ΕΠΙΣΗΜΗ ΕΦΗΜΕΡΙΔΑ
ΤΗΣ ΚΥΠΡΙΑΚΗΣ ΔΗΜΟΚΡΑΤΙΑΣ
ΠΑΡΑΡΤΗΜΑ ΤΡΙΤΟ
ΜΕΡΟΣ Ι
ΚΑΝΟΝΙΣΤΙΚΕΣ ΔΙΟΙΚΗΤΙΚΕΣ ΠΡΑΞΕΙΣ

Αριθμός 4236	Τετάρτη, 14 Νοεμβρίου 2007	3031

Αριθμός 441

Ο ΠΕΡΙ ΣΥΝΕΡΓΑΤΙΚΩΝ ΕΤΑΙΡΕΙΩΝ ΝΟΜΟΣ

ΚΑΝΟΝΙΣΤΙΚΗ ΑΠΟΦΑΣΗ ΤΗΣ ΕΠΙΤΡΟΠΗΣ ΤΗΣ ΥΠΗΡΕΣΙΑΣ ΕΠΟΠΤΕΙΑΣ ΚΑΙ ΑΝΑΠΤΥΞΗΣ ΣΥΝΕΡΓΑΤΙΚΩΝ ΕΤΑΙΡΕΙΩΝ ΑΝΑΦΟΡΙΚΑ ΜΕ ΤΟ ΠΛΑΙΣΙΟ ΑΡΧΩΝ ΛΕΙΤΟΥΡΓΙΑΣ ΚΑΙ ΚΡΙΤΗΡΙΩΝ ΑΞΙΟΛΟΓΗΣΗΣ ΤΗΣ ΟΡΓΑΝΩΤΙΚΗΣ ΔΟΜΗΣ, ΕΣΩΤΕΡΙΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ ΚΑΙ ΤΩΝ ΣΥΣΤΗΜΑΤΩΝ ΕΣΩΤΕΡΙΚΟΥ ΕΛΕΓΧΟΥ ΤΩΝ ΣΥΝΕΡΓΑΤΙΚΩΝ ΠΙΣΤΩΤΙΚΩΝ ΙΔΡΥΜΑΤΩΝ

Κανονιστική Απόφαση με βάση τα άρθρα 15Α, 41Ζ και 41Ι

Η Επιτροπή της Υπηρεσίας Εποπτείας και Ανάπτυξης Συνεργατικών Εταιρειών δυνάμει των άρθρων 15Α, 41Ζ(1)(ε) και 41Ζ(2) του περί Συνεργατικών Εταιρειών Νόμου και το άρθρο 41Ι(γ) το Νόμου αυτού σε συνδυασμό με το άρθρο 41Ι(στ) και την Κανονιστική Διοικητική Πράξη (ΚΔΠ) 110/2004, εκδίδει την παρούσα Κανονιστική Απόφαση αναφορικά με το «Πλαίσιο Αρχών Λειτουργίας και Κριτηρίων Αξιολόγησης της Οργανωτικής Δομής, Εσωτερικής Διακυβέρνησης και των Συστημάτων Εσωτερικού Ελέγχου των Συνεργατικών Πιστωτικών

Ιδρυμάτων», για σκοπούς εναρμόνισης με το άρθρο 22 και το Παράρτημα V της Οδηγίας 2006/48/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 14ης Ιουνίου 2006 σχετικά με την ανάληψη και την άσκηση δραστηριότητας πιστωτικών ιδρυμάτων (ΕΕ L 177 της 30.6.2006, σ.1).

ΜΕΡΟΣ Ι
ΤΙΤΛΟΣ, ΕΡΜΗΝΕΙΑ ΚΑΙ ΕΦΑΡΜΟΓΗ

Συνοπτικός τίτλος

1. Η παρούσα Κανονιστική Απόφαση θα αναφέρεται ως η περί του Πλαισίου Αρχών Λειτουργίας και Κριτηρίων Αξιολόγησης της Οργανωτικής Δομής, Εσωτερικής Διακυβέρνησης και των Συστημάτων Εσωτερικού Ελέγχου των Συνεργατικών Πιστωτικών Ιδρυμάτων Κανονιστική Απόφαση του 2007.

Κύριοι στόχοι

2. Κύριοι στόχοι της παρούσας Κανονιστικής Απόφασης είναι η ενίσχυση του γενικού πλαισίου της οργανωτικής δομής και εσωτερικής διακυβέρνησης καθώς επίσης η αναβάθμιση των τριών βασικών λειτουργιών του Συστήματος Εσωτερικού Ελέγχου, δηλαδή της Εσωτερικής Επιθεώρησης, της Διαχείρισης Κινδύνων και της Κανονιστικής Συμμόρφωσης, των Συνεργατικών Πιστωτικών Ιδρυμάτων, περιλαμβανομένης της Συνεργατικής Κεντρικής Τράπεζας Λτδ.

Ερμηνεία

3. Στην παρούσα Κανονιστική Απόφαση, εκτός αν από το κείμενο προκύπτει διαφορετική έννοια:

«Ανώτατη Εκτελεστική Διεύθυνση» σημαίνει το Γραμματέα ο οποίος πλαισιώνεται κατά την άσκηση των αρμοδιοτήτων και ευθυνών του με βάση την παρούσα Κανονιστική Απόφαση από άλλα διευθυντικά στελέχη του ΣΠΙ σύμφωνα με την εγκεκριμένη οργανωτική δομή του ΣΠΙ, και ανάλογα θα ερμηνεύεται ο όρος «Ανώτατοι Εκτελεστικοί Διευθυντές»,

«Έφορος» σημαίνει τον Έφορο της Υπηρεσίας Εποπτείας και Ανάπτυξης Συνεργατικών Εταιρειών (ΥΕΑΣΕ),

«Κεντρικός Φορέας» σημαίνει την Συνεργατική Κεντρική Τράπεζα Λτδ,

«Νόμος» σημαίνει τους περί Συνεργατικών Εταιρειών Νόμους,

«πρόσωπο» σημαίνει φυσικό ή νομικό πρόσωπο

«Συνεργατικό Πιστωτικό Ίδρυμα» ή «ΣΠΙ» έχει την έννοια που αποδίδεται στον όρο αυτό από τον περί Συνεργατικών Εταιρειών Νόμο.

Πεδίο εφαρμογής

4.-(1) Οι διατάξεις της παρούσας Κανονιστικής Απόφασης εφαρμόζονται σε όλα τα ΣΠΙ, περιλαμβανομένων των υποκαταστημάτων τους στο εξωτερικό, που κατέχουν άδεια λειτουργίας με βάση τον περί Συνεργατικών Εταιρειών Νόμο.

(2) Με βάση το άρθρο 15Α(1) του Νόμου και το Θεσμό 96 των περί Συνεργατικών Εταιρειών Θεσμών, οποιαδήποτε διάταξη των θεσμών, διαταγμάτων, αποφάσεων ή οδηγιών που εκδίδονται δυνάμει του Νόμου, εφαρμόζεται στην έκταση και κατά τρόπο που διασφαλίζεται η εφαρμογή των διατάξεων της παρούσας Κανονιστικής Απόφασης, περιλαμβανομένης της παραγράφου 4Α. Έπεται ότι οι ήδη εκδοθείσες οδηγίες και εγκύκλιοι του Εφόρου επί θεμάτων που ρυθμίζονται από την παρούσα Κανονιστική Απόφαση, στην έκταση που δεν συγκρούονται με οποιαδήποτε διάταξη της, εξακολουθούν να ισχύουν και να τυγχάνουν εφαρμογής.

(3) Τηρουμένων των διατάξεων της παραγράφου 4Α, ο Έφορος, εντός των βάσει της συνεργατικής νομοθεσίας εξουσιών και αρμοδιοτήτων του, έχει διακριτική εξουσία και ευχέρεια να ενεργεί και απαιτεί ικανοποίηση των προνοιών της παρούσας Κανονιστικής Απόφασης από κάθε ΣΠΙ βάσει της αρχής της αναλογικότητας, ήτοι ανάλογα με το μέγεθός του, τους κινδύνους που αναλαμβάνει, την πολυπλοκότητα των εργασιών του, την αδειοδότησή του ως αναγνωρισμένο ΣΠΙ αφ' εαυτού ή κατόπιν σύνδεσής του με τον Κεντρικό Φορέα, τις ρυθμίσεις της ΥΕΑΣΕ για τον εσωτερικό έλεγχο των ΣΠΙ, περιλαμβανομένων των συνδεδεμένων με τον Κεντρικό Φορέα ΣΠΙ και γενικά με βάση οποιαδήποτε άλλα κριτήρια, όρους και προϋποθέσεις που δυνατό να καθορίζονται με ειδική απόφαση της Επιτροπής ΥΕΑΣΕ.

Νοείται ότι η κατά τα ως άνω διακριτική εξουσία και ευχέρεια του Εφόρου περιλαμβάνει και τη δυνατότητα καθορισμού χρονοδιαγράμματος συμμόρφωσης, παραχώρησης εξαίρεσης με ή χωρίς όρους από την εφαρμογή οποιασδήποτε διάταξης εν όλω ή εν μέρει, για συγκεκριμένο χρονικό διάστημα ή επ' αόριστο, καθώς και τη διαφοροποίηση ορίων ή προθεσμιών.

Νοείται περαιτέρω ότι η προβλεπόμενη στο παρόν εδάφιο αρχή της αναλογικότητας εφαρμόζεται χωρίς να επηρεάζεται η υποχρέωση του ΣΠΙ να διασφαλίζει τα συμφέροντά του και την εύρυθμη λειτουργία και ασφαλή διαχείρισή του, λαμβανομένων υπόψη των δεδομένων και των εκάστοτε συνθηκών όπως και των υφιστάμενων ή εγκαθιδρυθυσόμενων συμπληρωματικών μηχανισμών, σε περιφερειακό ή κεντρικό επίπεδο, για τα συνδεδεμένα με τον Κεντρικό Φορέα ΣΠΙ που δικαιούνται εξαίρεσης από τις καθορισμένες ρυθμίσεις και άλλα κριτήρια, περιλαμβανομένης της υποχρέωσης για ύπαρξη δύο τουλάχιστον διευθυντικών στελεχών (four eyes principle).

(4) Τα υποκαταστήματα στην Κύπρο των ΣΠΙ που έχουν λάβει άδεια λειτουργίας σε κράτος άλλο από κράτος μέλος της Ευρωπαϊκής Ένωσης υπόκεινται στις πρόνοιες της παρούσας Κανονιστικής Απόφασης εκτός εάν ικανοποιηθεί ο Έφορος ότι υπόκεινται σε ισοδύναμο καθεστώς εποπτείας.

Συνεργατική Κεντρική Τράπεζα Λτδ

4Α.-(1) Για τους σκοπούς της παρούσας Κανονιστικής Απόφασης ο όρος ΣΠΙ περιλαμβάνει και τη Συνεργατική Κεντρική Τράπεζα Λτδ η οποία εφαρμόζει τις διατάξεις της αντίστοιχης Οδηγίας της Κεντρικής Τράπεζας της Κύπρου με τίτλο «Πλαίσιο αρχών λειτουργίας και κριτηρίων αξιολόγησης της οργανωτικής δομής, εσωτερικής διακυβέρνησης και των συστημάτων εσωτερικού ελέγχου των τραπεζών».

(2) Στα πλαίσια εφαρμογής των ρυθμίσεων εσωτερικής διακυβέρνησης με βάση το εδάφιο (1) πιο πάνω και λαμβανομένου υπόψη και του ρόλου της ως ο Κεντρικός Φορέας των

συνδεδεμένων ΣΠΙ, για τη Συνεργατική Κεντρική Τράπεζα Λτδ ισχύουν τα ακόλουθα :

(α) Η Συνεργατική Κεντρική Τράπεζα Λτδ δύναται να καθορίσει στους ειδικούς κανονισμούς της ότι θα προβεί στη σύσταση Επιτροπής Διαχείρισης Κινδύνων και στον ορισμό δεύτερου μη εκτελεστικού και ανεξάρτητου μέλους της Επιτροπείας της.

(β) Ο τρόπος εκλογής ή διορισμού των εκτελεστικών και των μη εκτελεστικών-ανεξάρτητων μελών της Επιτροπείας της Συνεργατικής Κεντρικής Τράπεζας Λτδ καθορίζεται στους ειδικούς κανονισμούς της.

(γ) Ανεξάρτητα από τις διατάξεις του Θεσμού 48(5) των περί Συνεργατικών Εταιρειών Θεσμών, οι όροι εργοδότησης και η διάρκεια της υπηρεσίας του εκάστοτε Γραμματέα της Συνεργατικής Κεντρικής Τράπεζας Λτδ καθορίζεται με απόφαση της Επιτροπείας της και έγκριση του Εφόρου.

(δ) Ο Γραμματέας της Συνεργατικής Κεντρικής Τράπεζας Λτδ φέρει και τον τίτλο «Γενικός Διευθυντής» ο οποίος χρησιμοποιείται εναλλακτικά του τίτλου «Γραμματέας».

ΜΕΡΟΣ ΙΙ
ΣΥΣΤΗΜΑ ΕΣΩΤΕΡΙΚΟΥ ΕΛΕΓΧΟΥ

Στόχοι του Συστήματος Εσωτερικού Ελέγχου

5.-(1) Το Σύστημα Εσωτερικού Ελέγχου αποτελεί ένα σύνολο ελεγκτικών μηχανισμών και διαδικασιών που καλύπτει, σε συνεχή βάση, κάθε δραστηριότητα του ΣΠΙ και συντελεί στην αποτελεσματική και ασφαλή λειτουργία του. Ειδικότερα, το Σύστημα Εσωτερικού Ελέγχου αποβλέπει στη διασφάλιση των ακόλουθων ιδίως στόχων:

(α) Τη συνεπή υλοποίηση της επιχειρησιακής στρατηγικής με αποτελεσματική χρήση των διαθέσιμων πόρων·

(β) την αναγνώριση και αντιμετώπιση των πάσης φύσεως κινδύνων που αναλαμβάνονται, περιλαμβανομένου και του λειτουργικού κινδύνου·

(γ) τη διασφάλιση της πληρότητας και της αξιοπιστίας των στοιχείων και πληροφοριών που απαιτούνται για τον ακριβή και έγκαιρο προσδιορισμό της χρηματοοικονομικής κατάστασης του ΣΠΙ και την παραγωγή αξιόπιστων οικονομικών καταστάσεων·

(δ) τη συμμόρφωση με το θεσμικό πλαίσιο που διέπει τη λειτουργία του, περιλαμβανομένων των ειδικών και εσωτερικών κανονισμών και των κανόνων δεοντολογίας·

(ε) την πρόληψη και την αποφυγή λανθασμένων ενεργειών και παρατυπιών που θα μπορούσαν να θέσουν σε κίνδυνο τη φήμη και τα συμφέροντα του ΣΠΙ, των μελών του και των συναλλασσομένων με αυτό.

(2) Αναπόσπαστο τμήμα του Συστήματος Εσωτερικού Ελέγχου αποτελούν οι βέλτιστες αρχές της εσωτερικής διακυβέρνησης ενός ΣΠΙ και ειδικότερα:

(α) Ο καθορισμός στρατηγικών στόχων και εταιρικών αξιών που να διαχέονται σε όλο το ΣΠΙ·

(β) ο καθορισμός και η εφαρμογή σαφών πλαισίων αρμοδιοτήτων και η υποχρέωση αναφοράς σε όλο το ΣΠΙ·

(γ) η διασφάλιση ότι τα μέλη της Επιτροπείας κατέχουν τα κατάλληλα προσόντα, έχουν πλήρη επίγνωση του ρόλου που αναλαμβάνουν σε σχέση με την εσωτερική διακυβέρνηση και είναι σε θέση να ασκήσουν τα καθήκοντά τους με ανεξαρτησία γνώμης·

(δ) η Επιτροπεία οφείλει να εφαρμόσει και να διατηρεί ένα επαρκές Σύστημα Εσωτερικού Ελέγχου που να διασφαλίζει το ενεργητικό του ΣΠΙ·

(ε) ο καθορισμός μιας αποτελεσματικής στρατηγικής και πολιτικής για τη διατήρηση, σε συνεχή βάση, του ύψους, των κατηγοριών και της κατανομής των ιδίων κεφαλαίων και αποθεματικών που χρειάζονται για να καλύπτονται επαρκώς οι κίνδυνοι που αντιμετωπίζει το ΣΠΙ·

(στ) η αποτελεσματική αξιοποίηση της εργασίας των εξωτερικών ελεγκτών και της Μονάδας Εσωτερικής Επιθεώρησης καθώς και των άλλων λειτουργιών του Συστήματος Εσωτερικού Ελέγχου, αναγνωρίζοντας τη

μείζονος σημασίας συμβολή τους στην εφαρμογή μιας επαρκούς εσωτερικής διακυβέρνησης·

(ζ) η διασφάλιση ότι οι πολιτικές και πρακτικές σε θέματα χρηματικών παροχών/μισθοδοσίας συνάδουν με τις ηθικές αξίες, τους στόχους, τη στρατηγική και το εποπτικό περιβάλλον του ΣΠΙ·

(η) η κατανόηση όλων των δραστηριοτήτων του ΣΠΙ·

(ι) η εφαρμογή της εσωτερικής διακυβέρνησης με διαφανή τρόπο.

ΜΕΡΟΣ ΙΙΙ
ΒΑΣΙΚΕΣ ΑΡΧΕΣ ΚΑΙ ΚΡΙΤΗΡΙΑ ΑΞΙΟΛΟΓΗΣΗΣ ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ ΕΣΩΤΕΡΙΚΟΥ ΕΛΕΓΧΟΥ

Επιχειρησιακή στρατηγική και αποτελεσματικότητα συστήματος εσωτερικού ελέγχου

6.- (1) Κάθε ΣΠΙ οφείλει να διαθέτει επιχειρησιακή στρατηγική και σαφείς στόχους που να είναι καταγεγραμμένοι, τεκμηριωμένοι και εγκεκριμένοι από την Επιτροπεία του και να αναφέρεται ιδίως στα ακόλουθα:

(α) Την καταγραφή και ιεράρχηση των άμεσων και μελλοντικών επιχειρησιακών στόχων·

(β) τη διαφανή διάρθρωση και επαρκή τεκμηρίωση της επιχειρηματικής δραστηριότητας στο εσωτερικό και εξωτερικό και κατάλληλες αναφορές που θα καθιστούν δυνατό τον έλεγχο από τις αρμόδιες εποπτικές αρχές·

(γ) τον προϋπολογισμό για το είδος και τον όγκο των δραστηριοτήτων, καθώς και τα προβλεπόμενα οικονομικά αποτελέσματα·

(δ) τα αποδεκτά όρια και το είδος των κινδύνων που πρόκειται να αναληφθούν, οι παραδοχές με βάση τις οποίες εκτιμώνται και η κάλυψή τους από τα ίδια κεφάλαια.

(2) Για την αποτελεσματικότητα του Συστήματος Εσωτερικού ελέγχου ως συνόλου, θα πρέπει να διασφαλίζεται ιδίως ότι:

(α) Είναι επαρκώς τεκμηριωμένο και λεπτομερώς καταγεγραμμένο ως προς τα σημεία ελέγχου και τις διαδικασίες·

(β) είναι κατάλληλα προσαρμοσμένο προς το εύρος, τον όγκο, τους κινδύνους και την πολυπλοκότητα των εργασιών του ΣΠΙ καθώς και προς τις ιδιαιτερότητες των χωρών στις οποίες δραστηριοποιείται·

(γ) καλύπτει πλήρως όλες τις δραστηριότητες και τις συναλλαγές του ΣΠΙ·

(δ) παρέχει δυνατότητα ελέγχου των εργασιών των οποίων η διεκπεραίωση ανατίθεται σε άλλες επιχειρήσεις σύμφωνα με το Παράρτημα 1 της παρούσας Κανονιστικής Απόφασης·

(ε) υποστηρίζεται από ολοκληρωμένο σύστημα διευθυντικής πληροφόρησης ("Management Information System") και επικοινωνίας με σαφώς καθορισμένες ιεραρχικές γραμμές αναφοράς που θα επιτρέπουν την έγκαιρη ροή και την αξιοπιστία της απαιτούμενης πληροφόρησης σε κάθε λειτουργό ή διοικητικό όργανο για την εκτέλεση του έργου του·

(στ) προβλέπει τη διεξαγωγή από τα αρμοδίως επιφορτισμένα όργανα ή μονάδες, περιοδικών ή/και έκτακτων ελέγχων, για τη διαπίστωση της συνεπούς εφαρμογής των κανόνων και διαδικασιών από όλες τις υπηρεσιακές μονάδες·

(ζ) διαθέτει εσωτερική συνοχή των μηχανισμών ελέγχου για το σύνολο του ΣΠΙ·

(η) προβλέπει διαδικασίες για την αξιολόγηση της επάρκειάς του, με κριτήρια:

(i) τη συνέπεια της εφαρμογής των διαδικασιών·

(ii) τις ποσοτικές και ποιοτικές επιπτώσεις από παραβιάσεις των κανόνων ασφαλείας ή από λάθη και παραλείψεις στην εφαρμογή τους·

(iii) την ύπαρξη μηχανισμών άμεσης αναθεώρησης των

διαδικασιών για την αντιμετώπιση των αδυναμιών που διαπιστώνονται από τις τακτικές ή έκτακτες αξιολογήσεις τους.

Οργανωτική Δομή Συστήματος Εσωτερικού Ελέγχου και Διαδικασίες

7. Για τη διασφάλιση μιας αποτελεσματικής οργανωτικής δομής και επάρκειας του Συστήματος Εσωτερικού Ελέγχου απαιτείται, για κάθε δραστηριότητα, αναλυτική περιγραφή και σαφής καθορισμός των αρμοδιοτήτων και ορίων ευθύνης κάθε εμπλεκόμενης υπηρεσιακής μονάδας και επιτροπής της Επιτροπείας, καθώς και αντίστοιχες διαδικασίες εξουσιοδότησης. Ειδικότερα απαιτείται:

(α) Η αναλυτική καταγραφή των διαδικασιών διεξαγωγής κάθε εργασίας, που κοινοποιείται στο αρμόδιο για την εκτέλεση και τον έλεγχό της προσωπικό·

(β) η ενσωμάτωση σε όλους τους κανονισμούς διεξαγωγής των εργασιών του ΣΠΙ, κατάλληλων μηχανισμών ελέγχου που θα διασφαλίζουν ότι όλες οι συναλλαγές είναι έγκυρες και νόμιμες, έχουν εκτελεστεί σύμφωνα με όλους τους κανόνες λειτουργίας της κάθε υπηρεσιακής μονάδας, έχουν αξιολογηθεί ως προς τους κινδύνους που ενέχουν, έχουν διεκπεραιωθεί από κατάλληλα εξουσιοδοτημένα και άμεσα εντοπιζόμενα άτομα, έχουν καταχωρηθεί στα προβλεπόμενα για κάθε περίπτωση αρχεία και έχουν ενταχθεί σύστημα διευθυντικής πληροφόρησης ("Management Information System")·

(γ) η πρόβλεψη για άμεση ή έμμεση εμπλοκή δύο τουλάχιστον λειτουργών του ΣΠΙ σε κάθε δραστηριότητα ή ελεγκτική λειτουργία ("four eyes principle") μέχρι την ολοκλήρωσή της·

(δ) η συμβουλευτική, τουλάχιστον συμμετοχή των Μονάδων Εσωτερικής Επιθεώρησης, Διαχείρισης Κινδύνων και Κανονιστικής Συμμόρφωσης στο σχεδιασμό νέων προϊόντων και διαδικασιών σε θέματα που αφορούν τη λήψη επιχειρηματικών αποφάσεων, καθώς και για την εκτίμηση του λειτουργικού κινδύνου που μπορεί να προκύψει, σε περιπτώσεις σημαντικών αλλαγών, για παράδειγμα

συγχωνεύσεων, προκειμένου να ενσωματωθούν οι κατάλληλοι ελεγκτικοί μηχανισμοί, οι μηχανισμοί διαχείρισης κινδύνων και να διασφαλισθεί η συμβατότητα με τους ισχύοντες κανόνες.

Διαχωρισμός καθηκόντων και σύγκρουση συμφερόντων

8.- (1) Τα ΣΠΙ οφείλουν να καθορίσουν διαδικασίες διαχείρισης και διαρκούς εκπαίδευσης του ανθρώπινου δυναμικού, έτσι ώστε η στελέχωση κάθε θέσης, εργασίας ή ευθύνης να γίνεται από πρόσωπα που διαθέτουν τις κατάλληλες γνώσεις και ικανότητες με τη θέσπιση των πλέον ενδεδειγμένων εκάστοτε κριτηρίων πρόσληψης και εξέλιξης.

(2) Οι αμοιβές των στελεχών και ιδίως αυτών που ασχολούνται με την προώθηση και διάθεση προϊόντων και υπηρεσιών ή διαχειρίζονται τα διαθέσιμα κεφάλαια του ΣΠΙ οφείλουν να διαμορφώνονται με συνεπή συνεκτίμηση της αρχής αποφυγής της παροχής κινήτρων για την ανάληψη υπερβολικών κινδύνων ή τον προσπορισμό βραχυπρόθεσμου οφέλους.

(3) Τα ΣΠΙ οφείλουν να διασφαλίζουν τον αποτελεσματικό διαχωρισμό καθηκόντων με την υιοθέτηση κατάλληλων διαδικασιών, ώστε να αποφεύγονται περιπτώσεις ασυμβίβαστων ρόλων, σύγκρουσης συμφερόντων μεταξύ των μελών της Επιτροπείας, των Ανώτατων Εκτελεστικών Διευθυντών και των άλλων στελεχών, αλλά και μεταξύ αυτών, του ΣΠΙ και των συναλλασσομένων, καθώς και της αθέμιτης χρήσης εμπιστευτικών πληροφοριών ή περιουσιακών στοιχείων. Θα πρέπει να λαμβάνονται υπόψη από τα ΣΠΙ οι βέλτιστες αρχές της εσωτερικής διακυβέρνησης που αναφέρονται στο Μέρος IV της παρούσας Κανονιστικής Απόφασης.

(4) Με κατάλληλες διαφοροποιήσεις στη διοικητική τους υπαγωγή και στις γραμμές διοικητικής αναφοράς τα ΣΠΙ οφείλουν να διασφαλίζουν την ανεξαρτησία, αφενός, των οργάνων ελέγχου από τις ελεγχόμενες δραστηριότητες και τους λειτουργούς τους και, αφετέρου, τη διαχείριση κινδύνων από τις δραστηριότητες ανάληψης κινδύνων και τους λειτουργούς τους, έτσι ώστε:

(α) Οι λειτουργίες υποδοχής και διεκπεραίωσης αιτημάτων μελών/πελατών, προώθησης και διάθεσης χρηματοοικονομικών προϊόντων στο κοινό (πιστώσεις, καταθετικά και επενδυτικά προϊόντα), διαπραγμάτευσης και εν γένει διενέργειας συναλλαγών ("front line") να είναι διοικητικά και λειτουργικά διαχωρισμένες από τις λειτουργίες έγκρισης αιτημάτων, επιβεβαίωσης, λογιστικοποίησης και διακανονισμού συναλλαγών, καθώς και φύλαξης τίτλων ή άλλων περιουσιακών στοιχείων του ΣΠΙ ή των μελών/πελατών·

(β) Ομοίως, διαχωρισμένες να είναι οι λειτουργίες διαχείρισης κινδύνων και ελέγχου αφενός μεταξύ τους και, αφετέρου, από τις πιο πάνω λειτουργίες.

(5) Τα ΣΠΙ οφείλουν να διασφαλίζουν το συστηματικό έλεγχο της πρόσβασης μόνο εξουσιοδοτημένων ατόμων σε περιουσιακά και λογιστικά στοιχεία και εν γένει εμπιστευτικές πληροφορίες.

(6) Τα ΣΠΙ οφείλουν, επίσης, να διασφαλίζουν, με κατάλληλες διαδικασίες, τη δυνατότητα πραγματοποίησης ανώνυμων αναφορών, καθώς και την προστασία των υπαλλήλων που μέσω αυτών των αναφορών ενημερώνουν την Επιτροπεία ή την Επιτροπή Ελέγχου, ή όπου αυτή δεν υφίσταται, τον εξουσιοδοτημένο υπάλληλο της Μονάδας Εσωτερικής Επιθεώρησης, για σοβαρές παρατυπίες, παραλείψεις ή αξιόποινες πράξεις που υπέπεσαν στην αντίληψή τους.

Συναλλαγές με πρόσωπα που έχουν «ειδική σχέση» με το ΣΠΙ

9. Ως προς τις συναλλαγές μεταξύ ΣΠΙ και προσώπων με τα οποία έχουν ειδική σχέση, τα ΣΠΙ εφαρμόζουν τις πρόνοιες του άρθρου 41ΚΔ του Νόμου καθώς και οποιαδήποτε σχετική διάταξη των θεσμών, κανονιστικών αποφάσεων και οδηγιών που εκδίδονται κατ' εξουσιοδότηση του Νόμου.

Παρεχόμενες υπηρεσίες προς μέλη/πελάτες

10. Για τη διασφάλιση της παροχής κατάλληλων υπηρεσιών προς τα μέλη/πελάτες, ως αναπόσπαστο τμήμα του λειτουργικού κινδύνου, απαιτείται ιδίως:

(α) Η υιοθέτηση από τα ΣΠΙ βέλτιστων πρακτικών, για την παροχή υπηρεσιών και προϊόντων, που να προσιδιάζουν στα χαρακτηριστικά του μέλους/πελάτη·

(β) η παρακολούθηση και αξιολόγηση του τρόπου εξυπηρέτησης και ειδικότερα των διαδικασιών παρουσίασης και συμφωνίας των όρων συνεργασίας τους με το ΣΠΙ και, ιδίως, με την εκάστοτε ισχύουσα νομοθεσία περί προστασίας του καταναλωτή·

(γ) η ύπαρξη κατάλληλων διαδικασιών για την εξέταση των καταγγελιών ή παραπόνων των μελών/πελατών·

(δ) η διαφύλαξη των συμφερόντων και προστασία από αλλότρια χρήση των προσωπικών δεδομένων σύμφωνα με τον περί Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμο.

Πρόληψη και καταστολή του ξεπλύματος παράνομου χρήματος και της χρηματοδότησης της τρομοκρατίας

11. Τα ΣΠΙ εφαρμόζουν τις πρόνοιες της Οδηγίας του Εφόρου προς τα ΣΠΙ αναφορικά με την Παρεμπόδιση Ξεπλύματος Παράνομου Χρήματος, που εκδόθηκε σύμφωνα με το άρθρο 60(3) του περί Συγκάλυψης, Έρευνας και Δήμευσης Εσόδων από Ορισμένες Εγκληματικές Πράξεις Νόμου. Αντίστοιχη οδηγία της Κεντρικής Τράπεζας της Κύπρου εφαρμόζει και η Συνεργατική Κεντρική Τράπεζα Λτδ.

Διαχείριση κινδύνων

12.-(1) Τα ΣΠΙ οφείλουν να διαθέτουν καταγεγραμμένη πολιτική και διαδικασίες που να αντιστοιχούν στην επιχειρησιακή τους στρατηγική, σχετικά με:

(α) την ανάληψη, την παρακολούθηση και τη διαχείριση των διαφόρων κινδύνων όπως είναι ο κίνδυνος αγοράς, ο πιστωτικός, ο λειτουργικός και ο κίνδυνος ρευστότητας, και τη διάκριση των συναλλαγών και μελών/πελατών κατά επίπεδο κινδύνου για παράδειγμα κατά χώρα, επάγγελμα, δραστηριότητα·

(β) τον καθορισμό των εκάστοτε αποδεκτών ανωτάτων ορίων

ανάληψης κινδύνου συνολικά για κάθε είδος κινδύνου και περαιτέρω κατανομή καθενός εκ των ορίων αυτών κατά μέλος/πελάτη, κλάδο, νόμισμα, υπηρεσιακή μονάδα·

(γ) τον καθορισμό ορίων τερματισμού ζημιογόνων δραστηριοτήτων ή άλλων διορθωτικών ενεργειών

οι οποίες πρέπει να κοινοποιούνται έγκαιρα και εγγράφως, με τη μορφή εξειδικευμένων στόχων ή κατευθύνσεων, όπου απαιτείται, σε όλα τα εντεταλμένα όργανα που εμπλέκονται στις διαδικασίες ανάληψης ("risk owners"), παρακολούθησης, αντιστάθμισης και μείωσης των κινδύνων.

(2) Τα ΣΠΙ οφείλουν να επαναξιολογούν, σε ετήσια βάση, τους κινδύνους και να ελέγχουν τις υψηλού κινδύνου δραστηριότητες ή τις πολύπλοκες συναλλαγές τους καθώς και τις προβληματικές πιστοδοτήσεις.

(3) Για το σχεδιασμό, την ανάπτυξη και την παρακολούθηση της πολιτικής κινδύνων, κάθε ΣΠΙ οφείλει να διαθέτει μια εξειδικευμένη και ανεξάρτητη λειτουργία διαχείρισης των κινδύνων σύμφωνα με τις διατάξεις της παραγράφου 27(1) που να καλύπτει όλο το φάσμα των δραστηριοτήτων για όλες τις μορφές των κινδύνων, περιλαμβανομένου και του λειτουργικού.

(4) Τα ΣΠΙ οφείλουν να εφαρμόζουν καταγεγραμμένες διαδικασίες ως προς:

(α) Τον περιοδικό εντοπισμό των σημαντικών ή αιφνίδιων μεταβολών στις παραμέτρους που διαμορφώνουν τους κινδύνους, όπως οικονομικά μεγέθη, εξελίξεις στην αγορά, και ισχύον νομικό πλαίσιο, την αξιολόγησή τους και την αναφορά τους στα αρμόδια όργανα για τυχόν διορθωτικές ενέργειες, ιδίως, όταν οδηγούν σε υπέρβαση των αποδεκτών ορίων·

(β) την αντιστάθμιση, δηλαδή την κάλυψη, μεταφορά, ασφάλιση της τυχόν ζημιάς και τη λογιστικοποίηση·

(γ) την τιμολόγηση των προσφερόμενων προϊόντων και περιοδική επαναξιολόγησή της, ώστε να διασφαλίζεται ότι λαμβάνονται υπόψη όλες οι παράμετροι διαμόρφωσης του κόστους, ο ανταγωνισμός και οι κίνδυνοι σε σχέση με τις αναμενόμενες αποδόσεις.

(5) Πριν από την επέκταση της δραστηριότητας ενός ΣΠΙ σε νέα χρηματοπιστωτικά προϊόντα ή υπηρεσίες πρέπει να υπάρχουν τεκμηριωμένες αποφάσεις ενσωμάτωσής τους στη στρατηγική ανάπτυξης του ΣΠΙ, να έχουν αναγνωρισθεί με ακρίβεια οι σχετικοί κίνδυνοι, συμπεριλαμβανομένου και του λειτουργικού κινδύνου και να έχει ολοκληρωθεί η ενσωμάτωση των αντίστοιχων ελέγχων και διαδικασιών ή η προσαρμογή των υφιστάμενων στο σύστημα διαχείρισης κινδύνων και εσωτερικού ελέγχου, γενικότερα.

(6) Κατά τη λήψη επιχειρηματικών αποφάσεων για την ανάληψη σημαντικών κινδύνων όπως αυτών της χορήγησης δανείων, αναδιάρθρωσης / ρύθμισης υφιστάμενων δανείων, συμμετοχών και επενδύσεων, ή ανάληψη κινδύνων που δεν υπόκεινται σε προκαθορισμένες παραμέτρους, καθώς και στον καθορισμό σχετικών ορίων ανάληψης κινδύνων, πρέπει να διασφαλίζεται από τα ΣΠΙ, τουλάχιστον η συμμετοχή της καθ' ύλην αρμόδιας υπηρεσιακής μονάδας και της Μονάδας Διαχείρισης Κινδύνων.

(7) Στους καταγεγραμμένους και εγκεκριμένους από την Επιτροπεία εσωτερικούς κανονισμούς ή διαδικασίες, πρέπει να προσδιορίζεται με πληρότητα ο βαθμός κατά τον οποίο η λήψη της τελικής απόφασης εξαρτάται από την εισήγηση της Μονάδας Διαχείρισης Κινδύνων.

Συστήματα λογιστικής παρακολούθησης των εργασιών του ΣΠΙ

13.-(1) Από το λογιστικό σύστημα που εφαρμόζει το κάθε ΣΠΙ πρέπει γενικά να προκύπτει η πραγματική εικόνα της οικονομικής κατάστασης, να παρέχονται οι απαραίτητες για τη λήψη αποφάσεων πληροφορίες, καθώς και να διασφαλίζεται η κατάρτιση αξιόπιστων ετήσιων ή περιοδικών χρηματοοικονομικών καταστάσεων, σύμφωνα με τα Διεθνή Λογιστικά Πρότυπα.

(2) (α) Πριν λογιστικοποιηθεί κάθε πράξη, είτε ομοειδείς πράξεις ή λογιστικά γεγονότα, πρέπει να ελέγχεται από τα αρμόδια όργανα η εγκυρότητα και συμφωνία τους, κατά τα προβλεπόμενα στους σχετικούς εσωτερικούς κανονισμούς του ΣΠΙ.

(β) Κάθε ελεγμένη, κατά τα ανωτέρω, πράξη ή πράξεις πρέπει να καταχωρείται στο λογιστικό σύστημα έγκαιρα, με ακρίβεια και με όλες τις απαραίτητες λεπτομέρειες, σύμφωνα με τα προβλεπόμενα από τα εφαρμοζόμενα λογιστικά πρότυπα και αρχές. Οι ανοικτές θέσεις από συναλλαγές που ενέχουν κινδύνους αγοράς θα πρέπει να συμφιλιώνονται (reconciliation) τουλάχιστον κάθε μήνα.

(3) Η συστηματική και ασφαλής τήρηση των αρχείων πρέπει να διασφαλίζεται με κατάλληλες διαδικασίες για χρονικό διάστημα όχι μικρότερο των δέκα ετών και με τρόπο που να επιτρέπει την πραγματοποίηση ελέγχων μεταγενέστερα ("audit trail") και την αναπαραγωγή όλων των συναλλαγών κατά χρονολογική σειρά, την υποστήριξη κάθε καταχωρημένου στοιχείου με πρωτότυπα δικαιολογητικά και την τεκμηρίωση οποιασδήποτε μεταβολής στα υπόλοιπα των λογαριασμών, με αναλυτικά στοιχεία για τις κινήσεις που μεσολάβησαν.

(4) Τα ΣΠΙ οφείλουν να διενεργούν περιοδικούς αλλά και έκτακτους ελέγχους επί των διενεργούμενων λογιστικών καταχωρίσεων, ώστε να παρακολουθείται η πιστή εφαρμογή των μεθόδων αποτίμησης των στοιχείων του ισολογισμού και αναγνώρισης του αποτελέσματος.

(5) Ειδικότερα όσον αφορά τις υποβαλλόμενες στον Έφορο οικονομικές πληροφορίες και στοιχεία θα πρέπει να διασφαλίζουν τα ΣΠΙ ότι:

(α) Είναι πλήρεις, έγκυρες και βασίζονται σε λογιστικά στοιχεία και, προκειμένου περί εξωλογιστικών υπολογισμών ή εκτιμήσεων, ότι έχουν διενεργηθεί με ορθό και κατάλληλα τεκμηριωμένο τρόπο·

(β) υποβάλλονται αρμοδίως εντός των καθορισμένων προθεσμιών.

(6) Τα ΣΠΙ οφείλουν να έχουν καταγεγραμμένες διαδικασίες για την επιλογή και την απόκτηση του κατάλληλου εξοπλισμού και λογισμικού καθώς και για την επαρκή στελέχωση των αρμοδίων υπηρεσιών, ανάλογα με τις εκάστοτε επιχειρησιακές ανάγκες, τις προοπτικές εξέλιξης του μεγέθους και της φύσης των εργασιών και τις οικονομικές δυνατότητές τους, προκειμένου να διασφαλίζεται, ανά πάσα στιγμή, η επαρκής και αποτελεσματική λογιστική και μηχανογραφική υποστήριξη των εργασιών τους.

(7) Τα ΣΠΙ οφείλουν επίσης να έχουν τα απαραίτητα μέσα και εφεδρικά αρχεία δεδομένων, στο πλαίσιο της απαιτούμενης διασφάλισης για τη συνέχιση της επιχειρηματικής τους δραστηριότητας.

Παράρτημα 1

Νοείται ότι, άνευ επηρεασμού της ευθύνης του ιδίου του ΣΠΙ και τηρουμένων των προνοιών του Παραρτήματός 1 της παρούσας Κανονιστικής Απόφασης, καθόσον αφορά θέματα μηχανογράφησης, οι προβλεπόμενες στα εδάφια (6) και (7) ανωτέρω υποχρεώσεις είναι δυνατό να πληρούνται μέσω ή και από κοινού με τη Συνεργατική Εταιρεία Μηχανογράφησης (ΣΕΜ) Λτδ όπως ειδικότερα δυνατό να εξειδικεύεται με οδηγίες του Εφόρου.

Συστήματα πληροφορικής

14. Η λειτουργία των συστημάτων πληροφορικής στοχεύει, αφενός στην αποτελεσματική υποστήριξη της επιχειρησιακής στρατηγικής των ΣΠΙ, αφετέρου στην ασφαλή διακίνηση, επεξεργασία και αποθήκευση των κρίσιμων επιχειρησιακών πληροφοριών. Παράλληλα, η αυξημένη ανάγκη χρήσης συστημάτων πληροφορικής από τα ΣΠΙ, σε συνδυασμό με την τυχόν ανάθεση κρίσιμων έργων πληροφορικής σε τρίτους, ενισχύει συγκεκριμένες κατηγορίες κινδύνων με σημαντικότερη αυτή του λειτουργικού κινδύνου. Οι κίνδυνοι αυτοί πρέπει να προσδιορίζονται, να εντοπίζονται έγκαιρα και να αντιμετωπίζονται αποτελεσματικά. Στο

πλαίσιο της αποτελεσματικής διαχείρισης των κινδύνων που απορρέουν από τη λειτουργία των συστημάτων πληροφορικής, τα ΣΠΙ οφείλουν να υλοποιούν το πλαίσιο αρχών ασφαλούς και αποτελεσματικής λειτουργίας των συστημάτων πληροφορικής που αναφέρεται στο Παράρτημα 2 της παρούσας Κανονιστικής Απόφασης.

Παράρτημα 2

Η επιφύλαξη του εδαφίου (7) της προηγούμενης παραγράφου εφαρμόζεται και για σκοπούς της παρούσας παραγράφου.

Κανονιστική συμμόρφωση

15.-(1) Η Επιτροπεία του ΣΠΙ οφείλει να διασφαλίσει την ύπαρξη πολιτικής για την κανονιστική συμμόρφωση και αποτελεσματικού συστήματος εφαρμογής της, που να αξιολογούνται από αυτή ετησίως. Η πολιτική κανονιστικής συμμόρφωσης αποσκοπεί:

(α) Στην αντιμετώπιση των πάσης φύσεως επιπτώσεων από τυχόν αδυναμία συμμόρφωσης του ΣΠΙ και των επιχειρήσεων προς τις οποίες έχουν εκχωρηθεί δραστηριότητες προς το ισχύον νομοθετικό και κανονιστικό πλαίσιο καθώς, επίσης, τους κώδικες δεοντολογίας στους οποίους τα ΣΠΙ τυχόν προσχωρούν και

(β) στη διαχείριση περιπτώσεων σύγκρουσης συμφερόντων.

(2) Για την υλοποίηση της ως άνω πολιτικής ενδείκνυται η σύσταση Μονάδας Κανονιστικής Συμμόρφωσης και από ΣΠΙ που δεν υποχρεούνται να συστήσουν μια τέτοια Μονάδα σύμφωνα με τις διατάξεις της παραγράφου 28(1), της παρούσας Κανονιστικής Απόφασης.

ΜΕΡΟΣ IV
ΒΕΛΤΙΣΤΕΣ ΑΡΧΕΣ ΕΣΩΤΕΡΙΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ

Βέλτιστες αρχές εσωτερικής διακυβέρνησης

16. (α) Η αποτελεσματική εσωτερική διακυβέρνηση αποτελεί ένα ουσιαστικό στοιχείο για την ασφαλή και υγιή λειτουργία ενός ΣΠΙ.

(β) Η Επιτροπεία είναι αρμόδια για τη χάραξη και την

εφαρμογή πολιτικών και την παρακολούθηση της συμμόρφωσής με αυτές.

(γ) Η αποτελεσματική εποπτεία των εργασιών και των δραστηριοτήτων ενός ΣΠΙ, από πλευράς της Επιτροπείας, συμβάλλει στη διατήρηση ενός αποτελεσματικού και οικονομικά αποδοτικού συστήματος εποπτείας και ελέγχου

Καθορισμός στρατηγικών στόχων και εταιρικών αξιών που πρέπει να διαχέονται σ' όλο το ΣΠΙ.

17. Οι ακόλουθες αρχές θεωρούνται ως στοιχεία μείζονος σημασίας για κάθε διαδικασία εσωτερικής διακυβέρνησης. Η Επιτροπεία του κάθε ΣΠΙ οφείλει να εφαρμόζει τις αρχές αυτές κατά τρόπο ανάλογο προς τη φύση, το μέγεθος και την περιπλοκότητα των λειτουργιών του ΣΠΙ.

(1)(α) Η Επιτροπεία οφείλει να θέσει στρατηγικούς στόχους και να καθιερώσει ηθικά πρότυπα που να κατευθύνουν τις καθημερινές δραστηριότητες του ΣΠΙ, λαμβάνοντας υπόψη τα συμφέροντα των μελών. Η Επιτροπεία οφείλει να πρωτοπορεί και να αποτελεί παράδειγμα προς μίμηση στη διαδικασία καθιέρωσης ενός κώδικα πρότυπων και εταιρικών αξιών για την ίδια την Επιτροπεία, τους Ανώτατους Εκτελεστικούς Διευθυντές και τους υπόλοιπους υπαλλήλους του ΣΠΙ. Είναι ιδιαίτερα σημαντικό όπως τα εν λόγω πρότυπα επιλαμβάνονται θεμάτων διαφθοράς, συμπεριλαμβανομένης και δωροδοκίας, αποκόμισης προσωπικού οφέλους ως, επίσης, και άλλων ανήθικων ή παράνομων συμπεριφορών σε σχέση με τις εσωτερικές και εξωτερικές δραστηριότητες του ΣΠΙ.

(β) Οι εταιρικές αξίες πρέπει να αναγνωρίζουν τη μεγάλη σημασία της έγκαιρης και ειλικρινούς συζήτησης των οποιωνδήποτε προβλημάτων. Οι υπάλληλοι των ΣΠΙ πρέπει να ενθαρρύνονται και να δύνανται να αναφέρουν στην Επιτροπεία ή την Επιτροπή Ελέγχου ή, όπου αυτή δεν υφίσταται, σε εξουσιοδοτημένο υπάλληλο της Μονάδας Εσωτερικής Επιθεώρησης, ελεύθερα τις ανησυχίες τους για οποιεσδήποτε σοβαρές παρατυπίες, παραλείψεις ή αξιόποινες πράξεις που υπέπεσαν στην αντίληψή

τους, χωρίς να φοβούνται για οποιαδήποτε διοικητικά αντίποινα. Η Επιτροπεία οφείλει να διασφαλίσει ότι το ΣΠΙ έχει καθιερώσει διαδικασίες οι οποίες να διευκολύνουν τους υπαλλήλους να αναφέρουν τις σημαντικές τους ανησυχίες, άμεσα ή έμμεσα, μέσω της Επιτροπής Ελέγχου και με εμπιστευτικό τρόπο στην Επιτροπεία, παρακάμπτοντας την ιεραρχία του ΣΠΙ. Οποιαδήποτε τέτοια διαδικασία αναφοράς συγκεκριμένων ανησυχιών θα πρέπει να επιτρέπει και ανώνυμες αναφορές. Η Επιτροπεία οφείλει να παρέχει την ανάλογη προστασία σε υπάλληλους που αναφέρουν οποιεσδήποτε αξιόποινες πράξεις, ανήθικες ή ύποπτες πρακτικές οι οποίοι δεν πρέπει να υπόκεινται σε οποιαδήποτε άμεση ή έμμεση πειθαρχική ή άλλη τιμωρία.

(γ) Η Επιτροπεία οφείλει να διασφαλίζει ότι η Ανώτατη Εκτελεστική Διεύθυνση και οι υπάλληλοι, γενικά, εφαρμόζουν τέτοιες πολιτικές προκειμένου να εντοπίζουν, να αποτρέπουν ή να διαχειρίζονται κατάλληλα καθώς και να αποκαλύπτουν, ανάλογα με την περίπτωση, ενδεχόμενες συγκρούσεις συμφερόντων, οι οποίες μπορούν να προκύψουν ως αποτέλεσμα των διάφορων δραστηριοτήτων και των ρόλων που διαδραματίζει ένα ΣΠΙ υπό την ιδιότητά του ως αποδέκτης καταθέσεων, παροχέας δανείων, επενδυτικών και άλλων χρηματοοικονομικών υπηρεσιών. Οι πολιτικές αυτές οφείλουν να διασφαλίζουν ότι εκείνες οι επιχειρηματικές δραστηριότητες του ΣΠΙ που, ενδεχομένως, θα οδηγήσουν σε σύγκρουση συμφερόντων, διεξάγονται ανεξάρτητα η μια από την άλλη, δημιουργώντας, επί παραδείγματι, κατάλληλους «φραγμούς πληροφοριών» μεταξύ των διάφορων δραστηριοτήτων και καθιερώνοντας ξεχωριστές γραμμές αναφοράς και εσωτερικούς ελέγχους.

(δ) Οι οποιεσδήποτε συγκρούσεις συμφερόντων μεταξύ των προσωπικών συμφερόντων των μελών της Επιτροπείας και του ΣΠΙ ή των μελών/πελατών του θα πρέπει να εντοπίζονται και είτε να αποτρέπονται ή να τυγχάνουν κατάλληλου χειρισμού και να αποκαλύπτονται ανάλογα με την περίπτωση.

(ε) Η Επιτροπεία οφείλει να διασφαλίσει ότι η Ανώτατη Εκτελεστική Διεύθυνση εφαρμόζει στρατηγικές, πολιτικές και διαδικασίες που στοχεύουν στην εμπέδωση επαγγελματικής συμπεριφοράς και ακεραιότητας. Η Επιτροπεία οφείλει, επίσης, να διασφαλίζει ότι η Ανώτατη Εκτελεστική Διεύθυνση εφαρμόζει πολιτικές, οι οποίες αποτρέπουν ή περιορίζουν, ανάλογα με την περίπτωση, δραστηριότητες και σχέσεις που υποβιβάζουν την ποιότητα της εσωτερικής διακυβέρνησης, όπως είναι:

(i) Οι συγκρούσεις συμφερόντων·

(ii) η δανειοδότηση, η αποδοχή καταθέσεων ή η παροχή άλλων υπηρεσιών προς τα μέλη της Επιτροπείας, το Γραμματέα και το λοιπό προσωπικό του ΣΠΙ κατά παράβαση του άρθρου 41ΚΔ του Νόμου ή οποιασδήποτε σχετικής διάταξης των θεσμών, κανονιστικών αποφάσεων ή οδηγιών που εκδίδονται δύναμη αυτού. Ενημέρωση για τη δανειοδότηση των πιο πάνω ατόμων θα πρέπει να παρέχεται στην Επιτροπεία και η δανειοδότηση αυτή θα πρέπει να υπόκειται στον έλεγχο τόσον των εσωτερικών όσον και των εξωτερικών ελεγκτών.

(στ) Η Επιτροπεία οφείλει, επίσης, να διασφαλίσει ότι το ΣΠΙ διατηρεί και εφαρμόζει μια αποτελεσματική λειτουργία κανονιστικής συμμόρφωσης, η οποία να παρακολουθεί συστηματικά τη συμμόρφωση του ΣΠΙ με τη νομοθεσία, κανονιστικές αποφάσεις, διατάγματα, οδηγίες και εγκυκλίους στις οποίες υπόκειται το ΣΠΙ και να εξασφαλίζει ότι οι οποιεσδήποτε αποκλίσεις αναφέρονται στο κατάλληλο ιεραρχικό επίπεδο, ή, εάν είναι αναγκαίο, και στην ίδια την Επιτροπεία.

(2)(α) Η Επιτροπεία

(i) οφείλει να προσδιορίσει με σαφήνεια τις αρμοδιότητές της και τις κυριότερες ευθύνες της καθώς και εκείνες της

Ανώτατης Εκτελεστικής Διεύθυνσης και

(ii) ευθύνεται, κυρίως, για την εποπτεία των ενεργειών της Ανώτατης Εκτελεστικής Διεύθυνσης και τη συμμόρφωσή της με τις πολιτικές της Επιτροπείας.

(β) Οι Ανώτατοι Εκτελεστικοί Διευθυντές ευθύνονται για την κατανομή των δραστηριοτήτων στο προσωπικό και τη δημιουργία μιας διοικητικής δομής και ιεραρχίας που να προάγει την υποχρέωση λογοδοσίας και αναφοράς. Επίσης, οι Ανώτατοι Εκτελεστικοί Διευθυντές έχουν την υποχρέωση όπως παρακολουθούν την εφαρμογή αυτής της κατανομής ευθυνών και να λογοδοτούν στην Επιτροπεία για την απόδοση του ΣΠΙ.

(3) Πριν το διορισμό ή την εκλογή οποιουδήποτε νέου μέλους της Επιτροπείας, το ΣΠΙ αναμένεται να διασφαλίσει ότι το προτεινόμενο μέλος ανταποκρίνεται σε όλες τις απαιτήσεις που προβλέπονται στο Νόμο ή στους Θεσμούς ή σε σχετική Κανονιστική Απόφαση που εκδίδεται κατ' εξουσιοδότησή του.

(4)(α) Η Επιτροπεία έχει την κύρια ευθύνη για τη λειτουργία και διασφάλιση της φερεγγυότητας του ΣΠΙ. Η Επιτροπεία ως σύνολο και ένας έκαστος των μελών του ενισχύουν την εσωτερική διακυβέρνηση του ΣΠΙ, όταν και εφόσον:

(i) Αντιλαμβάνονται τον εποπτικό τους ρόλο και το καθήκον εμπιστοσύνης και επιμέλειας που αναλαμβάνουν έναντι του ΣΠΙ και των μελών του·

(ii) αποφεύγουν τη σύγκρουση ή τη δημιουργία σύγκρουσης συμφερόντων στις δραστηριότητες ή στις δεσμεύσεις που αναλαμβάνουν έναντι άλλων οργανισμών·

(iii) εγκρίνουν τη συνολική επιχειρησιακή στρατηγική του ΣΠΙ, συμπεριλαμβανομένης και της συνολικής πολιτικής και των διαδικασιών διαχείρισης κινδύνων·

(iv) δεν συμμετέχουν σε αποφάσεις της Επιτροπείας όταν

υφίσταται σύγκρουση συμφερόντων που δεν τους επιτρέπει τη σωστή εξάσκηση των καθηκόντων τους·

(v) είναι σε θέση να αφιερώνουν τον απαιτούμενο χρόνο και ενέργεια στην εκτέλεση των καθηκόντων τους·

(vi) η αριθμητική δύναμη της Επιτροπείας είναι τέτοια που να προάγει την αποτελεσματικότητα στη λήψη αποφάσεων και την πραγματική ανταλλαγή απόψεων σε στρατηγικό επίπεδο·

(vii) συνεχίζει να διατηρεί και να αναπτύσσει το απαιτούμενο επίπεδο συλλογικής ειδίκευσης που να ανταποκρίνεται στο αυξανόμενο μέγεθος και πολυπλοκότητα των εργασιών του ΣΠΙ·

(viii) αξιολογεί, περιοδικά, την αποτελεσματικότητα των δικών της διαδικασιών εσωτερικής διακυβέρνησης, συμπεριλαμβανομένων και των διαδικασιών πρότασης και εκλογής νέων μελών της Επιτροπείας και στελεχών της Ανώτατης Εκτελεστικής Διεύθυνσης του ΣΠΙ, εντοπίζει τυχόν αδυναμίες και επιφέρει τις αναγκαίες αλλαγές·

(ix) καθορίζει τα στελέχη-κλειδιά της Ανώτατης Εκτελεστικής Διεύθυνσης, λαμβάνοντας σοβαρά υπόψη τη σπουδαιότητα και κρισιμότητα των καθηκόντων τους σε σχέση με τις επιχειρησιακές ή/και εποπτικές δραστηριότητες του ΣΠΙ·

(x) επιλέγει, παρακολουθεί και, όταν χρειάζεται, μεταθέτει τα στελέχη κλειδιά της Ανώτατης Εκτελεστικής Διεύθυνσης του ΣΠΙ, μεριμνά ούτως ώστε το ΣΠΙ να διαθέτει το απαιτούμενο σχέδιο διαδοχής στελεχών και κρίνει κατά πόσον τα στελέχη που θα διαδεχθούν τα υφιστάμενα είναι ικανά και κατάλληλα να διευθύνουν τις εργασίες του ΣΠΙ·

(xi) παρακολουθεί και εποπτεύει την Ανώτατη Εκτελεστική Διεύθυνση του ΣΠΙ, εξασκώντας το καθήκον και υποχρέωση που έχει να υποβάλλει ερωτήσεις και να

επιμένει να παίρνει σαφείς εξηγήσεις καθώς και έγκαιρες πληροφορίες που να της επιτρέπουν να αξιολογεί την αποτελεσματικότητα της Ανώτατης Εκτελεστικής Διεύθυνσης·

(xii) συναντά, σε τακτά χρονικά διαστήματα, τα στελέχη της Ανώτατης Εκτελεστικής Διεύθυνσης και της Μονάδας Εσωτερικής Επιθεώρησης για να διαμορφώνει και να εγκρίνει πολιτικές, να καθιερώνει γραμμές επικοινωνίας και να παρακολουθεί την πρόοδο επίτευξης των επιχειρησιακών στόχων του ΣΠΙ·

(xiii) προάγει την ασφάλεια και φερεγγυότητα του ΣΠΙ, αντιλαμβάνεται το ρυθμιστικό και εποπτικό περιβάλλον εντός του οποίου δραστηριοποιείται το ΣΠΙ και διατηρεί μια αποτελεσματική και παραγωγική σχέση με τον Έφορο.

(xiv) εκφράζει επαρκή και αντικειμενική γνώμη και συστήνει την υιοθέτηση επαρκών πρακτικών που έχουν εφαρμοσθεί σε άλλες παρόμοιες περιπτώσεις·

(xv) συνεισφέρει εξειδικευμένες γνώσεις στην παρακολούθηση των εργασιών του ΣΠΙ·

(xvi) δεν συμμετέχει στην καθημερινή διοίκηση του ΣΠΙ·

(xvii) εξασκεί επιμέλεια στην παρακολούθηση του έργου των εξωτερικών ελεγκτών.

(β) Η αριθμητική δύναμη και σύνθεση της Επιτροπείας πρέπει να είναι τέτοια που να μπορεί να διαμορφώνει τη δική της ανεξάρτητη γνώμη σε σχέση με εκείνη της Ανώτατης Εκτελεστικής Διεύθυνσης ή σε σχέση με τα διάφορα εξωγενή προς το ΣΠΙ συμφέροντα. Τα ΣΠΙ οφείλουν να προτείνουν για εκλογή προσοντούχα και ανεξάρτητα μέλη της Επιτροπείας που να εμπλουτίζουν και να βελτιώνουν τη στρατηγική κατεύθυνση που δίνει η Επιτροπεία προς την Ανώτατη Εκτελεστική Διεύθυνση του

(γ) Η Επιτροπεία πρέπει να είναι γνώστης όλων των κύριων χρηματοοικονομικών δραστηριοτήτων του ΣΠΙ. Σε περίπτωση, εντούτοις, που μέλη της Επιτροπείας δεν κατέχουν εξειδικευμένες γνώσεις των χρηματοπιστωτικών και άλλων συναφών δραστηριοτήτων του ΣΠΙ, το εν λόγω ΣΠΙ ενθαρρύνεται να εγκαινιάσει εξειδικευμένα και στοχευμένα εκπαιδευτικά προγράμματα για εκείνα τα μέλη της Επιτροπείας που τα χρειάζονται.

(5)(α) Η Επιτροπεία οφείλει να καθορίζει μια αποτελεσματική στρατηγική και πολιτική για τη διατήρηση, σε συνεχή βάση, του ύψους, των κατηγοριών και της κατανομής των ιδίων κεφαλαίων του ΣΠΙ που χρειάζονται για να καλύπτονται επαρκώς όλοι οι κίνδυνοι που αντιμετωπίζει το ΣΠΙ.

(β) Η στρατηγική και πολιτική, αναφορικά με τα ίδια κεφάλαια του ΣΠΙ πρέπει να είναι ολοκληρωμένες και ανάλογες με τη φύση, το μέγεθος και την περιπλοκότητα των δραστηριοτήτων του ΣΠΙ.

(6)(α) Ο ρόλος των εξωτερικών ελεγκτών καθώς και άλλων λειτουργιών ελέγχου, περιλαμβανομένων της κανονιστικής συμμόρφωσης και της νομικής υπηρεσίας, είναι ζωτικής σημασίας για την εσωτερική διακυβέρνηση προκειμένου να επιτευχθεί ένας σημαντικός αριθμός στόχων. Ο ρόλος των πιο πάνω περιλαμβάνει τον εντοπισμό προβλημάτων μέσω των συστημάτων διαχείρισης κινδύνων και του Συστήματος Εσωτερικού Ελέγχου του ΣΠΙ και τη διασφάλιση ότι τα λογιστικά συστήματα του ΣΠΙ παρουσιάζουν μια αληθή εικόνα της οικονομικής κατάστασης και επικερδότητας του ΣΠΙ. Η Επιτροπεία αναμένεται να βελτιώνει την αποτελεσματικότητά του με τους εξής τρόπους:

(i) Αναγνωρίζοντας τη σημασία των διαδικασιών εσωτερικής επιθεώρησης και του Συστήματος Εσωτερικού Ελέγχου και γνωστοποιώντας τη

σημασία τους σε όλο το ΣΠΙ,

(ii) διασφαλίζοντας ότι οι εξωτερικοί ελεγκτές κατανοούν το καθήκον τους έναντι του ΣΠΙ, ασκώντας τη δέουσα επαγγελματική προσοχή σε ότι αφορά τη διενέργεια των ελέγχων,

(iii) αξιοποιώντας με έγκαιρο και αποτελεσματικό τρόπο, τα ευρήματα των εξωτερικών ελεγκτών και έγκαιρα επιλύοντας οποιαδήποτε προβλήματα,

(iv) διασφαλίζοντας την ανεξαρτησία των εξωτερικών ελεγκτών μέσω της αναφοράς τους στην Επιτροπεία ή την Επιτροπή Ελέγχου της Επιτροπείας, και

(v) αναθέτοντας στους εξωτερικούς ελεγκτές την αξιολόγηση βασικών λειτουργιών εσωτερικών ελέγχων.

(β) Η Μονάδα Εσωτερικής Επιθεώρησης του ΣΠΙ οφείλει να δίνει αναφορά απευθείας στην Επιτροπεία μέσω της Επιτροπής Ελέγχου. Οι επικεφαλής της Κανονιστικής Συμμόρφωσης και της Νομικής Υπηρεσίας του ΣΠΙ οφείλουν, επίσης, να δίνουν κατευθείαν αναφορά στην Επιτροπεία. Επιπροσθέτως, συστήνεται όπως τα μη εκτελεστικά και ανεξάρτητα μέλη της Επιτροπείας συναντώνται, χωρίς την παρουσία της Ανώτατης Εκτελεστικής Διεύθυνσης του ΣΠΙ, τουλάχιστον μια φορά ετησίως, με τον εξωτερικό ελεγκτή, και τους επικεφαλής της Μονάδας Εσωτερικής Επιθεώρησης, της Κανονιστικής Συμμόρφωσης και της Νομικής Υπηρεσίας. Τέτοιες συναντήσεις ενισχύσουν την ικανότητα της Επιτροπείας του ΣΠΙ να εποπτεύει την εφαρμογή από την Ανώτατη Εκτελεστική Διεύθυνση των πολιτικών της Επιτροπείας και να διασφαλίζει ότι οι επιχειρηματικές στρατηγικές του ΣΠΙ και η έκθεσή του σε κινδύνους συνάδουν με τα εκάστοτε αποδεκτά ανώτατα όρια ανάληψης κινδύνων, όπως αυτά έχουν καθορισθεί

από την Επιτροπεία του ΣΠΙ.

(γ) Η Επιτροπεία οφείλει να αξιοποιεί το έργο των εξωτερικών ελεγκτών σε σχέση με τις πληροφορίες που λαμβάνονται από την Ανώτατη Εκτελεστική Διεύθυνση σχετικά με τις λειτουργίες και την απόδοση του ΣΠΙ. Οι Ανώτατοι Εκτελεστικοί Διευθυντές οφείλουν, παράλληλα, να κατανοούν τη σημασία ενός αποτελεσματικού εσωτερικού και εξωτερικού ελέγχου για τη μακροπρόθεσμη φερεγγυότητα του ΣΠΙ.

(7)(α) Η Επιτροπεία οφείλει να προσδιορίζει ή να εγκρίνει, όπου χρειάζεται, σύμφωνα με πρότερη εξουσιοδότηση της Ετήσιας Γενικής Συνέλευσης του ΣΠΙ, την αποζημίωση των μελών της Επιτροπείας και την αμοιβή των Ανώτατων Εκτελεστικών Διευθυντών και άλλων στελεχών-κλειδιών και οφείλει να διασφαλίζει ότι εφαρμόζονται οι σχετικές διατάξεις του Νόμου και των Θεσμών και ότι η αποζημίωση ή η αμοιβή αυτή συνάδει με την ιστορία του ΣΠΙ, το εποπτικό του περιβάλλον, τους μακροπρόθεσμους επιχειρηματικούς στόχους και στρατηγική του. Επιβάλλεται, επίσης, όπως οι πολιτικές χρηματικών παροχών/μισθοδοσίας/αποζημίωσης τυγχάνουν χειρισμού από την Επιτροπή Αμοιβών της Επιτροπείας που να αποτελείται καθ'ολοκληρίαν ή κατά πλειοψηφία από μη εκτελεστικά και ανεξάρτητα μέλη της Επιτροπείας προκειμένου να μετριάζει τις ενδεχόμενες συγκρούσεις συμφερόντων και να παρέχει ασφάλεια στα μέλη.

(β) η αποζημίωση των μη εκτελεστικών μελών, ειδικά εκείνων που είναι μέλη των επιτροπών της Επιτροπείας, όπως είναι η Επιτροπή Ελέγχου και η Επιτροπή Διαχείρισης Κινδύνων, πρέπει να εξαρτάται άμεσα από τις ευθύνες τους και τις χρονικές δεσμεύσεις που έχουν αναλάβει και όχι από τις βραχυπρόθεσμες αποδόσεις του ΣΠΙ.

(γ) Στις περιπτώσεις όπου σε Ανώτατους Εκτελεστικούς Διευθυντές ή άλλα στελέχη κλειδιά προσφέρονται κίνητρα με βάση την ετήσια απόδοση του ΣΠΙ, η αμοιβή τους θα πρέπει να υπόκειται

σε αντικειμενικούς όρους και προϋποθέσεις με στόχο την επίτευξη των στόχων και επιδιώξεων του ΣΠΙ στα πλαίσια της συνεργατικής νομοθεσίας.

(8)(α) Η διαφάνεια είναι απαραίτητη για μια επαρκή και αποτελεσματική εσωτερική διακυβέρνηση, καθώς είναι δύσκολο για τα μέλη να παρακολουθούν αποτελεσματικά και να καταλογίζουν ευθύνες στην Επιτροπεία όταν υπάρχει έλλειψη διαφάνειας.

(β) Η έγκαιρη και ακριβής δημοσιοποίηση, επί παραδείγματι, σε προσβάσιμη για το ευρύ κοινό ιστοσελίδα του ΣΠΙ καθώς και στην ετήσια έκθεσή του, είναι επιθυμητή σε ότι αφορά τα ακόλουθα θέματα:

(i) Δομή της Επιτροπείας, τον εσωτερικό κανονισμό λειτουργίας, σύνθεση, διαδικασία επιλογής, προσόντα μελών, διευθυντικές θέσεις μελών σε άλλους οργανισμούς, ανεξαρτησία, σημαντικά συμφέροντα σε σχέση με συναλλαγές ή ζητήματα που επηρεάζουν το ΣΠΙ, μέλη των επιτροπών, κανονισμούς λειτουργίας και υποχρεώσεις των επιτροπών και τη δομή της Ανώτατης Εκτελεστικής Διεύθυνσης, τις ευθύνες της, την ιεραρχική δομή, τα προσόντα και εμπειρία·

(ii) βασική οργανωτική δομή, γενικές συνελεύσεις των μελών και κύριες δραστηριότητες του ΣΠΙ·

(iii) πληροφορίες για το σχέδιο κινήτρων του ΣΠΙ, την πολιτική χρηματικών παροχών / μισθοδοσίας / αποζημίωσης στελεχών, χρηματική παροχή συνδεόμενη με κέρδη ("bonus")·

(iv) τον Κώδικα Δεοντολογίας του ΣΠΙ ή της Επιχειρηματικής Πολιτικής ή/και τον Κώδικα Ηθικής, περιλαμβανομένων οποιωνδήποτε εξαιρέσεων, εάν υπάρχουν, καθώς και

οποιεσδήποτε άλλες σχετικές πολιτικές συγκεκριμένα, το περιεχόμενο οποιουδήποτε κώδικα ή πολιτικής εσωτερικής διακυβέρνησης και τη διαδικασία μέσω της οποίας εφαρμόζεται, καθώς και μια αξιολόγηση από την Επιτροπεία αναφορικά με το βαθμό εφαρμογής αυτού του κώδικα ή της πολιτικής εσωτερικής διακυβέρνησης·

(ν) τη φύση και την έκταση των συναλλαγών με συνδεδεμένα μέρη περιλαμβανομένων οποιωνδήποτε χρηματοπιστωτικών θεμάτων για τα οποία τα μέλη της Επιτροπείας έχουν σημαντικό συμφέρον είτε έμμεσα είτε άμεσα είτε εκ μέρους τρίτων.

ΜΕΡΟΣ V
ΙΚΑΝΟΤΗΤΑ ΚΑΙ ΚΑΤΑΛΛΗΛΟΤΗΤΑΣ ΤΩΝ ΠΡΟΤΕΙΝΟΜΕΝΩΝ ΜΕΛΩΝ ΤΩΝ ΕΠΙΤΡΟΠΕΙΩΝ

Ικανότητα και Καταλληλότητα των Μελών των Επιτροπειών.

18. Το ΣΠΙ κατά την διαδικασία εκλογής και διορισμού των Μελών της Επιτροπείας οφείλει να εφαρμόζει τις σχετικές διατάξεις του Νόμου ή και των Θεσμών ή και οποιασδήποτε Κανονιστικής Απόφασης που εκδίδεται κατ΄ εξουσιοδότηση του Νόμου.

ΜΕΡΟΣ VI
Ο ΡΟΛΟΣ ΤΟΥ ΠΡΟΕΔΡΟΥ ΤΗΣ ΕΠΙΤΡΟΠΕΙΑΣ

Ο ρόλος του Προέδρου της Επιτροπείας

19. Ο Πρόεδρος είναι το κεντρικό πρόσωπο για τη δημιουργία των συνθηκών που συμβάλλουν στη δημιουργία μιας αποτελεσματικής Επιτροπείας ως συνόλου και αποτελεσματικών μελών της Επιτροπείας σε ατομική βάση, τόσο εντός όσο και εκτός της αίθουσας συνεδριάσεων της Επιτροπείας. Πιο συγκεκριμένα, ο Πρόεδρος φέρει την ευθύνη:

(α) Καθοδήγησης της Επιτροπείας και σύνταξης της ημερήσιας διάταξης, η οποία πρέπει να περιλαμβάνει όλα τα θέματα και τους προβληματισμούς όλων των μελών της Επιτροπείας, να προσβλέπει στο μέλλον και να επικεντρώνεται σε θέματα στρατηγικής και όχι σε τυποποιημένες εγκρίσεις διάφορων προτάσεων που μπορούν να συμπεριληφθούν στις εξουσίες που ανατίθενται στην Ανώτατη Εκτελεστική Διεύθυνση του ΣΠΙ·

(β) διασφάλισης ότι τα μέλη της Επιτροπείας λαμβάνουν ορθές, έγκαιρες και σαφείς πληροφορίες, ιδιαίτερα σε σχέση με την απόδοση του ΣΠΙ, που να τους βοηθούν στη λήψη ολοκληρωμένων αποφάσεων, στην αποτελεσματική παρακολούθηση των εργασιών του ΣΠΙ και στην παροχή συμβουλών που να προάγουν την επιτυχή λειτουργία του ΣΠΙ·

(γ) διασφάλισης του απαραίτητου χρόνου για τη συζήτηση περίπλοκων ή επίμαχων θεμάτων διευθετώντας, όταν χρειάζεται, ανεπίσημες συναντήσεις μεταξύ των μελών, για επαρκή προετοιμασία των θεμάτων πριν τη σύγκληση της Επιτροπείας. Είναι ιδιαίτερα σημαντικό να δίνεται ο απαραίτητος χρόνος στα μη εκτελεστικά μέλη της Επιτροπείας για να μελετήσουν τα πιο πάνω θέματα και να μη καλούνται να αποφασίσουν εντός ενός ασφυκτικού χρονοδιαγράμματος·

(δ) καθοδήγησης των νέων μελών της Επιτροπείας μέσω ειδικών προγραμμάτων που οργανώνει η γραμματεία που υποστηρίζει την Επιτροπεία·

(ε) εντοπισμού και ικανοποίησης των ατομικών εκπαιδευτικών αλλά και συλλογικών ενημερωτικών αναγκών των μελών της Επιτροπείας με στόχο τη βελτίωση της συνολικής αποτελεσματικότητας της Επιτροπείας. Η γραμματεία που υποστηρίζει την Επιτροπεία έχει την ευθύνη

διοργάνωσης των διάφορων εκπαιδευτικών προγραμμάτων·

(στ) αξιολόγησης, υπό μορφή έκθεσης, της αποδοτικότητας του συνόλου και ενός εκάστου των μελών της Επιτροπείας και των Επιτροπών της Επιτροπείας τουλάχιστον μια φορά το χρόνο την οποία καταθέτει στην Επιτροπεία·

(ζ) ενθάρρυνση ενεργούς συμμετοχής από όλα τα μέλη της Επιτροπείας.

ΜΕΡΟΣ VII
Ο ΡΟΛΟΣ ΤΟΥ ΜΗ ΕΚΤΕΛΕΣΤΙΚΟΥ ΜΕΛΟΥΣ ΤΗΣ ΕΠΙΤΡΟΠΕΙΑΣ

Ο ρόλος του μη Εκτελεστικού Μέλους της Επιτροπείας

20.-(1) Τα μη εκτελεστικά μέλη της Επιτροπείας, όπως και τα υπόλοιπα μέλη της Επιτροπείας, οφείλουν να:

(α) Διαδραματίζουν πρωτεύοντα ρόλο μεταλαμπαδεύοντας το κατάλληλο επιχειρηματικό πνεύμα ενεργώντας, όμως, εντός ενός πλαισίου συνετών και αποτελεσματικών ελέγχων που να διασφαλίζει την αξιολόγηση και τη διαχείριση των κινδύνων·

(β) συμβάλλουν ενεργά στον καθορισμό των στρατηγικών στόχων του ΣΠΙ, διασφαλίζουν ότι υπάρχουν οι απαραίτητοι οικονομικοί πόροι και το ανθρώπινο δυναμικό που απαιτείται για το ΣΠΙ ώστε να επιτυγχάνονται οι στόχοι του ΣΠΙ και αξιολογούν την απόδοση της διεύθυνσης·

(γ) καθορίζουν τις αξίες και τα πρότυπα του ΣΠΙ και διασφαλίζουν ότι οι υποχρεώσεις του προς τα μέλη του γίνονται κατανοητοί και επιτυγχάνονται.

(2) Πέραν των συνηθισμένων ευθυνών που αναλαμβάνουν, ως μέλη της Επιτροπείας, τα μη εκτελεστικά μέλη οφείλουν να διαδραματίζουν πρωτεύοντα ρόλο ιδίως στους εξής τομείς:

(α) Καθ' όσον αφορά τη στρατηγική, τα μη εκτελεστικά μέλη οφείλουν να εποπτεύουν, με κριτικό και εποικοδομητικό τρόπο, την υφιστάμενη επιχειρησιακή στρατηγική του ΣΠΙ και να βοηθούν στη χάραξη νέων προτάσεων στρατηγικής·

(β) καθ' όσον αφορά την αποδοτικότητα, τα μη εκτελεστικά μέλη οφείλουν να ελέγχουν την αποδοτικότητα των στελεχών της ανώτατης εκτελεστικής διεύθυνσης αναφορικά με την επίτευξη των συμφωνηθέντων στόχων και να παρακολουθούν στενά τις εκθέσεις που τους υποβάλλονται και που σχετίζονται με την αποδοτικότητα των στελεχών·

(γ) καθ' όσον αφορά τους κινδύνους, τα μη εκτελεστικά μέλη οφείλουν να ικανοποιούνται για την αξιοπιστία των οικονομικών πληροφοριών και ότι τα συστήματα οικονομικών ελέγχων και διαχείρισης κινδύνων είναι επαρκή·

(δ) καθ' όσον αφορά το προσωπικό, τα μη εκτελεστικά μέλη είναι υπεύθυνα για τον καθορισμό του κατάλληλου ύψους αποζημίωσης των εκτελεστικών μελών και διαδραματίζουν πρωτεύοντα ρόλο στο διορισμό και, όταν χρειάζεται, στην απομάκρυνση των εκτελεστικών μελών και στο σχεδιασμό πολιτικής διαδοχής.

(3) Για να είναι αποτελεσματικά τα μη εκτελεστικά μέλη της Επιτροπείας οφείλουν να είναι πλήρως ενήμερα για τις εργασίες και το εξωτερικό περιβάλλον εντός του οποίου λειτουργεί το ΣΠΙ και να είναι γνώστες των θεμάτων που σχετίζονται με τις χρηματοπιστωτικές εργασίες. Το μη εκτελεστικό μέλος, πριν το διορισμό, πρέπει να απαιτεί όπως τύχει μιας ολοκληρωμένης, επίσημης και εξειδικευμένης ενημέρωσης αναφορικά με τις εργασίες του ΣΠΙ.

ΜΕΡΟΣ VIII
Ο ΡΟΛΟΣ ΤΟΥ ΜΗ ΕΚΤΕΛΕΣΤΙΚΟΥ ΚΑΙ ΑΝΕΞΑΡΤΗΤΟΥ ΜΕΛΟΥΣ ΤΗΣ ΕΠΙΤΡΟΠΕΙΑΣ

Ο ρόλος του μη Εκτελεστικού και Ανεξάρτητου Μέλους της Επιτροπείας

21.-(1) Προ της εκλογής ενός μη εκτελεστικού και ανεξάρτητου μέλους, η Επιτροπεία οφείλει να διασφαλίσει ότι το υποψήφιο μέλος έχει ανεξάρτητο χαρακτήρα και κρίση και να εξακριβώσει κατά πόσον υφίστανται οποιεσδήποτε διασυνδέσεις ή συνθήκες που πιθανόν να επηρεάζουν ή να φαίνονται ότι μπορεί να επηρεάσουν την κρίση του υποψήφιου μέλους.

(2) Η Επιτροπεία οφείλει να εξηγήσει γιατί, ενδεχομένως, θεωρεί ένα μέλος ως ανεξάρτητο, έστω και αν υφίστανται διασυνδέσεις ή συνθήκες που συνηγορούν υπέρ του αντιθέτου όπως, για παράδειγμα, αν το υποψήφιο μέλος:

(α) Υπήρξε υπάλληλος του ΣΠΙ τα τελευταία πέντε έτη·

(β) διατηρεί ή διατηρούσε τα τελευταία τρία έτη, οποιαδήποτε σημαντική επιχειρηματική σχέση με το ΣΠΙ είτε άμεσα, είτε ως μέτοχος, μέλος Διοικητικού Συμβουλίου ή ανώτατο στέλεχος οργανισμού που διατηρεί ή διατηρούσε τέτοια σχέση με το ΣΠΙ. Για σκοπούς της παρούσας υποπαραγράφου «σημαντική επιχειρηματική σχέση», δεν περιλαμβάνει τη χορήγηση πιστωτικών διευκολύνσεων από το ΣΠΙ δυνάμει του άρθρου 41ΚΔ του Νόμου και του εδαφίου (2) του Θεσμού 57 των περί Συνεργατικών Εταιρειών Θεσμών·

(γ) αμειβόταν ή αμείβεται με πρόσθετα χρηματικά οφέλη από το ΣΠΙ, πέραν των συνηθισμένων δικαιωμάτων του ως μέλος της Επιτροπείας ή συμμετέχει σε σχέδιο απολαβών ανάλογα με την κερδοφορία του ΣΠΙ·

(δ) έχει στενή συγγενική σχέση με τους εξωτερικούς

συμβούλους, τους εξωτερικούς ελεγκτές ή τα άλλα μέλη της Επιτροπείας ή με στελέχη της Ανώτατης Εκτελεστικής Διεύθυνσης του ΣΠΙ. Για σκοπούς της παρούσας υποπαραγράφου «στενή συγγενική σχέση» περιλαμβάνει το σύζυγο ή τη σύζυγο και άτομα πρώτου βαθμού συγγένειας·

(ε) είναι μέλος Διοικητικών Συμβουλίων άλλων εταιρειών ή μέλος Επιτροπειών άλλων συνεργατικών εταιρειών στις οποίες συμμετέχουν άλλα μέλη της Επιτροπείας ή διατηρεί σημαντικές επιχειρηματικές σχέσεις με άλλα μέλη της Επιτροπείας μέσω άλλων εταιρειών και οργανισμών·

(στ) έχει στενή συγγενική σχέση με ένα εκτελεστικό μέλος της Επιτροπείας·

(ζ) έχει διατελέσει μέλος της Επιτροπείας για περίοδο πέραν των εννέα ετών από την ημερομηνία του πρώτου διορισμού του.

(3) Το ΣΠΙ οφείλει να διασφαλίζει τη συμμετοχή στην Επιτροπεία ενός ή στην περίπτωση που απαιτείται η σύσταση Επιτροπής Ελέγχου και Επιτροπής Διαχείρισης Κινδύνων, δύο μη εκτελεστικών και ανεξάρτητων μελών. Ο τρόπος εκλογής ή διορισμού των μη εκτελεστικών-ανεξάρτητων μελών καθορίζεται στους ειδικούς κανονισμούς του ΣΠΙ.

(4) Η Επιτροπεία οφείλει να ορίσει ένα από τα μη εκτελεστικά και ανεξάρτητα μέλη της να ενεργεί ως ανώτερο ανεξάρτητο μέλος της Επιτροπείας, το οποίο να είναι αποδέκτης τυχόν προβληματισμών που έχουν για το ΣΠΙ τα μέλη του, στις περιπτώσεις όπου ο Πρόεδρος της Επιτροπείας ή η Ανώτατη Εκτελεστική Διεύθυνση έχουν αποτύχει να ικανοποιήσουν τους εν λόγω προβληματισμούς ή όπου επαφή με τους πιο πάνω δεν είναι, υπό τις περιστάσεις, ενδεδειγμένη.

(5) Το μη εκτελεστικό και ανεξάρτητο μέλος της Επιτροπείας οφείλει:

(α) Κάτω από οποιεσδήποτε περιστάσεις να διατηρεί ανεξαρτησία σκέψης και γνώμης όταν αναλύει, αποφασίζει και ενεργεί για το ΣΠΙ·

(β) να μην επιδιώκει και να μην αποδέχεται οποιαδήποτε ωφελήματα που, ενδεχομένως, να θεωρηθούν ότι πλήττουν την ανεξαρτησία του·

(γ) με σαφήνεια να αντιτίθεται σε οποιεσδήποτε αποφάσεις της Επιτροπείας που, ενδέχεται, να παραβλάψουν τα συμφέροντα του ΣΠΙ.

(6) Σε περίπτωση που η Επιτροπεία λάβει κάποια απόφαση με την οποία ένα μη εκτελεστικό και ανεξάρτητο μέλος έχει σοβαρή διαφωνία, το τελευταίο πρέπει να αναλογισθεί πολύ σοβαρά τις ευθύνες του. Σε περίπτωση που αποφασίσει να υποβάλει την παραίτησή του, οφείλει να απευθύνει σχετική επιστολή προς την Επιτροπεία, την Επιτροπή Ελέγχου, τους εξωτερικούς ελεγκτές του ΣΠΙ και στον Έφορο στην οποία να αναφέρει τους λόγους της παραίτησής του.

ΜΕΡΟΣ IX
ΟΡΓΑΝΑ ΔΙΟΙΚΗΤΙΚΗΣ ΔΙΑΧΕΙΡΙΣΗΣ ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ ΕΣΩΤΕΡΙΚΟΥ ΕΛΕΓΧΟΥ

Εκτελεστικά μέλη της Επιτροπείας

22. (1) Το κάθε ΣΠΙ υποχρεούται να έχει δύο εκτελεστικά μέλη στην Επιτροπεία.

(2) Ως εκτελεστικά μέλη ορίζονται ο Γραμματέας και ένα εκ των ανωτάτων στελεχών του ΣΠΙ που προτείνεται από την Επιτροπεία και εγκρίνεται από τον Έφορο.

(3) Τηρουμένων των διατάξεων του περί Συνεργατικών Εταιρειών Νόμου και Θεσμών, η συμμετοχή των εκτελεστικών μελών είναι απαραίτητη για την αποτελεσματική διεύθυνση του ΣΠΙ.

Αρμοδιότητες της Επιτροπείας

23. Το κάθε μέλος της Επιτροπείας οφείλει να διαθέτει επαρκείς

γνώσεις και εμπειρία τουλάχιστον για τις σημαντικότερες των δραστηριοτήτων του ΣΠΙ, ώστε η Επιτροπεία να έχει τη δυνατότητα άσκησης εποπτείας επί του συνόλου των εργασιών είτε άμεσα είτε μέσω των Επιτροπών που θεσμοθετούνται υποχρεωτικά ή κατά τη διακριτική ευχέρεια του ΣΠΙ με βάση την παρούσα Κανονιστική Απόφαση. Η Επιτροπεία έχει, γενικά, την ευθύνη για τη συνεπή εφαρμογή των διατάξεων της παρούσας Κανονιστικής Απόφασης και, ιδίως, την ευθύνη:

(α) Του στρατηγικού προσανατολισμού του ΣΠΙ, της επαναξιολόγησής του, σε ετήσια βάση, και της υιοθέτησης κατάλληλων πολιτικών που αποσκοπούν στη διασφάλιση ενός επαρκούς και αποτελεσματικού Συστήματος Εσωτερικού Ελέγχου·

(β) της ύπαρξης κατάλληλης πολιτικής, τόσο για τη διαχείριση κινδύνων με καθορισμό των εκάστοτε αποδεκτών ανωτάτων ορίων ανάληψης κινδύνου, όσο και για την κανονιστική συμμόρφωση·

(γ) της διαμόρφωσης του κατάλληλου εσωτερικού περιβάλλοντος, που να διασφαλίζει ότι κάθε στέλεχος σε όλα τα ιεραρχικά επίπεδα του ΣΠΙ κατανοεί τόσο τη φύση κάθε κινδύνου, που σχετίζεται με τις δραστηριότητες στις οποίες μετέχει ή εποπτεύει, όσο και την ανάγκη της αποτελεσματικής αντιμετώπισής τους, αναγνωρίζει τη σημασία των ελεγκτικών διαδικασιών και διευκολύνει την εφαρμογή τους·

(δ) της υιοθέτησης ενός Κώδικα Ηθικής Συμπεριφοράς που να εφαρμόζεται από την Ανώτατη Εκτελεστική Διεύθυνση και το σύνολο του προσωπικού του ΣΠΙ επί τη βάσει των γενικώς αποδεκτών αρχών οι οποίες περιλαμβάνουν, μεταξύ άλλων, την επιμέλεια, την αποτελεσματικότητα, την υπευθυνότητα, την ευπρέπεια στις σχέσεις με το κοινό, τη μη αίτηση ή αποδοχή ασυνήθους αξίας ωφελημάτων, την

τήρηση επαγγελματικού απορρήτου·

(ε) της παροχής στην Ανώτατη Εκτελεστική Διεύθυνση και τις υπηρεσιακές μονάδες όλων των απαραίτητων μέσων για την υλοποίηση του έργου τους·

(στ) της ακρίβειας των ετήσιων οικονομικών καταστάσεων του ΣΠΙ καθώς και των υποβαλλομένων στον Έφορο στοιχείων

(ζ) της διασφάλισης ότι η λειτουργία του ΣΠΙ είναι σύμφωνη με τα προβλεπόμενα από το θεσμικό πλαίσιο, τους ειδικούς και εσωτερικούς κανονισμούς και τις αρχές της εταιρικής διακυβέρνησης, λαμβάνοντας τα κατάλληλα μέτρα ως προς την επιλογή και τυχόν αντικατάσταση των στελεχών που κατέχουν θέσεις-κλειδιά

(η) της ύπαρξης καταγεγραμμένων διαδικασιών περιλαμβανομένης της ανάθεσης συγκεκριμένων ρόλων και συντονισμό τους, εξουσιοδοτημένων προσώπων για επικοινωνία με τον Έφορο, εναλλακτικές πηγές κάλυψης αναγκών ρευστότητας οι οποίες να διασφαλίζουν:

(i) την αντιμετώπιση έκτακτων καταστάσεων που θέτουν σε κίνδυνο την ομαλή λειτουργία του ΣΠΙ και

(ii) την αποκατάσταση και απρόσκοπτη συνέχιση της επιχειρησιακής του λειτουργίας.

Αρμοδιότητες της Ανώτατης Εκτελεστικής Διεύθυνσης

24. Η Ανώτατη Εκτελεστική Διεύθυνση, η οποία για τους σκοπούς εφαρμογής της παρούσας Κανονιστικής Απόφασης νοείται ως το ανώτατο διοικητικό όργανο με εκτελεστικές αρμοδιότητες, έχει, μεταξύ άλλων, την ευθύνη:

(α) Της συνεπούς υλοποίησης της εγκεκριμένης από την Επιτροπεία επιχειρησιακής στρατηγικής και της εξειδίκευσής της με τη χάραξη κατάλληλης για κάθε λειτουργία πολιτικής, τον καθορισμό επιμέρους στόχων για κάθε τομέα

δραστηριότητας, διοικητικό όργανο και υπηρεσιακή μονάδα. Στο πλαίσιο αυτό εντάσσεται, μεταξύ άλλων:

(i) Η υλοποίηση της εγκεκριμένης από την Επιτροπεία πολιτικής διαχείρισης κινδύνων·

(ii) ο καθορισμός των επιμέρους ορίων και των αρμοδιοτήτων κάθε υπηρεσιακής μονάδας στη διαχείριση των κινδύνων και η αξιολόγηση της απόδοσής της·

(iii) ο διαρκής έλεγχος της διαχείρισης των κινδύνων του ΣΠΙ μέσα στα εγκεκριμένα από την Επιτροπεία όρια ανάληψης·

(β) της ανάπτυξης και ενσωμάτωσης των μηχανισμών και διαδικασιών εσωτερικού ελέγχου, που προσιδιάζουν στο εύρος, το μέγεθος και τη φύση των εργασιών του ΣΠΙ, της περιοδικής αξιολόγησης των σημαντικών, από πλευράς επιπτώσεων, δυσλειτουργιών και της εν γένει αποτελεσματικής εφαρμογής του Συστήματος Εσωτερικού Ελέγχου.

Επιτροπές της Επιτροπείας

25. -(1)(α) ΣΠΙ τα οποία:

(i) διατηρούν θυγατρικές εταιρείες ή υποκαταστήματα στο εξωτερικό ή

(ii) το ενεργητικό τους υπερβαίνει το ποσό των πενηνταπέντε εκατομμυρίων Λιρών Κύπρου,

οφείλουν να προβούν στη σύσταση Επιτροπής Ελέγχου

(β) Η Επιτροπή Ελέγχου ορίζεται από την Επιτροπεία και απαρτίζεται από τουλάχιστον τρία μη εκτελεστικά μέλη, από τα οποία, το ένα τουλάχιστον είναι ανεξάρτητο. Τα μέλη της Επιτροπής Ελέγχου δεν πρέπει να κατέχουν παράλληλες θέσεις ή ιδιότητες ή να διενεργούν συναλλαγές που θα μπορούσαν να

θεωρηθούν *ασυμβίβαστες* με την αποστολή της Επιτροπής.

(γ) Ο Πρόεδρος της Επιτροπής Ελέγχου πρέπει να διαθέτει τις απαιτούμενες γνώσεις και εμπειρία για την επίβλεψη των ελεγκτικών διαδικασιών και των λογιστικών θεμάτων που απασχολούν την Επιτροπή, ενώ η Επιτροπή, ως σύνολο, πρέπει να διαθέτει τη δέουσα κατάρτιση και εμπειρία περιλαμβανομένης της γνώσης για το ευρύτερο περιβάλλον λειτουργίας του ΣΠΙ και για συστήματα πληροφορικής.

(δ) Η λειτουργία της Επιτροπής Ελέγχου διέπεται από εσωτερικό Κανονισμό στον οποίο καθορίζονται η διάρκεια, τα μέλη, η συχνότητα εναλλαγής τους, οι διαδικασίες λήψης των αποφάσεων και τα κύρια καθήκοντά της, στα οποία περιλαμβάνονται μεταξύ άλλων:

(i) Η παρακολούθηση και η ετήσια αξιολόγηση της επάρκειας και αποτελεσματικότητας του Συστήματος Εσωτερικού Ελέγχου με βάση τα σχετικά στοιχεία και πληροφορίες της Μονάδας Εσωτερικής Επιθεώρησης, τις διαπιστώσεις και παρατηρήσεις των εξωτερικών ελεγκτών και του Εφόρου·

(ii) η υποβολή προτάσεων για την αντιμετώπιση των αδυναμιών που έχουν διαπιστωθεί·

(iii) η αξιολόγηση του έργου της Μονάδας Εσωτερικής Επιθεώρησης.

(ε) Η Επιτροπή Ελέγχου συνεδριάζει τουλάχιστον μια φορά κάθε τρίμηνο και ο Πρόεδρός της ενημερώνει την Επιτροπεία για το έργο της Επιτροπής.

(στ) Ανατίθεται τουλάχιστον ανά τριετία από κάθε ΣΠΙ, κατά προτίμηση σε εξωτερικούς ελεγκτές άλλους από τους υφιστάμενους εξωτερικούς ελεγκτές του ΣΠΙ, που διαθέτουν την απαραίτητη εμπειρία, η αξιολόγηση της επάρκειας του Συστήματος Εσωτερικού Ελέγχου. Η σχετική έκθεση αξιολόγησης γνωστοποιείται στον

Έφορο. Οι εν λόγω εξωτερικοί ελεγκτές θα εναλλάσσονται, τουλάχιστον, μετά από δύο διαδοχικές αξιολογήσεις. Σε περίπτωση που το ΣΠΙ επιλέγει τους υφιστάμενους εξωτερικούς ελεγκτές του, η αξιολόγηση θα πρέπει να διενεργείται από άτομα άλλα από αυτά που διεξάγουν ή/και εποπτεύουν το συνήθη έλεγχο του ΣΠΙ.

(2)(α) ΣΠΙ τα οποία διατηρούν θυγατρικές εταιρείες ή υποκαταστήματα στο εξωτερικό και το εντός και εκτός ισολογισμού ενεργητικό τους υπερβαίνει το ποσό των ενός δισεκατομμυρίου Λιρών οφείλουν να προβούν στη σύσταση Επιτροπής Διαχείρισης Κινδύνων.

(β) Κατ' απόκλιση από τα πιο πάνω, ΣΠΙ δύναται, επίσης, να αναθέσει με γνωστοποίηση στον Έφορο των λόγων που επιβάλλουν τη χρήση αυτής της δυνατότητας, τις αρμοδιότητες της Επιτροπής Διαχείρισης Κινδύνων σε ένα τουλάχιστον εκτελεστικό και ένα μη εκτελεστικό μέλος της Επιτροπείας, με επαρκείς γνώσεις και εμπειρία σε θέματα διαχείρισης κινδύνων.

(γ) Η Επιτροπή Διαχείρισης Κινδύνων ορίζεται από την Επιτροπεία και απαρτίζεται από μέλη της με επαρκείς γνώσεις και εμπειρία στον τομέα της διαχείρισης κινδύνων, εκ των οποίων ένα τουλάχιστον μέλος είναι εκτελεστικό και ένα μη εκτελεστικό και ανεξάρτητο.

(δ) Η Επιτροπή Διαχείρισης Κινδύνων διέπεται από εσωτερικό κανονισμό στον οποίο καθορίζονται η διάρκεια, τα μέλη, η συχνότητα εναλλαγής τους, οι διαδικασίες λήψης των αποφάσεων καθώς και τα κύρια καθήκοντά της, μεταξύ των οποίων, συγκαταλέγονται τα εξής:

(i) Η διαμόρφωση της στρατηγικής ανάληψης πάσης μορφής κινδύνων και διαχείρισης κεφαλαίων που ανταποκρίνεται στους επιχειρηματικούς στόχους του ΣΠΙ·

(ii) η ανάπτυξη εσωτερικού περιβάλλοντος διαχείρισης

κινδύνων και της ενσωμάτωσης αυτού στη λήψη των επιχειρηματικών αποφάσεων σε όλο το εύρος των δραστηριοτήτων / μονάδων του ΣΠΙ·

(iii) ο καθορισμός των αρχών που πρέπει να διέπουν τη διαχείριση των κινδύνων·

(iv) η λήψη και η αξιολόγηση, ανά τρίμηνο, αναφορών της Μονάδας Διαχείρισης Κινδύνων και η ενημέρωση της Επιτροπείας σχετικά με τους σημαντικότερους κινδύνους που έχει αναλάβει το ΣΠΙ·

(v) η αξιολόγηση, σε ετήσια βάση, της επάρκειας και της αποτελεσματικότητας της πολιτικής διαχείρισης κινδύνων και της καταλληλότητας των ορίων, της επάρκειας των προβλέψεων και της εν γένει επάρκειας των ιδίων κεφαλαίων σε σχέση με το ύψος και τη μορφή των αναλαμβανόμενων κινδύνων. Η πιο πάνω αξιολόγηση διενεργείται με βάση την ετήσια έκθεση του επικεφαλής της Μονάδας Διαχείρισης Κινδύνων·

(vi) η διατύπωση προτάσεων και η εισήγηση διορθωτικών ενεργειών στην Επιτροπεία, σε περίπτωση που διαπιστώνει αδυναμία υλοποίησης της στρατηγικής για τη διαχείριση κινδύνων.

(ε) Η Επιτροπή Διαχείρισης Κινδύνων πρέπει να συνεδριάζει τουλάχιστον μια φορά κάθε τρίμηνο και ο Πρόεδρός της να ενημερώνει την Επιτροπεία.

(3) Η σύσταση λοιπών επιτροπών από ΣΠΙ αποφασίζεται στη βάση της ανάλυσης κόστους-οφέλους (cost-benefit analysis) και, εν γένει, της αποτελεσματικότητας και η σύστασή τους κοινοποιείται στον Έφορο. Ενδεικτικά οι λοιπές επιτροπές περιλαμβάνουν:

(α) Την Επιτροπή Αμοιβών, η οποία είναι η Επιτροπή που εποπτεύει τις αμοιβές των Ανώτατων Εκτελεστικών Διευθυντών και άλλου σημαντικού προσωπικού και

διασφαλίζει ότι οι αμοιβές συνάδουν με την κουλτούρα, τους στρατηγικούς στόχους και το εποπτικό περιβάλλον του ΣΠΙ·

(β) την Επιτροπή Διορισμών/ Εσωτερικής Διακυβέρνησης η οποία αξιολογεί την αποτελεσματικότητα της ίδιας της Επιτροπείας και υποβάλλει προτάσεις και τροχιοδρομεί τη διαδικασία ανανέωσης και αντικατάστασης των μελών της Επιτροπείας. Η εν λόγω Επιτροπή αξιολογεί, επίσης σε ετήσια βάση, τη δομή, το μέγεθος, τη σύνθεση και την απόδοση της Επιτροπείας και υποβάλλει συστάσεις στην Επιτροπεία αναφορικά με οποιεσδήποτε αλλαγές. Περαιτέρω, η εν λόγω Επιτροπή αξιολογεί σε ετήσια βάση τις δεξιότητες, τη γνώση και την εμπειρογνωμοσύνη των μελών της Επιτροπείας, δίνει αναφορά επί αυτού στην Επιτροπεία, εξετάζει ζητήματα που σχετίζονται με το σχεδιασμό της διαδοχής και αξιολογεί τη συμμόρφωση που επετεύχθη σε σχέση με τις πολιτικές εσωτερικής διακυβέρνησης που ενέκρινε η Επιτροπεία.

(4) Οι επιτροπές της Επιτροπείας θα πρέπει να πληρούν αντιστοίχως τα ακόλουθα ως προς τη σύνθεση, όρους εντολής, διαθέσιμους πόρους, προσέλευσης στις συνεδριάσεις και διαφάνεια:

(α)(i) Οι Επιτροπές της Επιτροπείας, θα πρέπει να αποτελούνται από τουλάχιστον τρία μέλη. Σε ΣΠΙ με μικρό αριθμό μελών στην Επιτροπεία, οι εν λόγω Επιτροπές μπορούν, κατ'εξαίρεση να αποτελούνται από δύο μόνο μέλη.

(ii) Η Προεδρία και τα μέλη των Επιτροπών θα πρέπει να αποφασίζονται λαμβάνοντας υπόψη την ανάγκη ανανέωσης των μελών και διασφαλίζοντας ότι δεν δημιουργείται υπερβολική εξάρτηση της Επιτροπής από ένα συγκεκριμένο μέλος.

(β) Ο ακριβής κανονισμός λειτουργίας της κάθε Επιτροπής πρέπει να περιγράφεται στους όρους εντολής που καταρτίζει η Επιτροπεία.

(γ) Τα ΣΠΙ οφείλουν να διασφαλίζουν ότι οι Επιτροπές διαθέτουν επαρκείς πόρους για να επιτελούν τα καθήκοντά τους, γεγονός το οποίο περιλαμβάνει το δικαίωμα αναζήτησης όλων των απαραίτητων πληροφοριών, ιδιαίτερα από τα στελέχη του ΣΠΙ ή την αναζήτηση επαγγελματικής συμβουλευτικής αρωγής σε ζητήματα που εμπίπτουν στον τομέα αρμοδιότητάς τους.

(δ) Προκειμένου να διασφαλιστεί η αυτονομία και η αντικειμενικότητα των Επιτροπών, μέλη της Επιτροπείας που δεν συμμετέχουν σε Επιτροπές δικαιούνται να παρίστανται μόνο μετά από πρόσκληση της Επιτροπής. Η Επιτροπή δύναται επίσης να προσκαλέσει ή να ζητήσει από ορισμένα στελέχη ή εμπειρογνώμονες να παρίστανται.

(ε) (i) Οι Επιτροπές οφείλουν να ασκούν τα καθήκοντά τους εντός των καθορισμένων όρων εντολής και να διασφαλίζουν ότι υποβάλλουν τακτικά αναφορά στην Επιτροπεία σχετικά με τις δραστηριότητες και τα αποτελέσματά τους·

(ii) για οποιαδήποτε Επιτροπή ήθελε συσταθεί καθορίζονται οι όροι εντολής που επεξηγούν το ρόλο της και οποιαδήποτε εξουσία της δοθεί από την Επιτροπεία και γνωστοποιούνται στον Έφορο. Τα ΣΠΙ οφείλουν επίσης να κοινοποιούν στον Έφορο, σε ετήσια βάση, μια δήλωση που θα ετοιμάζεται από κάθε μία από τις υφιστάμενες Επιτροπές όσον αφορά τη σύσταση τους, τον αριθμό των συνεδριάσεων τους, την προσέλευση σε ετήσια βάση

και τις βασικές δραστηριότητες τους. Επιπλέον, η Επιτροπή Ελέγχου οφείλει να επιβεβαιώνει ότι είναι ικανοποιημένη από την ανεξαρτησία του εσωτερικού ελέγχου και να περιγράφει, εν συντομία, τα βήματα που ακολούθησε για να οδηγηθεί στο συμπέρασμα αυτό·

(iii) Ο Πρόεδρος κάθε Επιτροπής πρέπει να είναι σε θέση να επικοινωνεί άμεσα με τον Έφορο. Οι περιστάσεις κάτω από τις οποίες θα πρέπει να γίνεται κάτι τέτοιο θα πρέπει να καθορίζονται στον εσωτερικό κανονισμό λειτουργίας της κάθε επιτροπής.

Υπηρεσιακές μονάδες των ΣΠΙ
Μονάδα Εσωτερικής Επιθεώρησης

26.-(1) Τα ΣΠΙ οφείλουν να συστήσουν Μονάδα Εσωτερικής Επιθεώρησης που είναι διοικητικά ανεξάρτητη από μονάδες με εκτελεστικές αρμοδιότητες και που αναφέρεται στην Επιτροπεία μέσω της Επιτροπής Ελέγχου. Η Μονάδα Εσωτερικής Επιθεώρησης δεν υπάγεται ιεραρχικά σε άλλη υπηρεσιακή μονάδα του ΣΠΙ, πλην όμως όλες οι εκθέσεις της κοινοποιούνται στον Ανώτατο Εκτελεστικό Διευθυντή.

(2) Οι κύριες αρμοδιότητες της Μονάδας Εσωτερικής Επιθεώρησης είναι:

(α) Η διενέργεια ελέγχων·

(β) η διενέργεια ειδικών ελέγχων·

(γ) η αξιολόγηση του βαθμού εφαρμογής και της αποτελεσματικότητας των διαδικασιών που έχουν θεσπισθεί για τη διαχείριση κινδύνων και τον υπολογισμό των παραμέτρων στις οποίες βασίστηκε η εκτίμηση της κεφαλαιακής επάρκειας του ΣΠΙ·

(δ) μέχρι την πλήρη υιοθέτηση από τα ΣΠΙ της μεθοδολογίας εσωτερικών διαβαθμίσεων που προβλέπεται από τη Οδηγία 2006/48/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 14ης Ιουνίου 2006 σχετικά με την ανάληψη και

την άσκηση δραστηριότητας πιστωτικών ιδρυμάτων, ο Έφορος δύναται να θεωρεί τη Μονάδα Εσωτερικής Επιθεώρησης ως την αρμοδιότερη για την αξιολόγηση του ύψους τυχόν αποκλίσεων από την εκτιμηθείσα, εκ μέρους της Μονάδας Διαχείρισης Κινδύνων, πιθανή ζημιά·

(ε) η αξιολόγηση της οργανωτικής διάρθρωσης, διαχείρισης του ανθρώπινου δυναμικού καθώς και του βαθμού κατά τον οποίο έχουν καθιερωθεί κατάλληλες πολιτικές και διαδικασίες εταιρικής διακυβέρνησης·

(στ) η αξιολόγηση των συστημάτων και μηχανισμών που αφορούν την παραγωγή αξιόπιστης, πλήρους και έγκαιρης χρηματοοικονομικής και διοικητικής πληροφόρησης·

(ζ) η αξιολόγηση των λογιστικών συστημάτων και των συστημάτων πληροφορικής·

(η) η αξιολόγηση των διαδικασιών για την κανονιστική συμμόρφωση·

(θ) η αξιολόγηση του βαθμού κατά τον οποίο τα συλλογικά όργανα και οι μονάδες του ΣΠΙ χρησιμοποιούν αποτελεσματικά τα μέσα και τους πόρους, τηρούν τις κατευθύνσεις και τις διαδικασίες που έχουν αρμοδίως καθορισθεί, μεριμνούν για την εξασφάλιση της πληρότητας και ακρίβειας των στοιχείων και πληροφοριών, μεριμνούν για την ενσωμάτωση σε όλες τις διαδικασίες και συναλλαγές που διενεργούνται, των κατάλληλων προληπτικών και κατασταλτικών ελεγκτικών μηχανισμών·

(ι) η υποβολή προτάσεων για τη θεραπεία τυχόν αδυναμιών που εντοπίζονται στο Σύστημα Εσωτερικού Ελέγχου·

(κ) η παρακολούθηση της εφαρμογής και αποτελεσματικότητας των διορθωτικών μέτρων για την επαρκή αντιμετώπιση των αδυναμιών και των παρατηρήσεων που καταγράφονται στις εκθέσεις των πάσης φύσεως ελέγχων τόσο των εσωτερικών

και εξωτερικών ελεγκτών όσο και του Εφόρου·

(λ) η έγγραφη ενημέρωση της Επιτροπείας από τον επικεφαλής της Μονάδας, μέσω της Επιτροπής Ελέγχου, με κοινοποίηση προς τον Ανώτατο Εκτελεστικό Διευθυντή, τουλάχιστον ανά τρίμηνο, για τις κυριότερες διαπιστώσεις των διενεργούμενων ελέγχων και για τις τυχόν συστάσεις·

(μ) ο έλεγχος κατά πόσον το ΣΠΙ έχει αναπτύξει ικανοποιητικά Σχέδια Συνέχειας Εργασιών και Ανάκαμψης από Καταστροφή·

(ν) η συμμετοχή, ως παρατηρητή, στις δοκιμές των πιο πάνω σχεδίων και η σύνταξη ξεχωριστής έκθεσης αξιολόγησης των αποτελεσμάτων, την οποία να υποβάλλει στην Επιτροπή Ελέγχου και να την κοινοποιεί στις επηρεαζόμενες υπηρεσιακές μονάδες·

(ξ) η ετήσια υποβολή από τον επικεφαλής της Μονάδας στην Επιτροπεία, μέσω της Επιτροπής Ελέγχου, έκθεσης σχετικά με την επάρκεια και αποτελεσματικότητα του Συστήματος Εσωτερικού Ελέγχου, την αποτελεσματικότητα και την τήρηση των διαδικασιών διαχείρισης κινδύνων, των πιστοδοτικών διαδικασιών συμπεριλαμβανομένης της πολιτικής προβλέψεων ως, επίσης, και για την αποτελεσματικότητα των διαδικασιών σε σχέση με την εσωτερική αξιολόγηση της κεφαλαιακής επάρκειας του ΣΠΙ και την εκτίμηση για την πληρότητα της διαδικασίας / μεθοδολογίας υπολογισμού της απομείωσης της αξίας των δανείων και άλλων περιουσιακών στοιχείων·

(ο) η ταξινόμηση και αξιολόγηση των πιστοδοτήσεων κατά κατηγορία πιστωτικού κινδύνου τουλάχιστον κάθε 18 μήνες. Η αξιολόγηση πρέπει να καλύπτει τουλάχιστον το εβδομήντα επί τοις εκατόν του δανειακού χαρτοφυλακίου του ΣΠΙ. Περαιτέρω, θα πρέπει να εντοπίζει τυχόν υπάρχουσες αδυναμίες στην πιστοδοτική πολιτική του ΣΠΙ ή στον τρόπο εφαρμογής της που συντελούν στη δημιουργία προβληματικών απαιτήσεων. Η πρώτη ημερομηνία υποβολής της έκθεσης αυτής θα

καθορισθεί με εγκύκλιο του Εφόρου.

(3) Ο επικεφαλής της Μονάδας Εσωτερικής Επιθεώρησης ορίζεται από την Επιτροπεία, κατόπιν εισήγησης της Επιτροπής Ελέγχου, με γνωστοποίηση προς τον Έφορο, ο οποίος διατηρεί την ευχέρεια να ζητήσει την αντικατάσταση του επικεφαλής σε περίπτωση που κρίνει ότι δεν πληρούνται τα κριτήρια καταλληλότητας / επάρκειας για την εκπλήρωση των σχετικών αρμοδιοτήτων του. Τα καθήκοντα και υποχρεώσεις του επικεφαλής της Μονάδας Εσωτερικής Επιθεώρησης είναι, μεταξύ άλλων, τα ακόλουθα:

(α) Η εκ των υστέρων ενημέρωση του Εφόρου για σημαντικές μεταβολές σε σχέση με την οργάνωση και λειτουργία της Μονάδας Εσωτερικής Επιθεώρησης·

(β) η παρουσία του στις ετήσιες και έκτακτες γενικές συνελεύσεις του ΣΠΙ·

(γ) η παρακολούθηση της διεκπεραίωσης των δραστηριοτήτων που έχουν ανατεθεί σε τρίτους ("outsourcing").

Μονάδα Διαχείρισης Κινδύνων

27.-(1) Τα ΣΠΙ οφείλουν να συστήσουν υπηρεσιακή Μονάδα Διαχείρισης Κινδύνων η οποία είναι διοικητικά ανεξάρτητη από μονάδες με εκτελεστικές αρμοδιότητες.

(2) Η Μονάδα Διαχείρισης Κινδύνων δίνει αναφορά στην Επιτροπεία, μέσω της Επιτροπής Διαχείρισης Κινδύνων, και στον Ανώτατο Εκτελεστικό Διευθυντή.

(3) Η Μονάδα Διαχείρισης Κινδύνων υπόκειται στον έλεγχο της Μονάδας Εσωτερικής Επιθεώρησης ως προς την επάρκεια και αποτελεσματικότητα των διαδικασιών διαχείρισης κινδύνων.

(4) Οι αρμοδιότητες της Μονάδας Διαχείρισης Κινδύνων είναι, μεταξύ άλλων, οι ακόλουθες:

(α) Η χρησιμοποίηση κατάλληλων μεθόδων για τη διαχείριση κινδύνων τους οποίους εν γένει το ΣΠΙ αναλαμβάνει ή στους οποίους μπορεί να εκτεθεί, συμπεριλαμβανομένης της χρήσης υποδειγμάτων ("models") για την πρόβλεψη, αναγνώριση, μέτρηση, παρακολούθηση, αντιστάθμιση, μείωση και αναφορά τους·

(β) η εξειδίκευση των ορίων ανάληψης κινδύνων, καθορίζοντας τις επιμέρους παραμέτρους κατά είδος κινδύνου και ανά κατηγορία αντισυμβαλλομένου, κλάδο, χώρα, νόμισμα, είδος πιστοδοτήσεων, μορφή χρηματοπιστωτικών τίτλων, μετοχών και παραγώγων·

(γ) ο καθορισμός κριτηρίων έγκαιρου εντοπισμού κινδύνων ("early warning system") σε ατομικά και συνολικά χαρτοφυλάκια·

(δ) η διενέργεια, ετησίως, δοκιμών προσομοίωσης καταστάσεων κρίσης ("stress tests") για όλες τις μορφές κινδύνων όπως για παράδειγμα πιστωτικού, αγοράς, επιτοκίων και ρευστότητας·

(ε) προσδιορισμός των κεφαλαιακών απαιτήσεων και ανάπτυξη μεθοδολογιών εκτίμησής τους για την κάλυψη όλων των κινδύνων στους οποίους εκτίθεται το ΣΠΙ και η εισήγηση πολιτικών διαχείρισής τους·

(στ) η σύνταξη από τον επικεφαλής της Μονάδας Διαχείρισης Κινδύνων, τουλάχιστον ανά τρίμηνο, αναφορών προς τον Ανώτατο Εκτελεστικό Διευθυντή και την Επιτροπεία·

(5) η Μονάδα Διαχείρισης Κινδύνων πρέπει να διαθέτει προσωπικό με εξειδικευμένες γνώσεις.

(6) (α) Ο επικεφαλής της Μονάδας Διαχείρισης Κινδύνων ορίζεται από την Επιτροπεία, κατόπιν εισήγησης της Επιτροπής Διαχείρισης Κινδύνων, με γνωστοποίηση προς τον Έφορο, ο οποίος διατηρεί την ευχέρεια να ζητήσει την αντικατάσταση του επικεφαλής σε περίπτωση που κρίνει ότι δεν πληρούνται τα κριτήρια

καταλληλότητας / επάρκειας για την εκπλήρωση των σχετικών αρμοδιοτήτων του.

(β) Τα καθήκοντα του επικεφαλής, μεταξύ άλλων, είναι τα ακόλουθα:

(i) Η υποβολή ετήσιων εκθέσεων στην Επιτροπεία, μέσω της Επιτροπής Διαχείρισης Κινδύνων, σχετικά με τα θέματα που εμπίπτουν στην αρμοδιότητά του·

(ii) Η συμμετοχή στη διαδικασία αξιολόγησης από τον Έφορο της επάρκειας του Οικονομικού και Εποπτικού Κεφαλαίου.

Μονάδα Κανονιστικής Συμμόρφωσης

28.-(1)(α) Η Μονάδα Κανονιστικής Συμμόρφωσης συστήνεται από τα ΣΠΙ που διατηρούν υποκαταστήματα ή θυγατρικά πιστωτικά ιδρύματα στο εξωτερικό και το εντός και εκτός ισολογισμού ενεργητικό τους υπερβαίνει το ένα δισεκατομμύριο Λίρες Κύπρου. Η Μονάδα Κανονιστικής Συμμόρφωσης είναι διοικητικά ανεξάρτητη από μονάδες με εκτελεστικές αρμοδιότητες και αναφέρεται στην Επιτροπεία και στον Ανώτατο Εκτελεστικό Διευθυντή.

(β) Κύρια αρμοδιότητα της Μονάδας Κανονιστικής Συμμόρφωσης είναι η θέσπιση και εφαρμογή κατάλληλων διαδικασιών με στόχο να επιτυγχάνεται η έγκαιρη και διαρκής συμμόρφωση του ΣΠΙ προς το εκάστοτε ισχύον εποπτικό και ρυθμιστικό πλαίσιο. Εξασφαλίζει, ιδίως, ότι το ΣΠΙ συμμορφώνεται με το κανονιστικό πλαίσιο που σχετίζεται με την πρόληψη της χρησιμοποίησης του χρηματοπιστωτικού συστήματος για τη νομιμοποίηση εσόδων από το ξέπλυμα παράνομου χρήματος και την καταπολέμηση της τρομοκρατίας.

(γ) Στην περίπτωση ΣΠΙ που δεν υποχρεούνται δυνάμει της παρούσας Κανονιστικής Απόφασης να συστήσουν Μονάδα Κανονιστικής Συμμόρφωσης, τις σχετικές αρμοδιότητες

αναλαμβάνει και εκτελεί η Μονάδα Διαχείρισης Κινδύνων.

(2) Ο επικεφαλής της Μονάδας Κανονιστικής Συμμόρφωσης υποβάλλει αναφορές, τουλάχιστον, ετησίως στην Επιτροπεία.

(3) Η Μονάδα Κανονιστικής Συμμόρφωσης υπόκειται στον έλεγχο της Μονάδας Εσωτερικής Επιθεώρησης.

(4) Ο επικεφαλής της Μονάδας Κανονιστικής Συμμόρφωσης ορίζεται από την Επιτροπεία με γνωστοποίηση προς τον Έφορο, ο οποίος διατηρεί την ευχέρεια να ζητήσει την αντικατάστασή του επικεφαλής, σε περίπτωση που κρίνει ότι δεν πληρούνται τα κριτήρια καταλληλότητας/επάρκειας για την εκπλήρωση των σχετικών αρμοδιοτήτων του. Ο επικεφαλής λειτουργεί και ως σημείο επικοινωνίας, για τα θέματα ευθύνης του με τον Έφορο παρέχοντας τις αναγκαίες πληροφορίες.

ΜΕΡΟΣ Χ
ΥΠΟΒΟΛΗ ΕΚΘΕΣΕΩΝ ΣΤΟΝ ΕΦΟΡΟ

29. Τα ΣΠΙ οφείλουν να υποβάλλουν στον Έφορο το αργότερο μέχρι τις 30 Απριλίου έκαστου έτους τις πιο κάτω εκθέσεις μαζί με τις αντίστοιχες αξιολογήσεις των αρμόδιων Επιτροπών της Επιτροπείας και των σχετικών αποσπασμάτων από τα πρακτικά των συνεδριάσεων της Επιτροπείας:

(α) Ετήσια έκθεση για την επάρκεια και αποτελεσματικότητα του Συστήματος Εσωτερικού Ελέγχου από τον επικεφαλής της Μονάδας Εσωτερικής Επιθεώρησης·

(β) ετήσια έκθεση για τη διαχείριση κινδύνων από τον επικεφαλής της Μονάδας Διαχείρισης Κινδύνων·

(γ) ετήσια έκθεση από τον επικεφαλής της Μονάδας Κανονιστικής Συμμόρφωσης·

(δ) έκθεση, ανά τριετία, αξιολόγησης της επάρκειας του

Συστήματος Εσωτερικού Ελέγχου από εξωτερικούς ελεγκτές·

Παράρτημα 1

(ε) ετήσια έκθεση σχετικά με την ανάθεση δραστηριοτήτων σε τρίτους·

(στ) έκθεση από τον επικεφαλής της Μονάδας Εσωτερικού Ελέγχου, κάθε δεκαοκτώ μήνες, για τις πιστωτικές διευκολύνσεις που παραχωρήθηκαν.

Η πρώτη ημερομηνία υποβολής των πιο πάνω θα καθορισθεί με εγκύκλιο του Εφόρου,

ΜΕΡΟΣ XI

ΠΟΙΚΙΛΕΣ ΔΙΑΤΑΞΕΙΣ

Ερμηνευτικές Εγκύκλιοι

30. Ο Έφορος εκδίδει διευκρινιστικές ή και ερμηνευτικές εγκυκλίους και καθορίζει σχετικά έντυπα για καλύτερη εφαρμογή της παρούσας Κανονιστικής Απόφασης.

Έναρξη ισχύος

31. Η παρούσα Κανονιστική Απόφαση τίθεται σε ισχύ από την 1.1.2008 και εφαρμόζεται ως προβλέπεται στο μέρος Ι.

ΠΑΡΑΡΤΗΜΑ 1
(Παράγραφοι 6(2)(δ), 15(1)(α) και 29(ε))

ΑΝΑΘΕΣΗ ΔΡΑΣΤΗΡΙΟΤΗΤΩΝ ΣΕ ΤΡΙΤΟΥΣ ("OUTSOURCING")

ΕΙΣΑΓΩΓΗ

1.1. Η ανάθεση δραστηριοτήτων σε τρίτους εμπερικλείει την πιθανότητα μετακύλισης της ευθύνης διαχείρισης κινδύνων και συμμόρφωσης σε τρίτους οργανισμούς οι οποίοι, ενδεχομένως, να μην υπόκεινται σε εποπτικό έλεγχο και ρύθμιση ή / και που, ενδεχομένως, να λειτουργούν εκτός Κύπρου κάτω από διαφορετικά νομικά και ρυθμιστικά πλαίσια. Ο Έφορος απαιτεί όπως τα ΣΠΙ, πέραν της έγκαιρης ενημέρωσής του, εξασφαλίζουν ότι διατηρούν τον πλήρη έλεγχο των εργασιών τους, ότι έχουν υπό τον έλεγχό τους τους υφιστάμενους επιχειρησιακούς τους κινδύνους καθώς, επίσης, και τους νέους κινδύνους που εισάγονται με την ανάθεση δραστηριοτήτων και ότι, τέλος, συμμορφώνονται πλήρως με τις ρυθμιστικές υποχρεώσεις τους.

1.2. Δεν επιτρέπεται η ανάθεση σε τρίτους οποιωνδήποτε δραστηριοτήτων πιστωτικού ιδρύματος ή δραστηριοτήτων που είναι αναπόσπαστα συνδεδεμένες με δραστηριότητες πιστωτικού ιδρύματος ή σχετίζονται με αυτές χωρίς την προηγούμενη γραπτή συγκατάθεση του Εφόρου.

1.3. Τα ΣΠΙ καλούνται να προχωρήσουν και ολοκληρώσουν όλες τις απαραίτητες προπαρασκευαστικές δραστηριότητες προκειμένου να θεσπίσουν τις κατάλληλες διαδικασίες και μηχανισμούς που θα τους επιτρέπουν να συμμορφώνονται πλήρως με τις πρόνοιες του παρόντος Παραρτήματος από την ημερομηνία εφαρμογής της παρούσας Κανονιστικής Απόφασης από κάθε ΣΠΙ. Για όλες τις εργασίες που ήδη τυχόν διεκπεραιώνονται από φορείς παροχής υπηρεσιών, τα ΣΠΙ καλούνται να επαναξιολογήσουν τις σχετικές συμφωνίες και συμβόλαια λαμβάνοντας υπόψη τις διατάξεις του παρόντος Παραρτήματος και όπως λάβουν διορθωτικά μέτρα όπου αυτό είναι απαραίτητο ώστε, το συντομότερο δυνατό, να τροποποιηθούν οι συμβάσεις αυτές προκειμένου να αντιμετωπισθούν οι οποιεσδήποτε παραλείψεις ή αποκλίσεις. Για όλες τις υφιστάμενες συμβάσεις, ο Έφορος θα εκδώσει εγκύκλιο με την οποία θα καθορίζεται η περίοδος εντός της οποίας θα πρέπει οι συμβάσεις αυτές να τροποποιηθούν ώστε να συνάδουν με τις διατάξεις του παρόντος

Παραρτήματος. Με την ανανέωση των συμβάσεων, αυτές θα πρέπει να είναι πλήρως συμβατές με τις παρούσες πρόνοιες.

1.4. Έχοντας υπόψη τα πιο πάνω, απαιτείται όπως με την έναρξη εφαρμογής της παρούσας Κανονιστικής Απόφασης από το ΣΠΙ, υποβληθεί στον Έφορο έκθεση στην οποία να αναφέρονται, με επαρκή λεπτομέρεια, οι τυχόν εργασίες που έχουν ήδη ανατεθεί σε τρίτους, λεπτομέρειες σχετικά με τον αντίστοιχο φορέα παροχής υπηρεσιών και τη διάρκεια της κάθε σύμβασης. Στην έκθεση θα πρέπει, επίσης, να περιλαμβάνονται ικανοποιητικές πληροφορίες όσον αφορά το αποτέλεσμα της αξιολόγησης που έκανε το ΣΠΙ για τις σχετικές συμβάσεις σε σχέση με τις πρόνοιες του παρόντος Παραρτήματος, καθώς επίσης και το πρόγραμμα δράσης για την αποκατάσταση οποιωνδήποτε ανεπαρκειών ή / και αποκλίσεων που τυχόν εντοπισθήκαν, για κάθε σύμβαση χωριστά. ΣΠΙ που δεν έχουν συνάψει οποιεσδήποτε τέτοιες συμφωνίες θα πρέπει επίσης να απαντήσουν, ενημερώνοντας τον Έφορο ανάλογα. Ο Έφορος διατηρεί το δικαίωμα να ζητήσει αναθεώρηση των συμβάσεων ή και τερματισμό τους σε περιπτώσεις που δεν λαμβάνονται τα απαραίτητα μέτρα για σύγκλιση με τις πρόνοιες του παρόντος Παραρτήματος.

II. ΒΑΣΙΚΕΣ ΑΡΧΕΣ ΓΙΑ ΑΝΑΘΕΣΗ ΔΡΑΣΤΗΡΙΟΤΗΤΩΝ ΣΕ ΤΡΙΤΟΥΣ

Κατά την διαδικασία λήψης απόφασης για ανάθεση δραστηριοτήτων σε τρίτους, το ΣΠΙ θα πρέπει να καθοδηγείται και να εφαρμόζει τις πιο κάτω βασικές αρχές:

1. ΣΠΙ που επιθυμεί να προχωρήσει στην ανάθεση δραστηριοτήτων του σε ανεξάρτητους φορείς παροχής υπηρεσιών πρέπει να έχει σε ισχύ πλήρη πολιτική με βάση την οποία να εξετάζεται κατά πόσο ενδείκνυται η ανάθεση και με ποιόν τρόπο πρέπει να γίνεται. Την ευθύνη για την χάραξη της πιο πάνω πολιτικής και τη γενική ευθύνη για δραστηριότητες που υλοποιούνται με βάση την πολιτική αυτή έχει η Επιτροπεία του ΣΠΙ.

   1.1. Πριν από την ανάθεση δραστηριοτήτων σε τρίτους, το ΣΠΙ πρέπει να καθιερώσει συγκεκριμένη πολιτική και κριτήρια βάση των οποίων θα λαμβάνονται οι αποφάσεις για ανάθεση. Η πολιτική θα πρέπει να περιλαμβάνει και κριτήρια όσον αφορά το κατά πόσον και μέχρι ποιο βαθμό ενδείκνυται να γίνει ανάθεση συγκεκριμένων δραστηριοτήτων. Θα πρέπει επίσης να εξετασθούν θέματα

όπως το ενδεχόμενο της συγκέντρωσης κινδύνων, κίνδυνοι που προκύπτουν από την ανάθεση πολλαπλών δραστηριοτήτων στον ίδιο φορέα παροχής υπηρεσιών καθώς επίσης και τα γενικά επιτρεπτά όρια όσον αφορά το σύνολο των εργασιών που ενδείκνυται να ανατεθούν.

1.2. ΣΠΙ που επιθυμεί να αναθέσει οποιεσδήποτε δραστηριότητες του σε φορείς παροχής υπηρεσιών, πρέπει να έχει πλήρη αντίληψη των σχετικών ωφελημάτων, δαπανών και των κινδύνων που συνεπάγονται. Τέτοια ανάθεση απαιτεί ανάλυση και αξιολόγηση των κυρίων δραστηριοτήτων του ΣΠΙ, των δυνατών και αδυνάτων σημείων του, καθώς και των μελλοντικών σχεδίων και των στόχων του.

1.3. Το ΣΠΙ πρέπει να υιοθετήσει τέτοιες διαδικασίες που να του εξασφαλίζουν τη δυνατότητά να επιτηρεί αποτελεσματικά τη εργασία που ανατίθεται.

1.4. Το ΣΠΙ πρέπει να λαμβάνει τα κατάλληλα μέτρα για να εξασφαλίζει τη δυνατότητά του να συμμορφώνεται με όλες τις νομικές και ρυθμιστικές του υποχρεώσεις.

1.5. Καμιά εργασία δεν πρέπει να ανατίθεται από ΣΠΙ εάν αυτό θα εξασθένιζε τη δυνατότητα του Εφόρου να αξιολογεί και να εποπτεύει τις εργασίες του.

1.6. Τουλάχιστον μια φορά κάθε έτος, ο επικεφαλής της Μονάδας Εσωτερικής Επιθεώρησης υποβάλλει έκθεση στην Επιτροπεία, μέσω της Επιτροπής Ελέγχου, σκοπός της οποίας είναι η αξιολόγηση της πληρότητας της πολιτικής για ανάθεση εργασιών σε φορείς παροχής υπηρεσιών. Η Επιτροπεία εξετάζει την αποτελεσματικότητα της εφαρμογής της πολιτικής και καθορίζει τρόπους βελτίωσης της, στηριζόμενη στην πιο πάνω έκθεση καθώς και στις σχετικές παρατηρήσεις της Επιτροπής Ελέγχου, σε περίπτωση που έχει συσταθεί μια τέτοια Επιτροπή. Η έκθεση που ετοιμάζεται θα μπορεί να στηρίζεται σε τυχόν διαπιστώσεις των εξωτερικών ελεγκτών και τυχόν παρατηρήσεις του Εφόρου. Η έκθεση αυτή καθώς και τα σχετικά πρακτικά της συνεδρίασης της Επιτροπείας υποβάλλονται στον Έφορο. Η υποβολή γίνεται σε ετήσια βάση και ως τελευταία ημερομηνία υποβολής ορίζεται η 30η Απριλίου έκαστου έτους, αρχής γενομένης από την ημερομηνία που θα καθορισθεί με εγκύκλιο του Εφόρου. Σε περίπτωση όπου το ΣΠΙ δεν έχει αναθέσει εργασίες σε φορείς παροχής υπηρεσιών θα πρέπει να ενημερώνει σχετικά τον Έφορο με επιστολή του πάνω σε ετήσια βάση.

2. ΣΠΙ που αναθέτει δραστηριότητες σε φορείς παροχής υπηρεσιών πρέπει να υιοθετήσει ένα λεπτομερές πρόγραμμα διαχείρισης κινδύνων με βάση το οποίο θα αντιμετωπίζονται οι κίνδυνοι που σχετίζονται με τις εργασίες που ανατίθενται και θα ρυθμίζονται οι σχέσεις του με τον ανεξάρτητο φορέα παροχής υπηρεσιών.

2.1 Όταν ένα ΣΠΙ επεξεργάζεται το πρόγραμμα διαχείρισης κινδύνων που συνδέονται με τις εργασίες που αναθέτει, κατά την επιμέτρηση των κινδύνων λόγω της ανάθεσης εργασιών θα πρέπει να λαμβάνονται υπόψη διάφοροι παράγοντες όπως η έκταση και η σπουδαιότητα της εργασίας που ανατίθεται, η ικανότητα του ΣΠΙ να προσδιορίζει, διαχειρίζεται, επιτηρεί και ελέγχει τους κινδύνους που προκύπτουν από την ανάθεση και η ικανότητα του φορέα παροχής υπηρεσιών να διαχειρίζεται ικανοποιητικά και να ελέγχει τους πιθανούς κινδύνους του όλου εγχειρήματος.

2.2 Στους παράγοντες που θα συνέτειναν στον εντοπισμό της σπουδαιότητας των εργασιών που ανατίθενται και στην ετοιμασία του προγράμματος διαχείρισης κινδύνων περιλαμβάνονται:

(α) Ο οικονομικός και λειτουργικός αντίκτυπος στο ΣΠΙ καθώς και ο αντίκτυπος από δυσφήμηση και αρνητική δημοσιότητα λόγω αποτυχίας ενός ανεξάρτητου φορέα παροχής υπηρεσιών να εκτελέσει επαρκώς την εργασία.

(β) Το κόστος.

(γ) Πιθανές ζημιές τόσο για μέλη/πελάτες του ΣΠΙ όσο και για τους συνεργάτες τους σε περίπτωση αποτυχίας του ανεξάρτητου φορέα παροχής υπηρεσιών.

(δ) Συνέπειες από την ανάθεση της εργασίας στη δυνατότητα και την ικανότητα του ΣΠΙ να προσαρμόζεται σε εποπτικές/ ρυθμιστικές απαιτήσεις καθώς και σε αλλαγές στις εποπτικές/ρυθμιστικές απαιτήσεις.

(ε) Αλληλεξαρτήσεις και αλληλεπιδράσεις της ανατιθέμενης εργασίας με άλλες εργασίες εντός του ΣΠΙ.

(στ) Επαγγελματική ή άλλου είδους σχέση ανάμεσα στο ΣΠΙ και το φορέα παροχής υπηρεσιών.

(ζ) Την καταλληλότητα και ικανότητα του ανεξάρτητου φορέα παροχής υπηρεσιών καθώς και το αν αυτός υπόκειται σε οποιαδήποτε εποπτεία ή ρύθμιση.

(η) Ο βαθμός δυσκολίας και ο χρόνος που απαιτείται είτε για την επιλογή ενός εναλλακτικού φορέα παροχής υπηρεσιών είτε για την επαναφορά και διεκπεραίωση της δραστηριότητας από το ΣΠΙ, εάν αυτό κριθεί απαραίτητο

(θ) Η πολυπλοκότητα των διευθετήσεων για ανάθεση εργασιών. Παραδείγματος χάριν, η δυνατότητα να ελεγχθούν οι κίνδυνοι στην περίπτωση όπου συνεργάζονται περισσότεροι από ένας φορείς παροχής υπηρεσιών για να παραδώσουν μια ολοκληρωμένη λύση για μια ανάθεση που έγινε.

2.3 Η προστασία των δεδομένων και η ασφάλεια τους καθώς και άλλοι κίνδυνοι μπορούν να επηρεασθούν αρνητικά από την γεωγραφική θέση του φορέα παροχής υπηρεσιών. Για το λόγο αυτό πιθανόν να χρειάζεται εξειδίκευση και πείρα για την αξιολόγηση των κινδύνων που συνδέονται με μια χώρα για παράδειγμα πολιτικοί ή χρηματοοικονομικοί κίνδυνοι ή κίνδυνοι λόγω του νομικού πλαισίου κατά την σύναψη και εφαρμογή συμφωνιών με φορείς παροχής υπηρεσιών που βρίσκονται εκτός Κύπρου.

2.4 Γενικά, ένα πλήρες πρόγραμμα διαχείρισης των κινδύνων που προκύπτουν από αναθέσεις εργασιών πρέπει να προνοεί για συνεχή παρακολούθηση και έλεγχο όλων των πτυχών των σχετικών ρυθμίσεων που διέπουν την ανάθεση. Θα πρέπει, επίσης, να περιλαμβάνει και τις διαδικασίες που θα δίνουν καθοδήγηση ως προς τη λήψη διορθωτικών ενεργειών όταν παρουσιάζονται συγκεκριμένα περιστατικά.

3. ΣΠΙ που αναθέτει δραστηριότητες σε φορείς παροχής υπηρεσιών πρέπει να εξασφαλίζει ότι η ανάθεση εργασιών δεν μειώνει τη δυνατότητά του να εκπληρώνει τις υποχρεώσεις του προς στα μέλη/πελάτες του και προς τον Έφορο, ούτε και να παρεμποδίζεται η δυνατότητα του Εφόρου να ασκεί αποτελεσματική εποπτεία.

3.1. Οι ρυθμίσεις για ανάθεση δεν θα πρέπει να έχουν επιπτώσεις στα δικαιώματα του μέλους/πελάτη έναντι του ΣΠΙ, συμπεριλαμβανομένης της δυνατότητας του να ζητήσει αποζημίωση.

3.2. Οι ρυθμίσεις για ανάθεση δραστηριοτήτων δεν πρέπει να εξασθενίζουν τη δυνατότητα του Εφόρου να ασκεί τις ρυθμιστικές του ευθύνες, όπως είναι η αποτελεσματική εποπτεία του ΣΠΙ.

4. Κατά τη διαδικασία επιλογής ανεξαρτήτων φορέων παροχής υπηρεσιών το ΣΠΙ οφείλει να διεξάγει τον προσήκοντα έλεγχο για διαπίστωση της καταλληλότητας τους.

Το ΣΠΙ πρέπει να καθορίσει τα κριτήρια που θα του επιτρέπουν να αξιολογεί, πριν από την επιλογή, την ικανότητα και την δυνατότητα του ανεξάρτητου φορέα παροχής υπηρεσιών να εκτελεί τις εργασίες που θα του ανατεθούν αποτελεσματικά, με σοβαρότητα και σε υψηλά επίπεδα ποιότητας, σε συνάρτηση με τυχόν κινδύνους που συνδέονται με την επιλογή ενός συγκεκριμένου φορέα παροχής υπηρεσιών. Δεν θα πρέπει να ανατίθενται δραστηριότητες σε έναν φορέα παροχής υπηρεσιών ο οποίος δεν ικανοποιεί τα κριτήρια του ΣΠΙ. Ένας τέτοιος έλεγχος θα πρέπει να περιλαμβάνει:

4.1. Την επιλογή φορέων παροχής υπηρεσιών που να είναι κατάλληλοι και να διαθέτουν επαρκείς πόρους για την εκτέλεση των εργασιών που θα τους ανατεθούν.

4.2. Την εξασφάλιση ότι ο φορέας παροχής υπηρεσιών κατανοεί και είναι σε θέση να επιτύχει τους στόχους του ΣΠΙ σε σχέση με την εργασία που θα του ανατεθεί.

4.3. Την εξακρίβωση της οικονομικής ευρωστίας του φορέα παροχής υπηρεσιών η οποία θα του επιτρέψει να εκπληρώσει τις υποχρεώσεις του. Οποιεσδήποτε ειδικές ανάγκες, όπως η εξυπηρέτηση γεωγραφικά διασκορπισμένων δραστηριοτήτων, θα πρέπει να καθοριστούν και να ικανοποιηθούν με την επιλογή φορέων παροχής υπηρεσιών με ανάλογες ικανότητες και προσβάσεις.

4.4. Τομείς ανησυχίας

(α) Εάν ένας φορέας παροχής υπηρεσιών αποτύχει ή με οποιονδήποτε τρόπο δεν είναι σε θέση να εκτελέσει την εργασία, πιθανόν να είναι δαπανηρή ή / και προβληματική η διαδικασία για εξεύρεση και εφαρμογή, έγκαιρα, εναλλακτικών λύσεων.

(β) Οι δαπάνες κατά το μεταβατικό στάδιο, οι πιθανές περιπλοκές στην διεξαγωγή των εργασιών και η πιθανή απώλεια υφισταμένων εργασιών ή νέων επιχειρηματικών ευκαιριών είναι παράγοντες που θα πρέπει να λαμβάνονται υπόψη.

(γ) Εάν μια δραστηριότητα μεταφέρεται στο εξωτερικό τότε εγείρονται πρόσθετες ανησυχίες. Για παράδειγμα, σε μια έκτακτη κατάσταση, το ΣΠΙ ενδεχομένως να διαπιστώσει ότι του είναι δυσκολότερο να ανταποκριθεί

έγκαιρα. Σε μια τέτοια περίπτωση η διεύθυνση του ΣΠΙ πιθανόν να πρέπει να αξιολογήσει τις οικονομικές, νομικές και πολιτικές συνθήκες οι οποίες πιθανόν να έχουν αρνητική επίδραση στη δυνατότητα του φορέα παροχής υπηρεσιών να λειτουργεί αποτελεσματικά για το ΣΠΙ.

5. Οι αναθέσεις εργασιών και οι σχέσεις ανάμεσα στα συμβαλλόμενα μέρη θα πρέπει να ρυθμίζονται με γραπτές συμβάσεις μέσα από τις οποίες θα περιγράφονται με σαφήνεια και λεπτομέρεια όλες οι πτυχές της συνεργασίας, συμπεριλαμβανομένων των δικαιωμάτων, ευθυνών και προσδοκιών όλων των συμβαλλόμενων μερών.

Οι αναθέσεις εργασιών θα πρέπει να ρυθμίζονται μέσα από μια σαφή και λεπτομερή σύμβαση. Η φύση και η λεπτομέρεια της σύμβασης αυτής θα πρέπει να είναι τέτοια που να συνάδει με την σπουδαιότητα της δραστηριότητας που ανατίθεται σε σχέση με τις εργασίες του ΣΠΙ. Οι κατάλληλες πρόνοιες στη σύμβαση μπορούν να μειώσουν τον κίνδυνο μη εκτέλεσης των υπηρεσιών ή εμφάνισης διαφωνιών σχετικά με το πεδίο, τη φύση και την ποιότητα της υπηρεσίας που θα παρέχεται. Μερικές κύριες διατάξεις μιας σύμβασης είναι:

5.1. Η σύμβαση πρέπει να καθορίσει με σαφήνεια ποιες εργασίες πρόκειται να ανατεθούν, συμπεριλαμβανομένων και των επιθυμητών επιπέδων εξυπηρέτησης και απόδοσης. Η ικανότητα του φορέα παροχής υπηρεσιών να ανταποκριθεί στις υποχρεώσεις του με τις απαιτούμενες επιδόσεις, τόσο ποσοτικά όσο και ποιοτικά, θα πρέπει να αξιολογηθεί εκ των προτέρων.

5.2. Η σύμβαση δεν πρέπει ούτε να αποτρέπει ούτε να εμποδίζει το ΣΠΙ από την εκπλήρωση των εποπτικών/ρυθμιστικών υποχρεώσεών του, ούτε και τον Έφορο από την άσκηση των εποπτικών/ρυθμιστικών εξουσιών του.

5.3. Το ΣΠΙ πρέπει να εξασφαλίσει ότι έχει τη δυνατότητα να έχει πρόσβαση σε όλα τα βιβλία, αρχεία και πληροφορίες σχετικά με τις εργασίες που ανατίθενται.

5.4. Η σύμβαση πρέπει να προνοεί για το συνεχή έλεγχο και αξιολόγηση του φορέα παροχής υπηρεσιών από το ΣΠΙ έτσι ώστε να μπορούν να ληφθούν έγκαιρα οποιαδήποτε διορθωτικά μέτρα κριθούν απαραίτητα.

5.5. Η σύμβαση θα πρέπει να περιγράφει με σαφήνεια και λεπτομέρεια όλες τις πτυχές της διακοπής της συνεργασίας, λόγω κανονικής ή μη λήξης της σύμβασης. Η σύμβαση θα πρέπει επίσης να περιέχει ένα όρο στον οποίο θα καθορίζονται τα χρονοδιαγράμματα για εφαρμογή των όρων της λήξης. Αυτός

θα δίνει την δυνατότητα ανάθεσης των εργασιών σε κάποιο άλλο φορέα παροχής υπηρεσιών ή την ενσωμάτωση τους πίσω στο ΣΠΙ. Ο όρος αυτός θα πρέπει να περιλαμβάνει διατάξεις σχετικά με περιπτώσεις αφερεγγυότητας ή άλλων σημαντικών αλλαγών στην εταιρική μορφή του φορέα παροχής υπηρεσιών, καθώς και το σαφή καθορισμό του ιδιοκτησιακού καθεστώτος οποιασδήποτε πνευματικής ιδιοκτησίας μετά τη λήξη, συμπεριλαμβανομένης της μεταφοράς των πληροφοριών και στοιχείων ή / και όλων των μορφών τεχνογνωσίας πίσω στο ΣΠΙ.

5.6. Ουσιώδη ζητήματα τα οποία αποτελούν ιδιαίτερα χαρακτηριστικά της συμφωνίας για ανάθεση θα πρέπει να διευκρινιστούν. Παραδείγματος χάριν, όταν ο φορέας παροχής υπηρεσιών βρίσκεται στο εξωτερικό, η σύμβαση πρέπει να περιλαμβάνει διατάξεις που να διευκρινίζουν ποιας χώρας η νομοθεσία εφαρμόζεται. Επίσης θα πρέπει να υπάρχουν μηχανισμοί για την αποσαφήνιση, διευκρίνιση και επίλυση τυχόν διαφωνιών μεταξύ των συμβαλλόμενων μερών με βάση τη νομοθεσία.

5.7. Η σύμβαση πρέπει να περιλάβει, όπου είναι απαραίτητο, και όρους που να ρυθμίζουν την ανάθεση εκ μέρους του ανεξάρτητου φορέα παροχής υπηρεσιών της εκτέλεσης του συνόλου ή ενός μέρους της εργασίας που του ανατέθηκε, σε τρίτο φορέα υπηρεσιών. Σε περιπτώσεις όπου κρίνεται σκόπιμο, θα πρέπει να προβλέπεται η έγκριση του ΣΠΙ για τη χρήση τέτοιων υπεργολάβων από το φορέα παροχής υπηρεσιών για το σύνολο ή μέρος της εργασίας. Γενικά, η σύμβαση πρέπει να εξασφαλίζει στο ΣΠΙ τη δυνατότητα να διατηρεί επίπεδο ελέγχου των κινδύνων ίδιο με αυτό της αρχικής σύμβασης στην περίπτωση όπου ο φορέας παροχής υπηρεσιών αναθέτει εργασίες σε υπεργολάβους.

5.8. Κατά τη διαπραγμάτευση, προετοιμασία, ανανέωση ή τροποποίηση μιας σύμβασης για ανάθεση εργασιών, το ΣΠΙ πρέπει να συμβουλεύεται τους νομικούς του συμβούλους.

6. Το ΣΠΙ και οι φορείς παροχής υπηρεσιών πρέπει να καταρτίσουν και να διατηρούν σχέδιο αντιμετώπισης εκτάκτων περιστατικών, συμπεριλαμβανομένου και σχεδίου για την αποκατάσταση των εργασιών και επαναδραστηριοποίησης τα οποία και θα πρέπει να ελέγχουν περιοδικά. Τα εν λόγω σχέδια θα πρέπει να συμμορφώνονται με τις ρυθμιστικές υποχρεώσεις του ΣΠΙ και θα πρέπει να ελεγχθούν και να είναι

από λειτουργικής άποψης πλήρως έτοιμα πριν από την έναρξη της διεκπεραίωσης οποιασδήποτε εργασίας από το φορέα παροχής υπηρεσιών.

6.1. Το ΣΠΙ πρέπει να αξιολογεί και να είναι σε θέση να αντιμετωπίζει τις πιθανές συνέπειες λόγω οποιωνδήποτε δυσχερειών στις εργασίες ή άλλων προβλημάτων από την πλευρά του φορέα παροχής υπηρεσιών. Θα πρέπει επίσης να απαιτεί από αυτόν την ετοιμασία καταλλήλων σχεδίων αντιμετώπισης εκτάκτων περιστατικών-συμβάντων και να εξασφαλίζει τον συντονισμό των σχεδίων αντιμετώπισης εκτάκτων περιστατικών-συμβάντων του ΣΠΙ και αυτών του φορέα παροχής υπηρεσιών. Το ΣΠΙ θα πρέπει επίσης να έχει σχέδιο δράσης σε περίπτωση αδυναμίας του φορέα παροχής υπηρεσιών να ανταποκριθεί.

6.2. Η ύπαρξη συστημάτων πληροφορικής που να παρέχουν υψηλά επίπεδα ασφάλειας είναι μια αναγκαιότητα και για το ΣΠΙ και για το φορέα παροχής υπηρεσιών. Μια διακοπή στην παροχή υπηρεσιών από τα συστήματα πληροφορικής οποιουδήποτε από τους δύο, είτε μια αποτυχία της δυνατότητας των δύο συστημάτων να επικοινωνούν μεταξύ τους κατά τρόπο ασφαλή και αξιόπιστο, θα μπορούσε να εξασθενήσει τη δυνατότητα του ΣΠΙ να εκπληρώνει τις υποχρεώσεις του προς τρίτους, θα μπορούσε να υπονομεύσει τα συμφέροντα των μελών/πελατών του σε θέματα εμπιστευτικότητας, να βλάψει τη φήμη του ΣΠΙ και τέλος να έχει αρνητική επίδραση στο συνολικό προφίλ των λειτουργικών κινδύνων του ΣΠΙ.

6.3. Το ΣΠΙ πρέπει να βρίσκει τρόπους με τους οποίους θα εξασφαλίζει, σε συνεχή βάση, ότι φορείς παροχής υπηρεσιών διατηρούν σε κατάλληλα επίπεδα την ασφάλεια των Πληροφοριακών τους Συστημάτων καθώς και τις δυνατότητες τους για αντιμετώπιση εκτάκτων περιστατικών και αποκατάσταση της λειτουργίας των συστημάτων τους.

6.4. Στα σχέδια αντιμετώπισης εκτάκτων περιστατικών, θα πρέπει να λαμβάνονται υπόψη και τα κόστα για υιοθέτηση εναλλακτικών επιλογών σε περίπτωση όπου θα παρατηρηθεί επιδείνωση στην απόδοση. Σε περίπτωση ανεπαρκούς ανταπόκρισης από το φορέα παροχής υπηρεσιών, οι επιλογές του ΣΠΙ περιλαμβάνουν την αντικατάσταση του φορέα με άλλο, μεταφορά της εργασίας πίσω στο ΣΠΙ, ή σε ακραίες περιπτώσεις έξοδο από την επιχειρηματική δραστηριότητα που επηρεάζεται από την συγκεκριμένη εργασία. Τα πιο πάνω θα μπορούσαν να αποδειχτούν πολύ δαπανηρές επιλογές και θα πρέπει να

ληφθούν μόνο ως τελευταίο μέτρο. Εντούτοις, αυτές οι πιθανότητες και οι σχετικές δαπάνες θα πρέπει να εξεταστούν κατά τη διάρκεια της διαδικασίας διαπραγμάτευσης και να διευκρινιστούν στη σύμβαση.

7. Το ΣΠΙ πρέπει να λάβει τα κατάλληλα μέτρα για να εξασφαλίσει ότι οι φορείς παροχής υπηρεσιών προστατεύουν τις εμπιστευτικές πληροφορίες τόσο του ιδίου του ΣΠΙ όσο και εκείνων των μελών/πελατών του που βρίσκονται στην κατοχή του ΣΠΙ από εκούσια ή ακούσια αποκάλυψή τους σε μη εξουσιοδοτημένα πρόσωπα ή οργανισμούς.

7.1. ΣΠΙ το οποίο προχωρεί στην ανάθεση δραστηριοτήτων σε φορείς παροχής υπηρεσιών αναμένεται να λαμβάνει όλα τα κατάλληλα μέτρα προκειμένου να προστατευθούν οι εμπιστευτικές πληροφορίες των μελών/πελατών του και να εξασφαλίζει ότι οι πληροφορίες αυτές δεν χρησιμοποιούνται για σκοπούς άλλους από αυτούς για τους οποίους παραχωρήθηκαν και ότι αυτές δεν υπόκεινται σε κακή διαχείριση. Για τους σκοπούς αυτούς, στη σύμβαση θα μπορούσαν να περιλαμβάνονται κατάλληλες πρόνοιες που να απαγορεύουν στο φορέα παροχής υπηρεσιών και τους υπεργολάβους του τη χρησιμοποίηση ή την αποκάλυψη πληροφοριών που αποτελούν ιδιοκτησία του ΣΠΙ ή των μελών/πελατών του, εκτός από όσο είναι απαραίτητο για να παρέχουν τις υπηρεσίες που συμφωνήθηκε και για να ικανοποιούν ρυθμιστικές ή νομικές υποχρεώσεις.

7.2. Το ΣΠΙ, λαμβάνοντας υπόψη τις υφιστάμενες νομικές διατάξεις ή κανονισμούς πρέπει, επίσης, να εξετάζει κατά πόσον πρέπει να ειδοποιηθούν τα μέλη/πελάτες του ότι πληροφορίες που σχετίζονται με αυτούς πιθανόν να διαβιβαστούν σε ένα φορέα παροχής υπηρεσιών.

ΠΑΡΑΡΤΗΜΑ 2
(Παράγραφοι 14 και 26(2)(μ))

ΑΡΧΕΣ ΑΣΦΑΛΟΥΣ ΚΑΙ ΑΠΟΤΕΛΕΣΜΑΤΙΚΗΣ ΛΕΙΤΟΥΡΓΙΑΣ ΤΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΣΤΑ ΠΛΑΙΣΙΑ ΤΗΣ ΔΙΑΧΕΙΡΙΣΗΣ ΤΟΥ ΛΕΙΤΟΥΡΓΙΚΟΥ ΚΙΝΔΥΝΟΥ ΑΠΟ ΤΑ ΣΠΙ

Ι. ΕΙΣΑΓΩΓΗ

Το παρόν Παράρτημα παρουσιάζει ένα πλαίσιο γενικών αρχών και κριτηρίων για την ασφαλή και αποτελεσματική λειτουργία των Πληροφοριακών Συστημάτων, λαμβάνοντας, παράλληλα, υπόψη τις πρόσφατες εξελίξεις της πληροφορικής στον βαθμό που επηρεάζουν την λειτουργία των ΣΠΙ.

Το πλαίσιο αυτό αποτελεί τη βάση αξιολόγησης των ΣΠΙ στο συγκεκριμένο τομέα και η εφαρμογή των αρχών του αναμένεται να συμβάλει σημαντικά στην αποτελεσματική διαχείριση του λειτουργικού κινδύνου που σχετίζεται με τα Πληροφοριακά Συστήματα.

Οι αρχές αυτές ομαδοποιούνται στις εξής ενότητες :

1. Οργάνωση και Διοίκηση Πληροφορικής, όπου γίνεται αναφορά στην διακυβέρνηση της πληροφορικής, στην οργάνωση της Υπηρεσιακής Μονάδας της Πληροφορικής και στις σχέσεις με τους εξωτερικούς συνεργάτες.
2. Ανάπτυξη και προμήθεια συστημάτων, όπου γίνεται αναφορά στις μεθοδολογίες, πρότυπα και διαδικασίες ανάπτυξης και προμήθειας Πληροφοριακών Συστημάτων.
3. Λειτουργία και υποστήριξη, όπου γίνεται αναφορά στις διαδικασίες λειτουργίας των συστημάτων, στη φυσική και λογική τους ασφάλεια, καθώς και στη διασφάλιση της συνέχειας των εργασιών του ΣΠΙ.
4. Έλεγχος συστημάτων πληροφορικής, όπου γίνεται αναφορά σε κανόνες και βασικές απαιτήσεις για την επαρκή και αποτελεσματική λειτουργία της Μονάδας Εσωτερικής Επιθεώρησης αναφορικά με τα Πληροφοριακά Συστήματα.

ΙΙ. ΟΡΓΑΝΩΣΗ ΚΑΙ ΔΙΟΙΚΗΣΗ ΤΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

1. Διακυβέρνηση Πληροφορικής

Η Διακυβέρνηση της πληροφορικής ("Information technology governance") είναι ευθύνη της Ανώτατης Εκτελεστικής Διεύθυνσης του ΣΠΙ. Περιλαμβάνει το σύνολο των κατάλληλων επιχειρησιακών δομών και διαδικασιών μέσω των οποίων διασφαλίζεται ότι η πληροφορική υποστηρίζει τη στρατηγική και τους στόχους του ΣΠΙ, διαχειρίζεται αποτελεσματικά τους πόρους που της διατίθενται, αξιολογεί και διαχειρίζεται αποτελεσματικά τους κινδύνους που απορρέουν από την λειτουργία των Πληροφοριακών Συστημάτων, εφαρμόζει πιστά την πολιτική ασφάλειας, είναι σε θέση να μετρήσει την αποτελεσματικότητα και αποδοτικότητά της και τέλος υλοποιεί ένα σύνολο μηχανισμών ελέγχου στα πλαίσια ενός γενικότερου ελεγκτικού πλαισίου.

Για την επίτευξη των προαναφερθέντων το ΣΠΙ θα πρέπει:

(α) να διαθέτει καταγεγραμμένη και εγκεκριμένη στρατηγική για την πληροφορική, συμβατή με τη γενικότερη επιχειρησιακή στρατηγική του τόσο βραχυπρόθεσμα (ετήσια) όσο και μέσο - μακροπρόθεσμα (τριετή) σχέδια. Η στρατηγική της πληροφορικής οφείλει, αφενός μεν να υλοποιεί τους επιχειρησιακούς στόχους που έχουν τεθεί από την Ανώτατη Εκτελεστική Διεύθυνση του ΣΠΙ, αφετέρου δε να διαμορφώνει έγκαιρα την απαραίτητη τεχνολογική υποδομή για τις μελλοντικές ανάγκες του ΣΠΙ.

(β) να διαθέτει Ειδική Καθοδηγητική Επιτροπή για την Πληροφορική ("I.T. Steering Committee"). Επικεφαλής της Επιτροπής συνιστάται να είναι μέλος της Ανώτατης Εκτελεστικής Διεύθυνσης του ΣΠΙ με γνώση των θεμάτων πληροφορικής και μέλη άλλα διευθυντικά στελέχη του ΣΠΙ. Ο ρόλος, τα καθήκοντα και η ελάχιστη σύνθεση της Επιτροπής θα πρέπει να ορίζονται σε επίσημο κανονισμό. Η Επιτροπή, τέλος, θα πρέπει να λαμβάνει γνώση των πορισμάτων των ελέγχων που διενεργούνται στα Πληροφοριακά Συστήματα.

(γ) να αξιολογεί, κατηγοριοποιεί και διαχειρίζεται τους κινδύνους που απορρέουν από την ανάπτυξη, ενσωμάτωση και λειτουργία των Πληροφοριακών Συστημάτων. Οι κίνδυνοι αυτοί θα πρέπει να συνεκτιμούνται με τους υπόλοιπους κινδύνους στους οποίους είναι εκτεθειμένο το ΣΠΙ.

(δ) να διαθέτει καταγεγραμμένη και εγκεκριμένη από την Ανώτατη Εκτελεστική Διεύθυνση Πολιτική Ασφάλειας για τα Πληροφοριακά Συστήματα με τη μορφή αρχών – δεσμεύσεων, οι οποίες να προδιαγράφουν τις κατευθύνσεις και τους στόχους του ΣΠΙ για την αποτελεσματική διαχείριση, προστασία και κατανομή των πληροφοριακών του πόρων.

Το περιεχόμενο της Πολιτικής Ασφάλειας θα πρέπει να κοινοποιείται στο προσωπικό του ΣΠΙ και να υπάρχει από αυτό η έγγραφη αποδοχή του. Πέραν της Πολιτικής Ασφάλειας, να διαθέτει την κατάλληλη διοικητική δομή που να εγγυάται τη ασφάλεια των επιχειρησιακών πληροφοριών. Στο πλαίσιο αυτής της δομής θα πρέπει τουλάχιστον να προβλέπεται θέση Υπεύθυνου Ασφάλειας Πληροφοριακών Συστημάτων, η αμεροληψία και η ανεξαρτησία του οποίου θα πρέπει να είναι διασφαλισμένη.

(ε) να μεριμνά ώστε οι υπάρχουσες πολιτικές, πρότυπα, διαδικασίες και μεθοδολογίες να είναι επίσημα καταγεγραμμένες και εγκεκριμένες από τα αρμόδια υπηρεσιακά όργανα.

(στ)να διαθέτει πρότυπα και μεθοδολογίες για το σχεδιασμό και την ανάπτυξη των Πληροφοριακών Συστημάτων, καθώς και διαδικασίες για την καθημερινή τους λειτουργία και υποστήριξη.

(ζ) να διαθέτει πρότυπα και διαδικασίες για τη διαχείριση και την αποτελεσματική εκτέλεση των έργων πληροφορικής. Στην πρόταση για την υλοποίηση κάθε μεγάλου έργου πληροφορικής πρέπει να προσδιορίζεται ο επιχειρησιακός στόχος, καθώς και τα ποιοτικά και ποσοτικά οφέλη που θα αποφέρει η υλοποίησή του.

(η) να εγγυάται την ποιότητα των παρεχόμενων υπηρεσιών πληροφορικής μέσω της ύπαρξης διαδικασιών διασφάλισης ποιότητας και εναρμόνισης με τα πρότυπα ποιότητας σε όλα τα στάδια του κύκλου ζωής των συστημάτων.

(θ) να διαθέτει τις κατάλληλες διαδικασίες για τον έγκαιρο εντοπισμό και την αποτελεσματική αντιμετώπιση των προβλημάτων που προκύπτουν στα Πληροφοριακά Συστήματα.

(ι) να διαθέτει διαδικασίες καταγραφής και κατηγοριοποίησης των γεγονότων που δημιουργούν λειτουργικό κίνδυνο, συμπεριλαμβανομένων των ζημιών ("detailed event type logging" και "classification") που προέρχονται από προβλήματα στα Πληροφοριακά Συστήματα για παράδειγμα μη εξουσιοδοτημένη δραστηριότητα, κλοπή μηχανογραφικού εξοπλισμού, απάτη, παραβίαση ασφάλειας, μη

διαθεσιμότητα συστημάτων, καταστροφή μηχανογραφικού εξοπλισμού, κακόβουλη χρήση, και ενημέρωσης των αρμόδιων υπηρεσιακών μονάδων, της Διαχείρισης Κινδύνων και της Εσωτερικής Επιθεώρησης, για την αποτελεσματικότερη καταγραφή και αντιμετώπιση του λειτουργικού κινδύνου.

(κ) να διαθέτει σύστημα διοικητικών πληροφοριών ("Management Information System"), κατάλληλο για την αποτελεσματική πληροφόρηση της Ανώτατης Εκτελεστικής Διεύθυνσης του ΣΠΙ. Ένα τέτοιο σύστημα θα πρέπει να χαρακτηρίζεται από την ομοιόμορφη και βάσει καταγεγραμμένων διαδικασιών συλλογή και επεξεργασία, την έγκαιρη διάθεση, την ακρίβεια, την αξιοπιστία, και την πληρότητα των πληροφοριών.

(λ) να γνωρίζει και να συμμορφώνεται με το νομικό, εποπτικό και κανονιστικό πλαίσιο σε ό,τι αφορά θέματα πληροφορικής.

(μ) να μελετά, να αξιολογεί και να εφαρμόζει, όπου κρίνει απαραίτητο, τα διεθνή πρότυπα και μεθοδολογίες διαχείρισης και ασφάλειας των Πληροφοριακών Συστημάτων, καθώς επίσης να παρακολουθεί και να λαμβάνει υπόψη τις διεθνείς εξελίξεις στους συγκεκριμένους τομείς.

2. Οργάνωση της Υπηρεσιακής Μονάδας Πληροφορικής

Το ΣΠΙ θα πρέπει να διαθέτει εξειδικευμένη Υπηρεσιακή Μονάδα Πληροφορικής, λειτουργικά και διοικητικά ανεξάρτητη από τους τελικούς χρήστες των υπηρεσιών πληροφορικής, η οποία θα πρέπει:

(α) να διαθέτει οργανόγραμμα στο οποίο:

i. απεικονίζονται οι επιχειρησιακές και οργανωτικές ανάγκες της μονάδας και περιγράφονται με σαφήνεια οι αρμοδιότητες των επί μέρους υπηρεσιακών μονάδων που το αποτελούν,

ii. απεικονίζεται ο διαχωρισμός των καθηκόντων προκειμένου να αποκλείεται η ύπαρξη ασυμβίβαστων ρόλων, παρέχεται η δυνατότητα καταλογισμού των ευθυνών και αξιοποιούνται με τον καταλληλότερο τρόπο οι δυνατότητες του προσωπικού. Ειδικότερα, θα πρέπει να διασφαλίζεται ότι διαχωρίζονται πλήρως οι λειτουργίες που σχετίζονται με το σχεδιασμό και την ανάπτυξη των συστημάτων από τις λειτουργίες που αφορούν στην καθημερινή λειτουργία τους,

iii. προβλέπεται, ανάλογα με το μέγεθος του ΣΠΙ και την πολυπλοκότητα των συστημάτων, υπηρεσιακή Μονάδα Ασφάλειας των Πληροφοριακών

Συστημάτων. Στις αρμοδιότητές της περιλαμβάνονται, μεταξύ άλλων, η συμμετοχή στην αξιολόγηση και διαχείριση των κινδύνων των Πληροφοριακών Συστημάτων, η σύνταξη και ενημέρωση της πολιτικής ασφάλειας, η συμμετοχή στη διαδικασία εύρεσης λύσεων για την κάλυψη κενών ασφάλειας και την αντιμετώπιση έκτακτων περιστατικών και

iv. εξασφαλίζεται η αναπλήρωση του προσωπικού τουλάχιστον στις κρίσιμες μηχανογραφικές λειτουργίες.

(β) να διαθέτει καταγεγραμμένες και επίσημα εγκεκριμένες περιγραφές θέσεων εργασίας στις οποίες θα περιλαμβάνονται οι αρμοδιότητες, οι υπευθυνότητες και οι δεξιότητες που απαιτούνται για κάθε θέση.

3. Σχέσεις με Εξωτερικούς Συνεργάτες

Όταν το ΣΠΙ συνεργάζεται με εξωτερικούς συνεργάτες σε θέματα πληροφορικής, για παράδειγμα με πάροχους υπηρεσιών πληροφορικής και με προμηθευτές, κατά τα προβλεπόμενα στο "Παράρτημα 1" της παρούσας Κανονιστικής Απόφασης θα πρέπει να λαμβάνονται υπόψη ειδικότερα τα εξής:

(α) η χρήση εξωτερικών συνεργατών, ενώ μπορεί να επιλύει σημαντικά προβλήματα, δημιουργεί πεδίο πρόσθετων κινδύνων για το ΣΠΙ, οι οποίοι πρέπει να εντοπισθούν, εκτιμηθούν και αντιμετωπισθούν αποτελεσματικά. Στους κινδύνους αυτούς περιλαμβάνονται η πιθανή έλλειψη ουσιαστικού ελέγχου στις προσφερόμενες υπηρεσίες, η εξάρτηση από τρίτους, η απώλεια εσωτερικής τεχνογνωσίας, η ενδεχόμενη αδυναμία άμεσης προσαρμογής στις απαιτήσεις των μελών/πελατών και του οικονομικού περιβάλλοντος, η αδιαφανής κοστολόγηση των προσφερόμενων υπηρεσιών και η διαφορά νοοτροπίας μεταξύ του ΣΠΙ και παρόχου.

(β) σε περίπτωση που αποφασίσει να αναθέσει μέρος ή και το σύνολο των υπηρεσιών πληροφορικής σε εξωτερικούς συνεργάτες, πρέπει να τηρούνται οι αρχές του "Παραρτήματος 1" της παρούσας Κανονιστικής Απόφασης.

(γ) η ανάθεση υλοποίησης σημαντικών για το ΣΠΙ συστημάτων σε τρίτους, θα πρέπει να αιτιολογείται από την Ειδική Συντονιστική Επιτροπή για την Πληροφορική

εγγράφως προς την Ανώτατη Εκτελεστική Διεύθυνση, η οποία και παρέχει την τελική έγκρισή της.

ΙΙΙ. ΑΝΑΠΤΥΞΗ ΚΑΙ ΠΡΟΜΗΘΕΙΑ ΣΥΣΤΗΜΑΤΩΝ

Ο κύκλος ζωής ενός συστήματος πρέπει να χαρακτηρίζεται από διακριτές φάσεις, οι οποίες θα υλοποιούν πρότυπα, μεθοδολογίες και διαδικασίες επίσημα καταγεγραμμένες και εγκεκριμένες. Η εποπτεία του έργου της ανάπτυξης κάθε σημαντικού συστήματος πρέπει να ανατίθεται στην Ειδική Συντονιστική Επιτροπή για την Πληροφορική ("IT Steering Committee"). Με την ολοκλήρωση της ανάπτυξης του συστήματος, η επιχειρησιακή και τεχνική του εποπτεία θα πρέπει να ανατίθεται στις αρμόδιες υπηρεσιακές μονάδες ή στελέχη.

Πριν την ανάπτυξη ή προμήθεια ενός σημαντικού συστήματος πρέπει να γίνεται μελέτη σκοπιμότητας.

1. Ανάπτυξη Συστημάτων

Στις περιπτώσεις που το ΣΠΙ επιλέγει την εσωτερική ανάπτυξη ενός Πληροφοριακού Συστήματος, θα πρέπει:

(α) πριν την έναρξη της ανάπτυξης, να ορισθεί Ομάδα Έργου που θα αναλάβει την διαχείριση του έργου και την κατάρτιση ενός χρονοδιαγράμματος υλοποίησης

(β) το χρονοδιάγραμμα υλοποίησης να προσδιορίζει, μεταξύ άλλων, τις φάσεις, τη διάρκεια τους, και τους υπεύθυνους για την υλοποίηση της κάθε φάσης, καθώς και τα παραδοτέα.

(γ) να ορίζεται ένα σχέδιο επικοινωνίας, στο οποίο θα καθορίζονται οι διαδικασίες ενημέρωσης των εμπλεκομένων μερών για την πρόοδο του έργου.

(δ) να λαμβάνονται υπόψη θέματα αποδοχής και αποτελεσματικής λειτουργίας του νέου Πληροφοριακού Συστήματος από τους χρήστες.

(ε) να γίνει λεπτομερής σχεδιασμός για τη διαχείριση των δεδομένων του προϋπάρχοντος μηχανογραφικού ή μη συστήματος και να περιλαμβάνει θέματα εκκαθάρισης παλαιών δεδομένων ("data cleansing"), μετατροπής δεδομένων στην μορφή του νέου συστήματος ("data conversion") και μετάπτωσης δεδομένων ("data migration").

(στ) στις φάσεις της τεχνικής ανάλυσης και του σχεδιασμού να διενεργείται ανάλυση κινδύνων και να καθορίζονται με λεπτομέρεια οι απαιτήσεις ασφαλούς λειτουργίας του συστήματος σύμφωνα και με όσα προβλέπει η ισχύουσα Πολιτική Ασφάλειας του ΣΠΙ.

(ζ) η ανάπτυξη του συστήματος να υλοποιείται σε ξεχωριστό μηχανογραφικό περιβάλλον από αυτό της παραγωγής και να ακολουθεί πρότυπα που έχουν τεθεί

(η) οι δοκιμές του συστήματος να διενεργούνται σε πρώτη φάση από το προσωπικό της Υπηρεσιακής Μονάδας Πληροφορικής σε ξεχωριστό περιβάλλον. Σε δεύτερη φάση θα πρέπει να γίνονται τεκμηριωμένες και ολοκληρωμένες και είναι απαραίτητο να συμμετέχουν, πέραν των προγραμματιστών, η Μονάδα Διασφάλισης Ποιότητας (όπου υπάρχει), ο Υπεύθυνος Ασφάλειας ("Security Officer") και η Μονάδα Εσωτερικής Επιθεώρησης.

(θ) η μεταφορά του νέου συστήματος στην παραγωγή να πραγματοποιείται από εξειδικευμένο προσωπικό όπως για παράδειγμα βιβλιοθηκάριων (librarians) βάσει καταγεγραμμένων οδηγιών.

(ι) το σύστημα, πριν ακόμη τεθεί σε λειτουργία, να διαθέτει πλήρη τεκμηρίωση που θα ακολουθεί συγκεκριμένα ποιοτικά πρότυπα που έχουν τεθεί από το ίδιο το ΣΠΙ.

(κ) να πραγματοποιείται εκπαίδευση των χρηστών του συστήματος σε ξεχωριστό περιβάλλον, το οποίο και δεν θα επηρεάζεται από τα περιβάλλοντα ανάπτυξης και παραγωγής.

(λ) η λειτουργία και υποστήριξη του συστήματος να περιλαμβάνει διαδικασίες ελέγχου των αλλαγών ("change control"), ελέγχου των εκδόσεων του συστήματος ("versioning"), ελέγχου ενημερώσεων του συστήματος για την αντιμετώπιση προβλημάτων που εντοπίστηκαν ("patching"), ελέγχου της απόδοσης του συστήματος, λήψης και φύλαξης εφεδρικών αρχείων, συνέχειας των εργασιών, ενημέρωσης του "Help Desk" για την υποστήριξη των χρηστών του συστήματος, κτλ.

(μ) η φάση απόσυρσης του συστήματος να περιλαμβάνει διαδικασίες για τη διατήρηση των πληροφοριών σύμφωνα με τις νομικές και εποπτικές οδηγίες ("information preservation"), τη διαγραφή των πληροφοριών από τα μέσα αποθήκευσης ("media sanitization"), την απόσυρση του υλικού και λογισμικού ("hardware & software disposal").

2. Προμήθεια Συστημάτων

Στις περιπτώσεις που το ΣΠΙ αποφασίζει την προμήθεια Πληροφοριακών Συστημάτων θα πρέπει, εκτός των προαναφερθέντων:

(α) η όλη διαδικασία προμήθειας να χαρακτηρίζεται από διακριτές φάσεις, οι οποίες θα υλοποιούν πρότυπα, μεθοδολογίες και διαδικασίες επίσημα καταγεγραμμένες και εγκεκριμένες. Τέτοιες φάσεις, είναι αυτές της πρόσκλησης για υποβολή προτάσεων ("Request for proposal") με αναλυτική περιγραφή των αναγκών που θα καλύπτει το προς προμήθεια σύστημα, της επιλογής του εξωτερικού συνεργάτη, της σύναψης της συμφωνίας και της υπογραφής του συμβολαίου, της ένταξης και λειτουργίας των συστημάτων στην παραγωγή και, τέλος, της εποπτείας και του ελέγχου τους.

(β) η επιλογή του συστήματος να γίνεται με βάση τις αναλυτικές προδιαγραφές που οφείλει να θέτει το ΣΠΙ,

(γ) το είδος παρέμβασης του ΣΠΙ στο σύστημα να είναι εκ των προτέρων αυστηρά καθορισμένο. Οι όποιες παρεμβάσεις θα πρέπει να ακολουθούν εγκεκριμένες και καταγεγραμμένες διαδικασίες, να υλοποιούνται από εξειδικευμένο προσωπικό και να διατηρούνται στο ελάχιστο δυνατό επίπεδο έτσι ώστε να μην αλλοιώνεται η φυσιογνωμία του συστήματος και να είναι εύκολη η αναβάθμιση και συντήρησή του. Σημειώνεται ότι, σε περίπτωση σημαντικής απόκλισης των λειτουργικών διαδικασιών του ΣΠΙ από εκείνες που υποστηρίζει το αγορασθέν σύστημα, το ΣΠΙ είναι αυτό που συνήθως θα πρέπει να προσαρμόσει τις λειτουργικές του διαδικασίες στα χαρακτηριστικά του συστήματος και όχι το αντίστροφο.

(δ) στα κεντρικά συστήματα χρηματοπιστωτικών εργασιών, η ανάπτυξη περιφερειακών εφαρμογών που θα αντλούν πληροφορίες από το κεντρικό σύστημα και θα υλοποιούν τοπικές αλλά και επιχειρησιακές ιδιαιτερότητες να γίνεται με βάση τα ισχύοντα στο ΣΠΙ πρότυπα για την ανάπτυξη εφαρμογών, έτσι ώστε να διατηρείται η μηχανογραφική ομοιογένεια.

(ε) ο τρόπος υποστήριξης των συστημάτων να είναι αυστηρά προδιαγεγραμμένος, με σαφή καθορισμό των περιπτώσεων στις οποίες απαιτείται υποστήριξη από τον πάροχο αλλά και των χρονικών περιθωρίων ανταπόκρισής του.

(στ) να είναι απαραίτητη η απόκτηση τεχνογνωσίας, όχι μόνον μέσω της κατάλληλης εκπαίδευσης του εμπλεκόμενου στη λειτουργία τέτοιων συστημάτων προσωπικού, αλλά κυρίως μέσω της συμμετοχής του σε όλες τις φάσεις εξέλιξης των

συστημάτων, έτσι ώστε η εξάρτηση του ΣΠΙ από τον προμηθευτή βαθμιαία να ελαττώνεται.

(ζ) εφόσον έχουν υλοποιηθεί οι απαιτήσεις του ΣΠΙ - όπως αυτές αναφέρονται στο συμβόλαιο - και μετά το πέρας των απαραίτητων δοκιμών εκ μέρους του παρόχου, να υφίσταται διαδικασία επίσημης αποδοχής και παραλαβής του συστήματος εκ μέρους του ΣΠΙ με τη συμμετοχή όλων των εμπλεκομένων μερών.

IV. ΛΕΙΤΟΥΡΓΙΑ ΚΑΙ ΥΠΟΣΤΗΡΙΞΗ

Η απρόσκοπτη λειτουργία των Πληροφοριακών Συστημάτων και η αποτελεσματική υποστήριξή τους είναι παράγοντες κρίσιμοι τόσο για την εύρυθμη λειτουργία του ΣΠΙ και τη δημιουργία σχέσεων εμπιστοσύνης με τα μέλη/πελάτες, όσο και για την αποτελεσματική αντιμετώπιση του λειτουργικού κινδύνου. Η απρόσκοπτη λειτουργία και η αποτελεσματική υποστήριξη των Πληροφοριακών Συστημάτων προϋποθέτουν την τήρηση των πολιτικών, προτύπων και διαδικασιών του ΣΠΙ από όλες τις εμπλεκόμενες υπηρεσιακές μονάδες, αλλά και τους παρόχους υπηρεσιών πληροφορικής.

1. Λειτουργία Συστημάτων

Ο όρος «λειτουργία συστημάτων» αναφέρεται στο σύνολο των διαδικασιών που απαιτούνται για την καθημερινή λειτουργία των Πληροφοριακών Συστημάτων σε ένα ΣΠΙ. Για ένα αποδεκτό επίπεδο ασφαλούς και αποτελεσματικής λειτουργίας τους θα πρέπει να υφίστανται:

(α) πλήρης και λεπτομερής καταγραφή του μηχανογραφικού εξοπλισμού (κεντρικά συστήματα, εξυπηρετητές, προσωπικοί υπολογιστές, περιφερειακά, δίκτυα και τηλεπικοινωνίες), του αρχιτεκτονικού σχεδιασμού, του χρησιμοποιούμενου λογισμικού, καθώς και του ιστορικού των εκδόσεων, των ενημερώσεων, και των αδειών χρήσης. Αρχείο πρέπει να τηρείται επίσης για τα μέσα που αποθηκεύουν και διακινούν ευαίσθητα δεδομένα του οργανισμού.

(β) τήρηση πλήρους και ενημερωμένης τεκμηρίωσης για κάθε σύστημα με τα επίσημα εγχειρίδια των εταιρειών που προμηθεύουν το υλικό και το λογισμικό των συστημάτων και τα εγχειρίδια που συντάσσονται από το προσωπικό του ΣΠΙ.

(γ) επαρκής συντήρηση και τεχνική υποστήριξη των συστημάτων.

(δ) υποστήριξη των υπαλλήλων-χρηστών εντός, αλλά και των πελατών-χρηστών εκτός του οργανισμού η οποία και θα πρέπει να ανατίθεται σε κατάλληλα οργανωμένες και στελεχωμένες υπηρεσιακές μονάδες ("Help Desk").

(ε) διαδικασίες διαχείρισης των παραμέτρων λειτουργίας των συστημάτων.

(στ)διαδικασίες αποτροπής εγκατάστασης και χρήσης μη εγκεκριμένου από το ΣΠΙ λογισμικού, καθώς επίσης λογισμικού χωρίς την κατάλληλη αδειοδότηση.

(ζ) προγραμματισμός των εργασιών προς εκτέλεση, καταγραφή των προβλημάτων που προκύπτουν και των ενεργειών που πρέπει να γίνονται στις έκτακτες περιπτώσεις. Η επιτυχής ή μη εκτέλεση των προγραμματισμένων αλλά και έκτακτων εργασιών θα πρέπει να καταχωρείται σε ειδικό ημερολόγιο, το οποίο και θα φέρει τις υπογραφές του προσωπικού που τις εκτέλεσε. Η εκτέλεση έκτακτων εργασιών θα πρέπει να γίνεται κατόπιν ειδικής έγκρισης.

(η) έλεγχος των δεδομένων, για εξασφάλιση της ακεραιότητας, ορθότητας και εμπιστευτικότητάς τους, σε όλες τις φάσεις επεξεργασίας τους. Οι κάθε είδους ασυμφωνίες θα πρέπει να διαπιστώνονται και να αντιμετωπίζονται βάσει καταγεγραμμένων διαδικασιών.

(θ) διαδικασίες διαχείρισης της χωρητικότητας, του φόρτου και της απόδοσης των συστημάτων και δικτύων.

(ι) συνεχής παρακολούθηση της διαθεσιμότητας των συστημάτων και των δικτύων. Ειδικότερα για τα κρίσιμα συστήματα, το ΣΠΙ πρέπει να είναι σε θέση να υπολογίζει το ποσοστό διαθεσιμότητάς τους σε επίπεδο έτους και να το συγκρίνει με προκαθορισμένους στόχους.

(κ) επαρκείς διαδικασίες διαχείρισης αντιγράφων ασφαλείας

(λ) ειδικότερα, για τα συστήματα και τις υπηρεσίες που προσφέρονται μέσω του διαδυκτίου θα πρέπει να υφίστανται:

i. επαρκής πληροφόρηση στο διαδικτυακό τόπο ("web-site") του ΣΠΙ, έτσι ώστε να μπορούν τα εν δυνάμει μέλη/πελάτες τους να έχουν μια επαρκή γνώση για την ταυτότητα του ΣΠΙ και την εποπτεύουσα αρχή που παρέχει την άδεια λειτουργίας, πριν πραγματοποιήσουν τις ηλεκτρονικές τους συναλλαγές. Επίσης, γνωστοποίηση του τρόπου με τον οποίο μπορούν να επικοινωνήσουν τα μέλη/πελάτες με το σχετικό κέντρο υποστήριξης σε περίπτωση πάσης φύσεως προβλήματος, το ψηφιακό πιστοποιητικό του διαδικτυακού τόπου, το

οποίο θα πρέπει να έχει εκδοθεί από επίσημη αρχή πιστοποίησης, πληροφορίες για την ασφαλή χρήση των παρεχομένων υπηρεσιών και άλλες σχετικές πληροφορίες.

ii. ενημέρωση των μελών/πελατών για την πολιτική εμπιστευτικότητας που εφαρμόζει το ΣΠΙ σε σχέση με τα προσωπικά τους δεδομένα. Συνίσταται η πληροφόρηση αυτή να παρέχεται και μέσα από το διαδικτυακό τόπο του ΣΠΙ. Παροχή επίσης στα μέλη/πελάτες του δικαιώματος να αρνηθούν τη διάθεση – εκχώρηση σε τρίτους δεδομένων που τους αφορούν, για προώθηση προϊόντων ή άλλο λόγο. Τα δεδομένα των μελών/πελατών θα πρέπει να χρησιμοποιούνται μόνον για τους σκοπούς για τους οποίους τα μέλη/πελάτες γνωρίζουν ότι τα διαθέτουν.

iii. σαφής σήμανση στο διαδικτυακό τόπο του ΣΠΙ των συνδέσεων ("links") με διαδικτυακούς τόπους άλλων εταιρειών ή οργανισμών. Πρέπει να φαίνεται έκδηλα στο μέλος/πελάτη ότι, όταν εγκαταλείπει το διαδικτυακό τόπο του ΣΠΙ, συνδέεται με μια εντελώς ξεχωριστή επιχειρηματική μονάδα ή άλλη νομική οντότητα.

iv. αυτοματοποιημένα συστήματα παρακολούθησης των συναλλαγών, τα οποία και θα βασίζουν την αποτελεσματική λειτουργία τους στη δημιουργία εκ μέρους του ΣΠΙ στατιστικών προτύπων κίνησης λογαριασμού για κάθε μέλος/πελάτη. Τα συστήματα αυτά, με βάση τα διαμορφωμένα χαρακτηριστικά κίνησης των λογαριασμών των μελών/πελατών ("profiles"), θα πρέπει να εντοπίζουν και να καταγράφουν ασυνήθιστες συναλλακτικές συμπεριφορές και να παράγουν, σε πραγματικό χρόνο, προειδοποιητικά μηνύματα ("alerts") για τη διερεύνηση ενδεχόμενων περιπτώσεων απάτης.

v. αποτελεσματική αντιμετώπιση των κινδύνων νομιμοποίησης εσόδων από το ξέπλυμα παράνομου χρήματος και τη χρηματοδότηση της τρομοκρατίας. Οι συγκεκριμένοι κίνδυνοι στις ηλεκτρονικές συναλλαγές είναι ιδιαίτερα αυξημένοι λόγω της ευκολίας χρήσης των υπηρεσιών από οπουδήποτε και οποιαδήποτε χρονική στιγμή, της απρόσωπης φύσης των συναλλαγών και της αυτόματης διεκπεραίωσής τους. Ως εκ τούτου, το ΣΠΙ θα πρέπει να μεριμνά για την εγκατάσταση αυτοματοποιημένων συστημάτων και εργαλείων διαχείρισης των συναλλαγών, τα οποία κατ' ελάχιστο θα θέτουν όρια σε συγκεκριμένες ομάδες ή κατηγορίες συναλλαγών, θα παρέχουν τη δυνατότητα καθυστέρησης εκτέλεσης

της συναλλαγής μέχρι την εξακρίβωση συγκεκριμένων στοιχείων ("filters & monitoring tools/systems").

vi. δυνατότητα εύκολης προσπέλασης και επεξεργασίας στοιχείων παλαιότερων συναλλαγών, έτσι ώστε να γίνεται εφικτός ο εντοπισμός συναλλακτικών ιδιαιτεροτήτων και ανωμαλιών, για να διευκολύνεται η στοιχειοθέτηση αποδεικτικών στοιχείων και η επαρκής πληροφόρηση της ΜΟΚΑΣ και του Εφόρου, ειδικά στις περιπτώσεις απάτης και νομιμοποίησης εσόδων από το ξέπλυμα παράνομου χρήματος και τη χρηματοδότηση της τρομοκρατίας, παροχής επενδυτικών υπηρεσιών και άλλων συναλλαγών.

vii. εγχειρίδια σε ηλεκτρονική ή έντυπη μορφή, τα οποία θα ενημερώνουν τα μέλη/πελάτες για τον τρόπο χρήσης των συστημάτων με έμφαση σε θέματα ασφάλειας. Επιπλέον, το ΣΠΙ θα πρέπει να εφοδιάζει τους χρήστες με πρακτικές ασφαλούς χρήσης των προσωπικών υπολογιστών μέσω των οποίων προσπελαύνονται ορισμένα συστήματα ηλεκτρονικής τραπεζικής και ηλεκτρονικών πληρωμών. Στις πρακτικές αυτές θα πρέπει να γίνεται αναφορά, μεταξύ άλλων, σε θέματα προστασίας από ιούς και άλλο κακόβουλο λογισμικό, ασφαλούς αποθήκευσης και χρήσης προσωπικών κωδικών (ειδικά σε υπολογιστές κοινής χρήσης οι οποίοι γενικά θα πρέπει να αποφεύγονται για τέτοια χρήση).

viii. επαρκείς διαδικασίες ασφάλειας με έμφαση στην πιστοποίηση των συναλλασσόμενων μερών (ψηφιακό πιστοποιητικό διαδικτυακού τόπου του ΣΠΙ, πιστοποίηση δύο επιπέδων για το μέλος/πελάτη, με χρήση ψηφιακών πιστοποιητικών ή άλλης μεθόδου), τη μη αποποίηση των συναλλαγών, την κρυπτογράφηση της επικοινωνίας, την ασφάλεια των συναλλαγών (αποδεικτικά στοιχεία επιτυχούς ολοκλήρωσης, αποσύνδεση σε περίπτωση ανενεργού χρήστη, εντοπισμός ύποπτων συναλλαγών κλπ), και τέλος τη λειτουργία των συστημάτων που υποστηρίζουν τις εν λόγω υπηρεσίες σε ειδικές περιοχές του δικτύου που παρέχουν υψηλή προστασία από κακόβουλες ενέργειες εσωτερικών ή εξωτερικών χρηστών.

2. Φυσική Ασφάλεια

Ο όρος «φυσική ασφάλεια» αναφέρεται στα μέτρα που πρέπει να λαμβάνονται για την προστασία των συστημάτων και της υποδομής που τα υποστηρίζει, από κινδύνους που

προέρχονται από το περιβάλλον. Ανάλυση κινδύνων είναι απαραίτητο να προηγείται της λήψης μέτρων, αφού οι απαιτήσεις φυσικής ασφάλειας δεν είναι δυνατόν να είναι οι ίδιες για όλες τις περιοχές και χώρους που στεγάζουν συστήματα, ούτε και η κρισιμότητα των συστημάτων είναι η ίδια μέσα σε μια συγκεκριμένη περιοχή ή χώρο.

Στα μέτρα φυσικής ασφάλειας πρέπει τουλάχιστον να περιλαμβάνονται:

(α) μηχανισμοί ελέγχου φυσικής πρόσβασης ("Physical access controls"). Τέτοιοι μηχανισμοί πρέπει να περιορίζουν, να ελέγχουν και να καταγράφουν, αφ' ενός μεν την είσοδο και την έξοδο του προσωπικού και των επισκεπτών, αφ' ετέρου δε τη διακίνηση μηχανογραφικού εξοπλισμού και αποθηκευτικών μέσων. Το είδος των μηχανισμών ελέγχου που υλοποιούνται θα πρέπει να καθορίζεται από την κρισιμότητα των συστημάτων που καλούνται να προστατεύσουν.

(β) μηχανισμοί πρόληψης και αντιμετώπισης καταστροφών από φυσικά αίτια.

(γ) μηχανισμοί πρόληψης και αντιμετώπισης κακόβουλων ενεργειών όπως για παράδειγμα διάρρηξης / κλοπής, βανδαλισμού και τρομοκρατικής ενέργειας. Οι συγκεκριμένοι κίνδυνοι, όπως και οι κίνδυνοι από φυσικά αίτια, εκτός του ότι μπορεί να προκαλέσουν ολοσχερή καταστροφή των συστημάτων και των δικτύων, είναι δυνατό να διακυβεύσουν τις ζωές του προσωπικού.

(δ) μηχανισμοί πρόληψης και αντιμετώπισης προβλημάτων από διακοπή λειτουργίας και παροχής υπηρεσιών ή βλάβη υποστηρικτικών συσκευών. Είναι απαραίτητο τα συστήματα να λειτουργούν σε ένα αποτελεσματικά υποστηριζόμενο από τεχνικής άποψης περιβάλλον.

(ε) η αποτελεσματική διαχείριση της τηλεπικοινωνιακής και δικτυακής καλωδίωσης για την αντιμετώπιση θεμάτων φθοράς, παρεμβολών και έλλειψης κατάλληλης σήμανσης.

(στ) μηχανισμοί ασφάλειας φορητών συστημάτων. Η χρήση των φορητών υπολογιστών και οποιωνδήποτε άλλων φορητών συστημάτων θα πρέπει να λαμβάνεται σοβαρά υπόψη στην ανάλυση κινδύνων. Φορητοί υπολογιστές που αποθηκεύουν ευαίσθητα εταιρικά δεδομένα θα πρέπει, αφενός μεν να φυλάσσονται σε ασφαλή σημεία όταν δεν είναι σε χρήση, αφετέρου δε να αποθηκεύουν τα ευαίσθητα δεδομένα σε κρυπτογραφημένη μορφή.

(ζ) η ασφαλής μεταφορά και αποθήκευση των ευαίσθητων εγγράφων και μαγνητικών μέσων. Στην πρώτη κατηγορία ανήκουν ανάμεσα σε άλλα οι διαβαθμισμένες αναφορές, οι εφεδρικοί κωδικοί εισόδου των διαχειριστών συστημάτων, τα

συνθηματικά των μελών/πελατών μέχρι να τους αποσταλούν, η τεκμηρίωση των συστημάτων και εφαρμογών, και τα Σχέδια Συνέχειας Εργασιών και Ανάκαμψης από Καταστροφή. Στη δεύτερη ανήκουν, ανάμεσα σε άλλα, τα εφεδρικά αντίγραφα αρχείων και το πλαστικό υλικό των καρτών συναλλαγών.

(η) η επιλογή και κατάλληλη διαμόρφωση των χώρων με σκοπό την ελαχιστοποίηση των προαναφερθέντων κινδύνων, σε σχέση πάντοτε με τη χρήση για την οποία προορίζονται και την κρισιμότητα των συστημάτων που στεγάζουν.

3. Λογική ασφάλεια

Ο όρος «λογική ασφάλεια» αναφέρεται στο σύνολο των μέτρων που λαμβάνονται για τον περιορισμό της πρόσβασης στους πόρους των συστημάτων ("system resources"). Ως πόροι των συστημάτων θεωρούνται ο μηχανογραφικός εξοπλισμός, τα δίκτυα, το λογισμικό και τα δεδομένα. Τα μέτρα που υλοποιούν την λογική ασφάλεια καθορίζουν όχι μόνον το «ποιος» ή «τι», ποιο πρόγραμμα για παράδειγμα, θα έχει πρόσβαση σε συγκεκριμένους πόρους του συστήματος, αλλά και το είδος της πρόσβασης που επιτρέπεται να έχει. Τα μέτρα αυτά μπορεί να είναι ενσωματωμένα στα λειτουργικά συστήματα, να υλοποιούνται σε προγράμματα εφαρμογών, σε συστήματα διαχείρισης βάσεων δεδομένων, σε συστήματα επικοινωνιών ή ακόμη να υλοποιούνται μέσω πρόσθετων αυτόνομων πακέτων ασφάλειας.

Για τη διατήρηση ενός αποδεκτού επιπέδου λογικής ασφαλείας, κρίνεται σκόπιμο:

(α) για την ασφάλεια των προσβάσεων στα συστήματα:

i. να έχουν όλοι οι χρήστες ένα μοναδικό ατομικό λογαριασμό πρόσβασης σε κάθε σύστημα και μόνο για τους πόρους εκείνους που δικαιούνται πρόσβαση, ώστε κάθε ενέργεια να χρεώνεται μονοσήμαντα. Ως εκ τούτου, κοινοί – ομαδικοί λογαριασμοί πρόσβασης δεν θα πρέπει να χρησιμοποιούνται και, όπου αυτό δεν είναι εφικτό, θα πρέπει οι ενέργειες των κατόχων των λογαριασμών αυτών να καταγράφονται και να ελέγχονται σχολαστικά.

ii. να υπάρχουν καταγεγραμμένες και εγκεκριμένες διαδικασίες για τη διαχείριση των λογαριασμών πρόσβασης, τον καθορισμό και την αναθεώρηση των δικαιωμάτων που παρέχονται στον κάθε λογαριασμό. Να υπάρχει διαχωρισμός αρμοδιοτήτων στην έγκριση, υλοποίηση και έλεγχο των προσβάσεων.

iii. να καταγράφονται και να ελέγχονται συστηματικά οι ενέργειες που γίνονται με χρήση λογαριασμών πρόσβασης με προνομιακά δικαιώματα, όπως λογαριασμών διαχειριστών συστημάτων και γενικά χρηστών με αυξημένα δικαιώματα.

iv. οι λογαριασμοί πρόσβασης να απενεργοποιούνται άμεσα μόλις παύουν να είναι απαραίτητοι ή σε περίπτωση σημαντικής παραβίασης των κανόνων ασφάλειας.

v. να υπάρχει συγκεκριμένη διαδικασία που να προβλέπει τη δημιουργία προσωρινών λογαριασμών πρόσβασης, με καθορισμένο επίπεδο εξουσιοδοτήσεων, για συγκεκριμένες εργασίες ή για περιπτώσεις ανάγκης. Η χρήση των λογαριασμών αυτών θα πρέπει να ελέγχεται σχολαστικά και μόλις εκλείψει η ανάγκη για την οποία δημιουργήθηκαν θα πρέπει να απενεργοποιούνται.

vi. να πιστοποιείται ο ιδιοκτήτης ενός λογαριασμού πρόσβασης, κατά τη διαδικασία εισόδου του στο σύστημα μέσω μιας διαδικασίας υψηλής ασφάλειας, όπως για παράδειγμα ο κωδικός εισόδου, η χρήση «έξυπνης» κάρτας, ψηφιακού πιστοποιητικού ή με τη χρήση άλλων μεθόδων.

vii. να αλλάζονται άμεσα οι κωδικοί πρόσβασης που έχουν τεθεί από τις κατασκευάστριες εταιρίες σε κάθε νέο τεχνολογικό εξοπλισμό μετά την παραλαβή του.

viii. οι κωδικοί πρόσβασης:

1. να δημιουργούνται και να γίνεται η διαχείρισή τους βάσει προτύπων και διαδικασιών
2. να μην είναι εύκολα προβλέψιμοι
3. να διατηρούνται μυστικοί με ευθύνη των κατόχων τους
4. να αλλάζουν σε τακτική βάση και οπωσδήποτε την πρώτη φορά εισόδου του κατόχου τους στο σύστημα. Η αλλαγή των κωδικών να επιβάλλεται από το σύστημα και να κρατείται ιστορικό αλλαγών για την αποφυγή επανάληψης των ίδιων κωδικών, εφόσον αυτό είναι εφικτό

ix. οι εφεδρικοί κωδικοί των διαχειριστών συστημάτων ή λογαριασμών ειδικών προνομίων θα πρέπει να βρίσκονται αποθηκευμένοι σε ασφαλές σημείο, ώστε να μπορούν να χρησιμοποιηθούν βάσει ειδικής διαδικασίας σε περίπτωση έκτακτης ανάγκης.

x. όπου κρίνεται αναγκαίο, οι κωδικοί πρόσβασης λογαριασμών ειδικών προνομίων θα πρέπει να μη φυλάσσονται ενιαίοι, αλλά σε τμήματα με ευθύνη διαφορετικών ατόμων.

xi. να χρησιμοποιείται – όπου είναι εφικτό – ειδικό λογισμικό διαχείρισης και ελέγχου των προσβάσεων.

(β) για την προστασία των δεδομένων

i. να υπάρχουν επαρκείς ενσωματωμένοι μηχανισμοί ελέγχου ("controls") των δεδομένων στα διάφορα συστήματα, και ειδικότερα, στην προετοιμασία, εισαγωγή, και επεξεργασία τους.

ii. να υπάρχει καταγεγραμμένη και εγκεκριμένη διαβάθμιση των δεδομένων σύμφωνα με το βαθμό ευαισθησίας τους και να προβλέπονται επιπλέον διαδικασίες ασφάλειας των ευαίσθητων δεδομένων μέσω τεχνικών κρυπτογράφησης ή άλλων μεθόδων προστασίας.

iii. για την κρυπτογράφηση:

1. να καθορίζεται σαφώς το πότε και σε ποιο επίπεδο γίνεται κρυπτογράφηση

2. να χρησιμοποιείται υψηλής ασφάλειας κλειδί κρυπτογράφησης σε όλο το λογισμικό

3. να αναπτύσσεται στρατηγική υποδομής δημόσιου κλειδιού ("public key infrastructure") για τη διαχείριση των ψηφιακών πιστοποιητικών, κυρίως για την επικοινωνία του ΣΠΙ με τα μέλη/πελάτες του για παροχή υπηρεσιών ηλεκτρονικών χρηματοπιστωτικών συναλλαγών

4. να επιδιώκεται η συμμόρφωση με τους εθνικούς και διεθνείς κανονισμούς και πρακτικές κρυπτογράφησης

iv. να γίνονται οι απαραίτητες ενέργειες για τη συμμόρφωση με τη σχετική νομοθεσία και τους κανονισμούς προστασίας δεδομένων.

v. να υπάρχει πολιτική σχετικά με την ενημέρωση των μελών/πελατών στην περίπτωση διαρροής εμπιστευτικών προσωπικών τους δεδομένων λόγω παραβίασης της ασφάλειας των συστημάτων.

vi. για τις βάσεις δεδομένων:

1. να υπάρχει ολοκληρωμένη και ακριβής τεκμηρίωση της βάσης που να περιλαμβάνει τουλάχιστον τον λογικό σχεδιασμό, τον φυσικό σχεδιασμό και το λεξικό δεδομένων
2. να γίνεται αναδιοργάνωση της βάσης σε τακτά χρονικά διαστήματα
3. να εξασφαλίζεται η καταχώρηση μόνο ολοκληρωμένων συναλλαγών ("commit / rollback")

(γ) για την προστασία των συστημάτων

i. να υπάρχει εγκατεστημένο κατ' ελάχιστο στα κρίσιμα συστήματα, και όπου αλλού είναι αναγκαίο ειδικό λογισμικό προστασίας από ιούς ή άλλο «κακόβουλο» λογισμικό.

ii. να παρέχεται αποτελεσματική προστασία σε ευαίσθητους πόρους των συστημάτων, όπως τα αρχεία συστήματος και εφαρμογών.

iii. να συντηρείται αρχείο με το εγκεκριμένο από το ΣΠΙ λογισμικό

iv. να απεγκαθίσταται ή να απενεργοποιείται σε κάθε σύστημα, κάθε λογισμικό ή λειτουργία που δεν κρίνεται απαραίτητη.

v. να ενεργοποιούνται τουλάχιστον οι βασικές λειτουργίες ελέγχου και καταγραφής ("auditing & logging functions") σε κάθε σύστημα και να παραμετροποιούνται κατάλληλα σε συνεργασία με τον εσωτερικό έλεγχο.

vi. να εξασφαλίζεται όπου αυτό είναι αναγκαίο, κατόπιν σχετικής εγκριτικής διαδικασίας, η συνεχής ενημέρωση των συστημάτων με τις τελευταίες εκδόσεις λογισμικού και ενημερώσεων σε θέματα ασφάλειας, ώστε να ελαχιστοποιούνται οι αδυναμίες και τα τρωτά τους σημεία.

vii. να υπάρχουν καταγεγραμμένες διαδικασίες αποκατάστασης της ασφαλούς λειτουργίας ενός συστήματος σε περίπτωση που παραβιαστεί η ασφάλειά του.

viii. να προστατεύεται, όσο αυτό είναι εφικτό, το ηλεκτρονικό ταχυδρομείο από πιθανούς κινδύνους αναξιόπιστης γνησιότητας του αποστολέα, υποκλοπής ή/και παραποίησης του περιεχομένου, επικίνδυνων προσαρτημάτων και ανεπιθύμητων μηνυμάτων.

ix. να υπάρχουν περιορισμοί στις ενέργειες των χρηστών του διαδικτύου, για παράδειγμα στις προσβάσεις σε συγκεκριμένους διαδικτυακούς τόπους, στη διακίνηση αρχείων και σε άλλες σχετικές ενέργειες.

x. να γίνεται συνεχής εκπαίδευση και ενημέρωση των χρηστών σε θέματα ασφαλούς λειτουργίας των συστημάτων.

xi. να προστατεύονται αποτελεσματικά τα κρίσιμα συστήματα από κακόβουλες ενέργειες εξωτερικών ή εσωτερικών χρηστών. Προς αυτή την κατεύθυνση οφείλουν να υλοποιούνται διάφορες τεχνικές, όπως :

1. η χρήση ειδικών συστημάτων ("firewalls", "filtering routers" κλπ), τα οποία, ως σημεία ελέγχου των προσβάσεων, θα ρυθμίζουν και θα ελέγχουν την επικοινωνία από και προς περιοχές του δικτύου οι οποίες είναι συνήθως εκτεθειμένες σε αυξημένους κινδύνους

2. η δημιουργία στο δίκτυο ειδικών περιοχών ("Demilitarized zones"), ανάμεσα σε σημεία ελέγχου προσβάσεων, οι οποίες να λειτουργούν σαν απομονωμένο δίκτυο για τα προσβάσιμα από εσωτερικούς ή εξωτερικούς χρήστες συστήματα του ΣΠΙ, προστατεύοντας έτσι αποτελεσματικά το υπόλοιπο δίκτυο από κακόβουλες ενέργειες

(δ) για την ασφάλεια της δικτυακής υποδομής και των επικοινωνιών

i. να είναι σαφώς καθορισμένες, καταγεγραμμένες και ελεγχόμενες οι δίοδοι επικοινωνίας ("gateways") με εξωτερικά δίκτυα.

ii. να εκτιμάται η δυνατότητα κατάτμησης ("segmentation") του δικτύου σε ελεγχόμενα επί μέρους υποδίκτυα για τον καλύτερο έλεγχο των προσβάσεων.

iii. να μην παραμένουν ανοιχτές λογικές θύρες επικοινωνίας ("ports") σε κάθε συσκευή του δικτύου, επιπλέον όσων έχουν καθοριστεί σαφώς ως αναγκαίες για τις υπηρεσίες που υποστηρίζουν και αφού έχει συνεκτιμηθεί ο συνεπαγόμενος κίνδυνος από τη λειτουργία τους.

iv. να περιορίζεται και να ελέγχεται επαρκώς η πρόσβαση στις ειδικές λειτουργίες διαχείρισης και ελέγχου του δικτύου.

v. να υπάρχει αποτελεσματική διαχείριση των παραμετροποιήσεων των συσκευών του δικτύου.

vi. να υπάρχει η δυνατότητα εντοπισμού από το διαχειριστή του δικτύου λειτουργίας μη εξουσιοδοτημένων συσκευών.

vii. να περιορίζονται στα απολύτως απαραίτητα τα σημεία πρόσβασης στο δίκτυο τα οποία βρίσκονται σε χώρους μη ελεγχόμενης φυσικής πρόσβασης και εφόσον δε χρησιμοποιούνται να είναι ανενεργά.

viii. να περιορίζεται και να ελέγχεται συστηματικά η δυνατότητα ασύρματης σύνδεσης χρηστών στο δίκτυο, ώστε να αποτρέπεται η παρείσφρηση μη εξουσιοδοτημένων χρηστών σε αυτό.

ix. να μην παρέχεται η δυνατότητα εξ' αποστάσεως πρόσβασης στο δίκτυο και, όπου κρίνεται αναγκαία τέτοια πρόσβαση, να καταγράφεται και να ελέγχεται συστηματικά. Ειδικότερα, σε περίπτωση πρόσβασης στο δίκτυο χρηστών μέσω τηλεφωνικής σύνδεσης ("dial-up"), αυτή να πραγματοποιείται κατόπιν διαδικασίας επιστροφής κλήσης ("call-back") ή άλλης κατάλληλης μεθόδου επαλήθευσης του καλούντος.

x. να χρησιμοποιούνται τα κατάλληλα πρωτόκολλα επικοινωνίας ανάλογα με το είδος των δεδομένων που μεταδίδονται, αντιμετωπίζοντας αποτελεσματικά θέματα διαχείρισης και ασφάλειάς τους.

xi. να εξασφαλίζεται η εμπιστευτικότητα και η ακεραιότητα των δεδομένων που μεταδίδονται μέσω του δικτύου καθ' όλη τη διαδρομή τους σε αυτό.

xii. να γίνεται χρήση ειδικών εργαλείων λογισμικού για τον εντοπισμό κενών ασφαλείας ή σημείων μειωμένης ασφάλειας στο δίκτυο ("vulnerability tests").

xiii. να υπάρχουν διαδικασίες και συστήματα παρακολούθησης, αποτροπής και αντιμετώπισης προσπαθειών παρείσφρησης στο δίκτυο ή γενικότερα προσπαθειών παραβίασης της ασφάλειας του δικτύου ("intrusion detection/prevention systems").

xiv. να διενεργούνται σε τακτική βάση, από ειδικευμένες εταιρίες, δοκιμαστικές απόπειρες παραβίασης της ασφάλειας του δικτύου ("penetration tests"), βάσει καθορισμένων σεναρίων, με στόχο την αξιολόγηση της επάρκειας της ασφάλειας του δικτύου.

4. Σχέδια Συνέχειας Εργασιών και Ανάκαμψης από Καταστροφή

Το ΣΠΙ πρέπει να διαθέτει εγκεκριμένα από την Ανώτατη Εκτελεστική Διεύθυνση Σχέδια Συνέχειας Εργασιών για τα Πληροφοριακά Συστήματα, ενταγμένα στα γενικότερα εταιρικά Σχέδια Συνέχειας Εργασιών, έτσι ώστε να εξασφαλίζεται η συνέχεια των κρισιμότερων λειτουργιών τους. Επιπλέον, το ΣΠΙ πρέπει να διαθέτει αποτελεσματικά Σχέδια Ανάκαμψης από Καταστροφή που θα εφαρμόζονται στις περιπτώσεις καταστροφικών συμβάντων που μπορεί να προκαλέσουν παρατεταμένη διακοπή της λειτουργίας ενός κρίσιμου συστήματος ή ακόμη και ολόκληρου του μηχανογραφικού κέντρου.

Της δημιουργίας Σχεδίων Συνέχειας Εργασιών και Σχεδίων Ανάκαμψης από Καταστροφή θα πρέπει να προηγούνται διαδικασίες ανάλυσης επιχειρηματικών επιπτώσεων ("business impact analysis") και ανάλυσης κινδύνων ("risk assessment"). Βάσει αυτών:

(α) θα προσδιορίζονται όλες οι κρίσιμες λειτουργίες καθώς και τα συστήματα-πόροι που χρησιμοποιούν

(β) θα προσδιορίζονται όλοι οι κίνδυνοι που απειλούν τις κρίσιμες λειτουργίες και θα κατατάσσονται σύμφωνα με την πιθανότητα εμφάνισής τους και τις πιθανές επιπτώσεις τους στα συστήματα και τις λειτουργίες

(γ) θα σταθμίζεται το λειτουργικό κόστος από ενδεχόμενη διακοπή των κρίσιμων λειτουργιών και το κόστος ενεργοποίησης του Σχεδίου Συνέχειας Εργασιών και Σχεδίου Ανάκαμψης από Καταστροφή για να προσδιορίζονται οι συνθήκες που θα θέτουν σε εφαρμογή το αντίστοιχο σχέδιο

(δ) θα προσδιορίζεται ο χρόνος ανάκαμψης των κρίσιμων λειτουργιών – συστημάτων ("recovery time") αλλά και το σημείο ανάκαμψης ("recovery point"), δηλαδή σε πόσο χρόνο και σε ποια εικόνα χρονικά θα επανέλθουν τα συστήματα μετά την ανάκαμψη

Πρώτο επίπεδο εξασφάλισης συνέχειας εργασιών θεωρείται η ύπαρξη σχεδίου λήψης και διαχείρισης αντιγράφων ασφαλείας του λογισμικού, των παραμέτρων λειτουργίας και των δεδομένων, καθώς και η ύπαρξη του αναγκαίου εφεδρικού εξοπλισμού, συσκευών παροχής αδιάλειπτης τάσης και ηλεκτρογεννητριών και στους χώρους λειτουργίας των συστημάτων.

Με στόχο την εξασφάλιση της γρήγορης και επιτυχούς ανάκτησης των δεδομένων και του λογισμικού, θα πρέπει για τα αντίγραφα ασφαλείας να υφίστανται συγκεκριμένες διαδικασίες:

(α) δημιουργίας με συχνότητα που υπαγορεύεται από τη κρισιμότητα των πληροφοριών

(β) ασφαλούς φύλαξης στο χώρο των συστημάτων

(γ) ασφαλούς μεταφοράς και φύλαξης σε απομακρυσμένο χώρο των επιπλέον αντιγράφων

(δ) δοκιμών για τη διασφάλιση της ακεραιότητας των δεδομένων

(ε) αρχειοθέτησης με αναγραφή στα μέσα αποθήκευσης του περιεχομένου και του χρόνου αποθήκευσης των δεδομένων

(στ) ανακύκλωσης των μαγνητικών μέσων

Σε δεύτερο επίπεδο, ένα ολοκληρωμένο και αποτελεσματικό Σχέδιο Συνέχειας Εργασιών και Σχέδιο Ανάκαμψης από Καταστροφή για τα ΣΠΙ, συνιστάται:

(α) να είναι γραμμένο σε απλή και κατανοητή γλώσσα και να κοινοποιείται επίσημα σε όλο το προσωπικό. Τυχόν διαβαθμισμένες πληροφορίες του σχεδίου, όπως για παράδειγμα κωδικοί, κλείδες ασφαλείας και άλλες συναφείς πληροφορίες θα πρέπει να γνωστοποιούνται μόνο σε εξουσιοδοτημένο προσωπικό.

(β) αντίγραφό του να φυλάσσεται σε κατάλληλο χώρο σε ασφαλή απόσταση από το μηχανογραφικό κέντρο.

Ένα τέτοιο σχέδιο θα πρέπει να περιλαμβάνει:

(γ) κατάταξη των συστημάτων βάσει λειτουργικής ανάγκης. Στην κατάταξη αυτή θα πρέπει, μεταξύ άλλων, να αναφέρεται ο χρόνος που απαιτείται για την ανάκτηση ("recovery time") του κάθε συστήματος καθώς και η ελάχιστη εκτιμώμενη απόδοσή του μετά την ανάκτηση.

(δ) τη σαφή ιεραρχική δομή των στελεχών που συμμετέχουν στην εφαρμογή του, τις αρμοδιότητές τους, καθώς και τους υπεύθυνους λήψης αποφάσεων σε κάθε ομάδα έκτακτης ανάγκης.

(ε) τις διαδικασίες εκτίμησης του εύρους της καταστροφής, με βάση τις οποίες προσδιορίζονται επακριβώς τα τμήματα του σχεδίου τα οποία θα πρέπει να ενεργοποιηθούν.

(στ) τις διαδικασίες ενεργοποίησης του σχεδίου, ειδοποίησης των στελεχών και κινητοποίησης των ομάδων έκτακτης ανάγκης.

(ζ) τις ενέργειες που θα εκτελούνται σε συγκεκριμένες επείγουσες καταστάσεις, οι οποίες μεταξύ των άλλων θα πρέπει να διασφαλίζουν το προσωπικό σε περίπτωση κινδύνου / καταστροφής όπως για παράδειγμα σε περίπτωση φωτιάς, σεισμού και άλλων καταστροφών.

(η) τους εναλλακτικούς χώρους εργασίας των χρηστών, τον εξοπλισμό που θα χρησιμοποιηθεί, καθώς και τις απαιτούμενες προδιαγραφές τους.

(θ) τις διαδικασίες προετοιμασίας και ενεργοποίησης του εναλλακτικού μηχανογραφικού κέντρου.

(ι) τα συστήματα του εναλλακτικού κέντρου, την υποδομή τους καθώς και την τοπολογία δικτύου.

(κ) λίστα προμηθευτών με τους οποίους υπάρχουν συμβάσεις, οι υπηρεσίες που αυτοί προσφέρουν και οι αναμενόμενοι χρόνοι απόκρισής τους σε περίπτωση έκτακτης ανάγκης.

(λ) τις διαδικασίες που εξασφαλίζουν ότι τα σχέδια συντηρούνται, προσαρμόζονται και ενημερώνονται σε κάθε αλλαγή στις διαδικασίες λειτουργίας του ΣΠΙ.

(μ) τις διαδικασίες εκπαίδευσης του προσωπικού, σύμφωνα με τις αρμοδιότητες που αναλαμβάνουν κατά την υλοποίηση του Σχεδίου.

(ν) τις διαδικασίες εκτέλεσης δοκιμών, σύμφωνα με τις οποίες:

i. θα προσδιορίζεται η συχνότητά τους (κατ' ελάχιστον μία φορά το χρόνο)

ii. θα υπάρχουν σαφείς στόχοι εκ των προτέρων, είτε για την εξέταση συγκεκριμένων υποσυστημάτων, είτε για την εξέταση του συστήματος στο σύνολό του. Η εκτέλεση δοκιμών της τελευταίας κατηγορίας συνιστάται να περιλαμβάνει την πλήρη κάλυψη όλων των κρίσιμων λειτουργιών όπως αναγράφονται στο σχέδιο και να κάνει αποκλειστική χρήση του εναλλακτικού χώρου, του εξοπλισμού και των εφεδρικών αντιγράφων

iii. θα διεξάγονται υπό συνθήκες που θα προσομοιάζουν με περιπτώσεις έκτακτης ανάγκης

iv. θα εξασφαλίζεται η συμμετοχή της Μονάδας Εσωτερικής Επιθεώρησης

v. θα συντάσσεται έκθεση των αποτελεσμάτων μετά την ολοκλήρωσή των δοκιμών

vi. θα γίνονται οι απαραίτητες διορθώσεις στα σχέδια για όλα τα προβλήματα που διαπιστώνονται

vii. θα λαμβάνει γνώση των αποτελεσμάτων η Ανώτατη Εκτελεστική Διεύθυνση και η Επιτροπή Ελέγχου

Τέλος, θα πρέπει:

(ξ) να εξασφαλίζει την αποτελεσματική λειτουργία εναλλακτικού μηχανογραφικού κέντρου, το οποίο θα πρέπει να βρίσκεται σε κατάλληλη απόσταση, ώστε να μην επηρεάζεται από τους ίδιους κινδύνους που μπορεί να πλήξουν το κύριο μηχανογραφικό κέντρο. Το εναλλακτικό κέντρο θα πρέπει να διαθέτει κατάλληλο (εφεδρικό) εξοπλισμό που να παρέχει όλες τις κρίσιμες υπηρεσίες στους χρόνους που έχουν προκαθοριστεί, καθώς και τα εγχειρίδια των διαδικασιών και χρήσης των συστημάτων. Επιπλέον, θα πρέπει να επιτρέπει την απρόσκοπτη χρήση των εναλλακτικών μέσων μέχρι τη στιγμή της επαναφοράς των λειτουργιών στο κύριο μηχανογραφικό κέντρο.

(ο) να διασφαλίζει τη φυσική ασφάλεια του εναλλακτικού κέντρου, καθώς και ένα βασικό επίπεδο λογικής ασφάλειας κατά την εφαρμογή του σχεδίου.

(π) να φροντίζει για την ασφαλιστική κάλυψη του ΣΠΙ απέναντι σε κινδύνους που είναι δυνατόν να προκαλέσουν διακοπή της λειτουργίας των Πληροφοριακών Συστημάτων.

(ρ) σε περίπτωση που οι χώροι λειτουργίας του εναλλακτικού κέντρου, ο εξοπλισμός ή οι υπηρεσίες παρέχονται από τρίτους:

i. να προνοεί, μέσω κατάλληλων συμβάσεων, για την αποτελεσματική συνέχεια των εργασιών σε περίπτωση καταστροφής που θα πλήξει ταυτόχρονα πολλούς οργανισμούς οι οποίοι εξυπηρετούνται από τον ίδιο πάροχο

ii. να φροντίζει για την ενημέρωση του παρόχου για τυχόν αλλαγές στα συστήματα που πιθανό να απαιτήσουν αντίστοιχες προσαρμογές-ενημερώσεις στα Σχέδια Ανάκαμψης από Καταστροφή

5. Έλεγχος συστημάτων πληροφορικής

Μια΄ αποτελεσματική ελεγκτική λειτουργία για τα Πληροφοριακά Συστήματα θα πρέπει να εστιάζεται στους κινδύνους που απορρέουν από την ανάπτυξη, ενσωμάτωση και λειτουργία τους, να εξετάζει την επάρκεια των ελεγκτικών μηχανισμών ("controls") και

διαδικασιών, και να προτείνει, όπου χρειάζεται, τις κατάλληλες τροποποιήσεις. Επιπλέον, θα πρέπει να αξιολογεί το βαθμό συμμόρφωσης με την επιχειρησιακή στρατηγική και τις καταγεγραμμένες επιχειρησιακές πολιτικές, τα πρότυπα και τις διαδικασίες, και να παρακολουθεί το βαθμό συμμόρφωσης με τις διαπιστώσεις των πορισμάτων των ελέγχων. Τέλος, θα πρέπει να υπάρχει ολοκληρωμένη εικόνα για τη λειτουργία των Πληροφοριακών Συστημάτων ώστε να δίνεται η δυνατότητα επαρκούς ενημέρωσης σε ετήσια βάση της Επιτροπής Ελέγχου.

Για τους λόγους αυτούς, η υπηρεσιακή Μονάδα Εσωτερικής Επιθεώρησης θα πρέπει:

(α) να διαθέτει την τεχνογνωσία, την ποιοτική και ποσοτική επάρκεια προσωπικού, μέσων και διαδικασιών για τη διενέργεια εξειδικευμένων ελέγχων στα Πληροφοριακά Συστήματα. Η τεχνογνωσία και η εκπαίδευση του προσωπικού θα πρέπει να είναι τέτοιες ώστε να καλύπτονται ελεγκτικά οι τρέχουσες και οι μελλοντικές μηχανογραφικές λειτουργίες του ΣΠΙ.

(β) να καταρτίζει και να υλοποιεί ελεγκτικό πρόγραμμα, το οποίο θα βασίζεται σε ανάλυση κινδύνων που έχει διενεργηθεί στα Πληροφοριακά Συστήματα αλλά και σε ευρήματα προγενέστερων ελέγχων.

(γ) να ακολουθεί καταγεγραμμένες διαδικασίες σχεδιασμού, οργάνωσης και διενέργειας των ελέγχων, συγγραφής των πορισμάτων καθώς και διαδικασίες επανελέγχου ("follow-up"). Οι διαδικασίες αυτές, τα κάθε είδους ερωτηματολόγια που χρησιμοποιούνται στους εξειδικευμένους ελέγχους, καθώς και η χρησιμοποιούμενη μεθοδολογία ανάλυσης μηχανογραφικών κινδύνων, θα πρέπει να αποτελούν την επίσημη τεκμηρίωση της λειτουργίας του ελέγχου των Πληροφοριακών Συστημάτων.

(δ) να παρακολουθεί τα θέματα που αφορούν τα Πληροφοριακά Συστήματα του ΣΠΙ, ώστε να διαμορφώνει εικόνα για τους κινδύνους που υπάρχουν ή ενδέχεται να ανακύψουν. Για τη διαμόρφωση όσο το δυνατόν πληρέστερης εικόνας, συνιστάται η παρακολούθηση της λειτουργίας των Πληροφοριακών Συστημάτων μέσω ειδικών προσβάσεων, η συμμετοχή στις διάφορες επιτροπές έργων και η ύπαρξη διαδικασιών και μηχανισμών άμεσης ενημέρωσης της Μονάδας Εσωτερικής Επιθεώρησης στις περιπτώσεις εμφάνισης σημαντικών προβλημάτων και εκτάκτων περιστατικών.

(ε) να κάνει χρήση – ανάλογα με την περίπτωση - ειδικού ελεγκτικού λογισμικού για τον αποτελεσματικότερο έλεγχο της ασφάλειας των συστημάτων και της ακεραιότητας των δεδομένων τους.

(στ) να συμμετέχει στη φάση σχεδιασμού των συστημάτων για τη διαμόρφωση των κατάλληλων δικλείδων ασφαλείας, των ελεγκτικών αρχείων καταγραφής και αναφορών που παράγονται για τη διευκόλυνση του ελέγχου, καθώς και στη φάση των δοκιμών.

(ζ) να ελέγχει και να αξιολογεί τις διαδικασίες παραγωγής των στοιχείων που υποβάλλονται στη Ανώτατη Εκτελεστική Διεύθυνση του ΣΠΙ και τον Έφορο ώστε να διασφαλίζεται η πληρότητα και ακρίβειά τους.

(η) να μεριμνά για την άμεση και πλήρη ενημέρωση του Εφόρου στις περιπτώσεις σοβαρών προβλημάτων και έκτακτων περιστατικών στα Πληροφοριακά Συστήματα (περιπτώσεις απάτης, παραβίασης της ασφάλειας σημαντικών συστημάτων, μη διαθεσιμότητας κρίσιμων συστημάτων, ενεργοποίησης Σχεδίων Ανάκαμψης από Καταστροφή).

(θ) να ελέγχει και να αξιολογεί την επάρκεια και συμμόρφωση με τις διαδικασίες που διέπουν τις φάσεις συνεργασίας του ΣΠΙ με προμηθευτές και παρόχους μηχανογραφικών υπηρεσιών, για παράδειγμα την επιλογή συνεργάτη, τη σύναψη και τήρηση συμβολαίου, την ποιότητα των παρεχόμενων υπηρεσιών βάσει των προαναφερθέντων στην ενότητα III του παρόντος Παραρτήματος.

(ι) να μελετά, αξιολογεί και εφαρμόζει, όπου κρίνει πρόσφορο, τα διεθνή πρότυπα και μεθοδολογίες ελέγχου Πληροφοριακών Συστημάτων.

Σε ότι αφορά στους ελέγχους που ανατίθενται σε εξωτερικούς ελεγκτές, το ΣΠΙ θα πρέπει να διαθέτει πολιτική για το εύρος και το ρόλο του εξωτερικού ελέγχου στα Πληροφοριακά Συστήματα, καθώς και διαδικασίες αξιολόγησης των προσφερομένων υπηρεσιών. Η πολιτική θα πρέπει να τεκμηριώνει τις περιπτώσεις που ο εξωτερικός έλεγχος δρα, είτε παράλληλα με τον εσωτερικό προσφέροντας μια επιπλέον εξειδικευμένη άποψη, είτε συμπληρωματικά προκειμένου να καλύψει εξειδικευμένες ελεγκτικές απαιτήσεις όπου δεν υπάρχει η δυνατότητα να καλυφθούν εσωτερικά, ή και με τους δύο τρόπους.