και αν συμβεί οι συνέπειες που θα προκύψουν)

“Πρέπει να αποδεχθούμε ότι μπορεί να συμβεί κάτι αναπάντεχο”.

Αριστοτέλης

Risk Management

Health and Safety

Security

Business Continuity

Legal & Regulatory compliance

Public Acceptance

Environmental Protection

Product – Service Quality

Project Management

Efficiency in Operations – Operation Risks

Governance & Reputations

Είδη Ρίσκων

Οικονομικής Φύσης (αγορά, πιστωτικό, συναλλαγματικό, επιτοκιακό)

Λειτουργικής Φύσης (ανθρώπους, συστήματα, διαδικασίες, νομικά θέματα, εξωτερικά γεγονότα)

Ανθρώπους - λανθασμένη καταγραφή εμπορικών συναλλαγών /λογιστικών γεγονότων, εσφαλμένη υποβολή δηλώσεων φόρου, απάτες, καταχρήσεις, δόλιες ενέργειες …

Συστήματα - λανθασμένη ή καθυστερημένη παροχή πληροφοριών στους χρήστες των χρηματοοικονομικών καταστάσεων, πτώση του IT συστήματος σε ώρα εργασίας …

Είδη Ρίσκων

Διαδικασίες - ελλιπής καθοδήγηση των υπαλλήλων για το πώς διεκπεραιώνονται οι διαδικασίες που σχετίζονται με το αντικείμενο της εργασίας τους

Νομικό ρίσκο - ατελής διατύπωση όρων σε συμβόλαια

Εξωτερικά γεγονότα – καταστροφές των περιουσιακών στοιχείων της επιχείρησης που μπορεί να οφείλονται σε φυσικά αίτια π.χ πυρκαγιές, πλημμύρες κ.λ.π. ή στον ανθρώπινο παράγοντα π.χ ληστείες, διαρρήξεις, βανδαλισμοί

Προτεινόμενος τρόπος αντιμετώπισης του ρίσκου

ΤΡΙΠΤΥΧΟ:

- Προσδιορισμός (αναγνώριση, μέτρηση , διαχωρισμός προτεραιοτήτων)
- Διαχείριση
- Επικοινωνία (δηλαδή με την υπόδειξη της εφαρμογής της διαχείρισης του, εκ μέρους όλων των ενδιαφερομένων)

Απαιτήσεις του Προτύπου

Γενικά η διαδικασία εφαρμογής του προτύπου περιλαμβάνει τα εξής:

α) την απόκτηση εντολής και δέσμευσης

β) μια ανάλυση των ελλείψεων - gap analysis

γ) προσαρμογή με βάση τις ανάγκες της επιχείρησης και την κουλτούρα της ώστε να δημιουργεί αξίας

δ) αξιολόγηση των ρίσκων που συνδέονται με αλλαγές (μετάβαση από μια κατάσταση σε άλλη)

Απαιτήσεις του Προτύπου

ε) την ανάπτυξη ενός πλάνου για το έργο (ISO 31000)

- Θέτοντας στόχους, προτεραιότητες και μετρήσεις

- Business Case – γιατί να εγκατασταθεί το πρότυπο στον οργανισμό, συμπεριλαμβανομένης της ευθυγράμμισης του με τους στόχους του οργανισμού

- Τον καθορισμό του πεδίου εφαρμογής, την ευθύνη για το έργο, χρονοδιάγραμμα και πόρους

στ) προσδιορισμό του πλαισίου της εφαρμογής, συμπεριλαμβανομένης της επικοινωνίας με τους ενδιαφερόμενους φορείς.

Πλαίσιο Εργασίας

Είναι σημαντικό να λαμβάνονται υπόψη

- τυχόν νομικές υποχρεώσεις
- κανονιστικές υποχρεώσεις προς τον πελάτη
- απαιτήσεις πιστοποίησης που προκύπτουν από τυχόν συστήματα διαχείρισης και προτύπων που η επιχείρηση έχει επιλέξει να υιοθετήσει.

Πλαίσιο Εργασίας

Είναι σημαντικό να λαμβάνονται υπόψη τόσο η υφιστάμενη διαδικασία που χρησιμοποιείται για τη διαχείριση των ρίσκων και οι πτυχές του υφιστάμενου πλαισίου διαχείρισης

Πρέπει να θεσπιστούν κατάλληλα κριτήρια ρίσκου

Τα κριτήρια ρίσκου πρέπει να είναι ευθυγραμμισμένα με τους στόχους του οργανισμού

Εάν οι στόχοι αλλάζουν, τα κριτήρια ρίσκου θα πρέπει να προσαρμόζονται ανάλογα

Εξωτερικό Περιβάλλον

Κοινωνικό

Πολιτιστικό

Πολιτικό

Νομικό

Κανονιστικό

Οικονομικό

Τεχνολογικό

Το ανταγωνιστικό περιβάλλον (Διεθνή – Τοπικό)

Εσωτερικό Περιβάλλον

Πληροφορίες για τη εσωτερική διακυβέρνηση της Επιχείρησης

Δομή της Επιχείρησης

Ρόλους και Ευθύνες

Ικανότητες

Εσωτερικά ενδιαφερόμενα μέρη

Συστήματα

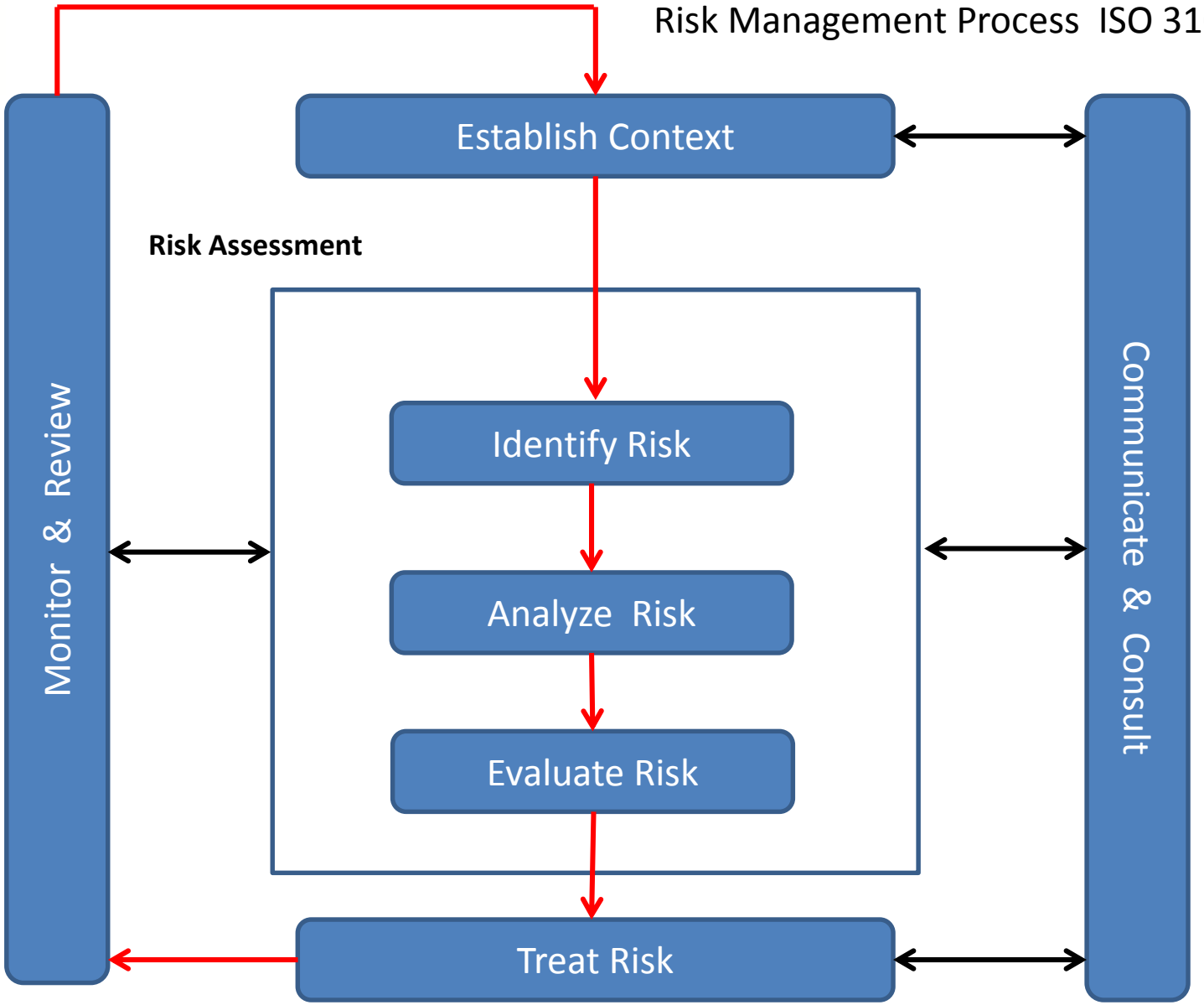
Κουλτούρα του οργανισμού

Πλαίσιο για τη Διαχείριση του Ρίσκου

Οι Αρχές του Risk Management

Η Διαχείριση Ρίσκου – Αρχές

1. Δημιουργεί και Προστατεύει την αξία
2. Είναι αναπόσπαστο μέρος των διεργασιών της Επιχείρησης
3. Είναι μέρος των αποφάσεων εντός της Επιχείρησης
4. Καθορίζει κάτι το οποίο είναι αβέβαιο
5. Είναι συστηματική και Δομημένη
6. Βασίζεται στην καλύτερη δυνατή πληροφόρηση
7. Είναι προσαρμοσμένη
8. Λαμβάνει υπόψη την κουλτούρα και τον ανθρώπινο παράγοντα
9. Είναι διαφανής και περιεκτική
10. Είναι δυναμική, επαναλαμβανόμενη και ανταποκρίνεται στις αλλαγές
11. Διευκολύνει τη συνεχή βελτίωση της Επιχείρησης


Risk Management Process ISO 31000
Establish Context
Risk Assessment
Identify Risk
Analyze Risk
Evaluate Risk
Treat Risk
Monitor & Review
Communicate & Consult

Risk Assessment


Backspace
Delete
End
Thanks!