

Governance, Risk and Compliance: 4 Βασικοί Οδηγοί

Στο άρθρο της κας Brenda Boulwood, senior Vice President of industry solutions at MetricStream, που δημοσιεύθηκε στον ιστότοπο της Διεθνούς Ένωσης των Επαγγελματιών Διαχείρισης Κινδύνων (Global Association of Risk Professionals) διαβάσαμε για τους τέσσερις βασικούς παράγοντες που θα πρέπει να ληφθούν υπόψη κατά την ανάλυση κόστους – οφέλους προκειμένου οι οργανισμοί να αποφασίσουν την εγκατάσταση ενός πλήρους συστήματος «Διακυβέρνησης, Κινδύνων και Συμμόρφωσης» (Governance, Risk and Compliance – GRC) δεδομένου ότι, σύμφωνα με την έκθεση Forester, το αρχικό κόστος για μία τέτοια επένδυση κυμαίνεται από \$200.000 έως \$600.000.

1. Το κόστος ενός «κακού» συστήματος GRC.

Το κόστος ενός αναποτελεσματικού συστήματος GRC (ή / και της απουσίας ενός τέτοιου συστήματος), με δεδομένο ότι το υπάρχον νομοθετικό και κανονιστικό πλαίσιο γίνεται όλο και πιο περίπλοκο και μεγαλώνει, είναι τα προβλεπόμενα πρόστιμα σε περίπτωση μη συμμόρφωσης, το κόστος των οποίων συνεχώς αυξάνεται. Για παράδειγμα, το 2013 η JP Morgan πλήρωσε πρόστιμα ύψους 4 δις δολαρίων λόγω μη συμμόρφωσης με ισχύοντες κανονισμούς και ρυθμίσεις. Με την εγκατάσταση ενός ολοκληρωμένου πλαισίου GRC, που να ενσωματώνει τα πρότυπα συμμόρφωσης σε συστήματα και διαδικασίες σε επίπεδο εταιρείας, διασφαλίζεται η συμμόρφωση με τους συνεχώς μεταβαλλόμενους κανονισμούς με αποτέλεσμα να αποφεύγονται τέτοιου είδους κόστη.

2. Η προβολή της σημασίας ενός συστήματος GRC

Οι αλλαγές στο τοπίο των κινδύνων (risk landscape), που οφείλονται σε μια σειρά από παράγοντες όπως η οικονομική κρίση, η απώλεια/παραβίαση εταιρικών δεδομένων, ο αυξημένος κανονιστικός έλεγχος κλπ, επέφεραν αλλαγές και στη στάση των εταιριών όσον αφορά την διαχείριση του ρίσκου. Έτσι,

σήμερα οι υπεύθυνοι Διαχείρισης Κινδύνων (risk managers) έχουν πρόσβαση στα ανώτερα κλιμάκια διοίκησης των εταιριών (C-suite), προβάλλοντας έτσι τις σχετικές λειτουργίες και καθιστώντας τη Διαχείριση Κινδύνων ως αναπόσπαστο κομμάτι του οργανισμού.

3. Η «ευκαιριακή» διαχείριση κινδύνων και η προώθηση της καινοτομίας και της ανάπτυξης.

Η Διαχείριση Κινδύνων όχι μόνο επιτρέπει στους οργανισμούς να μετριάσουν τους κινδύνους, αλλά και να εντοπίσουν τους τομείς εκείνους που προσφέρονται για ανάπτυξη και καινοτομία. Ένα ολοκληρωμένο σύστημα GRC μπορεί να βοηθήσει τους οργανισμούς να επιτύχουν αυτούς τους στόχους με μια σειρά από τρόπους όπως:

- Με τον προσδιορισμό της διάθεσης ανάληψης κινδύνου (risk appetite), βασικό στοιχείο για την ανάπτυξη ενός οργανισμού, μέσω της συστηματικής παρακολούθησης των επιπέδων κινδύνου.

- Με την συγκέντρωση γνώσης και δεδομένων, απαραίτητα στοιχεία για την λήψη καινοτόμων αποφάσεων αλλά και υπολογισμού του αναλογούντος κινδύνου. Για παράδειγμα, ιστορικά στοιχεία σχετικά με την αξιολόγηση των κινδύνων και την απώλεια δεδομένων παρέχει στους οργανισμούς τις απαραίτητες πληροφορίες για τη βελτιστοποίηση της κατανομής των πόρων αλλά και τη προσέγγιση του κινδύνου με τέτοιο τρόπο που ευθυγραμμίζεται με τους γενικότερους επιχειρηματικούς τους στόχους.

4. Η μακροπρόθεσμη αξία μία συστημικής προσέγγισης του GRC

Σε ένα περιβάλλον που ορίζεται από τη διασύνδεση και την αλληλεξάρτηση, η συστημική προσέγγιση του GRC συμβάλλει στην δημιουργία κοινής κατανόησης των κινδύνων που διατρέχουν όλα τα επίπεδα του οργανισμού, βοηθά στην εκτίμηση της αλληλεξάρτησης των κινδύνων και αυξάνει τη διαφάνεια και τη λογοδοσία μέσω της εφαρμογής των ελέγχων που είναι κοινά σε όλο

τον οργανισμό. Επιπλέον η υιοθέτηση μια συστημικής προσέγγισης αυξάνει την αποτελεσματικότητα και τη μακροπρόθεσμη αξία του προγράμματος GRC ενός οργανισμού, δημιουργώντας ένα κεντρικό αποθετήριο δεδομένων όσον αφορά τους κινδύνους το οποίο συμβάλλει στην απόκτηση και συγκέντρωση τόσο ενδοεπιχειρησιακής αλλά και κλαδικής γνώσης. Με την αύξηση της προβολής των κινδύνων που αντιμετωπίζει ένας οργανισμός, αυτό το κεντρικό σύστημα καταγραφής μειώνει τις αρνητικές επιπτώσεις από την κινητικότητα των εργαζομένων και μειώνει τον κίνδυνο που συνδέεται από την συγκέντρωση της γνώσης σε ένα περιορισμένο αριθμό εργαζομένων.

Η εφαρμογή ενός ολοκληρωμένου συστήματος GRC απέχει σίγουρα πολύ από το «ένα μέγεθος ταιριάζει σε όλους». Διαφορετικοί επιχειρηματικοί στόχοι υπαγορεύουν διαφορετικές ανάγκες, και το GRC δεν αποτελεί εξαίρεση. Παρέχοντας μια ολοκληρωμένη εκτίμηση του τοπίου των κινδύνων ενός

οργανισμού, μια ολοκληρωμένη πλατφόρμα GRC μπορεί να αποδειχθεί προσαρμοσίμο και ευέλικτο εργαλείο, επιτρέποντας στον οργανισμό να συμβαδίσει με τη συνεχή μετατόπιση των προτύπων συμμόρφωσης και των κανονιστικών ρυθμίσεων αλλά και με την εξέλιξη των επιχειρηματικών στόχων.

Δεν υπάρχει αμφιβολία ότι η μέτρηση του ROI ενός ολοκληρωμένου προγράμματος GRC αποτελεί ένα εξαιρετικά δύσκολο έργο. Ωστόσο, αυτό που παραμένει ξεκάθαρο είναι ότι, στα πλαίσια ενός περιβάλλοντος κινδύνων που υπόκεινται σε συνεχείς αλλαγές, και ενός ρυθμιστικού τοπίου που συνεχίζει να εξελίσσεται, οι μακροπρόθεσμες δαπάνες που προέρχονται από την απουσία ενός ολοκληρωμένου προγράμματος GRC σε έναν οργανισμό υπερβαίνουν κατά πολύ τις επενδύσεις που απαιτούνται για την εφαρμογή του.

ΠΙΣΤΟΠΟΙΗΣΕΙΣ CIA

Η πιστοποίηση “Certified Internal Auditor – CIA” είναι η μόνη παγκοσμίως αποδεκτή πιστοποίηση για τους Εσωτερικούς Ελεγκτές και παραμένει το πρότυπο βάσει του οποίου αποδεικνύεται η ικανότητα και ο επαγγελματισμός στο πεδίο του Εσωτερικού Ελέγχου. Από την εισαγωγή του προγράμματος το 1973, έδωσε την δυνατότητα και την ευκαιρία στους Εσωτερικούς Ελεγκτές σε παγκόσμιο επίπεδο να επικοινωνήσουν την ικανότητά τους να συνεισφέρουν ως “παίκτες – κλειδιά” στην επιτυχία των οργανισμών που προσφέρουν τις υπηρεσίες τους.

Από το 2000, το E.I.E.E. είναι ο μοναδικός επίσημα διαπιστευμένος φορέας στην Ελλάδα για τη διενέργεια και στη χώρα μας των εξετάσεων για τίτλους πιστοποίησης “Certified Internal Auditor – CIA”. Οι προϋποθέσεις για τη συμμετοχή στις εξετάσεις είναι:

- Ο υποψήφιος να είναι μέλος του Ελληνικού Ινστιτούτου Εσωτερικών Ελεγκτών (E.I.E.E.).
- Οι υποψήφιοι απαιτείται να υποβάλλουν για την συμμετοχή τους στις εξετάσεις, την αίτηση συμμετοχής, character reference form, αντίγραφο πτυχίου και το experience verification form με την ολοκλήρωση των εξετάσεων για την απόκτηση του πιστοποιητικού.
- Για να αποκτήσετε την πιστοποίηση θα πρέπει να έχετε προϋπηρεσία 2 χρόνια στο Εσωτερικό Έλεγχο ή στον εξωτερικό Έλεγχο, internal control, compliance, quality assurance.

Για περισσότερες πληροφορίες σχετικά με τις εξετάσεις (περιεχόμενο, τρόπος διεξαγωγής, εγγραφής για συμμετοχή κλπ) μπορείτε να επικοινωνείτε με την Γραμματεία του E.I.E.E. (210-82.59.504).

