Φραγκουλόπουλος Γιάννης,
Manager, Advisory Services
at Ernst & Young

Τρίπτυχο Governance, Risk Management and Compliance (GRC): Μεγιστοποίηση της Αξίας για τον Οργανισμό

Οι εταιρείες σήμερα εξαρτώνται ολοένα και περισσότερο από το τρίπτυχο GRC (Governance, Risk management and Compliance) προκειμένου να εξασφαλίσουν αποτελεσματική διαχείριση κινδύνων στις επιχειρηματικές τους δραστηριότητες.

Ωστόσο, στο υφιστάμενο επιχειρησιακό περιβάλλον, το οποίο χαρακτηρίζεται από ολοένα και περισσότερες προκλήσεις, η λειτουργία GRC για τους περισσότερους μεγάλους Οργανισμούς πασχίζει να φέρει την προσδοκώμενη αξία τόσο κατά την εκπλήρωση των δραστηριοτήτων του όσο και ως προς την εξοικονόμηση πόρων.

Η εμπειρία μας στην επιτυχημένη εφαρμογή συμβουλευτικών υπηρεσιών στην ευρεία βάση των πελατών μας, μας επιτρέπει να αναγνωρίσουμε τους παρακάτω άξονες ως τους πιο σημαντικούς για το μετασχηματισμό του GRC πλαισίου το οποίο μεγιστοποιεί την αξία για τον Οργανισμό[1].

- Ολιστική προσέγγιση για τη διαχείριση κινδύνων
- Απλοποίηση των διαδικασιών που σχετίζονται με GRC
- Υιοθέτηση GRC τεχνολογιών

Ολιστική Προσέγγιση για τη Διαχείριση Κινδύνων

Παραδοσιακά, ο πρωταρχικός στόχος του Πλαισίου GRC ήταν να εστιάσει σε διαδικασίες συμμόρφωσης που άπτονται των οικονομικών στοιχείων και του ευρύτερου κανονιστικού πλαισίου οι οποίες (ανάλογα και με το μέγεθος και τον τύπο του Οργανισμού) αποτελούσαν κυρίως ευθύνη του Εσωτερικού Ελέγχου, της Κανονιστικής Συμμόρφωσης ή της Διαχείρισης Επιχειρησιακών Κινδύνων (Enterprise Risk Management, ERM).

Πριν ακόμα κάθε Οργανισμός ευθυγραμμίσει τις προαναφερθείσες λειτουργίες ώστε να δημιουργηθούν οι συνθήκες για ένα αποδοτικό Πλαίσιο GRC πρέπει πρώτα να κατανοήσει με σαφήνεια τους τύπους των κινδύνων που αντιμετωπίζει. Το πλαίσιο διαχείρισης κινδύνων Robert Kaplan και Anette Mikes2 καθορίζει τρεις διακριτές κατηγορίες κινδύνων και δυνητικών τρόπων διαχείρισης τους:

• **Κίνδυνοι που μπορεί να προληφθούν** - Χρηματοοικονομικοί και λειτουργικοί κίνδυνοι τους οποίους ο Οργανισμός προσπαθεί να εξαλείψει, αποφύγει, μετριάσει, ή να μεταφέρει με έναν πιο οικονομικά αποδοτικό τρόπο. Οι επιπτώσεις που θα προκληθούν από την εμφάνιση κινδύνων αυτής της κατηγορίας αφορούν οικονομικά πρόστιμα και αρνητική επίπτωση στη φήμη του Οργανισμού.

• **Στρατηγικοί κίνδυνοι** – Απορρέουν από τις στρατηγικές αποφάσεις της ανώτερης Διοίκησης (για παράδειγμα ανάπτυξη μέσω εξαγορών, επέκταση σε αναδυόμενες αγορές, κ.ά.). Η λειτουργία μιας επιχείρησης συνδέεται με την ανάληψη κινδύνου. Ωστόσο, ο Οργανισμός επιδιώκει να επωφεληθεί από την ανοδική δυναμική των κινδύνων, αποφεύγοντας παράλληλα την αρνητική επίπτωση αυτών. Συνεπώς, η εξάλειψη αυτών των κινδύνων ή η μεταφορά τους ουσιαστικά δεν αποτελεί επιλογή.

• **Εξωτερικοί κίνδυνοι** – Οι οποίοι είναι έξω από τον έλεγχο του οργανισμού (φυσικές καταστροφές, μακροοικονομικοί παράγοντες, κ.ά.), Η ορθή αντιμετώπιση τέτοιου είδους κινδύνων είναι ο περιορισμός στην έκθεση τους, εφόσον συμβεί ένα τέτοιο γεγονός.

Εφόσον ο Οργανισμός κατανοήσει τους τύπους των κινδύνων που αντιμετωπίζει έχει τη δυνατότητα να τους διαχειριστεί επαρκώς σχεδιάζοντας τον τρόπο απόκρισης σε κάθε τέτοιο τύπο κινδύνου καθώς και τις αντίστοιχες δικλείδες ασφαλείας. Όταν αυτό υλοποιηθεί, ο Οργανισμός θα πρέπει να ευθυγραμμίζει τις λειτουργίες του με τους στρατηγικούς κινδύνους που αντιμετωπίζει καθώς και τα κριτήρια μέτρησης της απόδοσής του συνθέτοντας μια ολιστική προσέγγιση η οποία μπορεί να βελτιστοποιήσει την επενδυτική του στρατηγική, την κατανομή κεφαλαίων καθώς επίσης τον εντοπισμό περιοχών προς βελτίωση.

Απλοποίηση των Διαδικασιών που Σχετίζονται με GRC

Οι Οργανισμοί εξακολουθούν να επενδύουν

σε νέες τεχνικές όπως, advanced analytics και τεχνολογίες GRC, προκειμένου να βελτιώσουν τις διαδικασίες διαχείρισης κινδύνων (χρηματοοικονομικών, λειτουργικών και κινδύνων συμμόρφωσης). Ωστόσο, για τη διαχείριση στρατηγικών κινδύνων οι περισσότεροι Οργανισμοί εξακολουθούν να λειτουργούν με βάση τα παραδοσιακά ERM μοντέλα για τα οποία συχνά παρατηρούμε ότι δεν έχουν ευθυγραμμιστεί με την τρέχουσα επιχειρησιακή στρατηγική καθώς και την αποδεκτή έκθεση στον κίνδυνο από τον Οργανισμό. Με την ευθυγράμμιση των πολλαπλών λειτουργιών που σχετίζονται με τη διαχείριση στρατηγικών κινδύνων και κινδύνων που μπορούν να προληφθούν καθώς και με την τυποποίηση βασικών στοιχείων των σχετικών διαδικασιών η λήψη αποφάσεων θα καταστεί πιο γρήγορη, περισσότερο αποτελεσματική καθώς επίσης θα συμβάλει στην αποφυγή άσκοπων δαπανών.

Οι ακόλουθες βασικές συνιστώσες της στρατηγικής για τη Διαχείριση Κινδύνων είναι ζωτικής σημασίας:

1. Μοντέλο Διακυβέρνησης για τη διαχείριση κινδύνων σε όλο το εύρος του Οργανισμού

Ένα από τα σημαντικότερα βήματα είναι η διαμόρφωση ενός ολοκληρωμένου μοντέλου Διακυβέρνησης Διαχείρισης Κινδύνων σε όλο το εύρος του Οργανισμού το οποίο έχει την υποστήριξη της ανώτατης Διοίκησης, καθώς επίσης καθορίζει την ιδιοκτησία (ownership) και λογοδοσία (accountability)

2. Διακριτές λειτουργίες που επικεντρώνονται στη στρατηγική για τους κινδύνους, τον προσδιορισμό, την αξιολόγηση και τη διακυβέρνηση τους

Προκειμένου να είναι αποτελεσματική, η Διακυβέρνηση για τη διαχείριση των Κινδύνων σε όλο το εύρος του Οργανισμού πρέπει να φέρει τα παρακάτω δομικά στοιχεία:

a. Στρατηγική διαχείρισης κινδύνων στην οποία καθορίζονται το Όραμα και η ανεκτή έκθεση στον κίνδυνο
b. Διαδικασία για τον προσδιορισμό των Κινδύνων
c. Αξιολόγηση των Κινδύνων
d. Διακυβέρνηση ως προς τους Κινδύνους (Risk Governance)

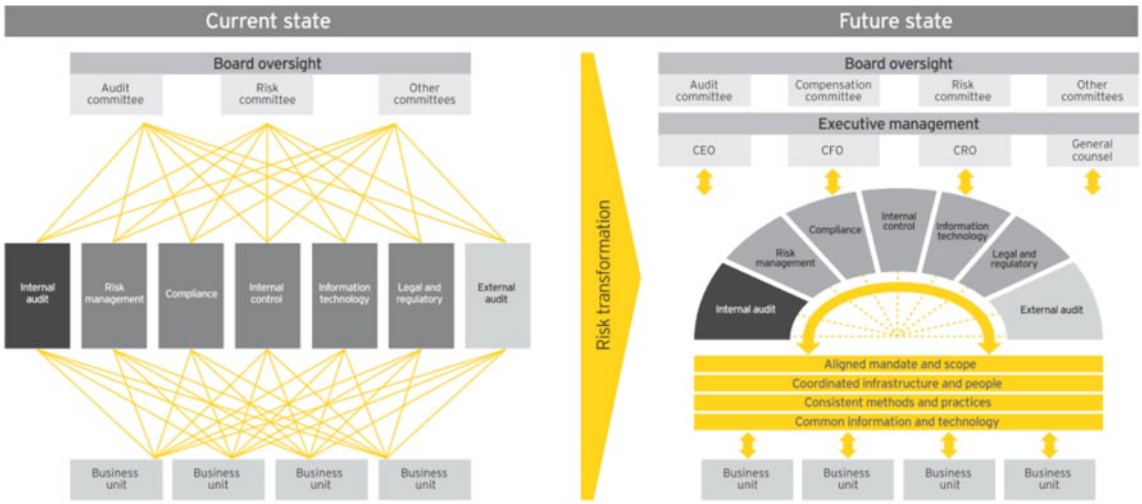
3. Σύγκλιση των λειτουργιών και δραστηριοτήτων GRC

Οργανισμοί που συγκλίνουν τις λειτουργίες τους που σχετίζονται με GRC μπορούν εύκολα να τεκμηριώσουν την αποτελεσματικότητα και την αποδοτικότητα των δραστηριοτήτων τους ως προς τη συμμόρφωση σε όλο το εύρος του Οργανισμού. Η ενοποίηση και η τυποποίηση των δραστηριοτήτων τους στα πλαίσια του Εσωτερικού Ελέγχου, της Κανονιστικής Συμμόρφωσης, του ERM μειώνει το κόστος, ενισχύει τις αλληλεπιδράσεις και μεγιστοποιεί την αξία των δραστηριοτήτων διαχείρισης κινδύνου.

Εναγκαλισμός Τεχνολογιών GRC

Οι λύσεις τεχνολογιών GRC είναι ένας κρίσιμος παράγοντας για την αποτελεσματική και αποδοτική εκτέλεση των διαδικασιών GRC παρέχοντας μία και μόνο γλώσσα για τη διαχείριση κινδύνων συμβάλλοντας παράλληλα στη συνοχή και την ολοκλήρωση αυτών των διαδικασιών. Ωστόσο, οι περισσότεροι Οργανισμοί εξακολουθούν να μην εκμεταλλεύονται όλες τις δυνατότητες των τεχνολογιών GRC. Παραδοσιακά, οι Οργανισμοί απέκτησαν εργαλεία λογισμικού GRC ως μια γρήγορη απόκριση σε ένα άμεσο σχετικό αίτημα (για παράδειγμα υλοποίηση ενός πλαισίου παρακολούθησης διαχωρισμού καθηκόντων ως απόκριση σε ένα εύρημα ελέγχου). Ως αποτέλεσμα, ευρύτερες εφαρμογές των τεχνολογιών GRC καθώς επίσης ανάλυση για την αποδοτικότητα της αρχικής επένδυσης δεν λήφθησαν υπόψη έχοντας ως αποτέλεσμα τον περιορισμό των απαιτήσεων και τη συνολική αξία τους.

Κορυφαίοι Οργανισμοί έχουν αναγνωρίσει αυτή την ευκαιρία ως μια στρατηγική επιταγή που επιτρέπει το μετασχηματισμό του Πλαισίου GRC δια μέσου κατάλληλων τεχνολογικών λύσεων. Ως αποτέλεσμα βελτιστοποίησαν την εκτέλεση των διαδικασιών τους μέσω των παρακάτω:



- Αυτοματοποίηση και τυποποίηση των διαδικασιών και των δικλείδων ασφαλείας
- Ενσωμάτωση και διατήρηση μίας ενιαίας έκδοσης των δεδομένων κινδύνου και δικλείδων ασφαλείας
- Διαχείριση μέσα από μία ολιστική εικόνα για τους Κινδύνους και των εκθέσεων συμμόρφωσης
- Δημιουργία δυναμικών, «έξυπνων» αναφορών σε πραγματικό χρόνο
- Ανάλυση των δεικτών κινδύνου και της λήψης αποφάσεων με γνώμονα τις εξαιρέσεις
- Κλιμάκωση μέσα από διαφορετικά επίπεδα της οργάνωσης μέσω της ροής εργασίας

Ανάληψη Δράσης

Από όλα όσα αναφέραμε παραπάνω πιστεύουμε πώς εφόσον η απάντηση σε οποιαδήποτε από τις ερωτήσεις που ακολουθούν είναι αρνητική, είναι καιρός να αναλάβετε δράση:

- Διαθέτετε μια ολοκληρωμένη στρατηγική για τη διαχείριση κινδύνων;
- Η στρατηγική σας για τη διαχείριση των κινδύνων αναφέρεται και αντιμετωπίζει τις τρεις κύριες κατηγορίες κινδύνων (κίνδυνοι που μπορούν να προληφθούν, στρατηγικοί και εξωτερικοί κίνδυνοι);
- Η ανώτερη Διοίκηση είναι πεπεισμένη ότι είναι γενικώς κατανοητό στον Οργανισμό το πλαίσιο κινδύνων και η αποδεκτή έκθεση στον κίνδυνο;
- Έχετε γνώση για τους κινδύνους τους οποίους διαχειρίζεται ο Οργανισμός;
- Η διαχείριση των κινδύνων και οι δραστηριότητες για τη συμμόρφωση εντός του Οργανισμού είναι οι βέλτιστες;
- Έχετε αξιοποιήσει αποτελεσματικά την τεχνολογία GRC για να στηρίξει το πρόγραμμα GRC σας;

1. *"Improve your business performance: transform your governance, risk and compliance program", http://www.ey.com/Publication/vwLUAssets/EY-improve-your-business-performance/$FILE/EY-transform-your-grc-program.pdf*
2. *Robert Kaplan and Anette Mikes, "Managing Risks: A New Framework", Harvard Business Review, http://hbr.org/2012/06/managing-risks-a-new-framework/ar/1, June 2012*