Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Πληροφορική»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Τίτλος:** **«Προσεγγίσεις, Πρότυπα και Πλαίσια Ασφάλειας στο τραπεζικό τομέα»**
Ονοματεπώνυμο Φοιτητή	**Όνομα και επώνυμο: Ευαγγελία Καραμανλή**
Πατρώνυμο	**Όνομα πατέρα: Εμμανουήλ**
Αριθμός Μητρώου	**ΜΠΠΛ/ 08036**
Επιβλέπων	**Δέσποινα Πολέμη, Επίκουρος καθηγήτρια**

Ημερομηνία Παράδοσης **Απρίλιος 2012**

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Δέσποινα Πολέμη Επίκουρος Καθηγήτρια	Χρήστος Δουληγέρης Καθηγητής	Παναγιώτης Κοντζανικολάου Λέκτορας

Περίληψη

Στη σύγχρονη εποχή, η πληροφορία (άρα και η πληροφόρηση) θεωρείται σαν περιουσιακό στοιχείο της επιχείρησης εξίσου σημαντικό με τα υπόλοιπα και έχει μεγάλη αξία για τον οργανισμό, άρα πρέπει να προστατευθεί. Το αντικείμενο που πραγματεύεται αυτή η διατριβή είναι η μελέτη περίπτωσης υλοποίησης των προτύπων ISO27001:2005 και Cobit σε ένα ελληνικό τραπεζικό οργανισμό XBANK, χρησιμοποιώντας τη μεθοδολογία και το ομώνυμο εργαλείο του οργανισμού ISF, IRAM. Αρχικά, γίνεται η επισκόπηση όλων των προτύπων και προσεγγίσεων για την ενίσχυση της ασφάλειας σε οργανισμούς που έχουν δημοσιευθεί από κυβερνητικούς και μη οργανισμούς μέχρι σήμερα και αξιολογείται η δυνατότητα εφαρμογής τους σε ένα ελληνικό τραπεζικό οργανισμό. Ακολουθεί η επισκόπηση όλων των μεθοδολογιών και προσεγγίσεων που έχουν δημοσιευθεί σχετικά με την Εκτίμηση της Επικινδυνότητας και τη Διαχείριση αυτής, προκειμένου οι αναλυτές και οι οργανισμοί να μπορέσουν να υλοποιήσουν ένα ολοκληρωμένο και εμπεριστατωμένο πλαίσιο ασφάλειας των πληροφοριών. Έχοντας πραγματοποιήσει αυτή την επισκόπηση στα πρότυπα και τις μεθοδολογίες συζητείται η απόφαση της προσέγγισής μας στον ελληνικό τραπεζικό οργανισμό XBANK με βάση το πρότυπο ISO27001:2005 και το πλαίσιο Cobit καθώς επίσης και η υλοποίηση αυτών υιοθετώντας την μεθοδολογία του ISF, IRAM. Στη μελέτη περίπτωσης παρουσιάζονται τα βήματα που ακολουθήθηκαν και μέρος των αποτελεσμάτων αυτής της εργασίας με τα μέτρα ασφάλειας που επιλέγονται με αναφορά στην ανάλυση επικινδυνότητας και την ανάλυση επιχειρησιακού αντίκτυπου που προηγήθηκαν.

Abstract

Nowdays, information and therefore information technology infrastructure is considered as one of the most important properties for an organization, it is of great value and therefore the need to protect it is evident. The object of this thesis deals with the case study implementation of the standards ISO27001: 2005 and Cobit in a Greek bank organization, using the ISF methodology and the tool IRAM. Initially, there is an overview of all the information security standards and approaches to implement an information security management system in organizations, which have been published by government agencies or non-governmental organizations today and we evaluate their applicability in a Greek banking institution. Afterwards, an overview is presented of all the methodologies and approaches that have been published on Risk Assessment and Risk Management, so that analysts and institutions are able to implement an integrated and comprehensive information security framework. Having carried out this review of the standards and methodologies, the decision is explained of our approach in the Greek banking institution XBANK to implement the standard ISO27001: 2005, having the Cobit as our framework by adopting ISF's IRAM methodology. The case study presents the steps followed and part of the results of this work together with the security measures and controls chosen, with reference to risk analysis and business impact analysis that were conducted.

Πίνακας περιεχομένων

Περιεχόμενα εικόνων και άλλων πινάκων

1. Εισαγωγή

Η πληροφορία είναι ένα περιουσιακό στοιχείο το οποίο, όπως άλλα σημαντικά περιουσιακά στοιχεία μιας επιχείρησης, είναι ζωτικής σημασίας για τις επιχειρηματικές δραστηριότητες ενός οργανισμού και κατά συνέπεια θα πρέπει να προστατεύεται κατάλληλα. Η πληροφορία μπορεί να σχετίζεται με τις δραστηριότητες της κάθε εταιρείας και να αφορά προϊόντα και υπηρεσίες που παράγει – εμπορεύεται αλλά μπορεί να αφορά και σε δεδομένα τρίτων που επεξεργάζεται όπως συμβαίνει στον κλάδο των Τραπεζών, Χρηματοοικονομικών Υπηρεσιών και Τηλεπικοινωνιών. Η πληροφορία βρίσκεται πλέον εκτεθειμένη σε ένα πλήθος απειλών και αδυναμιών, το οποίο διαρκώς αυξάνεται σε αριθμό και διευρύνεται σε ποικιλία. Η ασφάλεια της πληροφορίας είναι η προστασία από ένα ευρύ φάσμα απειλών, προκειμένου να διασφαλίζεται η συνέχεια της επιχειρηματικής δραστηριότητας, να ελαχιστοποιούνται οι επιχειρηματικοί κίνδυνοι και να μεγιστοποιείται η απόδοση των επενδύσεων και των επιχειρηματικών ευκαιριών.

Η ασφάλεια της πληροφορίας επιτυγχάνεται μέσω της εφαρμογής μιας κατάλληλης ομάδας ελέγχων, στους οποίους συμπεριλαμβάνονται πολιτικές, διεργασίες, διαδικασίες, οργανωτικές δομές και λειτουργίες λογισμικού και υλικού. Οι έλεγχοι αυτοί πρέπει να καθιερώνονται, να εφαρμόζονται, να παρακολουθούνται, να αναθεωρούνται και να βελτιώνονται, όποτε είναι απαραίτητο, προκειμένου να διασφαλίζεται ότι πληρούνται οι συγκεκριμένοι στόχοι ασφάλειας και οι επιχειρηματικοί στόχοι του οργανισμού. Αυτό βεβαίως θα πρέπει να γίνεται και σε συνδυασμό με άλλες επιχειρησιακές διεργασίες.

Γιατί όμως η ασφάλεια των πληροφοριών είναι απαραίτητη; Η πληροφορία, καθώς και οι διεργασίες, τα συστήματα και τα δίκτυα που την υποστηρίζουν, αποτελούν σημαντικό περιουσιακό στοιχείο της επιχείρησης. Ο καθορισμός, η επίτευξη, η διατήρηση και η βελτίωση της ασφάλειας των πληροφοριών μπορεί να είναι ουσιώδους σημασίας για τη διατήρηση της ανταγωνιστικότητας, της ρευστότητας, της κερδοφορίας, της συμμόρφωσης με το νομοθετικό πλαίσιο και της εμπορικής εικόνας του οργανισμού. Οι οργανισμοί και τα συστήματα και τα δίκτυα πληροφοριών τους αντιμετωπίζουν απειλές για την ασφάλεια από ένα ευρύ φάσμα πηγών, στις οποίες συμπεριλαμβάνονται η απάτη με τη βοήθεια υπολογιστή και η κατασκοπεία. Άλλες αιτίες πρόκλησης ζημιάς, όπως π.χ. οι κώδικες κακόβουλης λειτουργίας, η μη εξουσιοδοτημένη πρόσβαση σε υπολογιστές (hacking) και άλλες επιθέσεις, έχουν γίνει πιο συχνές, πιο φιλόδοξες και ολοένα και πιο πολύπλοκες.

Πολλά συστήματα πληροφοριών δεν έχουν σχεδιαστεί έτσι ώστε να είναι ασφαλή. Η ασφάλεια που μπορεί να επιτευχθεί με τεχνικά μέσα είναι περιορισμένη και θα πρέπει να υποστηρίζεται από κατάλληλη διαχείριση και διαδικασίες. Για να προσδιοριστεί ποιοι έλεγχοι αρμόζουν σε κάθε περίσταση, απαιτείται προσεκτικός σχεδιασμός και προσοχή στη λεπτομέρεια. Μπορεί επίσης να είναι απαραίτητη η συμμετοχή μετόχων, τρίτων προσώπων, πελατών ή άλλων εξωτερικών μερών. Ενδέχεται να χρειαστεί ακόμα και συμβουλή ειδικών από άλλους οργανισμούς εκτός της επιχείρησης. Η διαχείριση της ασφάλειας πληροφοριών δεν περιορίζεται σε εφαρμογή τεχνολογιών ελέγχου πρόσβασης και προστασίας αυτών από κακόβουλους εξωγενείς παράγοντες, όπως συστήματα firewalls, antivirus, intrusion detection κ.λπ. έναντι κακόβουλων “hackers”, αλλά επεκτείνεται και στη διαχείριση όσων έχουν πρόσβαση σε αυτήν. Και η απρόβλεπτη ανθρώπινη συμπεριφορά δεν αντιμετωπίζεται με τεχνολογικά μέτρα. Τα μέτρα που απαιτείται να εφαρμοστούν σε κάθε σύγχρονη εταιρεία και οργανισμό για την προστασία των πληροφοριών της, είναι πρωτίστως διοικητικά και εν συνεχεία τεχνολογικά.

Στη παρούσα εργασία θα επιχειρηθεί μια μελέτη περίπτωσης τραπεζικού οργανισμού και θα εξετασθεί η εφαρμογή μέτρων ή σημείων ελέγχου με τελικό στόχο την επίτευξη ασφάλειας της πληροφορίας. Πιο συγκεκριμένα, θα εξετασθούν τα δημοσιευμένα πρότυπα, από κυβερνητικούς και μη οργανισμούς, που προσφέρουν ένα ολοκληρωμένο πλαίσιο ασφάλειας και διαχείρισης της ασφάλειας της πληροφορίας και θα μελετηθεί η καταλληλότητα τους στη περίπτωση υλοποίησης σε ένα τραπεζικό οργανισμό. Εφόσον επιλεγούν τα πρότυπα που είναι κατάλληλα για την υλοποίηση, κρίνεται απαραίτητο και αναπόσπαστο κομμάτι αυτής της διαδικασίας η αποτίμηση της επικινδυνότητας έτσι ώστε να επιλεγούν τα κατάλληλα μέτρα που θα αντισταθμίσουν συγκεκριμένους κινδύνους. Χωρίς λοιπόν τη διεξαγωγή μιας άσκησης

αναγνώρισης των κινδύνων και αποτίμησης αυτών κρίνεται ότι δεν θα είναι αποτελεσματική η υλοποίηση ολοκληρωμένου συστήματος διαχείρισης ασφάλειας.

Διεξάγεται στη συνέχεια μια επισκόπιση των εργαλείων και μεθόδων που ουσιαστικά υλοποιούν τα πρότυπα ασφάλειας ξεκινώντας με την αποτίμηση της επικινδυνότητας. Επιλέγεται η μέθοδος που είναι κατάλληλη για την εφαρμογή της στο τραπεζικό οργανισμό και γίνεται χρήση αυτής της μεθόδου για την ανάλυσή μας στον έλεγχο του περιβάλλοντος πληροφορικής ενός τραπεζικού οργανισμού και συγκεκριμένα στο σύστημα ηλεκτρονικής τραπεζικής. Η μέθοδος είναι η IRAM (Information Risk Assessment Methodology) του ISF και είναι από τις λίγες που προάγει μια τόσο ξεκάθαρη και συγκεκριμένη διαδικασία με πολύ διακριτά βήματα και στάδια ώστε να διευκολύνει όσο το δυνατό περισσότερο τον αναλυτή. Τέλος, εξάγονται κάποια συμπεράσματα σχετικά με το εργαλείο/ μέθοδο που χρησιμοποιήθηκε, τη μεθοδολογία και τη προσέγγιση που σαν τελικό στόχο είχε την υλοποίηση μέτρων ασφάλειας της πληροφορίας σε ένα τραπεζικό οργανισμό.

Στο 2^{ο} κεφάλαιο γίνεται η επισκόπηση όλων των προτύπων που αφορούν την υλοποίηση μηχανισμών ώστε να ενισχύσουν την ασφάλεια των πληροφοριών τους. Ορίζονται τέσσερις κατηγορίες και παρουσιάζονται τα πρότυπα αντίστοιχα στις κατηγορίες τους. Η κατηγοριοποίηση έγινε με βάση την προσέγγιση των προτύπων. Σε γενικές γραμμές τα πρότυπα που έχουν δημοσιευθεί είτε προσεγγίζουν την ασφάλεια της πληροφορίας προσανατολιζόμενα στις επιχειρησιακές διαδικασίες και βλέπουν την πληροφορική σαν υποστηρικτική σε αυτές, είτε προσανατολιζόμενα στην υλοποίηση σημείων ελέγχου με βάση τους στόχους ελέγχου. Επιπλέον, υπάρχουν και εκείνα τα πρότυπα που επικεντρώνονται στην αξιολόγηση και υλοποίηση ασφάλειας ως προς ένα και μόνο σύστημα υποδομής ή αντίστοιχα σε κάποια εφαρμογή. Στα πλαίσια της εργασίας αυτής όμως η τελευταία κατηγορία δεν εξυπηρετεί στην υλοποίηση ενός γενικότερου πλαισίου ασφάλειας που θα μελετηθεί. Τέλος, στη τέταρτη κατηγορία συγκαταλέγονται αυτά που συγκεντρώνουν τις βέλτιστες πρακτικές σε παγκόσμιο επίπεδο, όπως το ISO27001:2005, και επιχειρηματολογούμε οτι αυτά σε συνδυασμό με τα πρότυπα που προσανατολίζονται και στις επιχειρησιακές διαδικασίες (όπως το πλαίσιο Cobit) είναι η καλύτερη πρακτική για την υλοποίηση ενός ολοκληρωμένου πλαισίου ασφάλειας σε τραπεζικό οργανισμό.

Στο 3^{ο} κεφάλαιο εξετάζονται όλες οι προσεγγίσεις που εξυπηρετούν την Εκτίμηση της Επικινδυνότητας σε έναν οργανισμό για να καταλήξουμε βάσει αυτής της εκτίμησης στους σημαντικότερους πληροφοριακούς κινδύνους που εκτίθεται ο οργανισμός καθώς όπως ειπώθηκε η πληροφορία, καθώς και οι διεργασίες, τα συστήματα και τα δίκτυα που την υποστηρίζουν, αποτελούν σημαντικό περιουσιακό στοιχείο της επιχείρησης. Αυτό γίνεται όχι μόνο γιατί τα πρότυπα που επιλέγονται το απαιτούν, αλλά επιπλέον λόγω του ότι είναι η πιο λογική και πρακτική προσέγγιση στην πορεία προς την υλοποίηση ενός σωστού πλαισίου ασφάλειας της πληροφορίας στον οργανισμό, εφόσον λαμβάνονται υπόψη οι σημαντικότεροι κίνδυνοι που υπόκειται το επιχειρησιακό περιβάλλον και συγκεκριμένα τα συστήματα πληροφορικής που το υποστηρίζουν. Επιλέγεται η μεθοδολογία του οργανισμού ISF (Information Security Forum), η λεγόμενη IRAM εφόσον είναι η μοναδική που παρέχει και το εργαλείο αλλά και είναι πλήρως εναρμονισμένη με τα πρότυπα ασφάλειας που επιλέχθηκαν προς υλοποίηση στον τραπεζικό οργανισμό κάνοντας τελικά αναφορά σε αυτά ανάλογα με τα μέτρα ασφάλειας που επιλέγονται. Οι φάσεις που απαιτούνται να για την υλοποίηση των καταλληλότερων μέτρων ασφάλειας της πληροφορίας είναι πρώτον μια ανάλυση επιχειρησιακού αντίκτυπου και δεύτερον μια εκτίμηση της επικινδυνότητας για να εντοπιστούν οι κύριοι τύποι κινδύνου στους οποίους υπόκειται ο τραπεζικός οργανισμός.

Στο 4^{ο} και τελευταίο κεφάλαιο διεξάγεται η μελέτη περίπτωσης (case study) υλοποίησης πλαισίου ασφάλειας σε ένα ελληνικό τραπεζικό οργανισμό XBANK. Γίνεται αρχικά η μελέτη της μέχρι τώρα κατάστασης (as is status) και με τη βοήθεια ορισμένων τεχνικών ελέγχου και συλλογής πληροφοριών, εκτιμώνται οι κύριοι τύποι επιχειρησιακού αντίκτυπου με αναφορά στην εφαρμογή ηλεκτρονικής τραπεζικής, που καθορίζεται ως το πιο κρίσιμο σύστημα για το τραπεζικό οργανισμό. Στη συνέχεια εκτιμάται η επικινδυνότητα σε σχέση πάλι με το συγκεκριμένο πληροφοριακό σύστημα και στη τελική φάση επιλέγονται τα κατάλληλα μέτρα ασφάλειας που ελαχιστοποιούν την πιθανότητα οι απειλές που αναγνωρίστηκαν να προκαλέσουν περιστατικό ασφάλειας στον τραπεζικό οργανισμό. Στο τέλος εξάγονται κάποια

συμπεράσματα σχετικά με τη μεθοδολογία που ακολουθήθηκε και την εφαρμογή/ εργαλείο που χρησιμοποιήθηκε.

Κεφάλαιο 2ο

2. Επισκόπηση προσεγγίσεων διαχείρισης ασφάλειας

2.1 Εισαγωγή

Η ενίσχυση της ασφάλειας των πληροφοριακών συστημάτων και των εφαρμογών ηλεκτρονικής τραπεζικής (e-banking), σαν επακόλουθο των παγκόσμιων εγκληματικών τάσεων και κακόβουλων επιθέσεων, είναι στις μέρες μας επιτακτική ανάγκη. Σύμφωνα με τους Robertson, Vigna, Kruegel και Kemmerer (2006) και την μελέτη των τρωτών σημείων ως προς την ασφάλεια των πληροφοριακών συστημάτων, το 25% περίπου από αυτά παρατηρείται στις web εφαρμογές. Το 2009 μάλιστα παρατηρήθηκε αύξηση σε αυτά, φτάνοντας το ποσοστό του 40% (Robertson, 2009). Με τα δεδομένα αυτά, και την αύξηση σε περιστατικά ασφάλειας κάποιοι κυβερνητικοί και μη οργανισμοί δημιούργησαν και δημοσίευσαν πλαίσια καθοδήγησης και βέλτιστων πρακτικών για την ενίσχυση της ασφάλειας των πληροφοριακών συστημάτων.

Η παρούσα επισκόπηση επικεντρώνεται στην διαχείριση της ασφάλειας της πληροφορίας γενικότερα και στα πρότυπα και προσεγγίσεις που σχετίζονται με αυτή και έχουν δημοσιευθεί σε παγκόσμιο επίπεδο. Ειδικότερα, η επισκόπηση αυτή αποσκοπεί στη παρουσίαση των σχετικών προτύπων και προσεγγίσεων, έτσι ώστε να καταλήξουμε σε αυτά που είναι πιο κατάλληλα να πλαισιώσουν μια εργασία ενίσχυσης της ασφάλειας του περιβάλλοντος πληροφοριακών συστημάτων στο τραπεζιτικό κλάδο. Με βάση τα αποτελέσματα από διάφορες έρευνες στην διεθνή βιβλιογραφία που εφιστούν τη προσοχή στις web εφαρμογές λόγω του οτι είναι οι περισσότερο εκτεθειμένες στις κακόβουλες επιθέσεις (Robertson, 2009), στην συνέχεια αυτής της εργασίας θα επιχειρηθεί μια μελέτη περίπτωσης ενίσχυσης της ασφάλειας σε web εφαρμογή τράπεζας και συγκεκριμένα σε σύστημα ηλεκτρονικής τραπεζικής (e-banking). Η ενίσχυση της ασφάλειας σε ένα πληροφοριακό σύστημα δεν μπορεί άμεσα να εφαρμοσθεί σε αυτό ή και αποκλειστικά σε αυτό. Θα πρέπει να περιβάλλεται και να υπόκειται σε ένα γενικότερο πλαίσιο διαχείρισης ασφάλειας που επιβάλλει η διοίκηση του οργανισμού και πλαισιώνει ολόκληρο τον οργανισμό. Για το λόγο αυτό κρίνεται απαραίτητο σαν πρώτο βήμα στην εργασία αυτή να γίνει επισκόπηση όλων των πλαισίων, προτύπων και προσεγγίσεων της ασφάλειας που έχουν δημοσιευθεί και εφαρμόζονται σε παγκόσμιο επίπεδο.

Στο κεφάλαιο αυτό παρουσιάζονται τα πρότυπα και οι προσεγγίσεις διαχείρισης της ασφάλειας της πληροφορίας με απώτερο στόχο την επιλογή αυτών που μπορούν να εφαρμοστούν σε ένα τραπεζικό οργανισμό και ειδικότερα σε έναν ελληνικό τραπεζικό οργανισμό, λαμβάνοντας υπόψη και τα κανονιστικά πλαίσια στα οποία αυτός υπόκειται. Η δομή της παρουσίασης των προτύπων και των προσεγγίσεων ακολουθεί τη λογική μιας κατηγοριοποίησης με βάση την οπτική του κάθε προτύπου/ προσέγγισης. Αυτή η κατηγοριοποίηση θα διευκολύνει τη διαδικασία επιλογής των πιο κατάλληλων προτύπων ως προς την εφαρμοστικότητά τους σε ένα τραπεζικό οργανισμό.

2.2 Κατηγορίες προσεγγίσεων και προτύπων

Με βάση την οπτική και την προσέγγιση που ακολουθεί το καθένα από τα πρότυπα και πλαίσια που παρουσιάζονται παρακάτω επιχειρήθηκε μια κατηγοριοποίηση με σκοπό να διευκολυνθεί η διαδικασία επιλογής του καταλληλότερου προτύπου και πλαισίου για την εφαρμογή του σε ελληνικό τραπεζικό οργανισμό. Ο Aceituno (2006) αναφέρεται σε μια πρώτη κατηγοριοποίηση των προτύπων και πλαισίων για την ασφάλεια της πληροφορίας με βάση την οπτική τους. Για παράδειγμα το Cobit και το ITIL τα εντάσσει στην κατηγορία αυτών που επικεντρώνονται στις διαδικασίες, το ISO 17799 και το ISF Standard of Good Practice τα εντάσσει στην κατηγορία των βέλτιστων πρακτικών, ενώ τα ISO 13355 και SP 800-53 τα εντάσσει στην κατηγορία αυτών που επικεντρώνονται άμεσα στην υλοποίηση ελεγκτικών μηχανισμών με στόχο την ασφάλεια. Ο Aceituno χρησιμοποιεί και μια άλλη κατηγορία αυτή των προτύπων που επικεντρώνονται στην διαχείριση της επικινδυνότητας αλλά στην παρούσα εργασία η προσέγγιση είναι διαφορετική και θα παρατεθούν στο 3^{ο} κεφάλαιο με τις προσεγγίσεις τις μεθόδους και τα εργαλεία για τη διαχείριση της επικινδυνότητας.

Μετά από την έρευνα στην βιβλιογραφία και τις δημοσιεύσεις προτύπων και προσεγγίσεων ασφάλειας από κυβερνητικούς και μη οργανισμούς που διεξήχθη, ορίζουμε τέσσερις βασικές κατηγορίες με βάση τις οποίες θα ακολουθήσει και η παρουσίαση των προτύπων στα πλαίσια αυτής της εργασίας. Στις τρείς κατηγορίες ακολουθείται η προσέγγιση του Aceituno (2006), ενώ ορίζουμε και μια τέταρτη, αυτή των προτύπων που προσανατολίζονται στην αξιολόγηση συγκεκριμένων τεχνολογικών προϊόντων. Οι κατηγορίες ανάλογα με τη προσέγγιση του κάθε προτύπου στην ασφάλεια των πληροφοριών είναι οι εξής:

1. Προσανατολισμός στις διαδικασίες (process oriented)
2. Προσανατολισμός στα σημεία ελέγχου (controls oriented)
3. Προσανατολισμός σε συγκεκριμένο τεχνολογικό προϊόν (product oriented)
4. Προσανατολισμός σε βέλτιστες πρακτικές (best practice oriented)

Κάθε πρότυπο ή πλαίσιο παρέχει διαφορετική όψη της ασφάλειας της πληροφορίας ανάλογα και με το βαθμό κινδύνου. Μερικά από αυτά ξεκινούν από την αξιολόγηση ασφάλειας του περιβάλλοντος, εννοώντας την αντίληψη του οργανισμού για την ασφάλεια, τη στάση ως προς αυτή και τις ενέργειες της διοίκησης για εφαρμογή ενός ασφαλούς περιβάλλοντος, και τη διακυβέρνηση της τεχνολογίας πληροφοριών (IT Governance), με επίκεντρο τις διαδικασίες του εκάστοτε οργανισμού όχι τόσο της πληροφορικής όσο τις επιχειρησιακές διαδικασίες στις οποίες η πληροφορική και η τεχνολογία λειτουργούν υποστηρικτικά (**Process oriented**).

Στη δεύτερη κατηγορία είναι τα πρότυπα τα οποία επικεντρώνονται απευθείας στην υλοποίηση σημείων ελέγχου για την ασφάλεια των πληροφοριών και αξιολογούν με βάση την ύπαρξη ή όχι αυτών, χωρίς να λαμβάνεται υπόψη πάντα το επιχειρησιακό κομμάτι και το κατά πόσο είναι εφαρμόσιμα αυτά σαν βάση για την επίτευξη των επιχειρησιακών στόχων. Τα πρότυπα της κατηγορίας αυτής επικεντρώνουν την αξιολόγηση στην ύπαρξη και υλοποίηση σημείων ελέγχου ή ελεγκτικών διαδικασιών **(Controls Oriented).**

Συνεχίζοντας την προσπάθεια κατηγοριοποίησης προτύπων βάσει της έρευνας στην βιβλιογραφία, ανακαλύφθηκαν και τα πρότυπα που επικεντρώνονται αποκλειστικά στην αξιολόγηση τεχνολογιών και πιο συγκεκριμένα λογισμικών ή άλλων εμπορικών προϊόντων που κυκλοφορούν στην αγορά. Αυτά εμπίπτουν στη κατηγορία για την αξιολόγηση ενός συγκεκριμένου τεχνολογικού προϊόντος **(Product Oriented).**

Τέλος, υπάρχει και μια τέταρτη κατηγορία σύμφωνα με τον Aceituno (2006) που είναι τα πρότυπα που προσανατολίζονται στις βέλτιστες πρακτικές **(Best Practice Oriented)**. Τα πρότυπα που ανήκουν στη τελευταία κατηγορία είναι και τα πιο ευρέως διαδεδομένα και αυτά που έχουν τη μεγαλύτερη απήχηση καθώς τα υπόλοιπα είτε κάνουν συχνές αναφορές σε αυτά είτε έχει γίνει προσπάθεια αντιπαραβολής με αυτά (benchmarking). Επιπλέον, από πλευράς συμμόρφωσης των εκάστοτε οργανισμών είναι κυρίως τα συγκεκριμένα που απαιτούνται, δηλαδή βάσει βέλτιστων πρακτικών, και σύμφωνα με αυτά γίνεται και η πιστοποίηση.

Στην έκθεση των προτύπων, πλαισίων και προσεγγίσεων που ακολουθεί, θα γίνει μια αξιολόγηση, ακολουθώντας τα κριτήρια αξιολόγησης του Ευρωπαϊκού οργανισμού ENISA (2006), με βάση την εφαρμοστικότητα τους, για παράδειγμα σε μικρό ή μεγάλο οργανισμό, το πεδίο εφαρμογής τους (αξιολόγηση ασφάλειας εφαρμογής, λογισμικού, διαδικασιών κλπ.) και τέλος τη καταλληλότητά τους για το συγκεκριμένο πεδίο ελέγχου που έχουμε σκοπό να μελετήσουμε, δηλαδή τους τραπεζικούς οργανισμούς, διερευνώντας τη διεθνή βιβλιογραφία και αρθρογραφία. Σε πρώτη φάση η κατηγοριοποίηση των προτύπων, που είναι το πρώτο βήμα για να αξιολογήσουμε την εφαρμοστικότητα ενός προτύπου, θα γίνει με βάση τη προσέγγιση και την οπτική τους ως προς την ασφάλεια της πληροφορίας στις περιοχές που καλύπτουν.

2.3 Πρότυπα με προσανατολισμό στις διαδικασίες

Στη κατηγορία αυτή των προτύπων ανήκουν με βάση τη παρούσα επισκόπηση, τα ITIL, ISM3, COSO και το πλαίσιο CoBit. Τα ITIL, COSO και το CoBit είναι πλαίσια που δίνουν έμφαση στην οργάνωση του εσωτερικού ελέγχου ενός οργανισμού και στη διακυβέρνηση αυτού. Η προσέγγιση που προωθούν, προβάλλει περισσότερο την υλοποίηση ενός πλαισίου διαδικασιών για τη διακυβέρνηση της πληροφορικής ώστε να επιτευχθεί ευθυγράμμιση των στόχων της πληροφορικής με τους επιχειρηματικούς στόχους.

2.3.1 ISM3

Η αρχική ιδέα υλοποίησης του προτύπου ISM3 (Information Security Management Maturity Model) ήταν να συλλέξει και να συγκεντρώσει τις καλύτερες πρακτικές σχετικά με τη διαχείριση συστημάτων και ελέγχου από το ISO 9000, το ITIL, το CMMI (Capability Maturity Model Integration) και το ISO 17799 /ISO 27001. Το ISM3 υλοποιήθηκε οχι μόνο στοχεύοντας στις μεγάλες αλλά και στις μικρές επιχειρήσεις να επιτύχουν μέγιστη απόδοση της επένδυσής τους στην ασφάλεια των πληροφοριών, ανεξάρτητα από το προϋπολογισμό τους, συχνά σε σχέση με τη χρήση ενός Συστήματος Διαχείρισης της Ασφάλειας των Πληροφοριών (Information Security Management System - ISMS). Το 2011, η ομάδα Open Group δημοσίευσε τη νέα έκδοση του ISM3, το Open Information Security Management Maturity Model (O- ISM3).

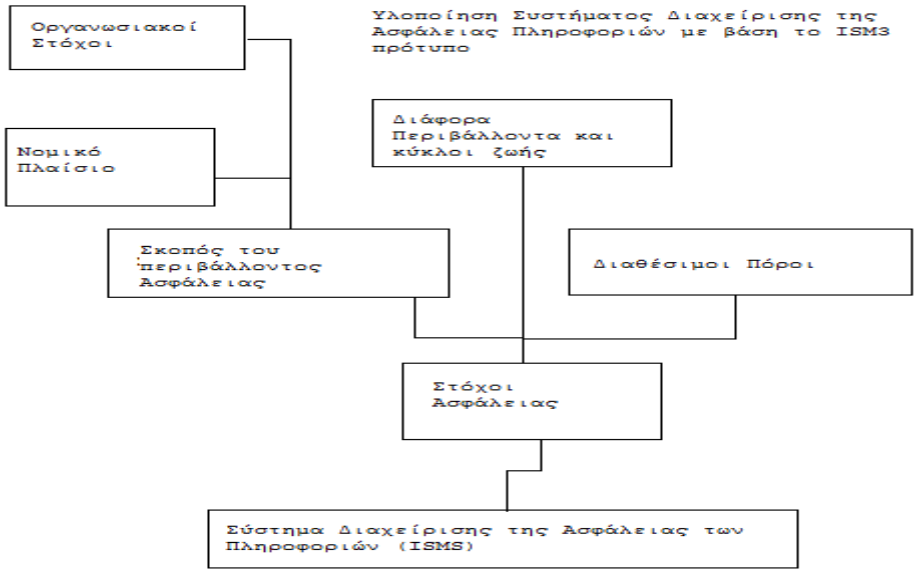
Το ISM3 μπορεί να χρησιμοποιηθεί με διάφορους τρόπους:

- Είναι ένα εργαλείο για τους διαχειριστές και τους ελεγκτές για την αξιολόγηση και την ενίσχυση του Συστήματος Διαχείρισης της Ασφάλειας των Πληροφοριών τους (ISMS).
- Παρέχει μια μετρήσιμη προσέγγιση για τη διαχείριση των Πληροφοριακών τους Συστημάτων.
- Μπορεί να χρησιμοποιηθεί για την επέκταση των απαιτήσεων ISO 9000 στο Σύστημα Διαχείρισης της Ασφάλειας των Πληροφοριών (ISMS) του εκάστοτε οργανισμού.

Σύμφωνα με τον Aceituno (2006), το ISM3 δεν έχει ως στόχο να καταστήσει τα συστήματα άτρωτα ή να παράσχει απόλυτη ασφάλεια, εφόσον δεν προσανατολίζεται και σε τεχνικά θέματα, αλλά να βοηθήσει στην επίτευξη της αποστολής του οργανισμού που ορίζει για θέματα ασφάλειας. Ευθυγραμμίζει τη διαχείριση της ασφάλειας με τις ανάγκες της επιχείρησής μέσω καθορισμού επιχειρηματικών στόχων, και στόχων για ασφάλεια της πληροφορίας. Οι επιχειρηματικοί στόχοι που τίθενται απορρέουν από την αποστολή του οργανισμού και το νομικό περιβάλλον, ενώ οι στόχοι ως προς το επίπεδο ασφάλειας καθορίζονται από τα υπό προστασία περιουσιακά στοιχεία, το περιβάλλον και τους διαθέσιμους πόρους του οργανισμού που διαθέτει για την προστασία αυτή.

Το ISM3 περιλαμβάνει πέντε επίπεδα ωριμότητας, καθένα από τα οποία μπορεί να αναγνωριστεί ως ένα σύστημα διαχείρισης. Χρησιμοποιώντας αυτά τα επίπεδα, μια εταιρεία μπορεί να προσαρμόσει το Σύστημα Διαχείρισης της Ασφάλειας των Πληροφοριών (ISMS) σε ρεαλιστικούς στόχους ασφάλειας, με τη χρήση των πόρων, έτσι ώστε να μεγιστοποιήσει τα οφέλη της και να βελτιώσει το επίπεδο ασφάλειας. Πλεονέκτημα των επιπέδων ωριμότητας, θεωρείται το γεγονός ότι κατά την επίτευξη βασικών στόχων ασφάλειας καθίσταται δυνατή η απόκτηση ενδιάμεσων πιστοποιήσεων.

Ένα άλλο πλεονέκτημα είναι ότι ένα Σύστημα Διαχείρισης της Ασφάλειας των Πληροφοριών (ISMS) που βασίζεται στο πρότυπο ISM3 μπορεί να διαπιστευτεί σύμφωνα με τα πρότυπα ISO 9001 ή ISO 27001, πράγμα που σημαίνει ότι το ISM3 μπορεί να χρησιμοποιηθεί σε ένα Σύστημα Διαχείρισης της Ασφάλειας των Πληροφοριών κατά ISO 27001. Άλλωστε οι διαδικασίες που καθορίζει προέρχονται από το CMMI και το ISO 9001. Από πλευράς συμβατότητας, το ISM3 πληρεί τις προϋποθέσεις και τις απαιτήσεις για συμμόρφωση με ISO 27001 αφού το ISM3 μπορεί να χρησιμοποιηθεί και σαν εργαλείο για την υλοποίηση του ISO 27001. Επιπλέον, το ISM3 εμβαθύνει το πλαίσιο ασφάλειας του ITIL και προσφέρει ένα αναλυτικό πλαίσιο για το συνδυασμό του ISO 17799 με το πλαίσιο COBIT.



ISM3, Πηγή: Aceituno 2006

Ένας από τους προβληματισμούς και κριτικές σε σχέση με το ISM3 είναι ότι δεν προάγει κάποιας μορφής σύνδεση μεταξύ των στόχων ασφάλειας της πληροφορίας (εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα) και των επιχειρησιακών στόχων αλλά συγχέει τα δυο χωρίς να τα διαχωρίζει ρητά. Επίσης, δεν μπορεί να αντικαταστήσει το ISO27001. Το μόνο που μπορεί να παράσχει στον οργανισμό είναι κάποιες περεταίρω προδιαγραφές για συμμόρφωση με το ISO27001. Ο Aceituno όμως, σε ένα από τα άρθρα του για τα επίπεδα ωριμότητας του ISM3 (Aceituno,2008), υποστηρίζει ότι σε αυτό που το ISM3 υπερτερεί των άλλων προσεγγίσεων/ πλαισίων για την ασφάλεια των πληροφοριών είναι ότι προωθεί την ιδέα της μέτρησης της αποτελεσματικότητας των διαδικασιών ελέγχου που προτείνει για υλοποίηση, και δεν αρκείται μόνο στη σχεδίαση διαδικασιών.

2.3.2 ITIL

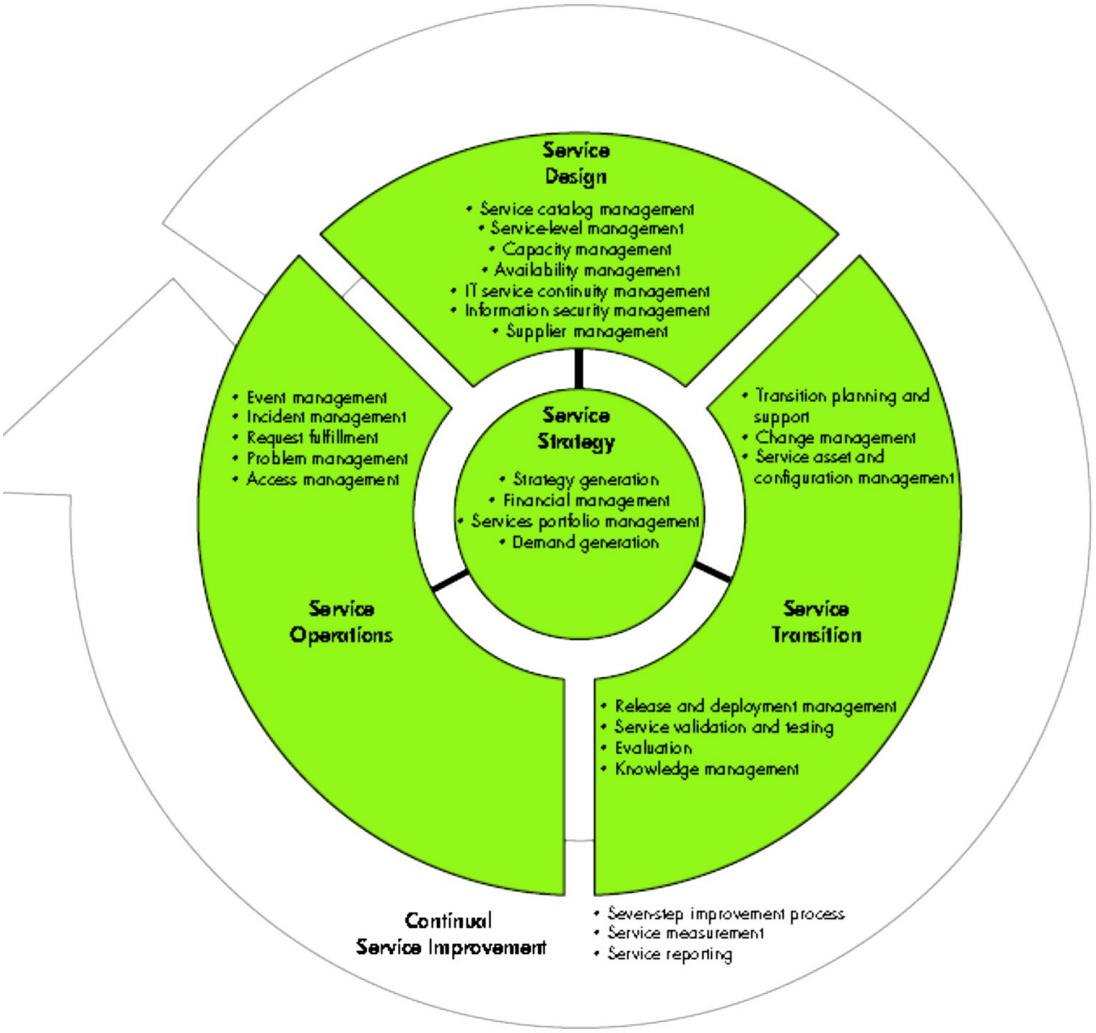
Το ITIL (Information Technology Infrastructure Library Security Management) είναι ένα κοινό πλαίσιο, που περιγράφει τις βέλτιστες πρακτικές στον τομέα της διαχείρισης των υπηρεσιών της πληροφορικής (διεργασίες - διαχείριση ποιότητας - διανομή -υποστήριξη - ασφάλεια). Εστιάζει στη συνεχή μέτρηση και βελτίωση της ποιότητας των υπηρεσιών που παρέχει η διεύθυνση πληροφορικής, τόσο από τη πλευρά της επιχείρησης όσο και από αυτή των πελατών. Ένα από τα πιο σημαντικά χαρακτηριστικά του ITIL v3 είναι ο βαθμός στον οποίο το μοντέλο κινείται από ένα διαχειριστικό ρόλο και οπτική της πληροφορικής σε ένα ρόλο που υποστηρίζει πλήρως τις δραστηριότητες και τις διαδικασίες στον επιχειρησιακό τομέα, καθώς επιδιώκει να βοηθήσει την επιχείρηση στην επίτευξη των στόχων της. Σε αυτό το πλαίσιο, το ITIL v3 προβάλλει πέντε κύρια στάδια του κύκλου ζωής των υπηρεσιών:

- Το στάδιο των υπηρεσιών στρατηγικής: Η πληροφορική λειτουργεί συνεργατικά με το επιχειρησιακό κομμάτι (π.χ. για τη διαχείριση της ζήτησης, τον προσδιορισμό των αγορών, το οικονομικό κομμάτι) και, τελικά αποφασίζεται ποιες υπηρεσίες θα πρέπει να παρέχει στον υπόλοιπο της επιχείρησης.
- Το στάδιο του σχεδιασμού των υπηρεσιών: Η πληροφορική αναπτύσσει ένα ρεαλιστικό πλαίσιο υπηρεσιών που εξισορροπεί τη λειτουργικότητα, την απόδοση και το κόστος και επίσης δίνει καίριες λύσεις για την εξεύρεση πόρων (εσωτερική ανάθεση, την εξωτερική ανάθεση - outsourcing, και από κοινού προμήθεια – co-sourcing).
- Το στάδιο της μετάβασης των υπηρεσιών: Η πληροφορική δοκιμάζει και εισάγει τις υπηρεσίες της στο κομμάτι της υποδομής με τους κατάλληλους ελέγχους σύμφωνα με σαφώς καθορισμένες διαδικασίες για την διαχείριση των αλλαγών, των στοιχείων του ενεργητικού της και τη διαχείριση της διαμόρφωσης αυτών (configuration).

• Το στάδιο της διαχείρισης των υπηρεσιών: Η πληροφορική παρέχει και υποστηρίζει τις υπηρεσίες που έχει αναπτύξει με στόχο τη σταθερότητα τους και την εξασφάλιση της απρόσκοπτης λειτουργίας αυτών, διατηρώντας την ευελιξία που απαιτείται για να ανταποκριθεί στις διακυμάνσεις του επιχειρησιακού και του τεχνολογικού περιβάλλοντος.

• Το στάδιο της συνεχούς βελτίωσης των υπηρεσιών: Η πληροφορική παρακολουθεί την απόδοση των υπηρεσιών και προσδιορίζει τρόπους για τη βελτίωση της ποιότητας αυτών και τη μείωση του κόστους ενώ συμβαδίζει με μεταβαλλόμενες απαιτήσεις των επιχειρήσεων.

Η βασική ιδέα που το πρότυπο ITIL προάγει είναι ότι με αυτές τις θεμελιώδεις τεχνολογίες και τις δυνατότητες που βοηθούν τους οργανισμούς να συνδέσουν τα διάφορα στάδια του κύκλου ζωής των υπηρεσιών (Service Management), οι εταιρίες μπορούν να προετοιμαστούν καλύτερα για το συντονισμό των δραστηριοτήτων τους σε όλους τους τομείς της Τεχνολογίας και των Πληροφοριών (IT) και να λειτουργήσουν πιο αποτελεσματικά με το υπόλοιπο του οργανισμού στο να εκτελεί στρατηγικές πρωτοβουλίες.



ITIL: Παρουσίαση κύκλου υπηρεσιών, Πηγή: επίσημος ιστότοπος του ITIL.

Συμπερασματικά, το πρότυπο ITIL παρουσιάζει τη πληροφορική σαν υποστηρικτική όλης της επιχειρησιακής δραστηριότητας και παράλληλα άρρηκτα συνδεδεμένη με αυτή και τη στρατηγική της. Αυτό που προβάλει μέσα από τα 5 προαναφερθέντα στάδια ωριμότητας του IT Service Management είναι οι διαδικασίες που πρέπει να αναπτύξει η Διοίκηση της πληροφορικής σε ένα οργανισμό σε 5 στάδια και σε συνάρτηση με το βαθμό ωριμότητας του επιχειρηματικού κόσμου

με στόχο τη καλύτερη υποστήριξη και βελτιστοποίηση των επιχειρησιακών διαδικασιών. Για αυτό το λόγο θεωρείται ότι και το ITIL πλαισιώνει αποτελεσματικά σαν πρότυπο τις διαδικασίες που θα πρέπει να αναπτύξουν από τη πλευρά και οι πάροχοι υπηρεσιών πληροφορικής, ώστε οι αντίστοιχοι οργανισμοί τους οποίους υποστηρίζουν να λειτουργούν αποδοτικά.

Ένα από τα κύρια μειονεκτήματα είναι ότι το ITIL περιορίζεται στην ανάπτυξη των υπηρεσιών της πληροφορικής (IT Service Management) και λόγω αυτού συνήθως χρησιμοποιείται σε συνδυασμό με ένα ή περισσότερα άλλα πρότυπα βέλτιστων πρακτικών για τη διαχείριση και ασφάλεια της τεχνολογίας των πληροφοριών, όπως:

• COBIT (πλαίσιο ηλεκτρονικής διακυβέρνησης και ελέγχου)

• Six Sigma (μεθοδολογία για την βελτιστοποίηση της ποιότητας)

• TOGAF (πλαίσιο για την αρχιτεκτονική)

• ISO 27000 (πρότυπα για την ασφάλεια των πληροφοριακών συστημάτων).

2.3.3 COSO

Το πλαίσιο COSO (Committee Of Sponsoring Organisations of the Treadway Commission) είναι ένα πλαίσιο το οποίο ενεργοποιεί μια ολοκληρωμένη διαδικασία εσωτερικού ελέγχου. Βοηθά στη βελτίωση των μέσων ελέγχου στις επιχειρήσεις μέσω της αξιολόγησης της αποτελεσματικότητας του εσωτερικού ελέγχου και αποτελείται από πέντε αλληλοσχετιζόμενες συνιστώσες εσωτερικού ελέγχου[1]**:**

1. *Περιβάλλον ελέγχου.* Το περιβάλλον ελέγχου θέτει το γενικό πνεύμα του οργανισμού. Αποτελεί το θεμέλιο για τις υπόλοιπες συνιστώσες παρέχοντας πειθαρχία και δομή. Οι παράγοντες που περιλαμβάνει είναι η ακεραιότητα των ατόμων μέσα στον οργανισμό, οι ηθικές αξίες, η φιλοσοφία της Διοίκησης και του τύπου λειτουργίας, η μέθοδος που η Διοίκηση εξουσιοδοτεί και αναθέτει ευθύνες, οργανώνει και αναπτύσσει το προσωπικό και τέλος η προσοχή και η κατεύθυνση που παρέχεται από το Διοικητικό Συμβούλιο.
2. *Εκτίμηση του κινδύνου.* Κάθε μονάδα αντιμετωπίζει μία ποικιλία από κινδύνους από εσωτερικές και εξωτερικές πηγές που πρέπει να εκτιμηθούν. Μία απαραίτητη προϋπόθεση της εκτίμησης των κινδύνων είναι ο καθορισμός επιχειρησιακών στόχων. Η εκτίμηση των κινδύνων είναι ο προσδιορισμός και η ανάλυση των σχετικών κινδύνων για την επίτευξη των παραπάνω στόχων, καταρτίζοντας μία βάση για τον προσδιορισμό της διαχείρισης τους.
3. *Ελεγκτικές δραστηριότητες*. Ελεγκτικές δραστηριότητες είναι οι πολιτικές και οι διαδικασίες που βοηθούν στην εκτέλεση των αρχών - οδηγιών της Διοίκησης. Αυτές εξασφαλίζουν ότι οι αναγκαίες ενέργειες έχουν λάβει χώρα για την αντιμετώπιση των κινδύνων και την επίτευξη των αντικειμενικών στόχων. Περιλαμβάνουν ένα εύρος από ενέργειες, όπως εγκρίσεις, εξουσιοδοτήσεις, επαληθεύσεις, διευθετήσεις, συμφωνίες, επισκοπήσεις της λειτουργικής απόδοσης, της ασφάλειας των περιουσιακών στοιχείων και το διαχωρισμό των καθηκόντων.
4. *Πληροφορία και επικοινωνία.* Ο προσδιορισμός και η διαβίβαση της πληροφορίας πρέπει να γίνεται με τον κατάλληλο τρόπο και στο κατάλληλο χρονικό διάστημα ώστε να καθιστά ικανό το προσωπικό να ασκεί τα καθήκοντα του. Το πληροφοριακό σύστημα παράγει καταστάσεις, περιέχοντας πληροφορίες λειτουργικές, οικονομικές και σχετικές με την πλήρωση των κανόνων, βασικές για την εκτέλεση και τον έλεγχο των επιχειρησιακών εργασιών. Η αποτελεσματική επικοινωνία πρέπει επίσης να υπάρχει με την ευρύτερη έννοια σε όλα τα επίπεδα του οργανισμού. Όλο δηλαδή το προσωπικό πρέπει να λαμβάνει ένα καθαρό μήνυμα από την κορυφή της μονάδας, ότι πρέπει να αναλαμβάνει αυστηρά τις ευθύνες του, σχετικά με το σύστημα εσωτερικού ελέγχου.

[1] http://www.srcosmos.gr/srcosmos/showpub.aspx?aa=9542

5. *Παρακολούθηση και εποπτεία.* Τα συστήματα εσωτερικού ελέγχου πρέπει να παρακολουθούνται (μία διεργασία που εκτιμά την ποιότητα, της απόδοσης του συστήματος). Αυτό επιτυγχάνεται μέσω των δραστηριοτήτων παρακολούθησης σε εξέλιξη και των εκτιμήσεων. Περιλαμβάνουν τακτικές εποπτικές και διοικητικές δραστηριότητες και άλλες ενέργειες που οφείλει το προσωπικό να κάνει για την άσκηση των καθηκόντων του. Το αντικείμενο και η συχνότητα των εκτιμήσεων εξαρτάται κατά πρώτο λόγο από την εκτίμηση των κινδύνων και από την αποτελεσματικότητα των τρεχουσών διαδικασιών ελέγχου.

Το πλαίσιο COSO είναι ένα πρότυπο για την αξιολόγηση των διαδικασιών εσωτερικού ελέγχου των οργανισμών. Αυτό το μοντέλο έχει υιοθετηθεί ως το γενικά αποδεκτό πλαίσιο για την αξιολόγηση του εσωτερικού ελέγχου και αναγνωρίζεται ευρέως ως το οριστικό πρότυπο βάσει του οποίου οι οργανώσεις μετρούν την αποτελεσματικότητα των συστημάτων εσωτερικού ελέγχου τους. Βασίζεται στην αναγνώριση και αξιολόγηση των κινδύνων και αντίστοιχα προτείνει την υλοποίηση σχετικών σημείων ελέγχου.

Παρόλα αυτά, έχουν ασκηθεί και πολλές κριτικές πάνω στο COSO με τον ισχυρισμό ότι συγχέει και αναμειγνύει το πλαίσιο (των οργανωτικών δομών, των πολιτικών και ρυθμίσεων που έχουν θεσπισθεί για την προώθηση, την ενσωμάτωση και τη βελτίωση της διαχείρισης των κινδύνων) με τις διαδικασίες που χρησιμοποιούνται για τη διαχείριση του κινδύνου, ιδιαίτερα εκείνες που χρησιμοποιούνται για την αξιολόγηση, την επεξεργασία και την παρακολούθηση των κινδύνων, ενώ είναι οι τελευταίες που το πρότυπο «θέλει» να ενσωματώσει στις διαδικασίες λήψης αποφάσεων για τον οργανισμό. Θεωρείται ταυτόχρονα πολύ πολύπλοκο στην υλοποίηση του και ασαφές (Beasley κ.α, 2010). Μαζί με το πλαίσιο Cobit αποτελούν τα δυο πιο διαδεδομένα πλαίσια που λαμβάνουν υπόψη τους την υλοποίηση διαδικασιών για την αξιολόγηση και διαχείριση του κινδύνου. Το COSO βέβαια αν και κατέστη το πλαίσιο μεγαλύτερης αποδοχής προς συμμόρφωση των εταιριών με το Sarbanes-Oxley Act δεν συμβάλει στη βοήθεια των εταιριών για σχεδιασμό και υλοποίηση της τεχνολογίας πληροφοριών.

2.3.4 Το Πλαίσιο CoBit

Στα πλαίσια των σημαντικότερων προτύπων που διέπουν την αξιολόγηση της ασφάλειας των συστημάτων πληροφορικής και ειδικότερα αυτών που υποστηρίζουν ηλεκτρονικές τραπεζικές συναλλαγές, η 4η έκδοση του COBIT παρέχει ολοκληρωμένο πλαίσιο εργασιών για την υλοποίηση της εταιρικής διακυβέρνησης, συμπεριλαμβάνοντας επίσης στοιχεία του ITIL και ISO 27001. Το Control Objectives for Information and related Technology - COBIT (Στόχοι Ελέγχου Πληροφοριών και Σχετικής Τεχνολογίας) είναι το πλέον αποδεκτό και διαδεδομένο πλαίσιο με τις βέλτιστες πρακτικές που αφορά στην αποτελεσματική Διακυβέρνηση και τον έλεγχο της Πληροφορικής μέσα στην επιχείρηση και εκδίδεται από το Ινστιτούτο Διαχείρισης της Πληροφορικής (IT Governance Institute) και το Ινστιτούτο Ελέγχου Συστημάτων Πληροφορικής (ISACA ή Information Systems Audit and Control Association). Πρόκειται για ένα πλαίσιο ελέγχου στον τομέα της πληροφορικής που βασίζεται κατά ένα μέρος στο πλαίσιο COSO (Committee of Sponsoring Organisations of the Tradeway Commission) που παρουσιάστηκε προηγουμένως.

Το COBIT είναι ένα «πλαίσιο ελεγκτικών μηχανισμών που συνδέει τις διαδικασίες και πρωτοβουλίες του τομέα της μηχανοργάνωσης με τις επιχειρησιακές απαιτήσεις, οργανώνει τις μηχανογραφικές διαδικασίες σε ένα πιο γενικευμένο μοντέλο διαδικασιών και αναγνωρίζει τους σημαντικότερους πληροφοριακούς πόρους που θα πρέπει να διαχειριστούν έτσι ώστε να οριστούν οι διοικητικοί στόχοι των ελεγκτικών μηχανισμών» (Cobit, 2007).

Η πληροφορία αποτελεί πλέον το πιο σημαντικό περιουσιακό στοιχείο για πολλούς Οργανισμούς οπότε και η τεχνολογία που την υποστηρίζει παίζει πρωτεύοντα ρόλο στη λειτουργία των Οργανισμών αυτών. Κατά συνέπεια η ευθυγράμμιση των μηχανογραφικών διεργασιών με τους επιχειρησιακούς στόχους και η εξασφάλιση της αποδοτικότητας και αποτελεσματικότητας του Τμήματος Πληροφορικής με γνώμονα τη στρατηγική του Οργανισμού αποτελεί πολλές φορές σημαντικό παράγοντα επιτυχίας. Για να λειτουργήσει το Τμήμα Πληροφορικής προς την κατεύθυνση αυτή, πρέπει να χρησιμοποιεί μια σειρά καλά δομημένων

και ομαδοποιημένων διεργασιών και η διοίκηση να είναι σε θέση να παρακολουθήσει τις διεργασίες αυτές και να μετρήσει την αποτελεσματικότητα και αποδοτικότητά τους.

Το πλαίσιο ελέγχου COBIT συμβάλλει στην επιτυχή ανταπόκριση της τεχνολογίας πληροφοριών επί των επιχειρησιακών απαιτήσεων:

- Κάνοντας σύνδεση της τεχνολογίας πληροφοριών με τις επιχειρησιακές απαιτήσεις
- Οργανώνοντας τις δραστηριότητες τεχνολογίας πληροφοριών σε ένα γενικά αποδεκτό πρότυπο διαδικασίας
- Προσδιορίζοντας τους σημαντικότερους πόρους τεχνολογίας πληροφοριών ώστε να επιδιωχθεί η μόχλευση τους
- Καθορίζοντας τους στόχους του διοικητικού ελέγχου που θα πρέπει να ληφθούν υπόψη.

Για να απαλλάξει αυτές τις ευθύνες, καθώς επίσης και για να επιτύχει τους στόχους της, η διεύθυνση πρέπει να κατανοήσει τη θέση της αρχιτεκτονικής της τεχνολογίας πληροφοριών και να αποφασίσει το είδος διακυβέρνησης και τον έλεγχο που θα πρέπει να παρέχει.

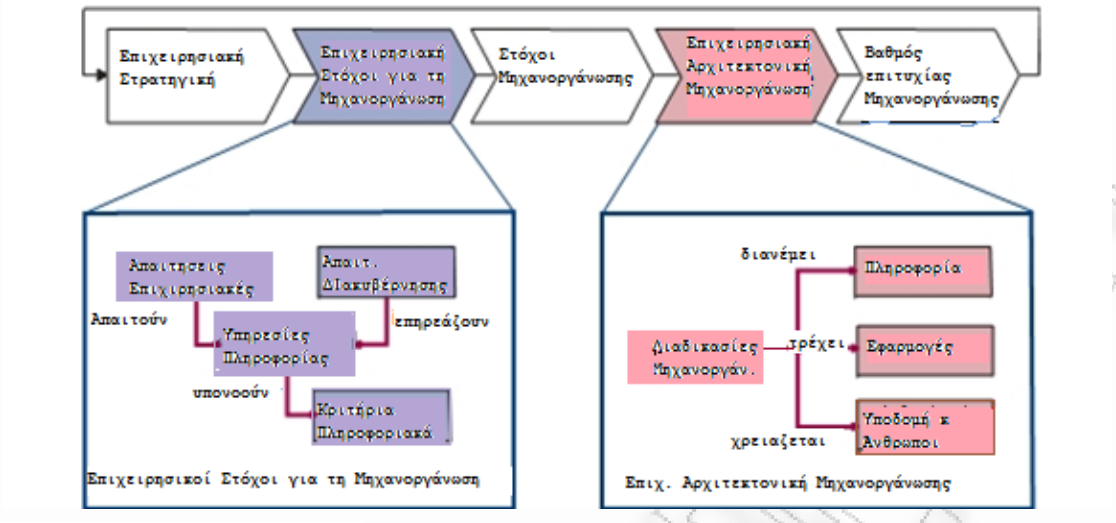
Το Control Objectives for Information and related Technology - COBIT παρέχει ορθές πρακτικές γύρω από ένα πλαίσιο περιοχών και διαδικασιών και παρουσιάζει τις δραστηριότητες σε μια διαχειριζόμενη και λογική δομή. Οι ορθές πρακτικές του COBIT αντιπροσωπεύουν την ομοφωνία εμπειρογνωμόνων, εστιάζονται κυρίως στον έλεγχο και λιγότερο στη διευθυντική εκτέλεση. Αυτές οι πρακτικές βοηθούν τη βελτιστοποίηση των εν δυνάμει επενδύσεων σε τεχνολογία πληροφοριών, την εξασφάλιση παροχής υπηρεσιών και την παροχή ενός μέτρου έναντι του οποίου να κρίνεται πότε υπάρχουν πραγματικά προβλήματα.

Το COBIT εισήχθηκε για πρώτη φορά το 1996. Αποστολή του ήταν να «ερευνήσει, αναπτύξει, δημοσιεύσει και προωθήσει ένα επίσημο, έγκυρο, διεθνές σύνολο γενικώς αποδεκτών προτύπων για την τεχνολογία των πληροφοριακών συστημάτων, για καθημερινή χρήση από τους διευθυντές και τους ελεγκτές». Το CobiT μπορεί να χρησιμοποιηθεί για λήψη αποφάσεων, ελέγχους και συντήρηση υπηρεσιών πληροφορικής (ΕΕΔΕ, 2008). Διευθυντές, ελεγκτές και χρήστες αποκομίζουν μεγάλα οφέλη από τη χρήση του COBIT, καθ' ότι τους βοηθά να κατανοήσουν τα πληροφοριακά συστήματα της επιχείρησής τους, ώστε να αποφασίσουν ποιο είναι το κατάλληλο επίπεδο ελέγχου και ασφάλειας για την προστασία του οργανισμού (Κατσίκας). Πιο συγκεκριμένα, οι διευθυντές αποκτούν μια βάση πάνω στην οποία θα στηρίζουν τις επενδύσεις και αποφάσεις γύρω από τα πληροφοριακά συστήματα, αφού διαθέτουν ένα πλαίσιο που τους βοηθά να επιλέξουν το κατάλληλο λογισμικό και υλικολογισμικό (firmware) – εξασφαλίζοντας συνεχείς υπηρεσίες και παρακολούθηση. Οι ελεγκτές διευκολύνονται στην αναγνώριση ορισμένων ζητημάτων ελέγχου, ενισχύοντας έτσι τα ευρήματα των ελέγχων που διεξάγουν.

Οι επιχειρήσεις πρέπει να ικανοποιήσουν απαιτήσεις ποιότητας, ασφάλειας και εμπιστοσύνης των πληροφοριών τους, όπως κάνουν και με όλα τα στοιχεία του ενεργητικού τους. Η διεύθυνση επίσης για να ανταποκριθεί στις επιχειρησιακές απαιτήσεις τεχνολογίας πληροφοριών, πρέπει να επενδύσει στους πόρους που απαιτούνται για να δημιουργηθεί τεχνική επάρκεια (π.χ. ένα σύστημα προγραμματισμού των επιχειρησιακών πόρων - ERP) για την υποστήριξη μιας επιχειρησιακής ικανότητας (π.χ. για την εφαρμογή μιας αλυσίδας ανεφοδιασμού) για την επίτευξη του επιθυμητού αποτελέσματος (π.χ., αύξηση τζίρου και οικονομικά οφέλη).

Η διαχείριση και ο έλεγχος των πληροφοριών αποτελούν την καρδιά του COBIT και βοηθούν στην εξασφάλιση της ευθυγράμμισης με τις επιχειρησιακές απαιτήσεις.

Από την αρχική του έκδοση το 1996, το COBIT ανανεώνεται συχνά προκειμένου να είναι συνεχώς επίκαιρο, με πιο πρόσφατη έκδοση αυτή του 05/2007 όπου δημοσιεύθηκε το COBIT 4.1. Μάλιστα ο οργανισμός ISACA ανακοίνωσε πρόσφατα την επικείμενη δημοσίευση της έκδοσης 5 του πλαισίου (ISACA).



Πλαίσιο COBIT, Πηγή: CoBit 4.1

Η σημασία της πληροφορίας στο COBIT, Επιχειρησιακές Διαδικασίες και Πληροφορική

Για να ικανοποιηθούν οι επιχειρησιακοί στόχοι, οι πληροφορίες πρέπει να προσαρμοστούν σε ορισμένα κριτήρια ελέγχου, τα οποία το COBIT αναφέρει ως επιχειρησιακές απαιτήσεις για τις πληροφορίες. Με βάση την ευρύτερη έννοια της ποιότητας, της εμπιστοσύνης και απαίτησης ασφάλειας, η πληροφορία για το COBIT έχει έννοια μόνο όταν είναι χρήσιμη για τον Οργανισμό και για να συμβαίνει αυτό θα πρέπει να είναι[2]:

- Αποτελεσματική. Αυτό έχει να κάνει με το κατά πόσο είναι σχετική με την επιχειρησιακή διεργασία και κατά πόσο παραδίδεται έγκαιρα, σωστά και με τρόπο συνεπή και χρήσιμο.
- Αποδοτική, που σημαίνει ότι παρήχθη με τη βέλτιστη χρήση των διαθέσιμων πόρων.
- Εμπιστευτική, που σημαίνει ότι προστατεύεται από μη εξουσιοδοτημένη πρόσβαση.
- Ακέραια, που σημαίνει ότι είναι ακριβής, πλήρης και έγκυρη με βάση τις αξίες και προσδοκίες του Οργανισμού.
- Διαθέσιμη. Αυτό σημαίνει ότι η πληροφορία είναι προσβάσιμη από αυτούς που έχουν την εξουσιοδότηση όταν την χρειάζονται και ότι οι αναγκαίοι πόροι φυλάσσονται σωστά.
- Σύννομη, που σημαίνει ότι η διάθεση της πληροφορίας δεν παραβιάζει τη νομοθεσία και τις επικείμενες κανονιστικές διατάξεις.
- Αξιόπιστη. Αυτό σημαίνει ότι ανταποκρίνεται στην πραγματικότητα και επιτρέπει στη Διοίκηση να λειτουργήσει σωστά τον Οργανισμό.

Έχοντας αναγνωρίσει τη σημαντικότητα στη ροή της πληροφορίας σε έναν οργανισμό και τις επιχειρησιακές διαδικασίες αυτού, με τη βοήθεια της ισχύουσας νομοθεσίας αλλά και των στρατηγικών στόχων του οργανισμού προσδιορίζονται και οι Επιχειρηματικοί στόχοι (βλ. Πίνακα ακολουθεί) από πλευράς χρηματοοικονομικής, πελατειακής κλπ.

Επιχειρησιακοί στόχοι		
Χρηματοοικομικά	1	Υψηλές αποδόσεις επιχειρησιακών επενδύσεων που πηγάζουν από τη πληροφορική
	2	Διαχείριση πληροφοριακού κινδύνου
Πελατειακές σχέσεις	3	Βελτίωση των προσφερόμενων υπηρεσιών
	4	Ανταγωνιστικά προϊόντα και υπηρεσίες
	5	Εξασφάλιση της συνέχειας και της διαθεσιμότητας των υπηρεσιών

[2]SeCure: http://www.secure.com.gr/pages/itgms.aspx

	6	Ευελιξία στις αλλαγές των επιχειρησιακών στόχων
	7	Ελάχιστο κόστος για παροχή υπηρεσιών
	8	Εξασφάλιση χρήσιμης και αξιόπιστης πληροφορίας για στρατηγικής σημασίας αποφάσεις
	9	Βελτίωση και εξασφάλιση λειτουργίας επιχειρηματικών διεργασιών
Εσωτερικές σχέσεις	10	Χαμηλά κόστη σε διεργασίες
	11	Συμμόρφωση με νομικά πλαίσια
	12	Συμμόρφωση με εσωτερικές πολιτικές
	13	Διαχείριση επιχειρησιακών αλλαγών
	14	Εξασφάλιση και βελτίωση της παραγωγικότητας του ανρώπινου δυναμικού
Μαθησιακά και αναπτυξιακά	15	Καινοτομία στις επιχειρησιακές διαδικασίες
	16	Απόκτηση καταρτισμένου προσωπικού

Επιχειρησιακοί Στόχοι, Πηγή: CoBit 4.1

Για να παραχθούν οι πληροφορίες που έχει ανάγκη η επιχείρηση ώστε να επιτύχει τους στόχους της, οι πόροι τεχνολογίας πληροφοριών πρέπει να διαχειριστούν από ένα σύνολο ομαδοποιημένων διαδικασιών. Η εκτίμηση των ικανοτήτων διαδικασιών βασισμένη στα πρότυπα ωρίμανσης του COBIT είναι πολύ βασικό μέρος της εφαρμογής διακυβέρνησης τεχνολογίας πληροφοριών. Αφού προσδιοριστούν οι κρίσιμες διαδικασίες και ο έλεγχος τεχνολογίας πληροφοριών, η μοντελοποίηση για ωρίμανση επιτρέπει τον προσδιορισμό και ανάδειξη ανικανοτητών στη διεύθυνση. Τα προγράμματα δράσης (action plans) μπορούν έπειτα να αναπτυχθούν για να φέρουν τις διαδικασίες αυτές στο επιθυμητό επίπεδο στόχων.

Το COBIT υποστηρίζει για το λόγο αυτό τη διακυβέρνηση τεχνολογίας πληροφοριών με την παροχή ενός πλαισίου για να εξασφαλίσει (πέντε σημεία εστίασης):

- Στρατηγική ευθυγράμμισης (Strategic alignment): εστιάζεται α) στην εξασφάλιση συνοχής των επιχειρησιακών σχεδίων και των σχεδίων τεχνολογίας πληροφοριών β) στον καθορισμό, τη διατήρηση και τη επιβεβαίωση της αξίας τεχνολογίας πληροφοριών που προτείνεται, γ) και στην ευθυγράμμιση των διαδικασιών τεχνολογίας πληροφοριών με τις επιχειρηματικές διαδικασίες.
- Απόδοση αξίας (Value delivery): πρόκειται για την προώθηση της απόδοσης αξίας σε όλο τον κύκλο παράδοσης, που εξασφαλίζει ότι η τεχνολογία πληροφοριών παραδίδει τα υποσχόμενα οφέλη έναντι της στρατηγικής, επικεντρωνόμενη στη βελτιστοποίηση των δαπανών και της παρουσίασης αποδείξεων της εγγενής της αξίας.
- Διαχείριση των πόρων (Resource management): αφορά τη βέλτιστη επένδυση, και τη σωστή διαχείριση, των κρίσιμων πόρων τεχνολογίας πληροφοριών: εφαρμογές, πληροφορίες, υποδομή και άνθρωποι. Τα βασικά ζητήματα αφορούν τη βελτιστοποίηση της γνώσης και της υποδομής.
- Διαχείριση κινδύνου (Risk management): απαιτεί την ενημέρωση για τον κίνδυνο από τα ανώτερα στελέχη, την απόλυτη κατανόηση της επιχειρηματικής ανοχής στον κίνδυνο, την κατανόηση των απαιτήσεων συμμόρφωσης, τη διαφάνεια των σημαντικών για την επιχείρηση κινδύνων, και την ενσωμάτωση ευθυνών όσον αφορά τη διαχείριση κινδύνου.
- Μέτρηση απόδοσης Performance (measurement): Παρακολουθεί και ελέγχει την εφαρμογή στρατηγικής, την ολοκλήρωση του προγράμματος, τη χρήση πόρων, την απόδοση των διαδικασιών και την παροχή υπηρεσιών, χρησιμοποιώντας, παραδείγματος χάριν, τα balanced scorecards που μεταφράζουν τη στρατηγική σε δράσεις ώστε να επιτευχθούν μετρήσιμοι στόχοι.

Το COBIT είναι ένα λειτουργικό πλαίσιο και όχι πρότυπο. Η εφαρμογή του όμως εξασφαλίζει ότι:

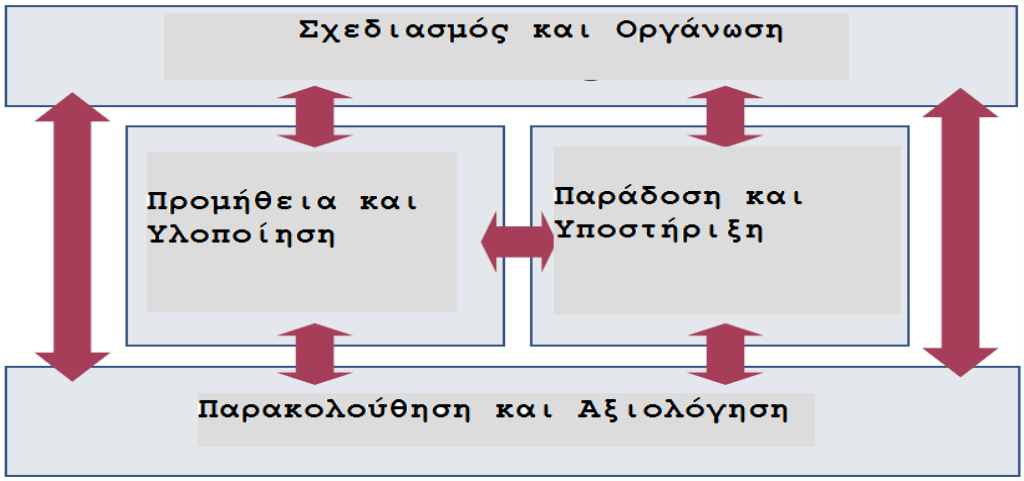
- Οι μηχανογραφικές διεργασίες του Οργανισμού είναι πλήρως ευθυγραμμισμένες με τους επιχειρησιακούς στόχους.
- Οι μηχανογραφικές διεργασίες έχουν το μέγιστο αποτέλεσμα για τον Οργανισμό.

- Οι πόροι της μηχανογράφησης χρησιμοποιούνται αποτελεσματικά και υπεύθυνα.
- Οι κίνδυνοι της μηχανογράφησης τυγχάνουν κατάλληλης διαχείρισης.

Οι πόροι που χρησιμοποιούνται κατά το COBIT από τη μηχανοργάνωση του Οργανισμού μπορεί να καθοριστούν ως εξής:

- Οι εφαρμογές, δηλαδή τόσο τα αυτοματοποιημένα συστήματα όσο και οι χειροκίνητες διαδικασίες που επεξεργάζονται την πληροφορία.
- Οι πληροφορίες, με την έννοια των δεδομένων σε οποιαδήποτε μορφή εισέρχονται και εξέρχονται από τα πληροφοριακά συστήματα.
- Η υποδομή, δηλαδή τα συστήματα, τα δίκτυα και οι εγκαταστάσεις που επιτρέπουν τη χρήση των εφαρμογών.
- Οι άνθρωποι, με την έννοια του προσωπικού που σχεδιάζει, οργανώνει και υλοποιεί τα πληροφοριακά συστήματα.

Εστιάζει στις διαδικασίες μέσα από ένα πρότυπο, που υποδιαιρεί την τεχνολογία πληροφοριών σε 34 διαδικασίες υψηλού επιπέδου που καλύπτουν 210 στόχους ελέγχου. Οι στόχοι κατηγοριοποιούνται σε 4 τομείς : Σχεδιασμός και Οργάνωση (Planning and Organization), Προμήθεια και Υλοποίηση (Acquisition and Implementation), Παράδοση και Υποστήριξη (Delivery and Support), Παρακολούθηση και Αξιολόγηση (Monitoring and Evaluation).



4 τομείς CoBit, Πηγή: CoBit 4.1

Κάθε μία από τις διεργασίες της πληροφορικής (μηχανογραφικές) σχηματοποιείται με τέτοιο τρόπο ώστε:

- Να καθορίζεται ο απώτερος σκοπός και οι άμεσοι στόχοι της καθώς και κατάλληλοι δείκτες που επιτρέπουν στη Διοίκηση να γνωρίζει κατά πόσο αυτοί οι στόχοι επιτυγχάνονται.
- Να καθορίζεται το στέλεχος που είναι υπεύθυνο για αυτήν.
- Να είναι επαναλήψιμη, να παράγει δηλαδή τα ίδια αποτελέσματα αν ακολουθηθούν τα ίδια βήματα ανεξάρτητα από το πρόσωπο που την εκτελεί.
- Να καθορίζονται και περιγράφονται πλήρως οι ρόλοι και οι αρμοδιότητες που προκύπτουν από αυτήν.
- Να περιγράφονται με σαφήνεια η πολιτική, τα σχέδια και οι διαδικασίες που σχετίζονται με αυτήν.
- Να μπορούν να καθοριστούν μέτρα σύγκρισης και να μετράται η αποτελεσματικότητα της διεργασίας με σκοπό τη βελτίωσή της.

Σχεδιασμός και οργάνωση	PO1	Οριστικοποίηση ενός στρατηγικού πλάνου πληροφορικής
	PO2	Ορισμό της αρχιτεκτονικής της πληροφορίας
	PO3	Ορισμός τεχνολογικής κατεύθυνσης

	PO4	Ορισμός πληροφοριακών διεργασιών, οργάνωσης και σχέσεων
	PO5	Διαχείριση επενδύσεων στη πληροφορική
	PO6	Γνωστοποίηση των στόχων στη Διοίκηση
	PO7	Διαχείριση των πόρων της πληροφορικής
	PO8	Διαχείριση ποιότητας
	PO9	Διαχείριση και εκτίμηση πληροφοριακών κινδύνων
	PO10	Διαχείριση έργων
Προμήθεια και εγκατάσταση	AI1	Διερεύνηση αυτοματοποιημένων λύσεων
	AI2	Προμήθεια εφαρμογών λογισμικού
	AI3	Προμήθεια και υλοποίηση τεχνολογικής υποδομής
	AI4	Διευκόλυνση Λειτουργίας και χρήσης
	AI5	Προμήθεια πληροφοριακών πόρων
	AI6	Διαχείριση αλλαγών
	AI7	Εγκατάσταση και πιστοδότηση λύσεων και αλλαγών
Παράδοση και υποστήριξη	DS1	Ορισμός επιπέδων υπηρεσιών
	DS2	Ορισμός υπηρεσιών τρίτων
	DS3	Ορισμός επιδόσεων και ικανοτήτων
	DS4	Εξασφάλιση συνέχειας των υπηρεσιών
	DS5	Εξασφάλιση της ασφάλειας των συστημάτων
	DS6	Αναγνώριση και καταμερισμός του κόστους
	DS7	Εκπαίδευση χρηστών
	DS8	Διαχείριση συμβάντων
	DS9	Διαχείριση παραμετροποίησης και διαμόρφωσης των συστημάτων
	DS10	Διαχείριση προβλημάτων
	DS11	Διαχείριση δεδομένων
	DS12	Διαχείριση φυσικού περιβάλλοντος
	DS13	Διαχείριση Λειτουργιών
Παρακολούθηση και αξιολόγηση	ME1	Παρακολούθηση και αξιολόγηση των υπηρεσιών της πληροφορικής
	ME2	Παρακολούθηση και αξιολόγηση του εσωτερικού ελέγχου
	ME3	Εξασφάλιση νομικής συμμόρφωσης
	ME4	Παροχή διακυβέρνησης πήροφορικής

Διαδικασίες της Πληροφορικής (Μηχανογραφικές Διεργασίες), Πηγή: CoBit 4.1

Ο επιχειρησιακός προσανατολισμός του COBIT εστιάζεται στη σύνδεση των επιχειρησιακών στόχων με τους στόχους της τεχνολογίας πληροφοριών, παρέχοντας μετρήσεις και πρότυπα ωριμότητας για τη σύγκριση των αποτελεσμάτων τους, και καθορίζοντας τις σχετικές ευθύνες των φορέων επιχειρήσεων και των φορέων διαδικασιών τεχνολογίας πληροφοριών. Οδηγίες Εφαρμογής προς τη Διοίκηση, Μετρικές, εργαλεία και τεχνικές, τα οποία είναι στη διάθεση της Διοίκησης του ΠΣ (Κατσίκας, 2010) είναι τα ακόλουθα:

- Μοντέλα Ωριμότητας (Maturity Models)
- Κρίσιμοι Παράγοντες Επιτυχίας (Critical Success Factors)
- Κύριοι Δείκτες Στόχων (Key Goal Indicators)
- Κύριοι Δείκτες Απόδοσης (Key Performance Indicators)
- Συμπυκνωμένη γνώση και εμπειρία από οργανισμούς οι οποίοι έχουν εφαρμόσει επιτυχώς το πλαίσιο COBIT

Περιορισμοί και ιδιαιτερότητες του COBIT

Κατά τον Καλαμάκι (2008) το COBIT υστερεί στα εξής:

- Απαιτεί αναδιοργάνωση της οπτικής των οντοτήτων του οργανισμού που εμπλέκονται στην εφαρμογή του (key players)
- Το COBIT είναι ένα πλαίσιο που πρέπει να προσαρμοστεί στον συγκεκριμένο οργανισμό
- Το COBIT συνιστάται να χρησιμοποιηθεί εκ παραλλήλου με άλλες ελεγκτικές προσεγγίσεις
- Οι Οδηγίες Εφαρμογής προς τη Διοίκηση είναι γενικές και πρέπει να προσαρμοστούν ανάλογα

Η εφαρμογή του COBIT όμως αποτελεί ουσιαστικό επιχείρημα για έναν Οργανισμό προκειμένου να πείσει οποιονδήποτε τρίτο ότι ακολουθεί σωστές αρχές εταιρικής διακυβέρνησης την οποία στηρίζουν κατάλληλες μηχανογραφικές διεργασίες. Αρχικά αναπτύχθηκε από ένα σύνολο βέλτιστων πρακτικών και τώρα πλαισιώνει τα πρότυπα και τις βέλτιστες πρακτικές εντάσσοντάς τα στις διαδικασίες της μηχανοργάνωσης για την υλοποίηση των απαραίτητων μηχανισμών ελέγχου (Tuttle & Vandervelde, 2007). Επιπλέον, είναι από τα πλαίσια που έχει σαν στόχο να βοηθήσει ένα οργανισμό στην ευθυγράμμιση των επιχειρηματικών στόχων με αυτούς της χρήσης της τεχνολογίας της πληροφορικής, καθώς δίνει έμφαση στην υλοποίηση σημείων ελέγχου που ικανοποιούν πλέον τις επιχειρησιακές ανάγκες και όχι αποκλειστικά τις ανάγκες για ασφάλεια της πληροφορίας (Ridley κ.α., 2004). Θα πρέπει να σημειωθεί ωστόσο, ότι κανένα πλαίσιο – ακόμα και αν εφαρμοστεί ακριβώς όπως ορίζεται – δεν μπορεί να εγγυηθεί την 100% διασφάλιση της πληροφορίας. Αντίθετα, υπάρχει μεγάλη εξάρτηση από νόμους, κανονισμούς και αποφάσεις της ίδιας της επιχείρησης και στη περίπτωσή μας του εκάστοτε Πιστωτικού Ιδρύματος γύρω από το επίπεδο του αποδεκτού κινδύνου και τη διαχείρισή του, που μπορούν να επηρεάσουν τα συστήματα αυτά (Καλαμάκι, 2008). Το COBIT βέβαια από τα προαναφερθέντα πλαίσια στη βιβλιογραφία θεωρείται το πιο διαδεδομένο, εφόσον και τα υπερκαλύπτει και μάλιστα στρέφεται συγκεκριμένα στους ελέγχους πληροφοριακών συστημάτων, σε αντίθεση και με το COSO που αναφέρεται σε όλο τον εσωτερικό έλεγχο.

2.4 Πρότυπα προσανατολισμένα στα σημεία ελέγχου

Στο παρόν τμήμα του κεφαλαίου 2, θα παρουσιαστούν τα πρότυπα που σύμφωνα με τον Aceituno, η διαχείριση των διαδικασιών ασφάλειας της πληροφορίας διεξάγεται με την υλοποίηση ελεγκτικών μηχανισμών και σημείων ελέγχου. Σε αυτή τη κατηγορία εντάσσονται τα πρότυπα FISMA και NIST καθώς και το PCI DSS. Κάποιοι ερευνητές όπως ο Aceituno (2006) εντάσσει και το ISO 27002 σε αυτή τη κατηγορία. Παρόλα αυτά το πρότυπο αυτό θεωρούμε ότι ανήκει σε αυτά που φέρουν τις βέλτιστες πρακτικές, εφόσον τα περισσότερα που έχουν δημοσιευθεί κάνουν διαρκώς αναφορά σε αυτό, και έτσι θα παρουσιαστεί σε αυτή τη κατηγορία.

2.4.1 FISMA

Η πράξη FISMA (Federal Information Security Management Act) παρέχει ένα ολοκληρωμένο πλαίσιο για να διασφαλίσει την αποτελεσματικότητα των σημείων ελέγχου για την ασφάλεια των πληροφοριών σε πληροφοριακά συστήματα που υποστηρίζουν δραστηριότητες και άλλα περιουσιακά στοιχεία. Επιβάλλει σε κάθε ομοσπονδιακή υπηρεσία να αναπτύξει, καταγράψει, και να εφαρμόσει καθολικά ένα πρόγραμμα για την ασφάλεια της πληροφορίας και των πληροφοριακών συστημάτων που υποστηρίζουν τις δραστηριότητες και τα περιουσιακά στοιχεία του οργανισμού, συμπεριλαμβανομένων εκείνων που παρέχονται ή διαχειρίζονται από άλλο οργανισμό, πάροχο, είτε άλλη πηγή. Επιπλέον, επιβάλλει ένα σύνολο από απαιτήσεις στο Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας των ΗΠΑ (NIST) για να συνδράμει το τελευταίο έτσι ώστε οι ομοσπονδιακές υπηρεσίες να συμμορφώνονται με τη πράξη FISMA.

Ένα τέτοιο πρόγραμμα πρέπει να περιλαμβάνει περιοδικές αξιολογήσεις του κινδύνου, πολιτικές και διαδικασίες που βασίζονται στην εκτίμηση των κινδύνων και τέλος περιοδικό έλεγχο της αποτελεσματικότητας αυτών των πολιτικών, διαδικασιών, πρακτικών και των σημείων ελέγχου της ασφάλειας των συστημάτων, με συχνότητα ανάλογα με το επίπεδο κινδύνου. Έτσι, για να καλυφθούν και οι ανάγκες αυτές του προτύπου, αναπτύχθηκε το πλαίσιο Διαχείρισης κινδύνου της πράξης FISMA (FISMA Risk Management Framework ή RMF). Η

πράξη αφορά όπως ειπώθηκε, όλους τους ομοσπονδιακούς οργανισμούς και τις ανάγκες τους για την ενίσχυση τις ασφάλειας λόγω των web εφαρμογών τους. Το RMF όμως δεν περιλαμβάνει αναλυτικά μετρικές έτσι ώστε να μπορεί κανείς να αποτιμήσει σε ποιο επίπεδο ασφάλειας έχει φτάσει ένας οργανισμός με βάση τις απαιτήσεις της πράξης FISMA, και είναι ο κυριότερος λόγος που το συγκεκριμένο πρότυπο έχει εισπράξει τις περισσότερες κριτικές. Επίσης, σύμφωνα με μια εκτίμηση της αποτελεσματικότητας που είχε η συγκεκριμένη πράξη στους οργανισμούς που αξιολογήθηκαν και τα διάφορα περιστατικά ασφάλειας στην Αμερική, η αποτελεσματικότητά της κρίθηκε τελικά ανεπιτυχής και δεν έχει τύχει ιδιαίτερης αποδοχής (Conklin, 2008). Τέλος, είναι από τα πρότυπα που έχουν αναπτυχθεί για την ανάπτυξη ενός συστήματος για τη διαχείριση της ασφάλειας σε ομοσπονδιακούς οργανισμούς και δεν μπορεί να εφαρμοστεί για τα ελληνικά δεδομένα.

2.4.2 Εγχειρίδιο Ασφάλειας Πληροφοριών SP800

Το Εγχειρίδιο Ασφάλειας Πληροφοριών 100 (The Information Security Handbook) είναι ένας οδηγός για διαχειριστές πληροφοριακών συστημάτων που παρέχει οδηγίες σε επικεφαλείς διευθυντές της ασφάλειας των πληροφοριών (CIO) σχετικά με διάφορες πτυχές της ασφαλείας των πληροφοριών που θα πρέπει να υλοποιήσουν και να εφαρμόζουν καθώς και να επιβλέπουν στους αντίστοιχους οργανισμούς τους. Το έγγραφο αυτό έχει αναπτυχθεί από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας των ΗΠΑ (NIST) το 2007, στα πλαίσια της πράξης FISMA του 2002. Ο οργανισμός NIST είναι υπεύθυνος για την ανάπτυξη προτύπων και κατευθυντηρίων γραμμών, συμπεριλαμβανομένων των ελάχιστων απαιτήσεων, καθώς και για την παροχή επαρκούς ασφάλειας πληροφοριών για όλες τις λειτουργίες των οργανισμών και τα περιουσιακά τους στοιχεία. Τα εν λόγω πρότυπα και πιο συγκεκριμένα αυτά της σειράς 800, που αφορούν τη κοινότητα της ασφάλειας των πληροφοριακών συστημάτων και οι κατευθυντήριες γραμμές παρόλα αυτά δεν έχουν ισχύ παρά μόνο στους οργανισμούς και τους δημόσιους φορείς των ΗΠΑ.

Το εγχειρίδιο Ασφάλειας Πληροφοριών παρέχει μια ευρεία επισκόπηση των στοιχείων του προγράμματος ασφάλειας των πληροφοριών για να βοηθήσει τους διαχειριστές να κατανοήσουν πώς να θεσπίσουν και να εφαρμόσουν ένα πρόγραμμα ασφάλειας των πληροφοριών που στηρίζεται σε υλοποίηση σημείων ελέγχου.

Οι περιοχές σε αυτό το έγγραφο επιλέχθηκαν με βάση τους νόμους και τους κανονισμούς που σχετίζονται με την ασφάλεια των πληροφοριών, συμπεριλαμβανομένης της Clinger-Cohen Act του 1996, της Ομοσπονδιακής Πράξης Διαχείρισης της Ασφάλειας Πληροφοριών (FISMA) του 2002, και το Ομοσπονδιακό Γραφείο Διαχείρισης και Προϋπολογισμού (OMB). Το υλικό σε αυτό το εγχειρίδιο μπορεί να γίνει αναφορά για γενικές πληροφορίες σε ένα συγκεκριμένο θέμα ή μπορεί να χρησιμοποιηθεί στη διαδικασία λήψης αποφάσεων για την ανάπτυξη ενός προγράμματος ασφάλειας πληροφοριών.

Οι περιοχές που καλύπτει είναι οι ακόλουθες:

- Διακυβέρνηση της Ασφάλειας Πληροφοριών (Information Security Governance)
- Κύκλος Ζωής Ανάπτυξης Συστημάτων (System Development Life Cycle)
- Ενημέρωση και Εκπαίδευση (Awareness and Training)
- Προγραμματισμός και έλεγχος επενδύσεων (Capital Planning and Investment Control)
- Διασύνδεση Συστημάτων και εφαρμογών (Interconnecting Systems)
- Διαχείριση και μέτρηση αποδοτικότητας (Performance Measures)
- Προγραμματισμός και Διαχείριση της Ασφάλειας Πληροφοριών (Security Planning)
- Προγραμματισμός και πρόβλεψη Απρόβλεπτων περιστατικών στη Τεχνολογία (Information Technology Contingency Planning)
- Διαχείριση Επικινδυνότητας (Risk Management)
- Πιστοποίηση και Αξιολόγηση Ασφάλειας (Certification, Accreditation, and Security Assessments)
- Υπηρεσίες Ασφάλειας και υιοθέτηση συστημάτων (Security Services and Products Acquisition)
- Απόκριση σε έκτακτα περιστατικά (Incident Response)
- Συγκρότηση και Διάρθρωση Συστημάτων (Configuration Management)

Οι οδηγίες του παραπάνω προτύπου δεν απευθύνονται ειδικά σε ένα συγκεκριμένο οργανισμό. Οι οργανισμοί θα πρέπει να προσαρμόσουν αυτές τις κατευθυντήριες γραμμές ανάλογα με τη τις απαιτήσεις ασφάλειάς τους και τις επιχειρηματικές τους απαιτήσεις. Είναι συνέχεια της υλοποίησης της πράξης FISMA και αν και είναι ομοσπονδιακό έγγραφο και έχει συνταχθεί σύμφωνα με τα πρότυπα και τις απαιτήσεις των ΗΠΑ, σήμερα χρησιμοποιείται και ως πρότυπο παγκοσμίως σαν οδηγός για την υλοποίηση σημείων ελέγχου στο τομέα της Πληροφορικής και ειδικότερα την ασφάλεια πληροφοριών.

2.4.3 PCI-DSS

Το PCI DSS ή διαφορετικά το Payment Card Industry Data Security Standard είναι ένα πρότυπο που έχει καταρτισθεί από τους οργανισμούς καρτών (VISA, MasterCard, AMEX, Discover/ DINERS, και JCB) και καθορίζει συγκεκριμένες προδιαγραφές ασφαλείας (12 απαιτήσεις) που πρέπει να πληρούν οι μεγάλες επιχειρήσεις, οι οποίες συναλλάσσονται με κάρτες, με στόχο την αποφυγή περιστατικών απάτης και υποκλοπής των σχετικών πληροφοριών που πρέπει να ικανοποιηθούν για τη πιστοποίηση ενός οργανισμού κατά PCI DSS.

Δημιουργήθηκε το Δεκέμβριο του 2004, για να καλύψει την ανάγκη δημιουργίας ενός μόνο προτύπου ηλεκτρονικής ασφαλείας που θα καλύπτει όλες τις ανάγκες για ηλεκτρονικές συναλλαγές από τους διάφορους ιστότοπους που κάνουν χρήση των υπηρεσιών της VISA, της MasterCard, και των άλλων οργανισμών καρτών. Ειδικότερα, το πρότυπο ορίζει τις διαδικασίες με τις οποίες γίνεται ο έλεγχος της ασφάλειας των συστημάτων της επιχείρησης και τις προϋποθέσεις για την απονομή στην επιχείρηση της σχετικής πιστοποίησης.

Οι τράπεζες-μέλη της Ελληνικής Ένωσης Τραπεζών, κρίνοντας επιβεβλημένο να συμβάλουν στην υποχρεωτική εφαρμογή αυτού του τόσο σημαντικού για τον εκσυγχρονισμό της ασφάλειας των επιχειρήσεων προτύπου, έχουν αναθέσει σε εξουσιοδοτημένη από το PCI Council εταιρία, σε συνεργασία με τις επιλεγμένες από τις ίδιες τις τράπεζες-επιχειρήσεις, να προχωρήσουν στην υλοποίησή του (ΕΕΤ, 2009).

Οι δημιουργοί του προτύπου διακρίνουν τους υπόχρεους για την υλοποίηση σε τρεις κατηγορίες, τους εμπόρους (ή Merchants), τους παροχείς υπηρεσιών (ή διαφορετικά τους service providers) και τους εκδότες πιστωτικών καρτών (δηλαδή τις τράπεζες). Πρέπει να σημειωθεί ότι ειδικότερα για τις ηλεκτρονικές εφαρμογές πληρωμών έχει αναπτυχθεί το πρότυπο PA-DSS. Το PA-DSS ισχύει για τους προμηθευτές λογισμικού και άλλους που αναπτύσσουν εφαρμογές πληρωμών που αποθηκεύουν, επεξεργάζονται ή διαβιβάζουν δεδομένα κατόχου της κάρτας.

Πεδίο εφαρμογής

Οι απαιτήσεις ασφαλείας PCI DSS εφαρμόζονται σε όλα τα μέρη του συστήματος. Τα "Μέρη συστήματος» ορίζονται ως εξής: «κάθε συνιστώσα του δικτύου, server, ή εφαρμογή που περιλαμβάνονται σε ή συνδέονται με το περιβάλλον δεδομένων του κατόχου της κάρτας». Συνεπώς, το πεδίο εφαρμογής εξαρτάται κατ' αρχάς από το επίπεδο κατακερματισμού/ διαχωρισμού του δικτύου του εκάστοτε οργανισμού υπό αξιολόγηση (π.χ. όσο πιο «διακριτά» διαχωρισμένο είναι –με firewalls ή άλλη τεχνολογία που να περιορίζει το επίπεδο προσβάσεων- τόσο πιο εύκολα διαχειρίσιμο είναι στο επίπεδο αξιολόγησης και άρα ο έλεγχος περιορίζεται στα κομμάτια που διακινούνται τα ευαίσθητα δεδομένα κατόχων καρτών). Αν υπάρχει ασύρματο δίκτυο στο οποίο διακινούνται τα δεδομένα των κατόχων καρτών, τότε διαδικασίες ελέγχου ειδικά γι' αυτό πρέπει να εφαρμοστούν.

Εμπλεκόμενα μέρη και υπηρεσίες

Τα εμπλεκόμενα μέρη καθώς και οι διαδικασίες παρουσιάζονται και αποτυπώνονται στην παρακάτω εικόνα:

- Οι οργανισμοί πιστωτικών καρτών (VISA, MasterCard κλπ.) καθορίζουν τα πρότυπα και τα ενσωματώνουν σε συμβατικές υποχρεώσεις των εμπορικών επιχειρήσεων. Τα

πρότυπα τώρα συντηρούνται από το PCI Συμβούλιο Προτύπων Ασφάλειας (Security Standards Council).

- Οι Τράπεζες (acquirers) διασφαλίζουν ότι οι εμπορικές επιχειρήσεις συμμορφώνονται όπως επιβάλλουν οι συμβατικές υποχρεώσεις.
- Οι εμπορικές επιχειρήσεις πρέπει να συγκεντρώνουν τεκμήρια συμμόρφωσης (QSA/self-certification / scan reports) και να τα προωθούν στις Τράπεζες.
- Οι Εξουσιοδοτημένοι Εκτιμητές Ασφάλειας ή QSA's (Qualified Security Assessor) και οι Εγκεκριμένοι Προμηθευτές Σαρώσεων ή ASV's (Approved Scanning Vendor) διενεργούν την εξέταση για τις εμπορικές επιχειρήσεις, καθώς και την παροχή συμβουλευτικών υπηρεσιών για τη πιστοποίησής τους.
- Το Συμβούλιο είναι αρμόδιο για την διαχείριση των προτύπων ασφάλειας, ενώ η συμμόρφωση με το σύνολο των προτύπων PCI επιβάλλεται από τα ιδρυτικά μέλη του Συμβουλίου (American Express, Discover Financial Services, JCB, MasterCard Worldwide και Visa Inc).

PCI-DSS: εμπλεκόμενα μέρη καθώς και οι διαδικασίες, Πηγή: EET

Απαιτήσεις του PCI DSS

Το PCI DSS αποτελείται από 12 απαιτήσεις που πρέπει να ικανοποιηθούν για να θεωρηθεί πως κάποιος είναι συμβατός με αυτό. Μια πολύ περιληπτική παρουσίασή τους ακολουθεί.

Απαίτηση 1: Εγκατάσταση και συντήρηση ενός firewall για την προστασία των στοιχείων των κατόχων κάρτας.

Απαίτηση 2: Μη χρήση των προεπιλεγμένων κωδικών των κατασκευαστών.

Απαίτηση 3: Προστασία των αποθηκευμένων δεδομένων των κατόχων κάρτας.

Απαίτηση 4: Κρυπτογράφηση της διαβίβασης στοιχείων κατόχων κάρτας στα ανοικτά, δημόσια δίκτυα.

Απαίτηση 5: Χρήση και συχνή αναβάθμιση αντιϊκών λογισμικών.

Απαίτηση 6: Συντήρηση και ανάπτυξη των ασφαλών συστημάτων και των εφαρμογών.

Απαίτηση 7: Περιορισμός της πρόσβασης στα στοιχεία κατόχων κάρτας από επιχειρησιακό need-to-know.

Απαίτηση 8: Ορισμός μιας μοναδικής ταυτότητας σε κάθε πρόσωπο με πρόσβαση σε υπολογιστή.

Απαίτηση 9: Περιορισμός της φυσικής πρόσβασης στα στοιχεία κατόχων κάρτας.

Απαίτηση 10: Έλεγχος και παρακολούθηση όλων των προσβάσεων στους πόρους δικτύου και στα στοιχεία των κατόχων κάρτας.

Απαίτηση 11: Τακτικές δοκιμές στα συστήματα ασφαλείας και στις διαδικασίες.

Απαίτηση 12: Διατήρηση μιας πολιτικής που εξετάζει την ασφάλεια πληροφοριών των υπαλλήλων και των αναδόχων.

Το PCI DSS είναι το επικρατέστερο αν όχι το μοναδικό πρότυπο ασφάλειας πληροφορικής που είναι σε τέτοιο βαθμό διαδεδομένο. Μακροπρόθεσμα ενδέχεται το πλήθος τον υλοποιήσεων να αυξηθεί και το πλήθος των συναλλαγών που απαιτείται για να πρέπει να είσαι συμβατός με PCI DSS να μειωθεί, μιας και η υποδομή θα υπάρχει. Ο σημαντικότερος λόγος για να επιδιώξει κάποιος ιδιοκτήτης μιας μέσου ή μικρού μεγέθους εταιρίας συμβατότητα με το PCI DSS είναι κυρίως οι αγορές μέσο διαδικτύου (πχ τα λεγόμενα e-shops). Πρότυπα όπως το BS7799 ή το ISO27001 και ISO27002 είναι πολύ καλά στο να δώσουν μια καλή αντίληψη του τι σημαίνει καλές πρακτικές ασφάλειας (good security practices), αν και δεν είναι τόσο λεπτομερή όσο το PCI DSS. Δυστυχώς όμως η ελληνική αγορά είναι πολύ ανώριμη να συμβαδίσει ακόμα και με αυτά τα πρότυπα και θα υπάρξουν πολλές προχειρότητες και κακές υλοποιήσεις μέχρι να αποκτηθεί η κατάλληλη ωριμότητα (Κασσάρας, 2008). Όσον αφορά στο τραπεζικό κλάδο και στα πλαίσια της παρούσας εργασίας το πρότυπο PCI DSS μπορεί να χρησιμοποιηθεί σαν σημείο αναφοράς, αλλά δεν λαμβάνει υπόψη πτυχές όπως συνέπειες και επιπτώσεις σε επιχειρησιακό επίπεδο και ανάλυση επικινδυνότητας. Είναι συγκεκριμένο και ένας οργανισμός μπορεί να πιστοποιηθεί με αυτό σε επόμενο στάδιο, ενώ είναι στην πορεία να ικανοποιεί τις απαιτήσεις άλλων προτύπων όπως ISO27001/ISO27002, αλλά είναι πολύ πιο αυστηρό και εύκολο στην εκτίμηση της μεχρι τώρα κατάστασης ασφάλειας ενός οργανισμού.

2.5 Πρότυπα προσανατολισμένα σε τεχνολογικά προϊόντα

Σε αυτή τη κατηγορία θα ενταχθούν εκείνα τα πρότυπα που αφορούν την αποτίμηση και αξιολόγηση σε συγκεκριμένα τεχνολογικά προϊόντα. Για παράδειγμα το ANSI/ISA 99.02.01 αφορά μόνο βιομηχανικά συστήματα και παρατίθεται αμέσως στην επόμενη παράγραφο, ενώ το Common Criteria χρησιμοποιείται ως πρότυπο για αξιολόγηση σε λογισμικό ή firmware.

2.5.1 ANSI/ISA 99.02.01

Το ANSI/ISA 99.02.01 συγκαταλέγεται στα πρότυπα ασφαλείας στο κυβερνοχώρο, τα οποία επιτρέπουν στους οργανισμούς να εφαρμόσουν επαρκείς πρακτικές και τεχνικές ασφάλειας για να ελαχιστοποιηθεί ο αριθμός των επιτυχημένων επιθέσεων στον κυβερνοχώρο. Εκδόθηκε από τον διεθνή οργανισμό International Society for Automation – ISA.

Το πρότυπο ANSI/ISA 99.02.01 αποτελεί μέρος σειράς προτύπων που ασχολούνται με το θέμα της ασφάλειας για βιομηχανικά συστήματα αυτοματισμού και ελέγχου. Έχει αναπτυχθεί από την 2η Ομάδα Εργασίας της επιτροπής ISA99 και περιγράφει στοιχεία που περιέχονται στο σύστημα διαχείρισης της ασφάλειας στον κυβερνοχώρο για χρήση στα συστήματα αυτοματισμού στη βιομηχανία και στο περιβάλλον ελέγχου αυτών και παρέχει καθοδήγηση για την εκπλήρωση των απαιτήσεων που περιγράφονται για κάθε στοιχείο. Από τις τέσσερις κατηγορίες που οργανώθηκαν τα πρότυπα ISA99 (έννοιες και ορολογία, ιδιοκτήτης συστήματος, σχεδιασμός προϊόντων ελέγχου και τέλος απαιτήσεις στη διαδικασία ανάπτυξης προϊόντων ελέγχου) ανάλογα με το τι καθένα από αυτά αφορά, το ANSI/ISA 99.02.01 απευθύνεται στον ιδιοκτήτη του συστήματος υπό έλεγχο και στις πρακτικές που πρέπει να ακολουθήσει για να δημιουργήσει και να εφαρμόσει ένα τέτοιο πρόγραμμα ασφάλειας.

Το συγκεκριμένο πρότυπο έχει αναπτυχθεί σε μεγάλο βαθμό από προηγούμενη τεχνική έκθεση της ISA99 επιτροπής, ANSI/ISA-TR99.00.02-2004, που έχει να κάνει με την ενσωμάτωση της ασφάλειας στη βιομηχανία και στο περιβάλλον ελέγχου των συστημάτων. Το μεγαλύτερο

μέρος του περιεχομένου αυτής της τεχνικής έκθεσης έχει συμπεριληφθεί σε αυτό το πρότυπο και ως εκ τούτου το πρότυπο αυτό αντικαθιστά τη προαναφερθείσα τεχνική έκθεση. Συμπερασματικά το πρότυπο αυτό αφορά συγκεκριμένο τομέα και δεν μπορεί να χρησιμοποιειθεί για όλο το εύρος των αυτοματοποιημένων συστημάτων και σε όλους τους επιχειρησιακούς κλάδους, παρά μόνο στη βιομηχανία. Περιγράφει τα στοιχεία που περιέχονται σε ένα σύστημα διαχείρισης της ασφάλειας στον κυβερνοχώρο και άρα λοιπόν θα λέγαμε οτι οι οδηγίες που παρέχονται αφορούν συγκεκριμένο σύστημα ελέγχου/ προϊόν.

2.5.2 Common Criteria

Το πρότυπο Common Criteria για την αξιολόγηση της Ασφάλειας των Πληροφοριακών Συστημάτων (CC)3 και η αντίστοιχη μεθοδολογία (CEM) χρησιμοποιούνται ως πρότυπα κριτήρια αξιολόγησης και μεθοδολογία για όλες τις αξιολογήσεις της ασφάλειας των προϊόντων πληροφορικής είτε αυτά εφαρμοστούν σε υλικό ή σε λογισμικό ή firmware. Τα Common Criteria είναι διεθνές πρότυπο (ISO / IEC 15408) και έχει λάβει παγκόσμια αποδοχή. Είναι ένα πολύ σημαντικό πλαίσιο για την αξιολόγηση των προϊόντων πληροφορικής και συστημάτων σε σχέση με τους μηχανισμούς ασφαλείας τους.

Το πρότυπο **Common Criteria** (CC) επιτρέπει τη συγκρισιμότητα μεταξύ των αποτελεσμάτων ανεξάρτητων αξιολογήσεων επι της ασφλαλειας ενός πληροφοριακού συστήματος ή/ και περιβάλλον πληροφοριακών συστημάτων. Αυτό επιτυγχάνεται παρέχοντας ένα κοινό σύνολο απαιτήσεων για τη λειτουργικότητα της ασφάλειας των προϊόντων πληροφορικής και για τα μέτρα διασφάλισης που εφαρμόζονται σε αυτά τα προϊόντα πληροφορικής κατά τη διάρκεια της αξιολόγησης. Αυτά τα προϊόντα πληροφορικής μπορεί να εφαρμόζονται σε hardware, firmware ή/και λογισμικό.

Η διαδικασία αξιολόγησης εξασφαλίζει την ασφαλή λειτουργία αυτών των προϊόντων πληροφορικής και οτι τα μέτρα που εφαρμόζονται ανταποκρίνονται στις απαιτήσεις αυτές. Τα αποτελέσματα της αξιολόγησης βοηθούν τον εκάστοτε αναλυτή να προσδιορίσει εάν τα προϊόντα πληροφορικής θα εκπληρώσουν τις ανάγκες ασφαλείας του οργανισμού.

Ουσιαστικά, το CC πρότυπο αποτελεί έναν οδηγό για την ανάπτυξη, την αξιολόγηση και / ή τη προμήθεια προϊόντων πληροφορικής με ασφαλή λειτουργία. Εξετάζει τη προστασία των περιουσιακών στοιχείων από μη εξουσιοδοτημένη χρήση, τροποποίηση, ή απώλεια. Οι κατηγορίες προστασίας σχετικά με τους τρείς εν λόγω τύπους αποτυχίας της ασφάλειας είναι οι ευρέως γνωστές στο κόσμο της ασφάλειας των πληροφοριών ως εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα της πληροφορίας, αντίστοιχα και μπορεί να εφαρμοστεί και σε άλλες πτυχές της ασφάλειας εκτός των τριών αυτών. Είναι εφαρμόσιμο στην αξιολόγηση του κινδύνου που προκύπτει από ανθρώπινες δραστηριότητες (ή μη) και σε κινδύνους προερχόμενους από μη-ανθρώπινες δραστηριότητες. Εκτός από την ασφάλεια στην πληροφορία και τη τεχνολογία το CC πρότυπο, μπορεί να εφαρμοστεί και σε άλλους τομείς της πληροφορικής, αλλά δεν γίνεται αναφορά από το ίδιο το πρότυπο σε αυτούς τους τομείς.

Το συγκεκριμένο πρότυπο δεν ασχολείται με τη μεθοδολογία αξιολόγησης βάσει της οποίας τα κριτήρια πρέπει να εφαρμόζονται. Η μεθοδολογία αυτή δίνεται στο CEM. Επίσης, δεν εξετάζει το διοικητικό και νομικό πλαίσιο σύμφωνα με το οποίο τα κριτήρια μπορούν να εφαρμοστούν από τις αρχές αξιολόγησης. Με άλλα λόγια, το πρότυπο παρέχει πιστοποίηση στο ότι η διαδικασία των προδιαγραφών, της εφαρμογής και της αξιολόγησης ενός προϊόντος ασφάλειας έχει διεξαχθεί με ένα αυστηρό και τυποποιημένο τρόπο. Είναι ένα πολύ γενικό πρότυπο και δεν απαρρυθμεί άμεσα τις απαιτήσεις ασφάλειας του προϊόντος ή τα χαρακτηριστικά για συγκεκριμένες (κατηγορίες) προϊόντων.

Αν ένα προϊόν πιστοποιηθεί κατά το πρότυπο αυτό, δεν σημαίνει απαραίτητα ότι είναι απολύτως ασφαλές. Για παράδειγμα, οι διάφορες εκδόσεις των Microsoft Windows, συμπεριλαμβανομένων των Windows Server 2003 και Windows XP, έχουν

[3] The Common Criteria for IT Security Evaluation (CC): http://www.commoncriteriaportal.org/thecc.html

πιστοποιηθεί κατά EAL4 + (έκδοση των Common Criteria), αλλά εξακολουθεί να εκδίδεται από τη Microsoft κώδικας ασφαλείας (patches) για τα τρωτά σημεία της ασφάλειας αυτών. Η πιστοποίηση EAL4 + των εκόσεων των Microsoft Windows παραμένει χωρίς να περιλαμβάνεται η εφαρμογή οποιουδήποτε Microsoft patch στην αξιολογηθείσα διάρθρωσή αυτών (configuration). Αυτό δείχνει τόσο τον περιορισμό όσο και τις δυνατότητες μιας τέτοιας αξιολόγησης.

2.6 Πρότυπα βέλτιστων πρακτικών

Τα πρότυπα που παρατίθενται σε αυτή τη παράγραφο έχουν παραχθεί με βάση τα πρότυπα και βέλτιστες πρακτικές που ακολουθούνται σε παγκόσμιο επίπεδο από διάφορους οργανισμούς κυβερνητικούς και μη. Το ISO 27001 αν και θεωρήθηκε ότι είναι από τα πρότυπα που επικεντρώνονται στα σημεία ελέγχου (Aceituno, 2006), είναι ευρέως διαδεδομένο σαν η βέλτιστη πρακτική για την υλοποίηση ενός συστήματος διαχείρισης της ασφάλειας (ISMS).

2.6.1 BS ISO/IEC 20000-1

Το πρότυπο BS ISO / IEC 20000-1 περιγράφει ένα ολοκληρωμένο σύνολο διαδικασιών διαχείρισης οι οποίες ορίζονται ως οι απαιτήσεις για την αποτελεσματική παροχή υπηρεσιών σε μια επιχείρηση και τους πελάτες της είτε από το ίδιο το τμήμα πληροφορικής είτε από ένα τρίτο πάροχο αντίστοιχων υπηρεσιών. Αυτό το πρότυπο θεωρείται όλο και περισσότερο ως το πρότυπο για την πιστοποίηση ποιότητας στη διαχείριση υπηρεσιών της Πληροφορικής (IT Service Management). Είναι το πρότυπο που προάγει την υιοθέτηση μιας προσέγγισης ολοκληρωμένων διαδικασιών για την αποτελεσματική παροχή διαχείρισης των υπηρεσιών έτσι ώστε να πληρωθούν οι απαιτήσεις των επιχειρήσεων και των πελατών.

Αποτελείται από 10 τμήματα:

- Σκοπός και πλαίσιο
- Όροι και Επεξηγήσεις
- Οργανώνοντας και υλοποιώντας την Διαχείριση των Υπηρεσιών
- Απαιτήσεις για ένα σύστημα διαχείρισης
- Οργάνωση και υλοποίηση νέων υπηρεσιών
- Διαδικασίες για παράδοση υπηρεσιών
- Διαδικασίες ανάπτυξης σχέσεων
- Διαδικασίες ελέγχου
- Διαδικασίες Επίλυσης
- Διαδικασίες Αποδέσμευσης

Η BS ISO / IEC 20000 σειρά προτύπων διακρίνει μεταξύ των βέλτιστων πρακτικών στις διαδικασίες οι οποίες είναι ανεξάρτητες από οργανωτικής μορφής ή μεγέθους και οργανωτικών δομών. Το πρότυπο όμως παραμένει στην υλοποίηση σημείων ελέγχου στις υπηρεσίες της πληροφορικής (IT Service Management) όπως και το ITIL και λόγω αυτού συνήθως χρησιμοποιείται σε συνδυασμό με ένα ή περισσότερα άλλα πρότυπα βέλτιστων πρακτικών για τη διαχείριση και ασφάλεια της τεχνολογίας των πληροφοριών.

2.6.2 CIS Benchmarks

Το CIS είναι το Κέντρο για την Ασφάλεια του Διαδικτύου, ένας μη κερδοσκοπικός οργανισμός του οποίου η αποστολή είναι να βοηθήσει τους οργανισμούς στη μείωση του επιχειρησιακού κινδύνου και των κινδύνων που συνδέονται με το ηλεκτρονικό εμπόριο και απορρέουν από διαταραχές εξαιτίας ανεπαρκών τεχνικών ελέγχων ασφαλείας. Τα κριτήρια αναφοράς CIS είναι οι μοναδικές βέλτιστες πρακτικές ασφαλείας (configuration) βασισμένες στη συναίνεση, που αναπτύχθηκαν και είναι αποδεκτές από κυβερνήσεις, επιχειρήσεις, τη βιομηχανία, και την ακαδημαϊκή κοινότητα.

Αυτά τα σημεία αναφοράς αναπτύχθηκαν με συναίνεση, σε μεγάλο βαθμό με τη βοήθεια της κοινότητας των χρηστών και στηρίζονται σε αναγνωρισμένες βέλτιστες πρακτικές για την

ανάπτυξη, διαμόρφωση, διάρθρωση και λειτουργία των δικτυωμένων συστημάτων. Καλύπτουν το τρίπτυχο των επιθέσεων στο διαδίκτυο: επίπεδο τεχνολογίας(λογισμικό και hardware), (λογισμικό και hardware), επίπεδο διαδικασιών (διαχείριση δικτύου και συστημάτων) και αυτό του ανθρώπινου παράγοντα (τελικού χρήστη και τη στάση της διοίκησης). Τα κριτήρια αξιολόγησης είναι διαθέσιμα στο κοινό χωρίς χρέωση. Επίσης το Κέντρο για την ασφάλεια του Διαδικτύου παρέχει και αντίστοιχα λογισμικά με ενσωματωμένα αυτά τα κριτήρια αναφοράς που τρέχουν στα εκάστοτε συστήματα και παρέχουν άμεσα αναφορές για τη κατάσταση της ασφάλειας σε αρκετά λεπτομερές επίπεδο.

Συμπερασματικά, τα κριτήρια και τα λεγόμενα σημεία αναφοράς (benchmarks) έχουν να κάνουν με συγκεκριμένη παραμετροποίηση σε servers και λογισμικά ούτως ώστε αυτά να είναι ασφαλή από τυχόν επιθέσεις προερχόμενες από το διαδίκτυο. Το συγκεκριμένο πρότυπο παρέχει συνεπώς οδηγίες σε πολύ χαμηλό επίπεδο (παραμετροποίηση) συστημάτων ως προς την ασφάλεια και δεν μπορεί να χρησιμοποιηθεί για γενικότερη καθοδήγηση ενός οργανισμού αναφορικά με την ανάπτυξη διαδικασιών ελέγχου και αξιολόγησης ασφάλειας στη Διακυβέρνηση της πληροφορικής.

2.6.3 The Standard of Good Practice (ISF 2011)

Το Forum Ασφάλειας Πληροφοριών (Information Security Forum) ιδρύθηκε το 1989 και είναι ένας ανεξάρτητος, μη κερδοσκοπικός οργανισμός με μέλη που προέρχονται από σημαντικούς οργανισμούς στον κόσμο. Στοχεύει στην έρευνα, την αποσαφήνιση και την επίλυση βασικών θεμάτων στον τομέα της ασφάλειας των πληροφοριών και τη διαχείριση των κινδύνων, με την ανάπτυξη μεθοδολογιών βάσει βέλτιστων πρακτικών, διαδικασιών και λύσεων που ανταποκρίνονται στις επιχειρηματικές ανάγκες των μελών του. Ο ISF έχει αναπτύξει ένα μοντέλο που δείχνει πώς πρέπει να αντιμετωπίζονται τα θεμελιώδη στοιχεία ενός προγράμματος για την ασφάλεια πληροφοριών. Παρέχει εκπαίδευση στα μέλη του, πρότυπα βέλτιστων πρακτικών και εργαλεία τα οποία αγγίζουν κάθε πτυχή του μοντέλου αυτού για να ενισχύσουν τον εκάστοτε οργανισμό στην αντιμετώπιση θεμάτων που έχουν να κάνουν με το περιβάλλον κινδύνου του.

Στα πλαίσια των διεθνών προτύπων, πολλά από τα οποία έχουν προαναφερθεί, και τις ανάγκες των οργανισμών για πιστοποίηση στα πλαίσια της ασφάλειας της πληροφορίας, ο ISF εξέδωσε το δικό του πρότυπο ISF Standard of Good Practice. Σήμερα είναι στην έκδοση 2011 με ένα αρκετά ολοκληρωμένο και περιεκτικό οδηγό που στοχεύει στην οργάνωση του τομέα της Τεχνολογίας και της Πληροφορικής ενός οργανισμού και τον επαρκή έλεγχο αυτού. Περιέχει αναλυτική καθοδήγηση και μεθοδολογίες που ξεκινούν από την ανάλυση της επικινδυνότητας από επιχειρησιακής πλευράς, με μεθοδολογίες ανάλυσης και αξιολόγησης των κινδύνων, των απειλών και των αδυναμιών αντίστοιχα στο τεχνολογικό περιβάλλον, καθώς επίσης και μια εκτενής σειρά από σημεία ελέγχου που κάθε οργανισμός επιλέγει να υλοποιήσει ανάλογα με την ανοχή σε επίπεδα κινδύνου. Το πρότυπο περιλαμβάνει πέντε οπτικές κάθε μια από τις οποίες καλύπτει ένα συγκεκριμένο τύπο αξιολόγησης:

- Διαχείριση της Ασφάλειας
- Κρίσιμες επιχειρηματικές εφαρμογές
- Πληροφοριακή υποδομή
- Δίκτυα
- Ανάπτυξη Συστημάτων

Το Πρότυπο του 2011 είναι ο πυρήνας όλων αυτών που παρέχει ο ISF στα μέλη του, και αποτελεί το πυρήνα των εργαλείων και τεχνικών της. Το πρότυπο του 2011 είναι στενά συνδεδεμένο με την Μεθοδολογία Ανάλυσης Επικινδυνότητας των Πληροφοριών του ISF, το λεγόμενο IRAM (Information Risk Analysis Methodology) το οποίο είναι και ένα από τα εργαλεία που υλοποιεί το πρότυπο αυτό. Καλύπτει πλήρως το φάσμα των διατάξεων ασφαλείας που πρέπει να γίνουν για να κρατήσει ένας οργανισμός τους επιχειρηματικούς κινδύνους που σχετίζονται με τα συστήματα πληροφοριών εντός των αποδεκτών ορίων, και παρουσιάζει αρκετά καλές πρακτικές για την πρακτική τους εφαρμογή, με σαφείς προτάσεις. Δεν στοχεύει ωστόσο μόνο στη βελτίωση της ποιότητας και της αποτελεσματικότητας των διατάξεων της ασφάλειας των πληροφοριών που εφαρμόζονται από έναν οργανισμό, αλλά λειτουργεί

επίσης ως ένα ισχυρό υπόβαθρο προς τη συμμόρφωση της ασφάλειας των πληροφοριών με άλλα διεθνώς αναγνωρισμένα και καθιερωμένα πρότυπα.

Δεδομένου ότι το Πρότυπο του 2011 αντιστοιχίζεται πλήρως με το περιεχόμενο του ISO 27001, ISO 27002, ISO 27005 και την έκδοση 4 του COBIT, χρησιμοποιώντας αυτό σαν μέσο για συμμόρφωση με τα προαναφερθέντα πρότυπα μπορεί να μειώσει σημαντικά την πολυπλοκότητα και τις δαπανηρές δραστηριότητες στη προσπάθεια ενός οργανισμού για πιστοποίηση. Περαιτέρω, καθώς το πρότυπο του 2011 είναι εναρμονισμένο με άλλες ρυθμιστικές απαιτήσεις και οδηγίες, όπως το Payment Card Industry Data Security Standard (PCI-DSS), το Sarbanes-Oxley (SOX), τη Βασιλεία III και το Cloud Security Alliance (CSA), μπορεί να συμβάλει σημαντικά στην εναρμόνιση των δραστηριοτήτων προς τη συμμόρφωση όσον αφορά το περιβάλλον ασφάλειας της πληροφορίας και σε όλους τους άλλους τομείς.

2.6.4 Σειρά Προτύπων ISO 27000

Αναπτύχθηκε από την κοινοπραξία μεταξύ δυο επιτροπών (ISO και IEC), στο εξής ISO/IEC JTC 1, *Information technology*, Υποεπιτροπή SC 27, *IT Security techniques*. Η τελευταία αποτελείται από μια επιτροπή που επικεντρώνεται στην ανάπτυξη διεθνών προτύπων για τη διαχείριση συστημάτων με σκοπό την ασφάλεια των πληροφοριών, γνωστά ως Information Security Management System (ISMS) family of standards. Με τη χρήση της σειράς προτύπων ISMS οι επιχειρήσεις και οι οργανισμοί μπορούν να αναπτύξουν και να υλοποιήσουν ένα πλαίσιο για τη διαχείριση της ασφάλειας των πληροφοριακών τους συστημάτων και έπειτα να αξιολογήσουν ανεξάρτητα την αποτελεσματικότητα με την εφαρμογή αυτών στην ασφάλεια των πληροφοριών τους (οικονομικά στοιχεία, πνευματική ιδιοκτησία, στοιχεία πελατών και γενικά δεδομένα που τρίτοι –πελάτες, προμηθευτές, εξωτερικοί συνεργάτες, μέτοχοι- έχουν εμπιστευτεί στον οργανισμό).

Η οικογένεια προτύπων ISMS αποτελείται από τα παρακάτω διεθνή πρότυπα υπό το γενικό τίτλο Τεχνικές Ασφάλειας των τεχνολογιών και πληροφοριών (IT Security Techniques):

ISO/IEC 27000:2009 Ορολογία και γενικότερο πλαίσιο για τα υπόλοιπα πρότυπα της σειράς 27000 (Information security management systems — Overview and vocabulary).

ISO/IEC 27001:2005 Απαιτήσεις ασφάλειας για συστήματα διαχείρισης της ασφάλειας (Information security management systems — Requirements).

ISO/IEC 27002:2005 Μετονομασία του ISO 17799: Παράθεση μιας σειράς από πιθανά σημεία ελέγχου και πρακτικές που μπορούν να εφαρμοστούν με βάση το ISO 27001. Ουσιαστικά είναι ο κώδικας πρακτικής για τη διαχείριση της ασφάλειας των πληροφοριών (Code of practice for information security management.

ISO/IEC 27003 Οδηγός Υλοποίησης συστήματος διαχείρισης ασφάλειας (Information security management system implementation guidance).

ISO/IEC 27004 Μέτρηση/ Αξιολόγηση του συστήματος διαχείρισης Ασφάλειας (Information security management — Measurement).

ISO/IEC 27005:2008 Οδηγός για την Εκτίμηση και Διαχείριση Επικινδυνότητας (Information security risk management).

ISO/IEC 27006:2007 Απαιτήσεις για τους σελεγκτικούς οργανισμούς που παρέχουν πιστοποίηση (Requirements for bodies providing audit and certification of information security management systems).

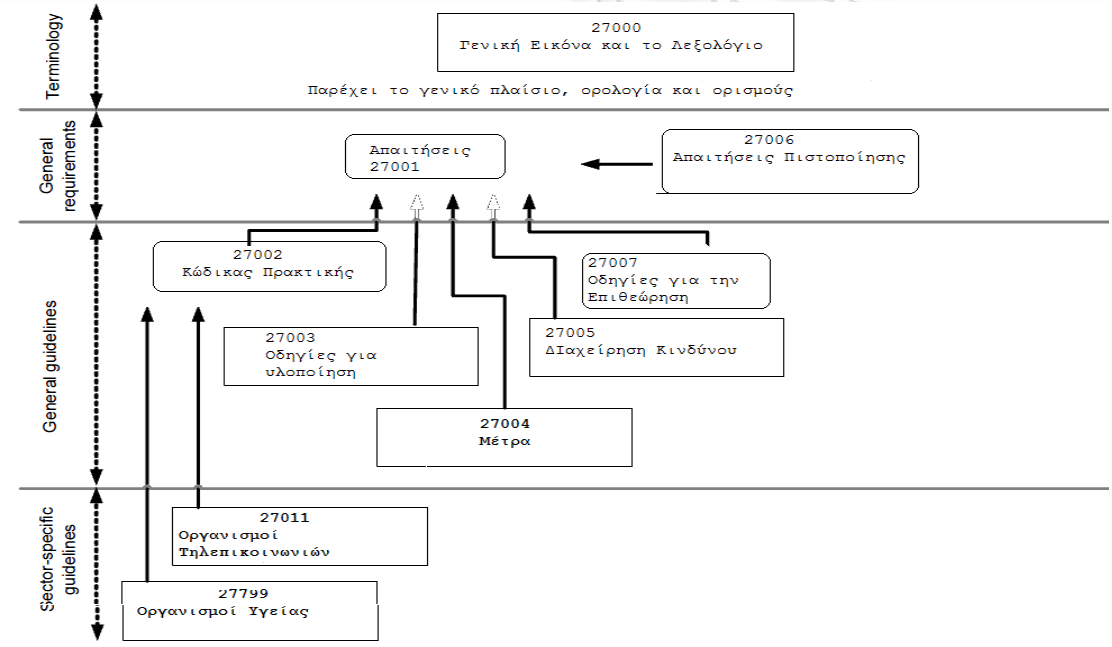
ISO/IEC 27007 Οδηγός για τη διεξαγωγή ελέγχου πληροφοριακών συστημάτων (Guidelines for information security management systems auditing)

ISO/IEC 27011 Οδηγός για τη διαχείριση ασφάλειας σε τηλεπικοινωνιακούς οργανισμούς - βασισμένο στο πρότυπο: ISO/IEC 27002 (Information security management guidelines for telecommunications organizations based).

Συγκεκριμένα, τα πρότυπα που μπορούν να βοηθήσουν στη παρούσα εργασία ώστε να ερευνήσουμε την εφαρμοστικότητα τους στο τραπεζικό οργανισμό είναι τα ISO/IEC 27001 και

ISO/IEC 27002. Το ISO/IEC 27001 είναι διεθνές πρότυπο που προσδιορίζει τις απαιτήσεις που πρέπει να πληροί ένας οργανισμός προκειμένου να διαχειριστεί συνολικά και αποτελεσματικά την ασφάλεια της πληροφορίας του. Σε οργανωτικό επίπεδο είναι συνυφασμένο με την έννοια της ασφάλειας της πληροφορίας και περιέχει τις απαιτήσεις για τη δημιουργία, εφαρμογή και βελτίωση ενός συστήματος διαχείρισης ασφάλειας πληροφοριών. Τέλος, είναι πιστοποιήσιμο και σε αυτό περιγράφονται οι απαιτήσεις που πρέπει να πληροί ένας οργανισμός προκειμένου να διαχειριστεί συνολικά και αποτελεσματικά την ασφάλεια της πληροφορίας του.

Το πρότυπο ISO 27002 από την άλλη πλευρά, παρέχει τις κατευθυντήριες οδηγίες για την κάλυψη του προτύπου. Αυτό το Διεθνές Πρότυπο θεσπίζει γενικές αρχές για την προετοιμασία, την εφαρμογή, τη διατήρηση και τη βελτίωση της διαχείρισης της ασφάλειας των πληροφοριών σε έναν οργανισμό. Οι στόχοι που περιγράφονται σε αυτό το Διεθνές Πρότυπο παρέχουν γενική καθοδήγηση σχετικά με τους κοινά αποδεκτούς στόχους της διαχείρισης της ασφάλειας των πληροφοριών. Μπορεί να χρησιμεύσει ως πρακτικός οδηγός για την ανάπτυξη οργανωτικών προτύπων ασφάλειας και αποτελεσματικών πρακτικών διαχείρισης ασφάλειας και να βοηθήσει στη δημιουργία εμπιστοσύνης στις δραστηριότητες εντός του οργανισμού. Οι στόχοι των ελέγχων και οι έλεγχοι αυτού του Διεθνούς Προτύπου προορίζονται να εφαρμοστούν έτσι ώστε να εκπληρωθούν οι απαιτήσεις που έχουν αναγνωριστεί, μέσω όμως μιας αξιολόγησης κινδύνου. Στο σημείο αυτό πρέπει να αναλυθεί περισσότερο το ISO/IEC 27001:2005 που σχετίζεται άμεσα με τις απαιτήσεις του προτύπου και βέλτιστες πρακτικές ασφάλειας.



Σχέσεις μεταξύ των προτύπων της Οικογένειας ISO 27000, Πηγή: ISO 27000

ISO/IEC 27001:2005

Το πρότυπο αυτό ορίζει τη διαδικασία προσέγγισης και μεταγωγής στην εφαρμογή ενός συνόλου διαδικασιών καθώς και τη μεταξύ τους αλληλεπίδραση. Στηρίζεται στην εφαρμογή του μοντέλου Plan-Do-Check-Act για τη δομή των διαδικασιών και είναι το πιο διαδεδομένο πρότυπο ασφαλείας πληροφοριακών συστημάτων. Βασική φιλοσοφία του προτύπου αποτελεί η μεθοδολογία γνωστή ως «Σχεδιάζω – Εκτελώ – Ελέγχω – Ενεργώ» - «Plan – Do – Check – Act» (ΣΕΕΕ – PDCA) που μπορεί να εφαρμοστεί σε όλες τις διεργασίες. Η ΣΕΕΕ μπορεί εν συντομία να περιγραφεί ως ακολούθως:

Σχεδιάζω: καθιερώνω τους αντικειμενικούς σκοπούς και τις διεργασίες που είναι απαραίτητες για να παραχθούν αποτελέσματα σε συμφωνία με τις απαιτήσεις των πελατών και τις πολιτικές του οργανισμού.

Εκτελώ: θέτω σε εφαρμογή τις διεργασίες

Ελέγχω: παρακολουθώ και μετρώ τις διεργασίες και το προϊόν ως προς τις πολιτικές, τους αντικειμενικούς σκοπούς και τις απαιτήσεις για το προϊόν και εκθέτω τα αποτελέσματα.

Ενεργώ: αναλαμβάνω δράσεις για τη διαρκή βελτίωση της επίδοσης των διεργασιών

Ειδικότερα το πρότυπο αυτό διακρίνει την ασφάλεια σε δέκα βασικούς τομείς για καθένα από τους οποίους δίδονται συγκεκριμένες προδιαγραφές ασφαλείας. Όσο πιο κοντά είναι μια επιχείρηση ή οργανισμός στις προδιαγραφές αυτές τόσο πιο ασφαλής είναι (Πενταφρόνημος, 2009). Το πρότυπο αυτό δίνει ουσιαστικά το γενικότερο πλαίσιο για την εφαρμογή επιμέρους πολιτικών ασφαλείας σε συγκεκριμένους τομείς που συνθέτουν το περιβάλλον των Πληροφοριακών Συστημάτων και προδιαγράφει σε υψηλό επίπεδο τους σκοπούς και τους βασικούς στόχους που πρέπει να τίθενται.

Καθορίζει τις απαιτήσεις για το σύστημα Διαχείρισης της Ασφάλειας των πληροφοριών, με σκοπό την εξασφάλιση ότι η επιχείρηση έχει καθορίσει και εφαρμόζει επαρκείς και κατάλληλους ελέγχους που σχετίζονται με την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα της πληροφορίας ώστε να προστατεύονται επαρκώς οι πληροφορίες και τα δεδομένα των «ενδιαφερόμενων μερών». Έχει εφαρμογή σε όλους τους τομείς της βιομηχανίας, εμπορίου και υπηρεσιών και η εφαρμογή του δεν περιορίζεται μόνο στις πληροφορίες που αποθηκεύονται σε Η/Υ. Απευθύνεται στην ασφάλεια των πληροφοριών με όποιον τρόπο και αν αυτές τηρούνται. Οι πληροφορίες μπορεί να είναι καταγεγραμμένες ή εκτυπωμένες σε χαρτί, μπορεί να είναι αποθηκευμένες ηλεκτρονικά, μπορεί να αποστέλλονται με κανονικό ή με ηλεκτρονικό ταχυδρομείο, μπορεί να παρουσιάζονται σε φιλμ ή να διατυπώνονται προφορικά σε συζητήσεις. Οποιαδήποτε μορφή και εάν έχουν οι πληροφορίες, με οποιοδήποτε τρόπο και αν αυτές διαμοιράζονται ή αποθηκεύονται, το ISO 27001 βοηθάει έναν οργανισμό να τις προστατεύει επαρκώς.

Έχει εφαρμογή σε επιχειρήσεις οποιουδήποτε επιχειρηματικού κλάδου όπου η εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα πληροφοριών και δεδομένων είναι ιδιαίτερα σημαντική και κρίσιμη για την λειτουργία και επιβίωσή του. Στην παρακάτω εικόνα βλέπουμε τη διαδικασία πιστοποίησης. Οι απαιτήσεις ασφαλείας του ISO 27001 εφαρμόζονται σε όλα τα μέρη ενός οργανισμού. Αυτά περιλαμβάνουν τα εξής: το πληροφοριακό σύστημα (server, δικτυακός εξοπλισμός, υπολογιστές δικτύου, λογισμικό, ανθρώπινο δυναμικό κ.α.), τις εγκαταστάσεις (κτίριο) και τη συμμόρφωση με το νομικό πλαίσιο. Συνεπώς, το πεδίο εφαρμογής εξαρτάται καταρχάς από τον εκάστοτε οργανισμό και στη συνέχεια από το επίπεδο ασφαλείας αυτού. Το επίπεδο ασφαλείας όσον αφορά το πληροφοριακό σύστημα σχετίζεται με την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα πληροφοριών και δεδομένων. Το επίπεδο ασφαλείας όσον αφορά τις εγκαταστάσεις σχετίζεται τόσο με την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα πληροφοριών όσο και τη διασφάλιση από φυσικές καταστροφές.

Απαιτήσεις Προτύπου ISO/IEC 27001:2005

Απαίτηση 1. Πολιτική Ασφαλείας.
Παρέχει κατευθυντήριες γραμμές στη διεύθυνση γύρω από την ασφάλεια των πληροφοριών. Όλοι οι οργανισμοί θα πρέπει να προδιαγράφουν μια πολιτική ασφαλείας η οποία θα πρέπει να περιλαμβάνει τον σκοπό της, τους βασικούς στόχους και τα βασικά τμήματα που συμμετέχουν σε αυτή. Λόγω της ανάπτυξης της τεχνολογίας και της νομοθεσίας θα πρέπει να καθορίζεται σαφώς η ανανέωσή της καθώς και ο έλεγχος σε τακτά χρονικά διαστήματα.
1.1 Σχεδιασμός και σύνταξη πολιτικής ασφαλείας
1.2 Έγκριση Πολιτικής Ασφαλείας από την Ανώτατη Διοίκηση του οργανισμού
1.3 Καθορισμός συνθηκών για τον *έλεγχο* (audit) και την αναθεώρηση (review) της Πολιτικής

Απαίτηση 2. Οργανωτική Ασφάλεια
Δημιουργήθηκε η ανάγκη οργάνωσης των οργανισμών η οποία καθορίζει σαφώς το ποιος είναι υπεύθυνος για τι (αρμοδιότητες - ρόλοι). Ύπαρξη οργανωτικής δομής ασφάλειας και δημιουργία επιτροπής ασφάλειας η οποία θα εγκρίνει και θα διασφαλίζει την υλοποίησή της. Ελεγχόμενη πρόσβαση τρίτων μερών όταν και για όσο είναι απαραίτητο και καθορισμός αυτών:
2.1 Καθορισμός Οργανωτικής Υποδομής Ασφάλειας Καθορισμός Επιτροπής Ασφάλειας, Καθορισμός Ρόλων και Αρμοδιοτήτων σχετικά με την Ασφάλεια, Συντονισμός της υλοποίησης των μέτρων ασφάλειας, Καθορισμός σχέσεων με άλλους Οργανισμούς, Πραγματοποίηση ανεξάρτητων ελέγχων της Πολιτικής Ασφάλειας.
2.2 Έλεγχος Πρόσβασης Τρίτων Μερών Προσδιορισμός κινδύνων λόγω της πρόσβασης τρίτων μερών, Καθορισμός επιτρεπτής πρόσβασης από Τρίτους, Εφαρμογή επιπλέον ελέγχων πρόσβασης, Χρήση συμβολαίων για την πρόσβαση τρίτων μερών και για υπηρεσίες outsourcing.

Απαίτηση 3. Ταξινόμηση και Έλεγχος Αγαθών (Πόρων)
Θα πρέπει να γίνει καταγραφή των πόρων του συστήματος. Κάθε οργανισμός θα πρέπει να έχει σαφή εικόνα των πόρων του. Για κάθε ένα από αυτά ή σύνολο αυτών θα πρέπει να καθορίζεται ένας υπεύθυνος ο οποίος θα τα ταξινομεί ανάλογα με τη φύση τους.
3.1 Καθορισμός Αρμοδιοτήτων και Ευθυνών για τους Ιδιοκτήτες Πόρων
Καταγραφή όλων των πληροφοριακών Πόρων
3.2 Καθορισμός Σχήματος Διαβάθμισης Πληροφορίας Ανάπτυξη οδηγιών για τον καθορισμό Σχήματος Διαβάθμισης Πληροφορίας, Ανάπτυξη διαδικασιών χειρισμού πληροφοριών ανάλογα με τη διαβάθμισή τους, Χρήση ετικετών διαβάθμισης (labels) σε πληροφορία κάθε μορφής (έντυπη, ηλεκτρονική).

Απαίτηση 4. Ασφάλεια σε Θέματα Προσωπικού
Μια ευπάθεια των οργανισμών είναι και ο ανθρώπινος παράγοντας. Λάθη, κλοπή, απάτη και κακή χρήση του συστήματος. Για τον λόγο αυτό ορίζονται διαδικασίες για το προσωπικό. Σημαντικό είναι επίσης να υπάρχουν διαδικασίες αναφοράς περιστατικών εισβολής στο σύστημα, ατελειών και κενών ασφαλείας.
4.1 Έλεγχος διαδικασίας πρόσληψης προσωπικού
4.2 Εκπαίδευση προσωπικού σε θέματα Ασφάλεια
4.3 Αντιμετώπιση περιστατικών ασφάλειας

Απαίτηση 5. Φυσική και Περιβαλλοντολογική Ασφάλεια
Συνεχής επιχειρηματική δραστηριότητα. Θα πρέπει να υπάρχει πρόβλεψη ασφαλείας από τις φυσικές καταστροφές (πυρκαγιές, πλημμύρες κ.α.). Η καταστροφή του πληροφοριακού εξοπλισμού είναι συχνά πιο σημαντική από την φυσική καταστροφή ενός οργανισμού.
5.1 Χρήση ασφαλών περιοχών για την προστασία των εγκαταστάσεων Καθορισμός και εφαρμογή περιμέτρων ασφάλειας, Έλεγχος φυσικής εισόδου-εξόδου, Ασφαλής σχεδίαση κτηρίων και εγκαταστάσεων.
5.2 Προστασία εξοπλισμού Προστασία εγκαταστάσεων παροχών, Προστασία καλωδιώσεων, Ασφάλεια εξοπλισμού εκτός εγκαταστάσεων, Ασφαλής καταστροφή εξοπλισμού.
5.3 Έλεγχος πρόσβασης σε πληροφορία Καθιέρωση πολιτικής “clear desk” και “clear screen”, Έλεγχος αφαίρεσης δικαιωμάτων.

Απαίτηση 6. Διαχείριση Τηλεπικοινωνιών και Λειτουργιών
Δημιουργία και καταγραφή μηχανισμών ελέγχου και τήρησης αρχείων για ότι σχετίζεται με το πληροφοριακό σύστημα.
6.1 Καθιέρωση Λειτουργικών διαδικασιών Καταγραφή λειτουργικών διαδικασιών, Έλεγχος μεταβολών σε εγκαταστάσεις και συστήματα, Διάκριση καθηκόντων από σημαντικές λειτουργίες, Διαχωρισμός ανάπτυξης και λειτουργίας συστημάτων.
6.2 Προστασία από κακόβουλο λογισμικό Ανίχνευση και πρόληψη κακόβουλου κώδικα, Χρήση λογισμικού προστασίας και τακτική ανανέωση
6.3 Καθιέρωση διαδικασιών καλής εσωτερικής λειτουργίας Διαδικασίες και μηχανισμοί λήψης εφεδρικών αρχείων, Αρχεία καταγραφής χρήσης και σφαλμάτων συστημάτων.

6.4 Προστασία υπολογιστικών δικτύων Καθιέρωση περιμέτρου δικτύου, Χρήση μέτρων ασφάλειας δικτύων, Έλεγχος δικτυακών μεταβολών, Τεκμηρίωση (documentation) δικτυακής υποδομής και μέτρων ασφάλειας

6.5 Προστασία αποθηκευτικών μέσων Προστασία αποσπωμένων μέσων, Έλεγχος αποθήκευσης και χρήσης πληροφορίας, Έλεγχος απομάκρυνσης πληροφορίας.

6.6 Έλεγχος Ανταλλαγής Πληροφορίας Ανάπτυξη συμφωνητικών για ανταλλαγή πληροφορίας, Προστασία μεταφοράς υπολογιστών και αποθηκευτικών μέσων, Μέτρα ασφάλειας ηλεκτρονικών συναλλαγών (e-commerce), Μέτρα προστασίας και ελεγχόμενη χρήση e-mail, Έλεγχος πληροφοριών που δημοσιεύονται σε συστήματα ανοικτής πρόσβασης (Web site, portal), Έλεγχος εξωτερικών επικοινωνιών.

Απαίτηση 7. Έλεγχος Πρόσβασης

Σαφής καθορισμός των προσβάσεων των χρηστών στο πληροφοριακό σύστημα. Για παράδειγμα άλλα δικαιώματα πρόσβασης θα έχει ένας διευθυντής και άλλα ένας απλός χρήστης στο σύστημα.

7.1 Έλεγχος Πρόσβασης σε πληροφορία Ανάπτυξη πολιτικής πρόσβασης σε πληροφορία, Ανάπτυξη κανόνων πρόσβασης

7.2 Έλεγχος απόδοσης δικαιωμάτων πρόσβασης σε Χρήστες Καθιέρωση διαδικασίας εγγραφής χρηστών, Διαδικασία ελέγχου δικαιωμάτων πρόσβασης σε συστήματα, Διαδικασία διαχείρισης συνθηματικών (password), Επανέλεγχος δικαιωμάτων πρόσβασης.

7.3 Έλεγχος Πρόσβασης σε υπολογιστικά δίκτυα Εφαρμογή πολιτικής χρήσης δικτύων, Διαχωρισμός εσωτερικών και εξωτερικών δικτύων, Χρήση καθορισμένων μονοπατιών δρομολόγησης για τον έλεγχο της πρόσβασης, Ενιαία χρήση κανόνων δρομολόγησης, Έλεγχος αυθεντικότητας απομακρυσμένης πρόσβασης, Περιορισμός συνδέσεων σε διαμοιρασμένους πόρους, Έλεγχος απομακρυσμένης πρόσβασης σε διαγνωστικά port, Επιβεβαίωση της ασφάλειας των δικτυακών υπηρεσιών.

7.4 Περιορισμός πρόσβασης σε επίπεδο Λειτουργικού Συστήματος Εφαρμογή μεθόδων log-on σε τερματικά, Αναγνώριση και αυθεντικοποίηση όλων των χρηστών, Εφαρμογή συστήματος διαχείρισης συνθηματικών, Έλεγχος χρήσης όλων των ευκολιών (utilities) του ΛΣ, Εφαρμογή χρόνου λήξης (time-out) για όλες τις συνδέσεις, Περιορισμός χρόνου και ωρών πρόσβασης τερματικών, Χρήση συναγερμών (alarm) και έλεγχος αρχείων καταγραφής ΛΣ.

7.5 Περιορισμός πρόσβασης σε επίπεδο εφαρμογών Αναγνώριση και αυθεντικοποίηση χρηστών εφαρμογών, Απομόνωση ευαίσθητων εφαρμογών

7.6 Παρακολούθηση πρόσβασης και χρήσης συστήματος Εφαρμογή και χρήση αρχείων καταγραφής, Εξέταση αρχείων καταγραφής για των εντοπισμό περιστατικών ασφάλειας, διαδικασίες παρακολούθησης ευαίσθητων εγκαταστάσεων.

7.7 Προστασία κατά την απομακρυσμένη εργασία Προστασία κινητού εξοπλισμού, Προστασία εξοπλισμού για τηλε-εργασία.

Απαίτηση 8. Ανάπτυξη και Συντήρηση Συστημάτων

Καθώς η τεχνολογία διαρκώς εξελίσσεται θα πρέπει αντίστοιχα να συντηρούνται και να εξελίσσονται τα συστήματα των οργανισμών. Ορίζονται διαδικασίες ελέγχου των δεδομένων εισόδου – εξόδου των εφαρμογών και διαδικασίες αυθεντικοποίησης μηνυμάτων.

8.1 Ενσωμάτωση ασφάλειας σε εφαρμογές και συστήματα Αναγνώριση απαιτήσεων ασφάλειας, Ενσωμάτωση τεχνολογιών ασφάλειας στις εφαρμογές, Ενσωμάτωση ελέγχων εισόδου (input validation), Ενσωμάτωση ελέγχων εξόδου (output validation), Ενσωμάτωση ελέγχων επεξεργασίας, Χρήση τεχνολογιών αυθεντικοποίησης και ελέγχου ακεραιότητας μηνυμάτων σε συστήματα και εφαρμογές.

8.2 Χρήση κρυπτογραφίας Ανάπτυξη πολιτικής κρυπτογραφίας, Κρυπτογράφηση ευαίσθητων πληροφοριών, Προστασία αυθεντικότητας εγγράφων με χρήση ψηφιακών υπογραφών, Χρήση μηχανισμών καταλογισμού ευθύνης, Εφαρμογή συστήματος διαχείρισης κρυπτογραφικών κλειδιών, Προστασία κρυπτογραφικών κλειδιών, Χρήση ασφαλών μεθόδων ανταλλαγής κλειδιών, Χρήση ασφαλών μεθόδων καταστροφής κλειδιών, Χρήση ασφαλών μεθόδων ανανέωσης κλειδιών.

8.3 Προστασία αρχείων συστήματος (system files) Έλεγχος υλοποίησης λογισμικού, Έλεγχος χρήσης δεδομένων συστήματος για λόγους δοκιμών, Έλεγχος πρόσβασης σε βιβλιοθήκες κώδικα προγράμματος

8.4 Έλεγχος ανάπτυξης συστημάτων Ανάπτυξη διαδικασιών ελέγχου μεταβολών, Έλεγχος μεταβολών ΛΣ, Περιορισμός αλλαγών σε λογισμικό, Προστασία συστημάτων από κρυφά κανάλια (covert channels), Δούρειους ίππους (Trojans), Έλεγχος εξωτερικής ανάπτυξης λογισμικού (outsourcing).

Απαίτηση 9. Διαχείριση Συνέχειας Λειτουργιών

Ένας οργανισμός στις μέρες μας έχει άμεση εξάρτηση από το πληροφοριακό σύστημα. Για το λόγω αυτό πρέπει να διασφαλιστεί η λειτουργία του ακόμα και αν το πληροφοριακό σύστημα σταματήσει να λειτουργεί. Η δημιουργία σχεδίου ανάκαμψης – επαναφοράς είναι ζωτικής σημασίας για έναν οργανισμό. Το σχέδιο ανάκαμψης – επαναφοράς θα πρέπει να είναι σε θέση να ανταπεξέλθει τόσο σε κακόβουλη επίθεση ή βλάβη όσο και σε ολική καταστροφή (backup server σε άλλη τοποθεσία).

Απαίτηση 10. Νομική Συμμόρφωση

Το τελευταίο τμήμα του προτύπου, έχει ως σκοπό να εξασφαλίσει ότι το σύστημα στο σύνολό του είναι ευθυγραμμισμένο με νόμους της πολιτείας, με εσωτερικούς ή εξωτερικούς κανονισμούς, ρυθμίσεις, πολιτικές και πρότυπα. Μερικοί από τους τομείς που αναφέρονται, είναι η προστασία προσωπικών δεδομένων, η προστασία του απορρήτου της επικοινωνίας, η ύπαρξη αδειών χρήσης λογισμικού, η προστασία των δικαιωμάτων του δημιουργού, η τήρηση της οδηγιών (κρατικών ή της ευρωπαϊκής κοινότητας) για τις ηλεκτρονικές υπογραφές κλπ.

Συνολικά το Σύστημα Διαχείρισης της ασφάλειας των πληροφοριών (ISMS) παρέχει ένα μοντέλο/πλαίσιο για την καθιέρωση, υλοποίηση, διαχείριση, παρακολούθηση, ανασκόπηση, διατήρηση και βελτίωση της προστασίας των πληροφοριακών περιουσιακών στοιχείων για την επίτευξη των επιχειρησιακών στόχων, βασιζόμενο στην αξιολόγηση των κινδύνων και τα επίπεδα ανοχής της επικινδυνότητας του εκάστοτε οργανισμού για την αντιμετώπιση αυτών. Στα πλαίσια του μοντέλου αυτού θα πρέπει να γίνει ταυτοποίηση και καταγραφή των αγαθών και των αντίστοιχων απαιτήσεων σε μηχανισμούς προστασίας, την αξιολόγηση των κινδύνων που τα συνοδεύουν, την εφαρμογή σημείων ελέγχου για την αποτροπή των κινδύνων αυτών και την παρακολούθηση για την αποτελεσματικότητα του μηχανισμού αυτού. Ο κύκλος των προαναφερθέντων εργασιών (σε υψηλό επίπεδο) περιγράφεται αναλυτικά στην οικογένεια προτύπων 27000 και πρέπει να εφαρμόζεται και να είναι παγιωμένη πρακτική έτσι ώστε να προλαμβάνονται εγκαίρως κίνδυνοι που ελλοχεύουν στην αλλαγή του περιβάλλοντος των πληροφοριακών συστημάτων.

Στο χώρο της ηλεκτρονικής τραπεζικής, το πρότυπο 27001 ειδικότερα και η οικογένεια προτύπων 27000 γενικότερα, που ορίζουν το περιεχόμενο και το τρόπο για αποτελεσματική εφαρμογή Πολιτικής Ασφάλειας σε πρώτο και σχετικά υψηλό επίπεδο, είναι κρίσιμης σημασίας για την αξιολόγηση των συστημάτων αυτών. Η συμμόρφωση με τα συγκεκριμένα πρότυπα (πιστοποίηση) εξασφαλίζει, για το εκάστοτε Πιστωτικό Ίδρυμα που φιλοξενεί ένα σύστημα η-τραπεζικής, ενισχυμένη ασφάλεια στο περιβάλλον Π.Σ. (πρώτο επίπεδο) και αποκλείει ουσιαστικά πιθανά τρωτά σημεία που οφείλονται σε κακή πρακτική ή ανυπακοή σε Πολιτικές Ασφάλειας. Δίνει έτσι το περιθώριο και την εναπόθεση των πόρων στην ενίσχυση της ασφάλειας των συστημάτων σε όλο και χαμηλότερο επίπεδο.

Επιπλέον, πιστοποίηση κατά ISO 27001 συνεπάγεται εμμέσως και την αποτελεσματική εφαρμογή όλων των κανονιστικών πλαισίων που διέπουν τη λειτουργία των Πιστωτικών Ιδρυμάτων και ειδικότερα αυτή των συστημάτων ηλεκτρονικής τραπεζικής μιας και η $10^{η}$ ενότητα προβλέπει τη συμμόρφωση και εφαρμογή συγκεκριμένων πολιτικών, βέλτιστων πρακτικών, προτύπων και νόμων.

2.7 Συμπεράσματα για τα πρότυπα και πλαίσια ασφάλειας

Από την ανάλυση που προηγήθηκε, συμπεραίνουμε ότι τα πρότυπα που υπάρχουν και εφαρμόζονται σε παγκόσμιο επίπεδο και μπορούν να εφαρμοστούν σε ένα ελληνικό τραπεζικό οργανισμό είναι το COBIT από αυτά που επικεντρώνονται στις επιχειρησιακές διαδικασίες, το PCI DSS από τα πρότυπα που επικεντρώνονται άμεσα στην υλοποίηση σημείων ελέγχου και το ISO/ IEC 27001:2005 από αυτά των βέλτιστων πρακτικών.

Τα δύο διεθνή πρότυπα που χρησιμοποιούνται σήμερα και είναι τα πιο διαδεδομένα είναι το COBIT και το ISO/IEC 17799:2000 που αντικαταστάθηκε από το ISO/IEC 27001. Το COBIT (στόχοι ελέγχου για τις πληροφορίες και τη σχετική τεχνολογία) απελευθερώθηκε και χρησιμοποιήθηκε πρώτιστα από την κοινότητα Πληροφοριακών Συστημάτων (ΠΣ). Το 1998, οι διοικητικές οδηγίες προστέθηκαν, και το COBIT έγινε το διεθνώς αποδεκτό πλαίσιο για τη διακυβέρνηση και τον έλεγχο ΠΣ. Το ISO/ IEC 27001:2005 (οι απαιτήσεις για την επιτυχή διαχείριση ασφάλειας πληροφοριών) είναι επίσης διεθνές πρότυπο και είναι η βέλτιστη πρακτική για την εφαρμογή της διαχείρισης ασφάλειας. Τα δύο πρότυπα δεν ανταγωνίζονται το ένα με το άλλο και συμπληρώνουν πραγματικά το ένα άλλο. Το COBIT καλύπτει χαρακτηριστικά μια ευρύτερη περιοχή ενώ το ISO/IEC 27001:2005 στρέφεται βαθειά στον τομέα της ασφάλειας (Security Procedures, 2010). Παρόλο που το ITIL είναι περίπου ίδιο με το COBIT με πολλές έννοιες, η βασική διαφορά είναι ότι το COBIT υιοθετεί μια οπτική των επιχειρησιακών διαδικασιών βασιζόμενες στο βαθμό κινδύνου, ενώ το ITIL υιοθετεί την οπτική της παροχής βασικών υπηρεσιών από την πληροφορική.

Ένα επιπλέον θετικό είναι ότι όλες οι εταιρείες ή οι οργανισμοί μπορούν να εφαρμόσουν και να πιστοποιηθούν σύμφωνα με το πρότυπο ISO 27001, ανεξαρτήτως μεγέθους και δραστηριότητας. Αυτό συμβαίνει γιατί αναφέρεται στην ασφάλεια της πληροφορίας κι όχι των υπολογιστών ή των εφαρμογών του. Οι απαιτήσεις του προτύπου είναι εκφρασμένες με τέτοιο τρόπο ώστε να μπορούν να εφαρμοστούν σε οποιαδήποτε οργανισμό ανεξάρτητα από τη δραστηριότητα του, το μέγεθος του ή την τοποθεσία του. Στα τέλη του 2009, είχαν εκδοθεί τουλάχιστον 12.934 πιστοποιητικά ISO/IEC 27001:2005 σε 117 χώρες, σημειώνοντας 40% αύξηση έναντι του 2008 (9.246 σε 82 χώρες). Πρωτοπόρες χώρες στην εφαρμογή του προτύπου είναι χώρες της Ασίας, καθώς σύμφωνα με επίσημα στοιχεία, μέσα στην πρώτη πεντάδα είναι η Ιαπωνία (με μεγάλη διαφορά από τη δεύτερη), η Κίνα, οι Ινδίες και η Ταϊβάν, ενώ μόνο το Ηνωμένο Βασίλειο βρίσκεται στην τέταρτη θέση και οι ΗΠΑ στην έκτη (www.iso27001certificates.org).

Σε αντίθεση με το πλαίσιο PCI DSS, το πρότυπο ISO 27001 είναι πιο ευέλικτο όσον αφορά το πεδίο εφαρμογής, τους ελέγχους, τη συμμόρφωση και την επιβολή. Ως ένα διεθνώς αναγνωρισμένο πρότυπο ασφάλειας, το ISO 27001 έχει σχεδιαστεί για να εφαρμόζεται σε ένα ευρύ φάσμα οργανισμών. Θεωρείται ως το de-facto πρότυπο ασφάλειας πληροφοριών από πολλούς οργανισμούς όπου η ασφάλεια των πληροφοριών είναι μια αυστηρή απαίτηση, αν και η συμμόρφωση είναι εθελοντική.

Στο πρότυπο PCI DSS οι απαιτήσεις ή έλεγχοι είναι υποχρεωτικά - εάν ένας οργανισμός επιθυμεί να συμμορφωθεί με PCI DSS τότε θα πρέπει να συμμορφωθεί με όλες τις απαιτήσεις που καθορίζονται στο πρότυπο σταδιακά με συνεχείς ελέγχους από τους αρμόδιους οργανισμούς πιστοποίησης. Αντίθετα, το πρότυπο ISO 27001 προτείνει μηχανισμούς ελέγχου, και κάθε οργανισμός έχει την ευελιξία να αποφασίσει ποια αντίμετρα βάση του ελέγχου θα εφαρμόσει.

Συγκρίνοντας τις απαιτήσεις του προτύπου ISO 27001, βλέπουμε ότι οι απαιτήσεις του PCI DSS είναι πιο συγκεκριμένες. Το πρότυπο ISO 27001 προτείνει μηχανισμούς ελέγχου, δεν ορίζει όμως το τρόπο που αυτά τα αντίμετρα θα υλοποιηθούν σε αντιπαράθεση με το PCI DSS που ορίζει συγκεκριμένες πρακτικές, μέτρα, και παραμετροποιήσεις στα συστήματα όλων των επιπέδων (δικτύου, εφαρμογών, βάσεων δεδομένων, servers, firewalls κ.α.). Αυτό θεωρητικά κάνει το PCI-DSS ευκολότερο στον έλεγχο. Στην πραγματικότητα όμως είναι πιο δύσκολο λόγω της έλλειψης ευελιξίας.

Τα δύο πρότυπα έχουν πολύ διαφορετικές απαιτήσεις συμμόρφωσης. Σε γενικές γραμμές, το ISO 27001 παρέχει οδηγίες σε έναν οργανισμό για την εφαρμογή και τη διαχείριση ενός προγράμματος για την ασφάλεια των πληροφοριών και του συστήματος διαχείρισης, ενώ το PCI DSS εστιάζει σε συγκεκριμένα στοιχεία της εφαρμογής. Οι περισσότεροι οργανισμοί που έχουν εφαρμόσει ένα πρότυπο ISO 27001 για τη διαχείριση της ασφάλειας δεν είναι υποχρεωμένοι να καλέσουν τρίτα μέρη για να επικυρώσουν ότι λειτουργούν εντός των ορίων ISMS. Αυτό ουσιαστικά σημαίνει ότι το πρότυπο ISO 27001 εστιάζει πλέον περισσότερο στην ανάπτυξη των ελέγχων με βάση τους κινδύνους, και εξασφαλίζει ότι η παρακολούθηση και η βελτίωση των κινδύνων που αντιμετωπίζει η επιχείρηση είναι βελτιωμένη. Ως εκ τούτου, ανεξάρτητα από τους διάφορους ισχυρισμούς πιστοποίησης με το ISO 27001 (ISO 17799) υπάρχουν πλέον

υποχρεωτικές απαιτήσεις κάτι που ισχύει ήδη για το PCI DSS. Οι περισσότερες PCI DSS απαιτήσεις καλύπτονται από το πρότυπο ISO 27001 - μόνο απουσιάζουν συγκεκριμένες λεπτομέρειες εφαρμογής σε ορισμένες περιοχές. Χρησιμοποιώντας το πρότυπο ISO 27001 ως μέσο για να επιτύχει τους στόχους της συμμόρφωσης θα μπορούσε να θεωρηθεί ως η κατάλληλη μεθοδολογία για να ανταποκριθούν και στις απαιτήσεις του πλαισίου PCI.

Θα πρέπει εδώ να σημειωθεί όμως ότι το πρότυπο ISO 27001 τουλάχιστον για τα Πιστωτικά Ιδρύματα που υπάγονται στην Ελληνική νομοθεσία δεν αποτελεί πλέον μια υπάρχουσα πρότυπη πολιτική που είναι στην επιλογή του εκάστοτε Πιστωτικού Ιδρύματος να την εφαρμόσει. Αντιθέτως, με τη Πράξη Διοικητή (Π.Δ.) της Τράπεζας της Ελλάδος αριθ. 2577/9.3.2006, καθορίζεται και ένα πλαίσιο γενικών αρχών και κριτηρίων για την ασφαλή και αποτελεσματική λειτουργία των Πληροφοριακών Συστημάτων (ΠΣ) των Πιστωτικών Ιδρυμάτων. Το πλεονέκτημα είναι οτι οι απαιτήσεις ασφάλειας που περιλαμβάνονται στη Πράξη Διοικητή (Π.Δ.) της Τράπεζας της Ελλάδος αριθ. 2577/9.3.2006 είναι πλήρως εναρμονισμένες με το ISO 27001:2005. Συνοψίζοντας, αν κανείς αναλύσει τις περιοχές και τις απαιτήσεις πρώτα του προτύπου και έπειτα της νομοθεσίας (Π.Δ.) θα συμπεράνει ότι η τελευταία καθιστά θεσμοθέτηση του προηγουμένως δημοσιευμένου προτυπου ISO 27001:2005 ή ISO 17799.

Συμπερασματικά, και στα πλαίσια αυτής της εργασίας θα χρησιμοποιήσουμε το πρότυπο ISO/ IEC 27001:2005 για την υλοποίηση και την αξιολόγηση των ελεγκτικών μηχανισμών σε ένα τραπεζικό οργανισμό και πιο συγκεκριμένα σε ένα σύστημα ηλεκτρονικής τραπεζικής και εφόσον λειτουργεί συμπληρωματικά με το Cobit και συνήθως πλαισιώνεται από αυτό, θα προσπαθήσουμε να διεξάγουμε αυτή την αξιολόγηση με μια προσέγγιση που να συνδυάζει και τα δυο. Στη πορεία για την ανεύρεση της κατάλληλης προσέγγισης που θα μας βοηθήσει να αξιολογήσουμε την κατάσταση της ασφάλειας στο τραπεζικό οργανισμό είναι σημαντικό να θέσουμε το θέμα της εκτίμησης επικινδυνότητας σε σχέση με τις απαιτήσεις ασφάλειας. Εκτός του ότι απαιτείται από το πρότυπο, η ανάλυση κινδύνου θεωρείται πολύ σημαντική εργασία στη πορεία υλοποίησης ενός προτύπου ασφάλειας, καθώς είναι η πλέον βασική διεργασία εντοπισμού, αξιολόγησης, εκτίμησης (ποσοτικοποίησης) του κινδύνου και των πιθανών επιπτώσεών του στην περίπτωση εκδήλωσης του συμβάντος. Στο κεφάλαιο που ακολουθεί διενεργείται μια επισκόπηση των προσεγγίσεων που έχουν εκδοθεί στα πλαίσια της Εκτίμησης της Επικινδυνότητας, προκειμένου να καταστεί εφικτή η προσπάθεια μελέτης της ασφάλειας ενός ελληνικού τραπεζικού οργανισμού με τρόπο που να προβάλλει τη λογική και τη πορεία από την αξιολόγηση της ασφάλειας ενός τραπεζικού οργανισμού ως έχει, προς την υλοποίηση των απαραίτητων ελεγκτικών μηχανισμών με βάση τις απαιτήσεις ασφάλειας.

Κεφάλαιο 3ο

3. Μέθοδοι και προσεγγίσεις Εκτίμησης Επικινδυνότητας

3.1 Εισαγωγή

Είναι απαραίτητο για κάθε οργανισμό να εντοπίσει τις απαιτήσεις ασφάλειας που τον αφορούν. Υπάρχουν τρεις βασικές πηγές απαιτήσεων ασφάλειας.

- Μία πηγή προέρχεται από την αξιολόγηση των κινδύνων για τον οργανισμό, αφού ληφθούν υπ' όψιν η συνολική επιχειρηματική στρατηγική και οι στόχοι του οργανισμού. Μέσω μιας αξιολόγησης κινδύνου, εντοπίζονται οι απειλές για τα περιουσιακά στοιχεία, αξιολογείται η τρωτότητα σε αυτές και η πιθανότητα εμφάνισής τους και εκτιμάται η δυνητική τους επίδραση.
- Μια άλλη πηγή είναι οι νομικές, θεσμικές, ρυθμιστικές και συμβατικές απαιτήσεις τις οποίες ο οργανισμός, οι εμπορικοί του εταίροι, οι ανάδοχοι και οι παροχείς υπηρεσιών θα πρέπει να ικανοποιήσουν, καθώς και το κοινωνικο-πολιτιστικό τους περιβάλλον.
- Μια επιπλέον πηγή είναι η συγκεκριμένη ομάδα αρχών, στόχων και επιχειρηματικών απαιτήσεων για την επεξεργασία των πληροφοριών, την οποία έχει αναπτύξει ο οργανισμός προκειμένου να υποστηρίξει τις εργασίες του.

Οι απαιτήσεις ασφάλειας προσδιορίζονται σωστά μέσω μιας μεθοδικής αξιολόγησης των κινδύνων ασφάλειας. Η δαπάνη για τους ελέγχους θα πρέπει να σταθμίζεται έναντι της επιχειρηματικής ζημίας που ενδέχεται να προκύψει ως αποτέλεσμα αποτυχίας της ασφάλειας. Τα αποτελέσματα της αξιολόγησης κινδύνου θα βοηθήσουν και θα οδηγήσουν στον προσδιορισμό των κατάλληλων ενεργειών διαχείρισης και προτεραιοτήτων για τη διαχείριση των κινδύνων για την ασφάλεια των πληροφοριών, καθώς και στην υλοποίηση ελέγχων οι οποίοι έχουν επιλεγεί για την προστασία από αυτούς τους κινδύνους. Η αξιολόγηση κινδύνου θα πρέπει να επαναλαμβάνεται περιοδικά ώστε να αντιμετωπίζει οποιεσδήποτε μεταβολές που ενδέχεται να επηρεάσουν τα αποτελέσματα της αξιολόγησης κινδύνου.

3.2 Μέθοδοι και εργαλεία εκτίμησης επικινδυνότητας

Η εκτίμηση επικινδυνότητας λοιπόν αποτελεί σημαντικό μέρος οποιασδήποτε διαδικασίας προσβλέπει στην εξασφάλιση της πληροφορίας και είναι η αρχή για την υλοποίηση ενός συστήματος Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ISMS). Η εκτίμηση των κινδύνων σαν διαδικασία και πρακτική εφαρμόζεται για να εκτιμήσουμε αρχικά το πλήθος των απειλών ως προς την ασφάλεια των πληροφοριών και τη πιθανότητα των απειλών αυτών να εμφανιστούν. Το αποτέλεσμα της διαδικασίας εκτίμησης της επικινδυνότητας τροφοδοτεί μετέπειτα την διαδικασία προτεραιοποίησης των κινδύνων και των ενεργειών για την έγκαιρη πρόληψη ή/και αντιμετώπιση αυτών (όπως για παράδειγμα υλοποίηση σημείων ελέγχου, διαδικασίες κ.α.). Βασικό όμως βήμα στην υλοποίηση αυτών των διαδικασιών είναι και η ανάλυση των επιπτώσεων στις εκάστοτε επιχειρησιακές δραστηριότητες και το αντικείμενο που δραστηριοποιείται ο εκάστοτε οργανισμός (Business Impact Analysis), αν θέλουμε να βλέπουμε και τη πληροφορική υποστηρικτικά στην επιχειρησιακή δραστηριότητα.

Στο κεφάλαιο αυτό θα επιχειρηθεί μια παρουσίαση των μεθοδολογιών και των εργαλείων που υπάρχουν διαθέσιμα για την εκπόνηση μιας εργασίας εκτίμησης της επικινδυνότητας σε ένα οργανισμό όσον αφορά την ασφάλεια της πληροφορίας και κατ' επέκταση των πληροφοριακών συστημάτων. Στη συνέχεια θα ακολουθήσει συζήτηση και σύγκριση αυτών σύμφωνα με ορισμένα κριτήρια, με κύριο γνώμονα το κατά πόσο υλοποιούν τα πρότυπα που παρουσιάστηκαν στο κεφάλαιο 2. Ο οργανισμός ENISA (European Network and Information Security Agency) δημοσίευσε το 2006 μια επισκόπηση των υπαρχουσών μεθοδολογίων και εργαλείων εκτίμησης της επικινδυνότητας (ENISA, 2006) στην οποία θα στηριχτούμε για την επιλογή των μεθοδολογιών που θα αναλύσουμε εδώ έτσι ώστε να επιλέξουμε τελικά εκείνη που θα αρμόζει καλύτερα στη μελέτη της περίπτωσης μιας ελληνικής τράπεζας. Η δημοσίευση αυτή δεν περιλαμβάνει μεθοδολογίες που αφορούν τη γενικότερη εταιρική διακυβέρνηση (Corporate

Governance) όπως Cobit, Basel III κ.α. για το λόγο του οτι δεν υπήρχε τη δεδομένη περίοδο πρόσβαση από την ομάδα εργασίας στα έγγραφα αυτά.

Η ομάδα έργου του ENISA έχει επιλέξει πέντε χαρακτηριστικά (ENISA, 2006) με βάση τα οποία αξιολογεί τις μεθόδους και τα οποία θα χρησιμοποιηθούν και στη συγκεκριμένη ανάλυση για τη κατηγοριοποίηση που θα επιχειρηθεί σε συνδυασμό με κάποια άλλα:

- *Στοιχεία και πηγή της μεδοθολογίας.* Η αξιολόγηση σε αυτό το επίπεδο βασίζεται σε βασικές πληροφορίες για το προϊόν, τον οργανισμό που το εξέδωσε (δημόσιου χαρακτήρα, οργανισμός διεθνών προτύπων, ιδιωτικός οργανισμός, κυβερνητικός οργανισμός κλπ.) και κυρίως το εύρος κάλυψης των βημάτων στη μεθοδολογία που χρησιμοποιείται (είτε για Αποτίμηση της Επικυνδυνότητας, είτε για Διαχείριση αυτής ή και των δύο). Στα πλαίσια της παρούσας εργασίας και έρευνας σημασία έχει το εύρος κάλυψης των βημάτων της Αποτίμησης Επικινδυνότητας (Risk assessment), εφόσον η Διαχείριση της επικινδυνότητας έχει να κάνει με τη μετέπειτα πορεία και στάση του εκάστοτε οργανισμού. Τα βήματα για τις δύο εργασίες με βάση τις οποίες αξιολογούνται οι μεθοδολογίες είναι τα εξής:

  Αποτίμηση της Επικινδυνότητας

  - Αναγνώριση των Απειλών (Threat Identification),
  - Χαρακτηρισμός των Απειλών (Threat Characterization),
  - Εκτίμηση της έκθεσης στις απειλές που έχουν αναγνωριστεί σε προηγούμενο στάδιο (Exposure Assessment),
  - Χαρακτηρισμός Επικινδυνότητας (Risk Characterization).

  Διαχείριση της Επικινδυνότητας

  - Αποτίμηση Επικινδυνότητας (Risk assessment),
  - Μεταχείριση/ προσέγγιση της Επικινδυνότητας (Risk treatment),
  - Αποδοχή των κινδύνων (Risk acceptance),
  - Ενημέρωση σχετικά με την επικινδυνότητα (Risk Communication).
- *Πεδίο εφαρμογής της μεδοθολογίας*. Αξιολόγηση σε αυτό το επίπεδο γίνεται με βάση το τύπο των επιχειρήσεων και οργανισμών όπου η μεθοδολογία μπορεί να εφαρμοστεί (κυβερνητικούς ή δημόσιους οργανισμούς, μικρομεσαίες ή μεγάλες επιχειρήσει, εμπορικές εταιρείες, μη κερδοσκοπικούς οργανισμούς κλπ.) καθώς επίσης και το γεωγραφικό ορίζοντα.
- *Χρηστικότητα της μεδοθολογίας*. Η αξιολόγηση σε αυτό το επίπεδο βασίζεται σε κριτήρια όπως το επίπεδο εξειδίκευσης των χρηστών και το επίπεδο ικανότητας του εκάστοτε αναλυτή.
- *Υλοποιησιμότητα προτύπων από τη μεδοθολογία*, δηλαδή ο βαθμός στον οποίο η μεθοδολογία μπορεί να χρησιμοποιηθεί για να υποστηρίξει την υλοποίηση των παραπάνω προτύπων.
- *Εργαλεία για την υλοποίηση της μεθοδολογίας*. Η αξιολόγηση γίνεται με βάση την δυνατότητα χρήσης κάποιου συγκεκριμένου εργαλείου, ή γενικότερα αυτό μπορεί να γίνει με οποιοδήποτε από αυτά που θα παρουσιαστούν παρακάτω.

3.2.1 Μέθοδος Cramm

Η Μέθοδος Cramm (CCTA Risk Analysis and Management Method) αναπτύχθηκε από δημόσιο/κυβερνητικό οργανισμό στο Ηνωμένο Βασίλειο και στοχεύει καθαρά στην Αποτίμηση της Επικυνδυνότητας (Risk Assessment) χωρίς να περιλαμβάνει ή να προτείνει περαιτέρω ενέργειες για διαχείριση των κινδύνων (Risk Management). Περιλαμβάνει και καλύπτει εκτενώς στο σύνολό τους τα 4 βήματα στην αποτίμηση της επικυνδυνότητας. Χρησιμοποιείται και προτείνεται σε μεγάλους οργανισμούς του Ηνωμένου Βασιλείου (Η.Β.), αλλά τελευταία χρησιμοποιείται και από άλλες χώρες εκτός Η.Β. Το μειονέκτημα στην υλοποίηση αυτής της μεθοδολογίας είναι οτι αυτό επιτυγχάνεται μόνο με το εργαλείο Cramm που έχει αναπτυχθεί στα πλαίσια της συγκεκριμένης μεθοδολογίας σε συνδυασμό με το γεγονός οτι η χρήση του συγκεκριμένου πακέτου έχει ένα σημαντικό κόστος για τον οργανισμό που σκοπεύει να την χρησιμοποιήσει. Επιπλέον, ο αναλυτής που θα εμπλακεί στην εργασία αυτή θα πρέπει να είναι

αρκετά εξειδικευμένος στο αντικείμενο της ασφάλειας και την ανάλυση του κινδύνου για την εκπόνηση αυτού του έργου (ENISA, 2006). Πλεονεκτήματα της μεθόδου είναι οτι είναι αρκετά αναλυτική και καλύπτει τόσο το κομμάτι της διαχείρισης (Management) και των Λειτουργιών (Operational) όσο και το τεχνικό (Technical). Τέλος, είναι συμβατή με και υλοποιεί το πρότυπο ISO/IEC IS 17799. Είναι σχεδιασμένη με βάση ένα μοντέλο, κατά το οποίο ο ερευνητής που την εφαρμόζει είναι υπεύθυνος για τη συλλογή των δεδομένων, την αξιολόγησή τους και την ολοκλήρωση της διαδικασίας που η μεθοδος ορίζει (Insight Consulting, 2005). Συνεπως, τα αποτελέσματα της μεθόδου εξαρτώνται πολύ από την εμπειρία και την ικανότητα του ερευνητή και βασίζεται όπως ειπώθηκε στη χρήση ειδικών (Πολέμη, 2011).

Όσον αφορά τα συστήματα ηλεκτρονικής τραπεζικής, η συγκεκριμένη μεθοδολογία μπορεί να χρησιμοποιηθεί για τη συγκεκριμένη μελέτη περίπτωσης, αφού μπορεί να χρησιμοποιηθεί στην Αποτίμηση της Επικυνδυνότητας και εφόσον υλοποιεί το πρότυπο ISO/IEC IS 17799. Παρόλα αυτά όμως δεν ενδείκνυται λόγω του οτι δεν συνδέει την ανάλυση με άλλες επιχειρησιακές διαδικασίες και συνεπώς δεν δίνει ένα πλάισιο που να λαμβάνει υπόψη τη κρισιμότητα και τις επιπτώσεις που θα μπορούσε να έχει στη συνέχεια των επιχειρησιακών λειτουργιών μια πιθανή απειλή.

3.2.2 Μέθοδος Ebios

Η μεθοδολογία Ebios (Expression des Besoins et Identification des Objectifs de Sécurité) η οποία έχει ως αντικειμενικό στόχο την αναγνώριση των στόχων της Ασφάλειας και των αναγκών του εκάστοτε οργανισμού ως προς τους στόχους που θέτει αναπτύχθηκε από το Γαλλικό κυβερνητικό οργανισμό DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information, Premier Ministre) στον οποίο συμμετέχουν και ένας σημαντικός αριθμός ιδιωτικών φορέων. Καλύπτει επαρκώς όλα τα βήματα και στην Αποτίμηση της Επικινδυνότητας όπως επίσης και στην Διαχείριση της Επικινδυνότητας και δίνει στους υπεύθυνους διαχείρισης επικινδυνότητας μια συνεπή και υψηλού επιπέδου προσέγγιση σχετικά με τους κινδύνους.

Η μεθοδολογία Ebios προωθεί μια σφαιρική και συνεκτική θεώρηση για τη λήψη αποφάσεων από ανώτατα διευθυντικά στελέχη, και είναι εφαρμόσιμη τόσο σε μεγάλα έργα (π.χ. σχέδιο επιχειρηματικής συνέχειας, ένα πλάνο ασφάλειας, πολιτική ασφάλειας), καθώς και σε μικρότερης εμβέλειας έργα, δηλαδή σε πιο συγκεκριμένα συστήματα (συστήματα ηλεκτρονικών μηνυμάτων, δίκτυα ή ιστοσελίδες κ.α.). Η μεθοδολογία αυτή μπορεί να χαρακτηριστεί ως συνεργατική καθώς απαιτεί τη συνεργασία μεταξύ των υπευθύνων των συστημάτων, των διευθυντών ασφαλείας και των αναλυτών που θα συμμετέχουν στην εκάστοτε εργασία. Έτσι,συμβάλλει στη σχετική επικοινωνία με τους φορείς ασφάλειας και προωθεί την ευαισθητοποίηση σε θέματα ασφάλειας.

Η προσέγγιση με βάση αυτή τη μεθοδολογία ολοκληρώνεται σε 5 στάδια, το πρώτο από τα οποία είναι η ανάλυση του περιβάλλοντος και των παραγόντων που εξαρτάται το εκάστοτε πληροφοριακό σύστημα προς ανάλυση. Δεν φτάνει όμως σε τόσο τεχνικό επίπεδο και εξαρτάται πάρα πολύ από τους χρήστες και τη συνεργασία τους. Δεν απαιτεί όμως ιδιαίτερα εξειδικευμένους χρήστες και είναι γενικά ευέλικτη σαν μεθοδολογία και ως προς τη δομή της ειδικότερα εφόσον μπορεί να εφαρμοστεί σε οποιοδήποτε οργανισμό ανεξάρτητα του μεγέθους αυτού. Το πλεονέκτημα που έχει είναι οτι το εργαλείο που την υλοποιεί είναι δωρεάν στη χρήση από οποιονδήποτε αναλυτή, αν και σαν μεθοδολογία υλοποιείται μόνο με το συγκεκριμένο εργαλείο. Υλοποιεί όμως μια σειρά προτύπων ξεκινώντας από τα ISO/IEC IS 17799 ή ISO/IEC IS 27001, ISO/IEC IS 15408, ISO/IEC IS 13335, και ISO/IEC IS 21827. Στην ανάλυση που θα επιχειρηθεί παρόλα αυτά δεν θα χρησιμοποιηθεί διότι απαιτεί συνεργασία και το εργαλείο που προσφέρεται για χρήση είναι καθαρά συνεργατικό.

3.2.3 Μέθοδος MARION

Η μέθοδος MARION (Méthodologie d'Analyse des Risques Informatiques et d'Optimisation par Niveau) αναπτύχθηκε από το Γαλλικό οργανισμό για την ασφάλεια των πληροφοριών CLUSIF, ο οποίος είναι ιδιωτικών συμφερόντων. Η μέθοδος γενικά που προτείνει επιτρέπει την ανάλυση όσον αφορά στην Αποτίμηση της Επικινδυνότητας αλλά δεν υποστηρίζει τη μετέπειτα

Διαχείριση της Επικινδυνότητας. Τουλάχιστον είναι αρκετά αναλυτική στο βαθμό που βοηθά στην διενέργια της αποτίμησης επικινδυνότητας και καλύπτει όλα τα στάδια αυτής. Και σε αυτή τη μέθοδο υπάρχει ένα προκαθορισμένο σύνολο απειλών τις οποίες ο αναλυτής πρέπει να αξιολογήσει.

Πρόκειται για μια μεθοδολογία ελέγχου, η οποία, όπως το όνομά της υποδηλώνει, επιτρέπει την εκτίμηση του επιπέδου επικινδυνότητας στην ασφάλεια μιας εταιρείας μέσω δομημένων ερωτηματολογίων σε επίκαιρα θέματα γύρω από τον τομέα της ασφάλειας. Είναι απλή στη χρήση και δεν απειτεί ιδιαίτερες ικανότητες από το χρήστη. Σαν εργαλείο μπορεί να χρησιμοποιηθούν φύλλα εργασίας Microsoft Excel. Παρόλο που χρησιμοποιείται ακόμα σε μεγάλες εταιρίες μόνο, δεν υποστηρίζεται πλέον από το CLUSIF και έχει αντικατασταθεί από τη μέθοδο Mehari η οποία αναλύεται παρακάτω.

3.2.4 Mehari (MEthode Harmonisée d'Analyse de RIsque)

Η μέθοδος **Mehari** αναπτύχθηκε από το Γαλλικό οργανισμό για την ασφάλεια των πληροφοριών CLUSIF, και όπως η MARION υποστηρίζει την διαδικασία Αποτίμησης της Επικινδυνότητας αλλά οχι τη Διαχείριση της Επικινδυνότητας. Είναι εφαρμόσιμη σε όλα τα μεγέθη και τύπους οργανισμών, σε αντίθεση με τη MARION, και πλέον πιο περίπλοκη αφού χρειάζεται ελάχιστα υψηλότερο επίπεδο εξειδίκευσης από τους χρήστες, παραμένοντας όμως φιλική προς το χρήστη. Υλοποιεί τα πρότυπα ISO/IEC 27001 και ISO/IEC IS 13335, η χρήση της όμως δεν είναι οικονομικά προσιτή. Το πεδίο εφαρμογής της Mehari είναι το ίδιο με αυτό της MAGERIT, αλλά έχει μεγαλύτερη αποδοχή (Πολέμη, 2011). Καλύπτει διαχειριστικά, λειτουργικά και τεχνικά ζητήματα. Η διαδικασία που προτείνει περιλαμβάνει την αναγνώριση των απειλών με βάση δώδεκα σενάρια που βρίσκονται στη βάση δεδομένων και τη διενέργεια ελέγχων για εντοπισμό ευπαθειών. Τέλος, η προσέγγιση που προτείνει περιλαμβάνει και βήματα για τον καθορισμό των μέτρων μείωσης του κινδύνου. Συγκριτικά, είναι η καλύτερη μέθοδος από όλες όσες έχουν αναφερθεί για την μελέτη περίπτωσης ασφάλειας τραπεζικού συστήματος στην Ελλάδα από την άποψη οτι καλύπτει και το στάδιο πρότασης μέτρων για τη μείωση κινδύνου. Το μειονέκτημα είναι μόνο οτι απαιτεί ένα σημαντικό χρηματικό ποσό για τη χρήση της και υλοποιείται μόνο με ένα συγκεκριμένο εργαλείο το RISICARE, το οποίο επίσης απαιτεί ένα σημαντικό ποσό για τη χρήση του.

3.2.5 Octave

Η μέθοδος Octave (Operationally Critical Threat, Asset, and Vulnerability Evaluation) αναπτύχθηκε από το πανεπιστήμιο Carnegie Mellon και είναι αρκετά διαδεδομένη ειδικά στις ΗΠΑ. Καλύπτει πρακτικές και για την Αποτίμηση της Επικινδυνότητας και για Διαχείριση της Επικινδυνότητας όχι όμως στο βαθμό που καλύπτονται από τις προαναφερθείσες και όχι σε τεχνικά θέματα. Η Octave μπορεί να χρησιμοποιηθεί σε μικρούς εμπορικούς οργανισμούς και υποθέτει οτι η ομάδα έργου θα αποτελείται απο 3-5 άτομα.

Βασικό χαρακτηριστικό της είναι πως έχει σχεδιαστεί να εκτελείται εσωτερικά στον οργανισμό, με αποτέλεσμα οι ίδιοι οι εργαζόμενοι να συμμετέχουν στις διαδικασίες λήψης αποφάσεων, σχηματίζοντας μια «ομάδα ανάλυσης», σε αντιδιαστολή με τη συνήθη πρακτική της χρήσης ειδικών (Πολέμη, 2011). Η προσέγγιση που προτείνεται είναι με βάση το επίπεδο κινδύνου και χαρακτηρίζεται ως αυτο-καθοδηγούμενη (self-directed) πράγμα που σημαίνει ότι η «ομάδα ανάλυσης» αναλαμβάνει την ευθύνη για τον καθορισμό της στρατηγική ασφάλειας του οργανισμού (ENISA, 2006).

Όσον αφορά την εφαρμοστικότητά της στη παρούσα μελέτη, κρίνεται ως μη εφαρμόσιμη για δυο λόγους. Πρώτον, σχεδιάστηκε για την εφαρμογή της περισσότερο σε εμπορικούς οργανισμούς, και ο τραπεζικός κλάδος έχει αρκετές ιδιαιτερότητες για να μπορέσουμε να τη προσαρμόσουμε. Δεύτερον, προάγει τη συνεργασία και αυτό δεν είναι εφικτό στη παρούσα μελέτη. Για τη διεξαγωγή της OCTAVE, ουσιαστικά, η ομάδα πρέπει να έχει ευρεία γνώση των δραστηριοτήτων της οργάνωσης και των διαδικασιών ασφαλείας, έτσι ώστε να είναι σε θέση να διεξάγει όλες τις πρακτικές που προτείνονται. Τέλος, δεν είναι από τις μεθόδους που υλοποιούν

κάποιο συγκεκριμένο πρότυπο όπως το ISO/IEC 27001/2 και τα εργαλεία για την εφαρμογή της απαιτούν αδειοδότηση.

3.2.6 Μέθοδοι και εργαλεία του ISF

Ο διεθνής οργανισμός ISF έχει εκδώσει πολλές πρακτικές, μεθόδους και εργαλεία για την Αποτίμηση της Επικινδυνότητας και για Διαχείριση της Επικινδυνότητας που συνεχώς ανανεώνει και επικαιροποιεί και τα οποία είναι στενά συνδεόμενα μεταξύ των, αναφέρονται συχνά το ένα στο άλλο και λειτουργούν και ως συμπληρωματικά ανάλογα με το εύρος της ανάλυσης που θέλει κανείς να πετύχει και τη περιοχή μελέτης. Όλα τα εργαλεία και οι μέθοδοι που παρέχει ο οργανισμός ISF βασίζονται στο Πρότυπο του ISF 2011 και είναι τα παρακάτω:

- FIRM (Fundamental Information Risk Management) ή/και FIRM Scorecard
- Information Security Status Survey
- Information Risk Analysis Methodologies (IRAM) project
- SARA (Simple to Apply Risk Analysis)
- SPRINT (Simplified Process for Risk Identification)

Σαν γενικότερη μεθοδολογία αυτή του ISF, με τη σειρά των εργαλείων και των μεθόδων που διαθέτει, καλύπτει πλήρως, αναλυτικά και επαρκώς όλα τα βήματα και στην Αποτίμηση της Επικινδυνότητας (Risk Assessment) όπως επίσης και στην Διαχείριση της Επικινδυνότητας (Risk Management) των πληροφοριακών συστημάτων. Τα εργαλεία που μπορούν να χρησιμοποιηθούν στα πλαίσια αυτής της εργασίας Αποτίμησης τη Επικινδυνότητας είναι το IRAM, το SARA και το SPRINT. Τα δύο τελευταία είναι πολύ σύντομα και περιορίζονται ως προς το εύρος της ανάλυσης. Το IRAM όμως είναι ένα αρκετά ευέλικτο εργαλείο, μπορεί να χρησιμοποιηθεί και ως συνεργατικό εγκαθιστώντας το σε IIS σαν web εφαρμογή αλλά και ένας εξειδικευμένος αναλυτής μπορεί εξίσου να το τρέξει χωρίς προβλήματα με την απλή έκδοσή του που είναι φτιαγμένη σε φύλλα εργασίας (Microsoft Excel).

Το πλεονέκτημα είναι ότι το IRAM αποτελείται από τρείς διακριτές φάσεις και τα αποτελέσματα της μιας είναι σημείο αναφοράς της επόμενης. Υπάρχουν προκαθορισμένα σετ με βάση τα οποία ο αναλυτής κρίνει το εύρος της επίπτωσης σε επιχειρησιακό επίπεδο, απειλής ή ευπάθειας στην εκτίμηση της επικινδυνότητας και τα αποτελέσματα συνυπολογίζονται αυτόματα και συνολικά. Στο τρίτο και τελευταίο κομμάτι υπάρχει μια βάση με πάνω από 100 ελεγκτικές πρακτικές (σημεία ελέγχου) και ο αναλυτής, βάσει των πιο υψηλών κινδύνων και επιχειρησιακών αντικτυπων που έχει αναγνωρίσει στα δυο προηγούμενα στάδια καθώς επίσης και άλλων παραμέτρων που συνυπολογίζονται από το IRAM, επιλέγει τα απαραίτητα σημεία ελέγχου για να υλοποιήσει στον εκάστοτε οργανισμό για τον οποίο γίνεται η εργασία. Κατά σειρά οι φάσεις της μεθόδου αυτής είναι:

- Ανάλυση επιχειρησιακού αντίκτυπου (Business Impact Analysis)
- Εκτίμηση Απειλών και Ευπαθειών (Threat and Vulnerability Assessment)
- Επιλογή Σημείων Ελέγχου (Controls Selection)

Το μειονέκτημα είναι οτι το σετ από όλα εργαλεία είναι διαθέσιμα μόνο σε όσους είναι μέλη του οργανισμού ISF. Εντούτοις, είναι εφαρμόσιμα σε όλους τους τύπους εταιριών εμπορικές και μη, κυβερνητικές αλλά όχι σε μικρομεσαίες επιχειρήσεις και το επίπεδο ανάλυσης είναι υψηλό τόσο στο κομμάτι της διαχείρισης (Management) και των Λειτουργιών (Operational) όσο και στο τεχνικό (Technical). Υλοποιεί το ISO/IEC IS 17799 ή ISO/IEC IS 27001/2 και τη μεθοδολογία Cobit 4.1 και αυτό μπορεί να θεωρηθεί μεγάλο συγκριτικό πλεονέκτημα σε σχέση με τις άλλες μεθόδους, αφού η αξιολόγηση εφαρμόζεται σε ένα πληροφοριακό σύστημα μεν, αλλά λαμβάνεται υπόψη και το περιβάλλον που το πλαισιώνει και κυρίως η επιχειρησιακή δραστηριότητα.

3.3 Μεθοδολογία προσέγγισης

Στο δεύτερο κεφάλαιο διεξήχθη μια επισκόπηση των προτύπων και προσεγγίσεων για την ασφάλεια της πληροφορίας προκειμένου να επιλεγεί εκείνο το οποίο θα μπορούσε να αποτυπώσει πλήρως τις απαιτήσεις ασφάλειας ενός ελληνικού τραπεζικού οργανισμού. Αυτό

έγινε με μια αρχική προσπάθεια κατηγοριοποίησης αυτών και τελικά με κάποια επιπλέον κριτήρια επιλέχθηκαν αυτά που κρίθηκαν ως τα πιο αποτελεσματικά για να πλαισιώσουν ένα έργο υλοποίησης συστήματος διαχείρισης της ασφάλειας. Συνοψίζοντας και από την διερεύνηση των προτύπων που προηγήθηκε στο προηγούμενο κεφάλαιο, επιλέχθηκε το πρότυπο ISO 27001, το οποίο είναι το πιο ευρέως διαδεδομένο και πλήρως συνυφασμένο με τη Πράξη Διοικητή (Π.Δ.) της Τράπεζας της Ελλάδος αριθ. 2577/9.3.2006. Επιπλέον, εφόσον το ISO 27001 λειτουργεί συμπληρωματικά με το Cobit και συνήθως πλαισιώνεται από αυτό, η μελέτη της περίπτωσης ενός τραπεζικού οργανισμού θα βασιστεί στην αξιολόγηση με μια προσέγγιση που να συνδυάζει και τα δυο.

Βάσει των προϋποθέσεων που θέτουν τα προτύπα που επιλέχθηκαν (ISO 27001 και Cobit), αλλά και της προσέγγισης στα πλαίσια αυτής της εργασίας κρίνεται απαραίτητη η άσκηση της εκτίμησης των κινδύνων για να καταλήξει ο οργανισμός στην υλοποίηση των κατάλληλων μέτρων ασφάλειας της πληροφορίας. Στα πλαίσια αυτά, στο κεφάλαιο αυτό έγινε επισκόπηση των μεθοδολογιών και προσεγγίσεων που προσφέρονται για τη διεξαγωγή μιας τέτοιας εργασίας. Με βάση τα κριτήρια που τέθηκαν, η μεθοδολογία που βασίζεται στο Πρότυπο του ISF 2011 και τα εργαλεία/ μέθοδοι που προσφέρει ο ISF κρίνονται τα πιο κατάλληλα, σε συνδυασμό με το γεγονός οτι η υλοποίηση των μηχανισμών ελέγχου για την ασφάλεια που τελικά προτείνουν αντιπαραβάλονται με τα δύο πρότυπα που επιλέχθηκαν.

Το Πρότυπο του ISF 2011 (Standard of Good Practice), στο οποίο είναι βασισμένη η μέθοδος IRAM, είναι πλήρως ευθυγραμμισμένο με τις απαιτήσεις για ένα Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ISMS) που καθορίζονται από το ISO 27001 και παρέχει μια ευρύτερη και βαθύτερη κάλυψη των σημείων ελέγχου και των αντικειμενικών τους στόχων που περιλαμβάνονται στο ISO 27002. Καλύπτει επίσης αρκετά εξίσου σημαντικά θέματα που δεν καλύπτονται από το πρότυπο ISO 27002, όπως το cloud computing, τη διαρροή πληροφοριών, και τη διακυβέρνηση της ασφάλειας. Το Πρότυπο ISF του 2011 κρίνεται επομένως ιδανικό πλαίσιο με τις μεθόδους που προσφέρει για τη διευκόλυνση στην αξιολόγηση και κατά συνέπεια στη πιστοποίηση κατά ISO 27001. Επιπλέον, καθώς το Πρότυπο του 2011 παρέχει πλήρη κάλυψη των θεμάτων που περιλαμβάνει το COBIT v4 και παρέχει και τα εργαλεία για τη διεξαγωγή μιας αξιολόγησης στα πλαίσια των δύο αυτών προτύπων (ISO 27001 και Cobit) καθώς επίσης και το γεγονός ότι τα αποτελέσματα και τα σημεία ελέγχου που προτείνει τελικά αντιπαραβάλλονται στο τέλος της ανάλυσης με τα αντίστοιχα των προτύπων ISO 27001 και COBIT v4, θα χρησιμοποιηθεί η μεθοδολογία του ISF που στηρίζεται στο πρότυπο ISF του 2011, το IRAM (Information Risk Assessment Methodology). Μια εκτενής αντιπαράθεση (benchmark) μεταξύ των δυο προτύπων (ISF Standard of Good Practice, και ISO 27002) έχει επίσης διεξαχθεί από τον ISF. Το εργαλείο ή εφαρμογή που χρησιμοποιείται για τη διεξαγωγή αυτής της ανάλυσης και θα παρουσιαστεί εκτενώς παρακάτω είναι το ομώνυμο IRAM.

Κεφάλαιο 4ο

4. Μελέτη Περίπτωσης

4.1 Εισαγωγή στην υλοποίηση προτύπου 27001/27002 βάσει Cobit με το εργαλείο IRAM του ISF

Στο κεφάλαιο που ακολουθεί διεξάγεται η υλοποίηση συστήματος ασφάλειας της πληροφορίας στον ελληνικό τραπεζικό οργανισμό XBANK. Η υλοποίηση βασίζεται στο πρότυπο ISO27001:2005 και το πλαίσιο Cobit και διεξάγεται με τη μεθοδολογία του ISF, IRAM. Όπως αναφέρθηκε και στο προηγούμενο κεφάλαιο, η μέθοδος IRAM αποτελείται από τρεις διακριτές φάσεις. Η τελική φάση είναι η επιλογή των κατάλληλων σημείων ελέγχου που στην ουσία υλοποιούν το σύστημα διαχείρισης ασφάλειας του τραπεζικού οργανισμού.

Στην ακόλουθη παράγραφο γίνεται μια συνοπτική ανάλυση και περιγραφή των βημάτων σε κάθε φάση σαν πρακτική που πρέπει να ακολουθηθεί (1. Εκτίμηση Επιχειρησιακού αντίκτυπου, 2. Εκτίμηση Επικινδυνότητας και 3. Επιλογή Σημείων Ελέγχου). Στη συνέχεια περιγράφονται ο σκοπός και το εύρος του ελέγχου στη τράπεζα XBANK και τέλος αρχίζει η περιγραφή της άσκησης για κάθε φάση παραθέτοντας και όπου είναι εφικτό εκτυπώσεις οθόνης (screen shots) από την εφαρμογή/ εργαλείο που χρησιμοποιήθηκε και παρουσιάζονται τα αποτελέσματα από ένα μέρος αυτής καθώς είναι πολύ μεγάλη σε έκταση και δεν μπορεί να παρουσιαστεί στα πλαίσια της εργασίας αυτής.

Σε αυτό το σημείο θα πρέπει να αναφερθεί οτι η συνολική άσκηση επικεντρώθηκε στο σύστημα ηλεκτρονικής τραπεζικής της XBANK. Αυτό γίνεται λόγω του οτι η εκτίμηση του επιχειρησιακού αντίκτυπου μπορεί να διεξαχθεί με αναφορά σε μόνο ένα σύστημα/ εφαρμογή της τράπεζας, αφού η πληροφορία που φέρει κάθε σύστημα και η διαχείριση αυτής από το εκάστοτε σύστημα είναι διαφορετικής σημασίας για το τραπεζικό οργανισμό. Το ίδιο ισχύει και για τις απειλές και κινδύνους που το περιβάλλουν. Άλλωστε απαιτείται και από το ίδιο το εργαλείο IRAM η επιλογή ενός και μόνο συστήματος. Στη συγκεκριμένη περίπτωση που θα μελετηθεί, θα είχε πολύ μεγαλύτερο αντίκτυπο στις επιχειρησιακές διαδικασίες και τη λειτουργία της τράπεζας η απώλεια του συστήματος ηλεκτρονικής τραπεζικής από ένα σύστημα που απλά τηρεί πληροφορίες πελατών. Η υλοποίηση σημείων ελέγχου ωστόσο θα δούμε οτι τελικά δεν αφορούν μόνο το συγκεκριμένο σύστημα. Αφορούν όλο τον οργανισμό από τη διοίκηση μέχρι τις πρακτικές ελέγχου που εφαρμόζει ένας απλός υπάλληλος ή ακόμα και μια εφαρμογή με την υλοποίηση αυτοματοποιημένων σημείων ελέγχου.

4.2 Φάσεις της μεθοδολογίας IRAM

Σε αυτή τη παράγραφο θα γίνει μια παρουσίαση των φάσεων της διαδικασίας υλοποίησης ενός συστήματος ασφάλειας της πληροφορίας και ελέγχου όπως αυτές εκτελούνται με τη χρήση της εφαρμογής του IRAM. Οι τρείς φάσεις της άσκησης που θα διεξαχθεί είναι:

- Ανάλυση Επιχειρησιακού Αντίκτυπου (Business Impact Analysis)
- Εκτίμηση Απειλών και Ευπαθειών (Threat and Vulnerability Assessment)
- Επιλογή Σημείων Ελέγχου (Controls Selection)

Μια συνοπτική απεικόνιση συμπεριλαμβανομένης και μιας σύντομης περιγραφής τους αποτυπώνεται στην ακόλουθη εικόνα.

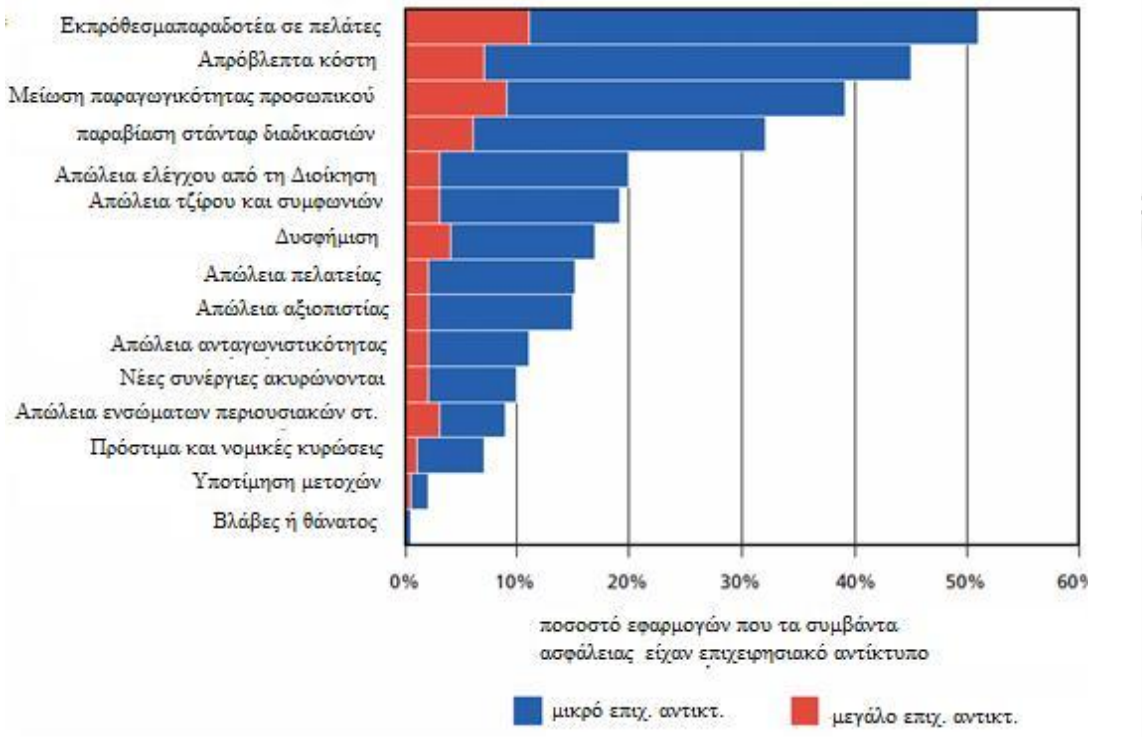
IRAM 1: Διαδικασία ανάλυσης επικινδυνότητας στη ροή των πληροφοριών

4.2.1 Ανάλυση Επιχειρησιακού Αντίκτυπου (Business Impact Analysis)

Η Ανάλυση Επιχειρησιακού Αντίκτυπου στις επιχειρήσεις είναι μια μέθοδος προσδιορισμού των δυνατών επιπτώσεων που ένας οργανισμός θα μπορούσε να υποστεί ως αποτέλεσμα ενός συμβάντος που θέτει σε κίνδυνο τις πληροφορίες που φέρει ένα σύστημα. Βοηθά στον προσδιορισμό των απαιτήσεων ασφάλειας για ένα σύστημα σε επιχειρησιακό επίπεδο και τα επόμενα βήματα που πρέπει να ακολουθήσει ο εκάστοτε οργανισμός για την προστασία των πληροφοριών επαρκώς. Η ανάλυση αυτή είναι το πρώτο βήμα στη συνολική διαδικασία ανάλυσης κινδύνου που αποσκοπεί και επιτρέπει τον προσδιορισμό αποτελεσματικών μέτρων ασφάλειας με στόχο την ελαχιστοποίηση στη συχνότητα και τον αντίκτυπο των πιθανών καταστρεπτικών γεγονότων.

Σαν πρώτο βήμα στην συνολική ανάλυση - και με γνώμονα τις ανάγκες σε επιχειρησιακό επίπεδο για προστασία των πληροφοριών - βοηθά στον προσδιορισμό τόσο της εμβέλειας όσο και του επίκεντρου όλων των μετέπειτα βημάτων της διαδικασίας ανάλυσης και εκτίμησης της επικινδυνότητας.

Όλα ξεκινούν από το γεγονός οτι οι περισσότεροι οργανισμοί έχουν να αντιμετωπίσουν ένα σταθερό μπαράζ απειλών στη ροή της πληροφορίας. Οι απειλές αυτές ποικίλουν - από δυσλειτουργίες υλικού και λογισμικού μέχρι κακοδιαχείριση ή κακή χρήση και εξωτερικές επιθέσεις (π.χ. από hackers ή ιούς). Αν και εφόσον οι απειλές στα πληροφοριακά συστήματα δεν αντιμετωπιστούν με κατάλληλα μέτρα και ελέγχους πρόληψης, έχουν πολύ μεγάλη πιθανότητα περιστατικά παραβίασης της ασφάλειας να συμβούν. Η έρευνα του ISF το 2003 σχετικά με τη κατάσταση Ασφάλειας Πληροφοριών (Information Security Status Survey) έδειξε ότι κατά μέσο όρο οι εφαρμογές, των οργανισμών που συμμετείχαν, παρουσίαζαν160 περιστατικά ετησίως, ή τρία επεισόδια ανά εβδομάδα εργασίας. Το επιχειρησιακό αντίκτυπο των περιστατικών αυτών σε οργανισμούς είναι σημαντικό. Το σχήμα παρακάτω, το οποίο βασίζεται σε στοιχεία από την έρευνα του ISF, δείχνει το είδος του επιχειρησιακού αντίκτυπου από τα συμβάντα ασφάλειας που υφίστανται οι επιχειρησιακές εφαρμογές/ πληροφοριακά συστήματα (έκθεση του ISF με τίτλο *«Critical Business Applications: Improving Security»*).



ISF: Επίπεδο επιχειρησιακού αντίκτυπου από περιστατικά ασφάλειας

Επιπτώσεις στην επιχειρηματική δραστηριότητα, όπως απρόβλεπτα έξοδα, καθυστέρηση σε παραδοτέα στους πελάτες και μείωση της παραγωγικότητας του προσωπικού επηρεάζουν άμεσα την ικανότητα ενός οργανισμού να λειτουργήσει αποτελεσματικά και μπορούν να έχουν σημαντική επίπτωση στο κόστος (το μέσο κόστος των «πιο σοβαρών συμβάντων» που καταγράφεται στην έρευνα ISF για κρίσιμες επιχειρηματικές εφαρμογές ήταν $ 1,9 εκατ.).

Το γεγονός οτι ένα μεγάλο ποσοστό οργανισμών υφίσταται σοβαρές επιπτώσεις στις επιχειρηματικές διεργασίες και το μεγάλο κόστος που επιφέρουν τα περιστατικά ασφάλειας σημαίνει οτι πολλοί οργανισμοί δεν προστατεύουν επαρκώς τις πληροφοριακές τους ροές και κατά συνέπεια τα συστήματα που συμμετέχουν σε αυτές. Η ανάλυση επιχειρησιακού αντίκτυπου σαν πρώτο μέρος μιας αποτελεσματικής ανάλυσης της επικινδυνότητας επομένως επιβάλλεται να γίνει, ετσι ώστε να βοηθήσει τους οργανισμούς να αναγνωρίσουν αποτελεσματικά μέτρα ασφαλείας για την αντιμετώπιση αυτού του τόσο σημαντικού - σε επιχειρηματικό επίπεδο - προβλήματος.

Παρακάτω παρατίθεται ένας πίνακας αναφοράς του εργαλείου IRAM για την εκτίμηση του επιχειρησιακού αντίκτυπου μεταφρασμένος στην ελληνική. Εξηγούνται τα κύρια πεδία και αποτυπώνονται τα επίπεδα του αντίκτυπου (από πολύ χαμηλό μέχρι πολύ υψηλό) για το κάθε τύπο επιχειρησιακού αντίκτυπου (π.χ. απώλειες σε τζίρο, νομικές κυρώσεις κλπ.). Αυτή είναι και η δομή της φόρμας που θα αποτυπωθεί η εκτίμηση επιχειρησιακού αντίκτυπου στην XBANK.

Υπο εξέταση ιδιότητα της πληροφορίας (διαθεσιμότητα, ακεραιότητα, εμπιστευτικότητα)

Το μέγιστο επίδο επιχειρησιακού αντίκτυπου που είναι πιθανό να προκύψει

Ιδιότητα της πληροφορίας		Κατάλληλο μέτρο αντιμετώπισης	Επίπεδο Επιχειρησιακού αντίκτυπου				
#	Τύπος Επιχειρησιακού Αντίκτυπου		A Πολύ Υψηλό	B Υψηλό	C Μεσαίο	D Χαμηλό	E Πολύ Χαμηλό
Οικονομικές Επιπτώσεις							
F1	Απώλειες σε τζίρο και ευκαιρίες αύξησης πωλήσεων	Οικονομικές Συνέπειες	20%+	11% to 20%	6% to 10%	1% to 5%	Λιγότερο από 1%
F2	Ενσώματα περιουσιακά στοιχεία	Οικονομικές Συνέπειες	$20 εκ. +	$1εκ. με $20εκ	$100 χιλ με $1εκ.	$10χιλ. με $100K	Λιγότερο από $10K
F3	Κυρώσεις/ Νομικές συνέπειες (π.χ. παράβαση νομικών διατάξεων)	Οικονομικές Συνέπειες	$20 εκ. +	$1εκ. με $20εκ	$100 χιλ με $1εκ.	$10χιλ. με $100K	Λιγότερο από $10K
F4	Απρόβλεπτα Κόστη (Κόστος επανάκαμψης)	Οικονομικές Συνέπειες	$20 εκ. +	$1εκ. με $20εκ	$100 χιλ με $1εκ.	$10χιλ. με $100K	Λιγότερο από $10K
F5	Υποτίμηση μετοχών	Απώλεια μετοχικής αξίας	20%+	11% to 20%	6% to 10%	1% to 5%	Λιγότερο από 1%

IRAM 2: Πίνακας αναφοράς επιχειρησιακού αντίκτυπου

4.2.2 Εκτίμηση Απειλών και Ευπαθειών (Threat & Vulnerability Assessment)

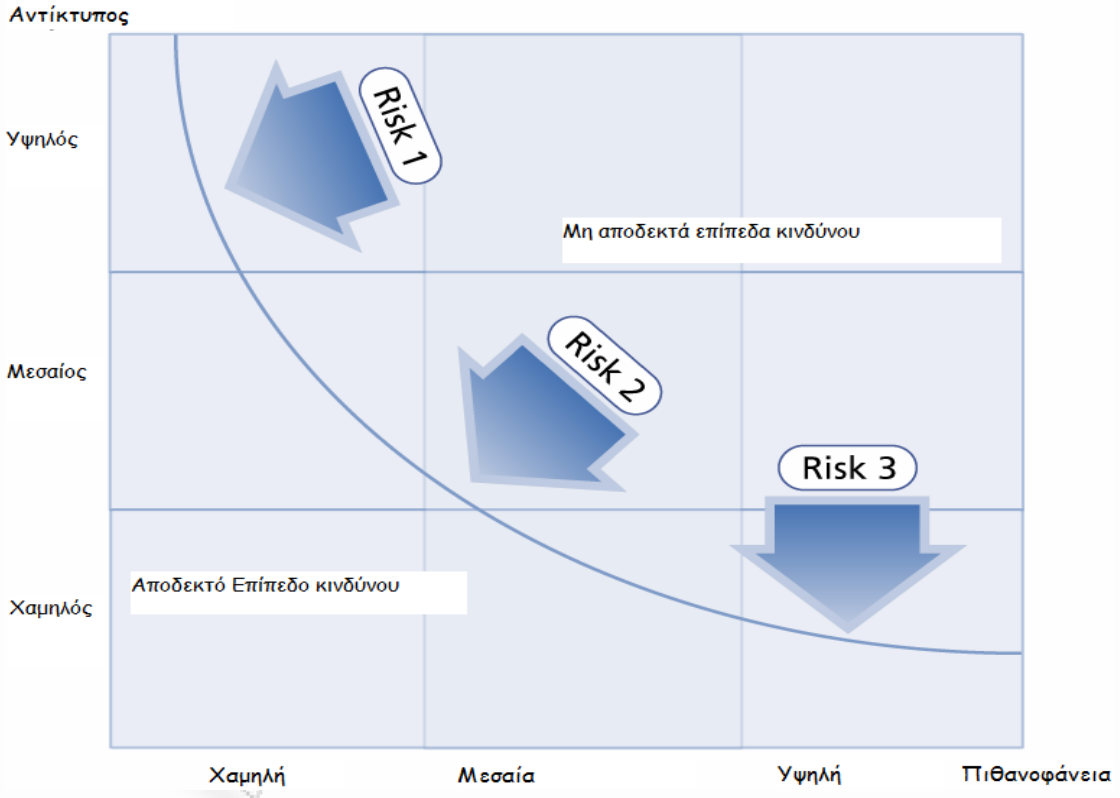
Η άσκηση της εκτίμησης απειλών και ευπαθειών χρησιμοποιείται σαν μέθοδος για τον προσδιορισμό της πιθανότητας συμβάντων ασφαλείας στο σύστημα υπο αξιολήγηση. Σαν δεύτερο μέρος στην εκτίμηση και αξιολόγηση της επικινδυνότητας μέσω της Μεθοδολογίας Ανάλυσης Επικινδυνότητας (IRAM) σχεδιάστηκε για την ανάλυση του κινδύνου στα πληροφοριακά συστήματα (π.χ. επιχειρησιακά πακέτα και εφαρμογές, συστήματα διαχείρησης παραγγελιοληψίας, συστήματα διαχείρισης παραγωγής κλπ.). Δεν μπορεί να χρησιμοποιηθεί όμως στην εκτίμηση απειλών και ευπαθειών σε άλλα περιβάλλοντα όπως κέντρα συστημάτων (data centers) και δίκτυα (networks) παρόλο που η συνολική προσέγγιση μπορεί να είναι εν μέρει εφορμόσιμη.

Η άσκηση αυτή, μετά από τις επιπτώσεις που αναλύθηκαν σε επίπεδο οργανισμού (επιχειρησιακό) και διαδικασιών από τυχόν συμβάντα στο σύστημα ηλεκτρονικής τραπεζικής, βοηθάει στην αναγνώριση των πιο λεπτομερών απαιτήσεων ασφαλείας ενός συστήματος και στο καθορισμό των απαιτούμενων βημάτων στα μετέπειτα στάδια για τη προστασία της πληροφορίας που φέρει το σύστημα. Μετά από αυτό το στάδιο γίνεται και πιο εύκολη και πιο αποτελεσματική η διαδικασία αναγνώρισης των απαραίτητων μέτρων ασφάλειας (σημείων ελέγχου) που είναι το τρίτο και τελευταίο μέρος της Μεθοδολογίας Ανάλυσης Επικινδυνότητας (IRAM), έτσι ώστε να υπάρχει ένα ολοκληρωμένο πλαίσιο για την ελαχιστοποίηση της συχνότητας και τις επιπτώσεις από τυχόν καταστροφικά συμβάντα ασφάλειας στο σύστημα ηλεκτρονικής τραπεζικής. Η άσκηση ευτή έχει βέβαια πιο τεχνική κατεύθυνση από την Εκτίμηση του Επιχειρησιακού Αντίκτυπου και βοηθά στον καθορισμό πιο στοχευμένων μέτρων ασφάλειας στο τεχνολογικό εξοπλισμό και την εφορμαγή.

Ένας από τους κύριους στόχους της ανάλυσης κινδύνου στην ροή της πληροφορίας είναι να διευκολύνει τους αναλυτές στην επιλογή των πιο κατάλληλων μέτρων για να ελαχιστοποιηθεί η πιθανότητα συμβάντων καταστροφικών για το σύστημα υπο αξιολόγηση. Ένα συμβάν ασφαλείας μπορεί να επέλθει όταν μια απειλή (π.χ. κακόβουλος χρήστης ή hacker) εκμεταλλεύεται μια γνωστή αδυναμία ή αδυναμίες στα ήδη υπάρχοντα μέτρα ασφάλειας (π.χ. μη ενημερωμένο λογισμικό με τις τελευταίες ενημερώσεις ασφάλειας στο web server) και

παραβιάζει την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα της πληροφορίας (πιο πιθανό σε σύστημα που υποστηρίζει κάποιες από τις επιχειρησιακές διαδικασίες, εδώ το σύστημα ηλεκτρονικής τραπεζικής). Για να καταστεί λοιπόν εφικτή η επιλογή κατάλληλων μέτρων ασφάλειας, είναι απαραίτητο να κατανοήσουμε τις **απειλές** (threats) στις οποίες το σύστημα ηλεκτρονικής τραπεζικής μπορεί να είναι εκτεθειμένο και τις εγγενείς αδυναμίες (inherent vulnerabilities) του συστήματος σε αυτές τις απειλές.

Με μια προσεκτική εξέταση των διάφορων απειλών και ευπαθειών που σχετίζονται με το υπο εξέταση σύστημα είμαστε σε θέση να αποκομίσουμε μια πιο ξεκάθαρη εικόνα της **πιθανοφάνειας** (likelihood) συγκεκριμένων συμβάντων ασφαλείας. Σε αυτό το σημείο θα ήταν απαραίτητη μια επεξήγηση του όρου πιθανοφάνεια. Όταν το επίπεδο απειλής είναι υψηλό (π.χ. επίθεση με ιούς στο πληροφοριακό σύστημα) και ο βαθμός αδυναμίας είναι επίσης υψηλός (π.χ. ένα μη συστηματικά και επιμελώς συντηρημένο αντιϊκό λογισμικό) τότε η πιθανότητα του συμβάντος ασφάλειας είναι μεγάλη (δηλαδή μόλυνση των συστημάτων από ιό). Εφορμόζοντας λοιπόν ένα σύστημα για το καθορισμό και την διαβάθμιση της πιθανοφάνειας για τα πιθανά συμβάντα ασφάλειας, καθιστά τον αναλυτή ικανό να επικεντρωθεί στην αντιμετώπιση των κύριων απειλών. Έχοντας λοιπόν τα αποτελέσματα και τη πληροφορία από την άσκηση αυτή σε συνδυασμό με την πληροφορία από τον πιθανό επιχειρησιακό αντίκτυπο που μπορεί να ανακύψει (όπως τα αποτελέσματα που εξάγαμε από την πρώτη φάση – Αποτίμηση Επιχειρησιακού Ανίκτυπου – της Ανάλυσης Επικινδυνότητας), είναι πλέον δυνατή η αναγνώριση συγκεκριμένων **πληροφοριακών κινδύνων** (information risks) στη ροή της πληροφορίας στο σύστημα ηλεκτρονικής τραπεζικής που πρέπει να αντιμετωπιστούν και να ληφθούν άμεσα υπόψη. Ο κίνδυνος σε ένα πληροφοριακό σύστημα να υποστεί ένα σοβαρό συμβάν ασφάλειας ως προς τη φέρουσα πληροφορία αυξάνεται όταν η πιθανότητα που μετρήθηκε είναι υψηλή και ο πιθανός αντίκτυπος είναι εξίσου υψηλός. Στο παρακάτω διάγραμμα αποτυπώνεται η συσχέτιση των δυο μεγεθών.



IRAM 3: Χρήση του επιχειρησιακού αντίκτυπου και της πιθανοφάνειας για την αναγνώριση κινδύνων. Πηγή: ISF.

Στο παραπάνω διάγραμμα αποτυπώνονται και οι ζώνες του αποδεκτού ή μη επιπέδου κινδύνου, έτσι ώστε καθίσταται πιο εύκολο να καθοριστεί αν κάποια επιπλέον ενέργεια πρέπει

να γίνει (π.χ. υλοποίηση πιο αυστηρών μέτρων ή ελέγχων ασφάλειας). Η γραμμή που οριοθετεί το αποδεκτό από το μη αποδεκτό επίπεδο κινδύνου αντιπροσωπεύει το ελάχιστα αποδεκτό επίπεδο κινδύνου για τον οργανισμό. Έτσι, ακολουθώντας τα παραπάνω βήματα μεθοδικά, ο αναλυτής μπορεί πιο εύκολα να αναγνωρίσει με λεπτομέρια τις απαιτήσεις ασφάλειας με σκοπό να μετριαστεί το επίπεδο κινδύνου και να διεξαχθεί συνεπώς αποτελεσματικά η επόμενη φάση Ανάλυσης Επικινδυνότητας που είναι η επιλογή των κατάλληλων σημείων ελέγχου στο IRAM (Controls Selection).

4.2.3 Επιλογή Σημείων Ελέγχου (Controls Selection)

Η Επιλογή Σημείων ελέγχου είναι μια προσέγγιση για την αναγνώριση, αξιολόγηση και επιλογή σημείων ελέγχου με απώτερο σκοπό την ασφάλεια της πληροφορίας, για να μετριάσουμε το επίπεδο κινδύνου σε ένα πληροφοριακό σύστημα. Η διαδικασία αυτή εξυπηρετεί στην προδιαγραφή συγκεκριμένων απαιτήσεων σε ελεγκτικές διαδικασίες γύρω από μια εφαρμογή και στο καθορισμό των κατάλληλων ενεργειών σε επόμενο στάδιο έτσι ώστε να εξασφαλίσουμε όσο το δυνατόν την πληροφορία που φέρει το εκάστοτε πακέτο (πληροφοριακό σύστημα). Είναι η τρίτη και τελευταία φάση στη συνολική διαδικασία ανάλυσης και αποτίμησης της επικινδυνότητας στη ροή της πληροφορίας. Σε αυτή τη φάση ο στόχος είναι να ελαχιστοποιηθεί η συχνότητα και το μέγεθος του αντίκτυπου από καταστροφικά περιστατικά ασφαλείας.

Η επιλογή κατάλληλων σημείων ελέγχου είναι μια διαδικασία η οποία χρειάζεται τεχνική κατάρτιση που μας εξασφαλίζει στο οτι όλες οι απαιτήσεις σε ελεγκτικές διαδικασίες έχουν περάσει από αξιολόγηση και έχουν επίσημα παρουσιαστεί στη διοίκηση προς έγκριση. Όπως προειπώθηκε τελικός στόχος είναι να μειωθεί η πιθανοφάνεια, δηλαδή η πιθανότητα περιστατικών ασφάλειας. Παρόλα αυτά η διαδικασία επιλογής ελεγκτικών μηχανισμών για τη μείωση του επιπέδου κινδύνου είναι αρκετά περίπλοκη διαδικασία και απαιτεί επαρκής κατανόηση και γνώση για τις ήδη υπάρχουσες ελεγκτικές διαδικασίες που θα μπορούσαν να καλύψουν μια από τις απαιτήσεις, πως αυτές λειτουργούν και πόσο αποτελεσματικές είναι για το συγκεκριμένο σύστημα που υπόκειται στην ανάλυση επικινδυνότητας.

Όλο και περισσότερο, φυσικά αυτό που απασχολεί τους οργανισμούς είναι και η αποτελεσματικότητα των ελεγκτικών μηχανισμών. Συνεπώς, άλλοι παράγοντες που θα πρέπει να ληφθούν υπόψη σε μια τέτοια διαδικασία είναι οι εξής:

- Κόστος υλοποίησης ελεγκτικών μηχανισμών
- Χρόνος και πόροι (χρηματικοί και μη) για την υλοποίησή τους
- Πόροι για τη συντήρηση αυτών, δηλαδή επιπλέον πόροι και περισσότερο ανθρώπινοι πόροι που να επιβεβαιώνουν οτι οι ελεγκτικοί μηχανισμοί λειτουργούν σύμφωνα με τα αρχικά σχέδια και λειτουργούν αποτελεσματικά ως προς το σκοπό που έχουν υλοποιηθεί
- Χρήση των ελεγκτικών μηχανισμών για την ελαχιστοποίηση και άλλων κατηγοριών κινδύνου
- Η εξυπηρέτηση των ελεγκτικών διαδικασιών που εφαρμόζονται και σε απαιτήσεις συμμόρφωσης με νομικές απαιτήσεις και άλλα ρυθμιστικά πλαίσια (π.χ. στο τραπεζικό κλάδο με το πλαίσιο για τις ηλεκτρονικές πληρωμές που εξυπηρετεί το πρότυπο που αναλύθηκε σε προηγούμενο κεφάλαιο PCI DSS)

Για να γίνει λοιπόν σωστή επιλογή στα σημεία ελέγχου θα πρέπει να έχουν αποτιμηθεί επαρκώς όλες οι πιθανές απειλές που το σύστημα είναι πιθανό να δεχθεί, τις εγγενείς ευπάθειες του συστήματος σε αυτές τις απειλές και τον πιθανό επιχειρησιακό αντίκτυπο. Την εργασία δηλαδή που προηγήθηκε στις δύο προηγούμενες φάσεις της άσκησης αποτίμησης επικινδυνότητας για την συγκεκριμένη μελέτη περίπτωσης που διεξάγεται στα πλαίσια αυτής της εργασίας.

Η επιλογή των κατάλληλων ελεγκτικών μηχανισμών (σαν μέρος της συνολικής αποτίμησης της επικινδυνότητας) θα πρέπει να διεξάγεται κατα τη διάρκεια ανάπτυξης του εκάστοτε συστήματος υπο εξέταση. Άλλωστε έχοντας προσδιορίσει ποιές είναι οι απαιτήσεις σε ελεγκτικούς μηχανισμούς σε αυτό το προγενέστερο στάδιο θα είναι σίγουρα πιο αποτελεσματικό κυρίως από πλευράς οικονομικών πόρων από οτι στο στάδιο που το σύστημα είναι πλήρως λειτουργικό, όπως και στη παρούσα μελέτη περίπτωσης του συστήματος ηλεκτρονικής τραπεζικής.

Έχοντας λοιπόν σαν δεδομένο οτι το σύστημα ηλεκτρονικής τραπεζικής είναι ήδη στην παραγωγή, η διαδικασία επιλογής των κατάλληλων σημείων ελέγχου μπορεί να ξεκινήσει υποθέτοντας πάντα οτι όλοι οι συμμετέχοντας στη διαδικασία έχουν πλήρη αντίληψη των κινδύνων και της αποτίμησης αυτών που έγινε σε προηγούμενη φάση καθώς επίσης και της αποτίμησης επιχειρησιακού αντίκτυπου που περιγράψαμε στη πρώτη φάση της παρούσας μελέτης.

Η επιλογή των σημείων ελέγχου υποστηρίζεται από ένα αυτοματοποιημένο εργαλείο του ISF το λεγόμενο IRAM Control Solution Assistant. Το εργαλείο αυτό αποτελείται από ένα σύνολο φορμών και αναφορών που η μια διαδέχεται την άλλη και τα αποτελέσματα από τη κάθε μια είναι εισροή για την εξαγωγή των συμπερασμάτων στην επόμενη. Κατά σειρά οι φόρμες/ αναφορές και ουσιαστικά τα στάδια αυτής της φάσης αποτελούνται από τα εξής:

- Κατασκευή της βάσης δεδομένων από ελγκτικούς μηχανισμούς και σημεία ελέγχου
- Προσδιορισμός των κύριων πληροφοριακών κινδύνων στους οποίους υπόκειται το σύστημα υπο αξιολόγηση
- Προσδιορισμός και αναγνώριση σημείων ελέγχου για την κάλυψη ή ελαχιστοποίηση του επιπέδου του εκάστοτε κινδύνου που έχουν αναγνωριστεί σε προηγούμενο στάδιο της ανάλυσης επικινδυνότητας και έχουν ενσωματωθεί στο προηγούμενο βήμα αυτής της φάσης
- Επιλογή των καταλληλότερων σημείων ελέγχου
- Σχεδιασμός και προγραμματισμός των απαραίτητων ενεργειών για την υλοποίηση των επιλεγμένων σημείων ελέγχου
- Τελικές αναφορές

4.3 Σκοπός και εύρος ανάλυσης και ελέγχου στην XBANK

Σκοπός της παρούσας ανάλυσης είναι η εξέταση των ήδη υπαρχόντων δικλείδων ασφάλειας / σημείων ελέγχου που διασφαλίζουν την επαρκή και ασφαλή λειτουργία των Πληροφοριακών Συστημάτων της Τράπεζας XBANK και η υλοποίηση επιπλέον πρακτικών ελέγχου με στόχο την υλοποίηση ενός ολοκληρωμένου συστήματος ασφάλειας των πληροφοριών. Ο έλεγχος αφορά μόνο τα Πληροφοριακά Συστήματα της Τράπεζας και επικεντρώθηκε κυρίως στην εφαρμογή ηλεκτρονικής τραπεζικής (e-banking).

Οι κύριες ενότητες που επικεντρώνονται τα σημεία έλεγχου στα πλαίσια αυτής της μελέτης και της βάσης σημείων ελέγχου του IRAM είναι:

α) Οργάνωση και Διοίκηση Πληροφορικής

Περιλαμβάνονται τα σημεία ελέγχου που συντελούν στη ευρύτερη διακυβέρνηση της Πληροφορικής.

β) Προμήθεια, Ανάπτυξη και Διαχείριση αλλαγών Πληροφοριακών Συστημάτων

Περιλαμβάνονται τα σημεία ελέγχου που διασφαλίζουν ότι τα Πληροφοριακά Συστήματα της Τράπεζας προμηθεύονται, αναπτύσσονται, παραμετροποιούνται και συντηρούνται μέσω συγκεκριμένων διαδικασιών που αποσκοπούν στην επίτευξη των αντικειμενικών στόχων της διοίκησης.

γ) Ασφάλεια Πληροφοριακών Συστημάτων

Περιλαμβάνονται τα κύρια σημεία ελέγχου που διασφαλίζουν την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα της πληροφορίας.

δ) Λειτουργία και Υποστήριξη Πληροφοριακών Συστημάτων

Περιλαμβάνονται τα σημεία ελέγχου που διασφαλίζουν ότι τα παραγωγικά συστήματα της Τράπεζας επεξεργάζονται ολοκληρωμένα και με ακρίβεια τα δεδομένα σε συνάρτηση πάντοτε με τους αντικειμενικούς σκοπούς της διοίκησης και τις ανάγκες της Τράπεζας. Επίσης διασφαλίζουν ότι τυχόν προβλήματα αναγνωρίζονται έγκαιρα και επιλύονται πλήρως και με ακρίβεια με σκοπό την ορθή συντήρηση της πληροφορίας.

Για την συλλογή της πληροφορίας που χρησιμοποιήθηκε στο IRAM η προσέγγισή μας περιέλαβε:

- Αποστολή και συμπλήρωση σχετικών ερωτηματολογίων με σκοπό την κατανόηση της υπάρχουσας κατάστασης στην πληροφορική.

- Πραγματοποίηση σειράς συνεντεύξεων με εργαζομένους της τράπεζας κυρίως του Τομέα Πληροφοριακών Συστημάτων και της Διεύθυνσης Ασφάλειας Πληροφοριακών Συστημάτων αλλά και των υπολοίπων επιχειρησιακών διευθύνσεων.
- Επιλογή δείγματος και εξέταση κατά πόσο ακολουθούνται οι διαδικασίες και οι πολιτικές που έχουν επίσημα εγκριθεί.
- Χρήση ειδικών προγραμμάτων ελέγχου κυρίως για Λειτουργικά Συστήματα και Βάσεις Δεδομένων.
- Χρήση αυτοματοποιημένων εργαλείων ελέγχου.
- Επιτόπιους ελέγχους σε καταστήματα της Τράπεζας.
- Εξέταση της σχετικής τεκμηρίωσης του ελέγχου όπου αυτή ήταν διαθέσιμη.

4.4 Εξέταση, αποτίμηση και υλοποίηση σημείων ελέγχου στην XBANK με τη χρήση του IRAM

Στις επόμενες τρείς παραγράφους περιγράφεται λεπτομερώς η άσκηση που διενεργήθηκε στον τραπεζικό οργανισμό XBANK με τη χρήση της μεθόδου και εργαλείου IRAM. Κάθε παράγραφος αντιστοιχεί και σε μια φάση της συνολικής άσκησης. Στιγμιότυπα από την ανάλυση παρουσιάζονται με εκτυπώσεις οθόνης (Screen Shots) καθώς επίσης και τα αποτελέσματα κάθε φάσης ή μερος αυτών όπου δεν ήταν δυνατή η συνολική παρουσίαση αυτών.

4.4.1 Φάση 1η: Ανάλυση επιχειρησιακού αντίκτυπου στην XBANK

Αρχικά καθορίστηκε από τον κατάλογο απογραφής των συστημάτων της τράπεζας το σύστημα με τη μεγαλύτερη σημαντικότητα για τον οργανισμό, δηλαδή το σύστημα ηλεκτρονικής τραπεζικής, με βάσει τα παρακάτω κριτήρια:

- Σημαντικότητα του συστήματος στα ανώτερα κλιμάκια της Διοίκησης.
- Ιστορικότητα σε περιστατικά ασφαλείας (π.χ. ένα σύστημα που έχει υποστεί πολλά περιστατικά επιδέχεται μεγαλύτερης προσοχής).
- Παροχή οδηγειών από το τμήμα εσωτερικού ελέγχου του οργανισμού.
- Προτεινόμενες ενέργειες από τον επιχειρησιακό τομέα και τους ειδικούς στα Πληροφοριακά συστήματα της τράπεζας.

Με βάση αυτά τα κριτήρια, δύο ήταν τα πιο σημαντικά συστήματα. Το σύστημα διαχείρισης πελατών και το σύστημα ηλεκτρονικής τραπεζικής (e-banking). Ενώ η επιλογή με βάση όλους τους παραπάνω παράγοντες έχει τα πλεονεκτήματά της, συνιστάται και επιλέχθηκε μια πιο αντικειμενική προσέγγιση που βασίζεται στη χρήση του «εργαλείου» εκτίμησης κρισιμότητας Information Risk Scorecard της μεθοδολογίας του ISF. Αυτή η γρήγορη και εύκολη στη χρήση, προσέγγιση μας παρείχε μια πιο υψηλού επιπέδου άποψη των απαιτήσεων του συστήματος σε εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα της πληροφορίας που πρέπει να προσδιοριστούν και διευκόλυνε τη συγκρισιμότητα ως προς το επίπεδο σημαντικότητας. Για να προσδιοριστεί σε ποιό από τα δυο συστήματα θα διεξαχθεί η Ανάλυση του Επιχειρησιακού Αντίκτυπου, απαντήθηκαν οι εξής ερωτήσεις που προσδιορίζουν τη κρισιμότητα του εκάστοτε συστήματος:

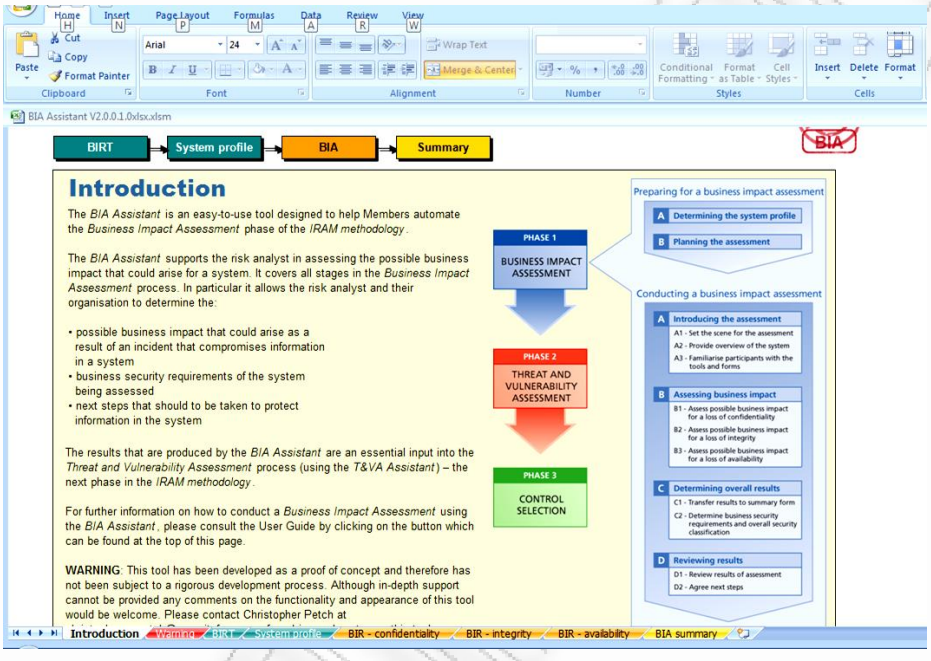
Ποιο είναι το μέγιστο επίπεδο των βλαβών που η επιχείρηση θα μπορούσε να υποστεί όταν οι βασικές πληροφορίες που περιέχονται, επεξεργάζονται ή διαβιβάζονται από την δεδομένη πηγή δεδομένων, τυχαία ή σκόπιμα:

- Γνωστοποιούνταν σε λάθος ανρώπους (Απώλεια επμπιστευτικότητας)
- Ψευδεπιγράφονταν ή αλλοιώνονταν (Απώλεια ακεραιότητας)
- Καθίσταντο μη διαθέσιμη για
    - Λιγότερο από μια ώρα (Απώλεια Διαθεσιμότητας)
    - Μισή μέρα
    - Μια μέρα
    - 2-3 μέρες
    - Μια εβδομάδα
    - Ένα μήνα

Και για τα δύο συστήματα το εύρος των απαντήσεων ήταν από ελάχιστη έκταση βλαβών μέχρι, εξαιρετικά σοβαρές βλάβες. Σε όλες τις περιπτώσεις ο οργανισμός XBANK θα υφίσταντο μεγαλύτερες βλάβες από το σύστημα ηλεκτρονικής τραπεζικής. Συνεπώς, η ανάλυση επικινδυνότητας επιχειρήθηκε στο σύστημα ηλεκτρονικής τραπεζικής.

Ο βασικός στόχος της προσέγγισης του ISF στην ανάλυση επιχειρησιακού αντίκτυπου είναι να καθορίσει τις επιχειρησιακές/ τραπεζικές απαιτήσεις ασφαλείας ως προς το σύστημα ηλεκτρονικής τραπεζικής και να προσδιορίσει τις επόμενες ενέργειες που πρέπει να γίνουν για την επαρκή προστασία των πληροφοριών σε αυτό το σύστημα.

Οι στόχοι αυτοί επιτυγχάνονται με την αξιολόγηση του επιχειρησιακού αντίκτυπου ως αποτέλεσμα της παραβίασης της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των πληροφοριών. Πριν λοιπόν ξεκινήσει η διεξαγωγή της ανάλυσης, ένα από τα βήματα που πραγματοποιήθηκαν είναι ο καθορισμός και η περιγραφή του προφίλ του συστήματος υπο ανάλυση όπως και απαιτείται από τα βήματα του IRAM. Στην εικόνα παρακάτω αποτυπώνεται η αρχική οθόνη εισαγωγής του IRAM που κάνει μια υψηλού επιπέδου εισαγωγή στην διαδικασία ανάλυσης του επιχειρησιακού αντίκτυπου (BIA).



IRAM 4: Συνοπτική παρουσίαση της διαδικασίας BIA

Προφίλ συστήματος ηλεκτρονικής τραπεζικής

Παρακάτω καταγράψαμε κάποιες πληροφορίες στο IRAM σχετικά με το σύστημα υπό ανάλυση, όπως το όνομα του ιδιοκτήτη συστήματος στη τράπεζα (Γ. Παπαδόπουλος), τον αριθμό των συναλλαγών κατα μέσο όρο (5.000 – 10.000), τον αριθμό των χρηστών (5 εσωτερικοί και 500.000 εξωτερικοί), τις πλατφόρμες πάνω στις οποίες αναπτύχθηκε η εφαρμογή (κεντρικός server Windows 2000 και η βάση SQL Server 2000). Οι πληροφορίες αυτές συλλέχθηκαν μετά από συνεντεύξεις με τον ιδιοκτήτη του συστήματος και τους διαχειριστές της εφαρμογής στη διεύθυνση μηχανοργάνωσης της τράπεζας. Στο πίνακα που ακολουθεί φαίνεται μέρος από τη καταγεγραμμένη πληροφορία όπως αποτυπώθηκε στο εργαλείο IRAM.

System Profile	
General	
Application/system	E-Banking application

name	
System owner	G. Papadopoulos
Business unit	IT department
Status (eg development, live)	live
Age	2 years
Key contacts	
Type of stream	
Main business function (eg funds transfer, sales order processing, accounting)	Bank transactions processing
Description of system	The e-banking system allows customers to conduct financial transactions on a secure website operated by their retail bank.
Scope of the system (eg whole organisation, single business unit, department)	Whole organisation
Business contribution	
Importance of the system to the business	Low [ ] Medium [ ] High [√]

Contribution of the system to key business objectives *(H – High, M – Medium, L – Low)*	Financial targets	L	Operational efficiency	H	Customer satisfaction	H	Employee satisfaction	M
Technical information								
Origin of system (eg in-house)	Third party application with internal support							
Network type	Internet	√	Intranet		Extranet		Other	
Number of platforms	Mainframes		Severs (eg UNIX, Windows 2003)	√	Workstations (eg Windows XP)			
System management	Internal	√	Outsourced					

IRAM 5: Παρουσίαση προφίλ συστήματος ηλεκτρονικής τραπεζικής

Στο σύστημα ηλεκτρονικής τραπεζικής (ή e-banking), κάθε χρήστης με έναν προσωπικό υπολογιστή και ένα πρόγραμμα περιήγησης μπορεί να συνδεθεί με την την ιστοσελίδα της τράπεζάς του για να εκτελέσει οποιαδήποτε από τις διαθέσιμες ηλεκτρονικά τραπεζικές λειτουργίες. Το ηλεκτρονικό τραπεζικό σύστημα έχει μια 'web-enabled' κεντρική βάση δεδομένων και όλες οι υπηρεσίες που η τράπεζα έχει επιτρέψει να εμφανίζονται διαδικτυακά εμφανίζονται στο μενού της ιστοσελίδας. Ανάλογα με το βαθμό πρόσβασης που δίνει η XBANK στους πελάτες της το ηλεκτρονικό τραπεζικό σύστημα μπορεί να λειτουργήσει με τους δύο παρακάτω τρόπους:

1. Σύστημα μεταφοράς ηλεκτρονικών δεδομένων

Το σύστημα παρέχει στον πελάτη συγκεκριμένες πληροφορίες είτε με τη μορφή των υπολοίπων των λογαριασμών, στοιχεία της συναλλαγής, είτε και την κατάσταση ή κίνηση των λογαριασμών. Οι πληροφορίες σε αυτή τη περίπτωση στο μεγαλύτερο βαθμό είναι «μόνο για ανάγνωση" με την έννοια οτι ο πελάτης δεν μπορεί να κάνει συναλλαγές. Η αναγνώριση και επαλήθευση ταυτότητας του πελάτη γίνεται μέσω κωδικού πρόσβασης. Οι πληροφορίες που προσκομίζονται από την εφαρμογή του συστήματος της είναι μέσω batch. Οι εφαρμογές του τραπεζικού συστήματος δεν είναι προσβάσιμες απευθείας μέσω του διαδικτύου.

2. Πλήρες ηλεκτρονικό σύστημα συναλλαγών

Αυτό το σύστημα επιτρέπει αμφίδρομες δυνατότητες. Οι συναλλαγές μπορούν να υποβάλλονται από τον πελάτη για online ενημέρωση. Αυτό το σύστημα βέβαια απαιτεί υψηλότερο βαθμό ασφάλειας και ελέγχου αφού θέτει τις επιχειρησιακές λειτουργίες της τράπεζας σε υψηλότερο κίνδυνο. Σε αυτό το περιβάλλον, ο web server και οι εφαρμογές συνδέονται μέσω πιο ασφαλών υποδομών. Περιλαμβάνει την τεχνολογία πληροφορικής που καλύπτει τη δικτύωση και την ασφάλεια, τις διατραπεζικές πύλες πληρωμής και τη νομική υποδομή.

Η XBANK χρησιμοποιεί και τους δυο παραπάνω τρόπους, ακόμα ένα γεγονός που καθιστά απαραίτητη την ανάλυση επιχειρησιακού αντίκτυπου στο σύστημα ηλεκτρονικής τραπεζικής.

Ανάλυση επιχειρησιακού Αντίκτυπου

Σε αυτό το στάδιο θα γίνει η αξιολόγηση του επιχειρησιακού αντίκτυπου με βάση τα τρία σενάρια απώλειας μιας ιδιότητας της πληροφορίας (εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα). Για παράδειγμα, ποιές θα είναι οι επιπτώσεις στην επιχειρησιακή/ τραπεζική δραστηριότητα αν το σύστημα ηλεκτρονικής τραπεζικής δεχθεί επίθεση από κακόβουλους χρήστες και υποκλέψουν δεδομένα (σε αυτή τη περίπτωση απώλειας της εμπιστευτικότητας της πληροφορίας και ίσως και ακεραιότητας της πληροφορίας αν παραποιηθούν δεδομένα). Κατά την αξιολόγηση και μέτρηση του επιχειρησιακού αντίκτυπου οι συμμετέχοντες κλήθηκαν να ακολουθήσουν τα ακόλουθα βήματα ως προς τον πίνακα αναφοράς επιχειρησιακού αντίκτυπου (βλ. Πίνακα IRAM No2) που παρατέθηκε προηγουμένως στην εισαγωγή της παρούσας ανάλυσης:

- ✓ Εξέταση του είδους/ τύπου του αντίκτυπου στην επιχειρησιακή δραστηριότητα
- ✓ Καθορισμός της χείριστης και πιο σοβαρής επίπτωσης που θα μπορούσε να προκύψει
- ✓ Ομόφωνη απόφαση από όλη την ομάδα εργασίας (workgroup) ως προς το επίπεδο του αντίκτυπου που τελικά θα καταγραφεί στην εκάστοτε περίπτωση.
- ✓ Στην αξιολόγηση του επιχειρησιακού αντίκτυπου για απώλεια της διαθεσιμότητας, το επίπεδο του αντίκτυπου θα πρέπει να καταγραφεί για όλες τις περιπτώσεις που μπορεί να διαρκέσει η απώλεια της διαθεσιμότητας του συστήματος (μια ώρα, μια μέρα, 2-3 μέρες, μια βδομάδα ή ένα μήνα).
- ✓ Για διαβαθμίσεις επιπέδου «υψηλού» ή/και πολύ υψηλού παρατίθεται πάντα επεξήγηση.

Μετά από την αξιολόγηση όλων των τύπων επιχειρησιακού αντίκτυπου (π.χ. απώλειες τζίρου, μείωση πωλήσεων κλπ), βγαίνει αυτόματα και συνολικά ο ελάχιστος βαθμός αρνητικών επιπτώσεων που θα μπορούσαν να προκύψουν στις επιχειρησιακές διαδικασίες και την τραπεζική δραστηριότητα και λειτουργίες γενικότερα.

Στον παρακάτω πίνακα αποτυπώνονται τα αποτελέσματα της ανάλυσης επιχειρησιακού αντίκτυπου στην περίπτωση συμβάντος με απώλεια της εμπιστευτικότητας της πληροφορίας, όπως καταχωρήθηκαν στο εργαλείο IRAM. Η λογική με την οποία εργαστήκαμε είναι η εξής: για το πρώτο τύπο επιχειρησιακού αντίκτυπου και στην κατηγορία οικονομικών επιπτώσεων θεωρήθηκε οτι δεδομένου οτι η τράπεζα είναι εδραιωμένη στο χώρο, η απώλεια σε εμπιστευτικότητα της πληροφορίας με αιτία για παράδειγμα την υποκλοπή δεδομένων θα επιφέρει 11 με 20 τοις εκατό απώλειες σε τζίρο και ευκαιρίες αύξησης πωλήσεων, λόγω της απώλειας εμπιστοσύνης από τους πελάτες. Για το δεύτερο παράγοντα παρόλα αυτά, που είναι οι απώλειες σε ενσώματα περιουσιακά στοιχεία, οι επιπτώσεις μπορεί να είναι της τάξης των 10.000 $ ή και λιγότερο (δηλαδή μηδαμινές) γιατί απώλεια σε εμπιστευτικότητα της πληροφορίας δεν σχετίζεται – ούτε άμεσα ούτε έμμεσα – με απώλειες σε ενσώματα περιουσιακά στοιχεία.

Διαβάθμιση επιχειρησιακού αντίκτυπου - Απώλεια Εμπιστευτικότητας (Business Impact Rating, BIR Confidentiality)

Business Impact Rating
Confidentiality

Ref.	Business impact type *Business impact of unintended or unauthorised disclosure of information (most serious case)*	Business impact rating A-Very high, B-High, C-Medium, D-Low, E-Very low					Explanatory comments
		A	*B*	*C*	*D*	*E*	
Financial							
F1	Loss of sales, orders or contracts	20% +	11% to 20%	6% to 10%	1% to 5%	Less than 1%	Loss of customers trust and loyalty resulting in loss of sales.
			X				
F2	Loss of tangible assets (eg fraud, theft of money, lost interest)	$20m+	$1m to $20m	$100K to $1m	$10K to $100K	Less than $10K	
						X	
F3	Penalties/legal liabilities (eg breach of legal, regulatory or contractual obligations)	$20m+	$1m to $20m	$100K to $1m	$10K to $100K	Less than $10K	Penalties for electronic payments regulations breach and Bank of Greece regulation 2577.
		X					
F4	Unforeseen costs (eg recovery costs)	$20m+	$1m to $20m	$100K to $1m	$10K to $100K	Less than $10K	Remunerations to customers impacted from the incident.
			X				
F5	Depressed share price (eg sudden loss of share value)	25% +	11% to 25%	6% to 10%	1% to 5%	Less than 1%	
				X			
Operational							
O1	Loss of management control (eg impaired decision-making)	Severe loss of control	Serious loss of control	Significant loss of control	Moderate loss of control	Minor loss of control	
				X			
O2	Loss of competitiveness (eg delays in the introduction of new production capabilities)	20% +	11% to 20%	6% to 10%	1% to 5%	Less than 1%	Customers will not be loyal anymore and will prefer other Bank institutions.
		X					
O3	New ventures held up (eg delayed new products or services)	New ventures aborted	New ventures delayed by years	New ventures delayed by months	New ventures delayed by weeks	New ventures delayed by days	Customers will not be loyal anymore
			X				
O4	Breach of operating standards (eg contravention of regulatory standards)	Closure of building or operation	Serious sanctions imposed	Significant sanctions imposed	Moderate sanctions imposed	Minor sanctions imposed	
				X			
Customer-related							
C1	Delayed deliveries to customers or clients (eg failure to meet product delivery deadlines)	Deliveries delayed by 6 months	Deliveries delayed by 3 months	Deliveries delayed by one month	Deliveries delayed by one week	Deliveries delayed by one day	
					X		
C2	Loss of customers or clients (eg customer/client defection to competitors)	25% +	11% to 25%	6% to 10%	1% to 5%	Less than 1%	Customers will not be loyal anymore and will prefer other Bank institutions.
		X					
C3	Loss of confidence by key institutions (eg adverse criticism by investors)	Complete loss of confidence	Serious loss of confidence	Significant loss of confidence	Moderate loss of confidence	Minor loss of confidence	Customers will not be loyal anymore and will prefer other Bank institutions.
		X					
C4	Damage to reputation (eg confidential financial information published in media)	World-wide negative publicity	Continent-wide negative publicity	Nation-wide negative publicity	Local negative publicity	Minor negative publicity	
			X				
Employee-related							
E1	Reduction in staff morale / productivity (eg reduced efficiency)	Complete loss of morale	Serious loss of morale	Significant loss of morale	Moderate loss of morale	Minor loss of morale	
						X	
E2	Injury or death (eg harm to staff)	Multiple loss of life	Loss of life	Serious harm	Moderate harm	Minor harm	
						X	

IRAM 6: Διαβάθμιση επιχειρησιακού αντίκτυπου - Απώλεια Εμπιστευτικότητας

Διαβάθμιση επιχειρησιακού αντίκτυπου - Απώλεια Ακεραιότητας

(BIR - Integrity)

Στην συνέχεια ακολουθεί η παρουσίαση της αντίστοιχης ανάλυσης όταν τυχαίο συμβάν επιφέρει απώλεια στην ακεραιότητα των δεδομένων εξαιτίας της παραποίησης αυτών. Στην περίπτωση αυτή κρίνεται οτι οι οικονιμικές επιπτώσεις θα είναι πολύ υψηλού επιπέδου μιας και το χειρότερο σενάριο είναι η παραποίηση οικομικών δεδομένων, ή η αλλαγή προσωπικών δεδομένων σε συνδυασμό με οικονομικά. Συνεπώς, στη πρώτη περίπτωση επιχειρησιακού αντίκτυπου που είναι οι απώλειες σε τζίρο και πωλήσεις θα έχουμε τη μέγιστη δυνατή διαβάθμιση «Α - πολύ υψηλή» σε πιθανές επιπτώσεις, γιατί όπως και παρατίθεται και στα επεξηγηματικά σχόλια μπορεί να επέλθει και παραποίηση σε δεδομένα συναλλαγών. Αντίστοιχα οι επιπτώσεις θα είναι πολύ υψηλού βαθμού και ως προς τις νομικές κυρώσεις και ως προς τις απαιτήσεις συμμόρφωσης όπως για παράδειγμα τη νομοθεσία για τις ηλεκτρονικές πληρωμές και τη πράξη διοικητή της Τράπεζας της Ελλάδος (2577). Μια παραποίηση ή αλλοίωση όμως στα δεδομένα δεν θα είχε σαν συνέπεια κάποιο θανάσιμο συμβάν. Συνεπώς η διαβάθμιση σε αυτό το τύπο επιχειρησιακού αντίκτυπου είναι η πιο χαμηλή. Ο επόμενος πίνακας είναι η αποτύπωση μέρους της εν λόγω ανάλυσης στο εργαλείο IRAM.

Business Impact Rating

Integrity

Ref.	Business impact type *Business impact of errors in information or of deliberate manipulation of information to perpetrate or conceal fraud (most serious case)*	Business impact rating A-Very high, B-High, C-Medium, D-Low, E-Very low					Explanatory comments
		A	*B*	*C*	*D*	*E*	
Financial							
F1	Loss of sales, orders or contracts	20% +	11% to 20%	6% to 10%	1% to 5%	Less than 1%	Manipulation of transactions information and customers accounts information would seriously impact sales
		X					
F2	Loss of tangible assets (eg fraud, theft of money, lost interest)	$20m+	$1m to $20m	$100K to $1m	$10K to $100K	Less than $10K	Manipulation of information to perpetrate fraud would mean loss of money for the XBANK.
			X				
F3	Penalties/legal liabilities (eg breach of legal, regulatory or contractual obligations)	$20m+	$1m to $20m	$100K to $1m	$10K to $100K	Less than $10K	Penalties for electronic payments regulations breach and Bank of Greece regulation 2577.
		X					
F4	Unforeseen costs (eg recovery costs)	$20m+	$1m to $20m	$100K to $1m	$10K to $100K	Less than $10K	Remuneration to customers, regulatory penalties, investment on maximizing security, standards organizations etc.
			X				
F5	Depressed share price (eg sudden loss of share value)	25% +	11% to 25%	6% to 10%	1% to 5%	Less than 1%	
				X			
Operational							
O1	Loss of management control (eg impaired decision-making)	Severe loss of control	Serious loss of control	Significant loss of control	Moderate loss of control	Minor loss of control	
				X			
O2	Loss of competitiveness (eg delays in the introduction of new production capabilities)	20% +	11% to 20%	6% to 10%	1% to 5%	Less than 1%	Deliberate corruption of information would seriously impact XBANK's fame, sales and consequently its competitiveness.
			X				
O3	New ventures held up (eg delayed new products or services)	New ventures aborted	New ventures delayed by years	New ventures delayed by months	New ventures delayed by weeks	New ventures delayed by days	
				X			
O4	Breach of operating standards (eg contravention of regulatory standards)	Closure of building or operation	Serious sanctions imposed	Significant sanctions imposed	Moderate sanctions imposed	Minor sanctions imposed	
					X		

IRAM 7: Διαβάθμιση επιχειρησιακού αντίκτυπου - Απώλεια Ακεραιότητας

Διαβάθμιση επιχειρησιακού αντίκτυπου - Απώλεια Διαθεσιμότητας (BIR – Availability)

Business Impact Rating
Availability

Ref.	Business impact type *Business impact of a prolonged outage of the system (most serious case)*	Business impact rating A-Very high, B-High, C-Medium, D-Low, E-Very low *Duration of outage*					Explanatory comments
		1 hour	*1 day*	*2-3 days*	*1 week*	*1 month*	
Financial							
F1	Loss of sales, orders or contracts	C	C	C	C	C	Transactions can be performed
F2	Loss of tangible assets (eg fraud, theft of money, lost interest)	B	B	B	B	B	
F3	Penalties/legal liabilities (eg breach of legal, regulatory or contractual obligations)	B	B	B	B	B	
F4	Unforeseen costs (eg recovery costs)	B	B	B	B	B	if the period of outage exceeds 1 week then it would normally mean unforseen costs
F5	Depressed share price (eg sudden loss of share value)	A	A	A	A	A	
Operational							
O1	Loss of management control (eg impaired decision-making)	A	A	A	A	A	
O2	Loss of competitiveness (eg delays in the introduction of new production capabilities)	A	A	A	A	A	
O3	New ventures held up (eg delayed new products or services)	C	C	C	C	C	
O4	Breach of operating standards (eg contravention of regulatory standards)	B	B	B	B	B	
Customer-related							
C1	Delayed deliveries to customers or clients (eg failure to meet product delivery deadlines)	C	C	C	C	C	
C2	Loss of customers or clients (eg customer/client defection to competitors)	B	A	A	A	A	
C3	Loss of confidence by key institutions (eg adverse criticism by investors)	B	B	B	B	B	
C4	Damage to reputation (eg confidential financial information published in media)	C	A	A	A	A	
Employee-related							
E1	Reduction in staff morale / productivity (eg reduced efficiency)	E	E	E	E	E	
E2	Injury or death (eg harm to staff)	E	E	E	E	E	
Overall Rating							
In summary, what is the most serious impact which would arise from an outage of the system? (This would normally be at least as high as the highest individual rating)		1 hour A	1 day A	2-3 days A	1 week A	1 month A	
Overall Critical Timescale							
What is the critical timescale for recovering of this system (ie the timescale beyond which an outage is unacceptable to the business)?		1 hour X	1 day	2-3 days	1 week	1 month	

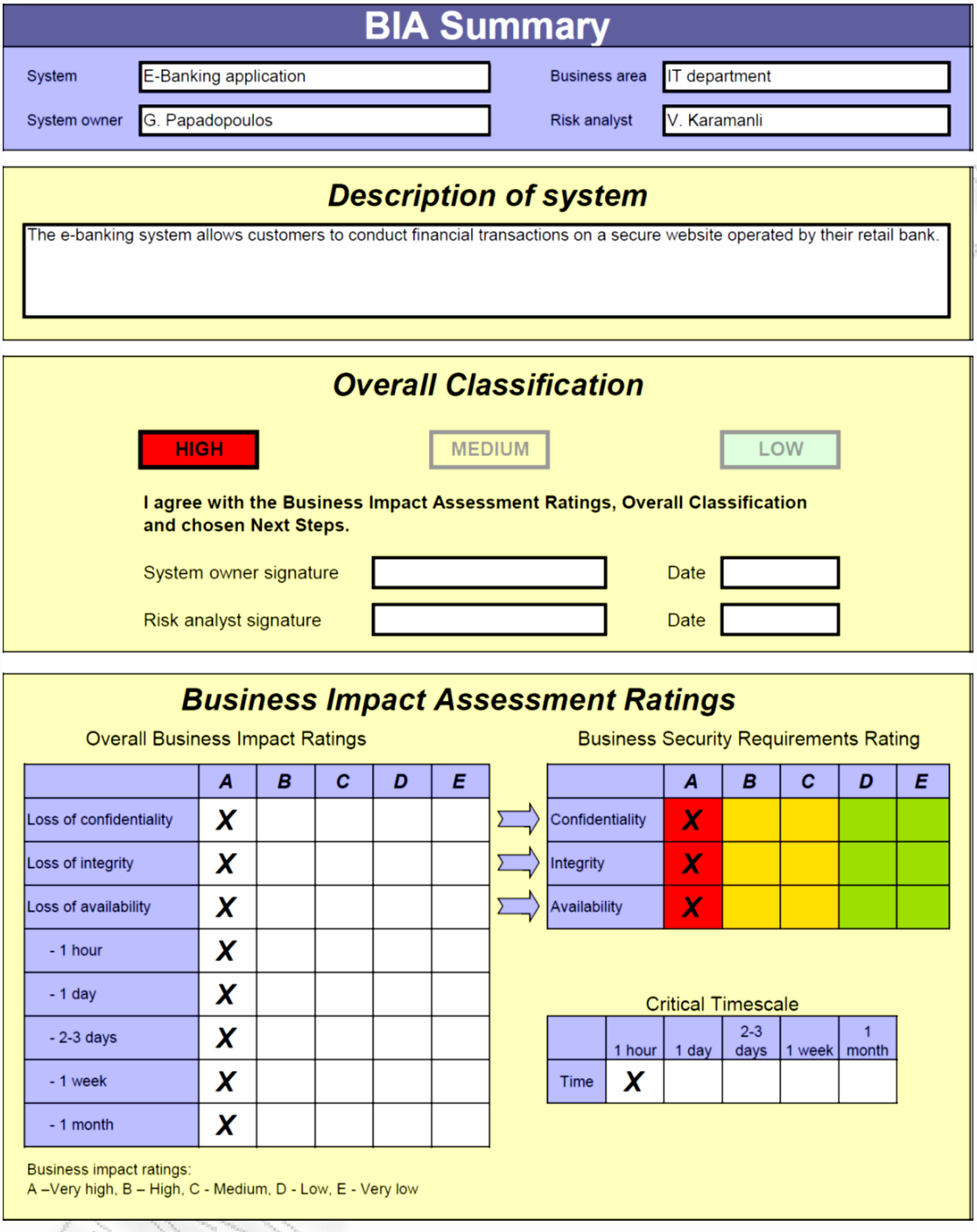
IRAM 8: Διαβάθμιση επιχειρησιακού αντίκτυπου - Απώλεια Διαθεσιμότητας

Στη πιθανότητα ενός συμβάντος που θα επιφέρει απώλεια στην διαθεσιμότητα των συστημάτων και συνεπώς στη διαθεσιμότητα των δεδομένων, των πληροφοριών και των υπηρεσιών, οι

επιπτώσεις θα είναι από αρκετά εως πολύ σοβαρές σε όλους τους τύπους επιχειρησιακών κινδύνων. Απώλεια στη διαθεσιμότητα του συστήματος ηλεκτρονικής τραπεζικής σίγουρα επιφέρει κολλήματα και στις καθημερινές εργασίες της τράπεζας προκαλώντας μεταξύ άλλων συμφόρηση στη κίνηση των φυσικών καταστημάτων, δυσαρέσκεια στους πελάτες, απώλεια εμπιστοσύνης, απώλεια φήμης και πελατείας λόγω του οτι η τράπεζα ουσιαστικά δεν είναι διαθέσιμη για να εξυπηρετήσει τη πελατεία της. Άρα μακροχρόνια και συνολικά και σε όλες τις περιπτώσεις που μπορεί να διαρκέσει η απώλεια της διαθεσιμότητας (μια ώρα, μια μέρα, 2-3 μέρες, μια εβδομάδα ή ακόμα και ένα μήνα) οι επιπτώσεις είναι βαθμού Α, δηλαδή πολύ ψηλού βαθμού. Τα αποτελέσματα του βήματος αυτού φαίνονται στον προηγούμενο πίνακα.

Συνολική Αξιολόγηση Επιχειρησιακού Αντίκτυπου

Εφόσον έχει ολοκληρωθεί η συμπλήρωση όλων των πινάκων αναφοράς στο IRAM, υπολογίζεται αυτόματα η απαίτηση ασφάλειας του συστήματος σε επίπεδο εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των πληροφοριών. Το IRAM υπολόγισε αυτόματα οτι η συνολική διαβάθμιση του επιχειρησιακού αντίκτυπου είναι Υψηλή (Overall Classification: High). Υψηλή διαβάθμιση σημαίνει οτι υπάρχει μεγάλη απαίτηση για προστασία της πληροφορίας, εφόσον απώλεια σε οποιδήποτε επίπεδο θα επέφερε πολύ ισχυρές επιπτώσεις στην τραπεζική δραστηριότητα τόσο σε χρηματοοικονομικό επίπεδο (financial) όσο και σε λειτουργικό/ διαχειριστικό (operational). Σαν αναλυτές κατά τη διεξαγωγή της εργασίας Αξιολόγησης Επικινδυνότητας επιβεβαίωσαμε οτι όλοι οι συμμετέχοντες από τη τράπεζα XBANK έχουν πλήρη αντίληψη της σημασίας των αποτελεσμάτων αυτών και το πως αυτα θα επηρεάσουν το επίπεδο ασφάλειας που θα χρειασθεί να υλοποιηθεί. Σύμφωνα με τα δεδομένα που εισήχθησαν για ανάλυση και συνολική αποτίμηση του συστήματος ηλεκτρονικής τραπεζικής το σύστημα κρίνεται υψηλής κρισιμότητας όσον αφορά τις επιπτώσεις στην επιχειρησιακή δραστηριότητα με απαίτηση για επαναφορά μέσα στο σύνολο μιας ώρας ετσι ώστε ο επιχειρησιακός αντίκτυπος να είναι στο ελάχιστο δυνατό. Στους επόμενους πίνακες παρατίθενται οι τελικές αναφορές που παράγονται από το εργαλείο αυτόματα και τονίζεται η ανάγκη για λεπτομερή – και όχι απλά τυπική - διεξαγωγή μιας άσκησης για την Εκτίμηση Απειλών και Ευπαθειών.



BIA Summary

System	E-Banking application	Business area	IT department
System owner	G. Papadopoulos	Risk analyst	V. Karamanli

Description of system

The e-banking system allows customers to conduct financial transactions on a secure website operated by their retail bank.

Overall Classification

HIGH MEDIUM LOW

I agree with the Business Impact Assessment Ratings, Overall Classification and chosen Next Steps.

System owner signature _____ Date _____

Risk analyst signature _____ Date _____

Business Impact Assessment Ratings

Overall Business Impact Ratings

	A	B	C	D	E
Loss of confidentiality	X				
Loss of integrity	X				
Loss of availability	X				
- 1 hour	X				
- 1 day	X				
- 2-3 days	X				
- 1 week	X				
- 1 month	X				

Business Security Requirements Rating

	A	B	C	D	E
Confidentiality	X				
Integrity	X				
Availability	X				

Critical Timescale

	1 hour	1 day	2-3 days	1 week	1 month
Time	X				

Business impact ratings:
A –Very high, B – High, C - Medium, D - Low, E - Very low

IRAM 9: Συνολική Αποτίμηση Επιχειρησιακού Αντίκτυπου (BIA Summary)

Συνολικά από την συνολική αποτίμηση επιχειρησιακού αντίκτυπου φαίνεται στην παραπάνω απεικόνιση οτι η διαβάθμιση είναι της κατηγορίας Α δηλαδή Πολύ Υψηλή (Very High) σε όλες τις περιπτώσεις απλώλειας της εμπιστευτικότητας, απώλειας της ακεραιότητας και διαθεσιμότητας της πληροφορίας. Τα αποτελέσματα αυτά, συνολικά για κάθε σενάριο απώλειας μιας από τις ιδιότητες της πληροφορίας (εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα) θα χρησιμοποιηθούν και στην επόμενη φάση της ανάλυσης που περιλαμβάνει την εκτίμηση των απειλών και των ευπαθειών προκειμένου να βγάλουμε συμπεράσματα για την αποτίμηση και διαβάθμιση του κινδύνου της πληροφορίας (Information Risk Rating) ανά τύπο απειλής.

Top impact types

No.	Impact type	Impact ratings			Comments
		C	I	A	
1	F1 Loss of sales, orders or contracts	High	Very high	Medium	
2	F2 Loss of tangible assets (eg fraud, theft of money, lost interest)	Very low	High	High	
3	F3 Penalties/legal liabilities (eg breach of legal, regulatory or contractual obligations)	Very high	Very high	High	
4	F4 Unforeseen costs (eg recovery costs)	High	High	High	
5	F5 Depressed share price (eg sudden loss of share value)	Medium	Medium	Very high	
6	O1 Loss of management control (eg impaired decision-making)	Medium	Medium	Very high	
7	O2 Loss of competitiveness (eg delays in the introduction of new production capabilities)	Very high	High	Very high	
8	O3 New ventures held up (eg delayed new products or services)	High	Medium	Medium	
9	O4 Breach of operating standards (eg contravention of regulatory standards)	Medium	Low	High	
10	C2 Loss of customers or clients (eg customer/client defection to competitors)	Very high	High	Very high	
11	C3 Loss of confidence by key institutions (eg adverse criticism by investors)	Very high	Medium	High	
12	C4 Damage to reputation (eg confidential financial information published in media)	High	Medium	Very high	

IRAM 10: Τύποι επιχειρησιακού αντίκτυπου με την υψηλότερη διαβάθμιση (Top Impact Ratings)

Στον παραπάνω πίνακα αποτυπώνεται η λίστα που παράχθηκε από το IRAM με τους τύπους του επιχειρησιακού αντίκτυπου που έχουν αξιολογηθεί με την υψηλότερη διαβάθμιση όσον αφορά το βαθμό αντίκτυπου στην επιχειρηματική δραστηριότητα. Σύμφωνα με το πίνακα αυτό σαν αναφορά του εργαλείου, παρατηρείται οτι έχουν περιληφθεί όλοι οι τύποι επιχειρησιακού αντίκτυπου που αφορούν τις οικονομικές επιπτώσεις (Απώλειες σε τζίρο, απώλειες σε ενσώματα περιουσιακά στοιχεία, Νομικές κυρώσεις/ πρόστιμα, Κόστος επανάκαμψης, Υποτίμηση μετοχών). Επιπλέον, εμφανίζονται και όλοι οι παράγοντες που έχουν να κάνουν με το διαχειριστικό μέρος των λειτουργιών της τράπεζας και τη διακυβέρνηση και τέλος το σημαντικότερο με τη πελατειακή σχέση της τράπεζας (απώλεια εμπιστοσύνης από σημαντικά ιδρύματα, απώλεια φήμης και πελατείας κλπ.).

4.4.2 Φάση 2η: Εκτίμηση Απειλών και Ευπαθειών στην XBANK

Εφόσον η άσκηση Ανάλυσης της Επικινδυνότητας έχει ξεκινήσει με την εκτίμηση του επιχειρησιακού αντίκτυπου, και όλοι οι συμμετέχοντες είναι ενήμεροι και της άσκησης αλλά και των παραμέτρων του συστήματος ηλεκτρονικής τραπεζικής, η μετάβαση στη δεύτερη φάση μπορεί να προχωρήσει. Η περιγραφή των βασικών στοιχείων που συνθέτουν το προφίλ της εφαρμογής ηλεκτρονικής τραπεζικής έχει διεξαχθεί στη πρώτη φάση και δεν κρίνεται απαραίτητο να επαναληφθεί σε αυτή τη φάση. Εφόσον οι πληροφορίες σχετικά με την εφορμογή ηλεκτρονικής τραπεζικής έχουν παρουσιαστεί στη προηγούμενη φάση, μπορούμε να περάσουμε στο πρωτο βήμα της εν λόγω άσκησης που είναι η εκτίμηση των απειλών.

Σε αυτό το βήμα θα πρέπει να εξετάσουμε ποιές από τις ήδη καταγεγραμμένες απειλές από τον ISF ισχύουν και για το σύστημα ηλεκτρονικής τραπεζικής της XBANK και αν χρειάζεται να προστεθούν και άλλες. Στη συνέχεια θα πρέπει να εξετάσουμε το βαθμό στον οποίο κρίνουμε

οτι η εκάστοτε απειλή μπορεί είναι απειλή και στο συγκεκριμένο σύστημα. Μια συνοπτική παρουσίαση του πίνακα που χρησιμοποιήθηκε για να καταγραφεί αυτή η εργασία παρατίθεται εδώ μεταφρασμένη στα ελληνικά και παρέχονται τέσσερα παραδείγματα απειλών ενδεικτικά. Στις απειλές που αξιολογούνται ως υψηλές παρέχεται και επεξηγηματικό σχόλιο όπου κρίνεται απαραίτητο. Υπάρχουν πάρα πολλοί τύποι απειλών που μπορούν να παραβιάσουν την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των δεδομένων από μη σκόπιμα ανθρώπινα λάθη μέχρι κακόβουλες απειλές. Η αποτύπωση όλων είναι αδύνατη σύμφωνα με χρονικούς και οικονομικούς περιορισμούς.

Εκτίμηση Απειλών									
#	Τύπος Απειλής	Ιδιότητες της πληροφορίας που επηρεάζονται			Εκτίμηση Απειλής κατά ISF	Επιπρόσθετη πληροφόρηση για το τύπο της απειλής		Συνολική εκτίμηση Απειλής	Επεξηγηματικά Σχόλια
		Εμπιστευτικότητα	Ακεραιότητα	Διαθεσιμότητα		Εσωτερικά	Εξωτερικά		
					Διαβάθμιση A - Πολύ Υψηλή, B -Υψηλή, C - Μεσαία, D - Χαμηλή, E - Πολύ Χαμηλή				
Εξωτερικές Απειλές									
T1	Επιθέσεις DoS (Denial of Service)			X	A	B	A	A	Η DoS επίθεση είναι σοβαρή απειλή
T2	παράνομη επέμβαση στο σύστημα (hacking)	X	X		C	C	B	C	
T3	Διενέργεια κακόβουλων σαρώσεων (probes & scans)	X			B	A	B	B	Έχει συνεχή χαρακτήρα και πρέπει να παρακολουθειται
T4	Σπάσιμο κωδικών (password cracking)	X			C	D	C	C	

IRAM 11: Πίνακας καταγραφής και Εκτίμησης Απειλών

Όπως φαίνεται και στο παραπάνω πίνακα η φόρμα έχει σχεδιαστεί ώστε η διαβάθμιση της κάθε απειλής να γίνει με βάση τη πληροφόριση που παρέχεται από τον ISF (πεδίο: «εκτίμηση απειλής ISF»), με βάση την εσωτερική πληροφόριση, δηλαδή βάσει των περιστατικών που έχει δεχθεί και έχει καταγράψει ο τραπεζικός οργανισμός και τέλος την εξωτερική πληροφόριση δηλαδή βάσει σχεδίων και αξιόπιστων ιστοτόπων (πεδίο: «Επιπρόσθετη πληροφόρηση για το τύπο της απειλής»). Εφόσον βάσει των αποτελεσμάτων της ανάλυσης επιχειρησιακού αντίκτυπου, απαιτείται μια λεπτομερής αποτίμηση απειλών και ευπαθειών θα πρέπει και οι τρείς τύποι πληροφόρησης να ληφθούν υπόψη και να συνυπολογιστούν, δηλαδή η διαβάθμιση να ληφθεί υπόψη και από τις τρεις πηγές. Οι τύποι των απειλών που έχουν αναγνωριστεί προέρχονται και είναι βασισμένοι στην έρευνα του ISF: Information Security Status Survey (ISF, 2004).

Για να καθορίσουμε ποιές είναι οι κύριες απειλές που αφορούν το σύστημα υπο εξέταση, επιλέξαμε τις απειλές από το πίνακα του ISF που μπορούν να επηρεάσουν άμμεσα την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα της πληροφορίας στην εφαρμογή e-banking. Η φόρμα που παρατίθεται στο εργαλείο περιλαμβάνει συνολικά 49 τύπους απειλών έτσι ώστε ο αναλυτής να μπορεί να αξιολογήσει το κίνδυνο στα πληροφοριακά συστήματα.

Τέλος, γίνεται μια επιπλέον ομαδοποίηση σε 9 κατηγορίες – Εξωτερική επίθεση, εσωτερική κατάχρηση, κλοπή, ανθρώπινο λάθος, δυσλειτουργίες, διακοπή υπηρεσίας, και μη προβλέψιμα περιστατικά εξαιτίας μη ελεγχόμενων αλλαγών στην εφαρμογή. Η επιλογή των συγκεκριμένων απειλών έγινε αφού λήφθηκε υπόψη ο αριθμός των συμβάντων, η καθοδήγηση του διοικητικού συμβουλίου της τράπεζας και τα σχόλια από τον υπεύθυνο σφαλείας της XBANK τράπεζας. Το εργαλείο του IRAM T&VA Assistant υποστηρίζει αυτόματα τη διαδικασία επιλογής ή αντίστοιχα αποεπιλογής καποιων από τις απειλές που εμφανίζονται ανάλογα με το ποιές από αυτές είναι σχετικές με την αξιολόγηση του συστήματος ηλεκτρονικής τραπεζικής.

Εδώ παρατίθεται ενδεικτικά μέρος από το πίνακα στο εργαλείο IRAM όπου έγινε η εργασία εκτίμησης απειλών για την XBANK και συγκεκριμένα για το σύστημα ηλεκτρονικής τραπεζικής. Για τον πρώτο τύπο απειλής Τ1 «Επίθεση Denial of Service» (DoS attack) η εργασία που έγινε συνοψίζεται εδώ. Εξηγήθηκε σε όλα τα μέλη τι είναι οι Επιθέσεις άρνησης εξυπηρέτησης (Denial-of-service attack, DoS attack). Είναι οι επιθέσεις εναντίον ενός υπολογιστή, ή μιας υπηρεσίας που παρέχεται, οι οποίες έχουν ως σκοπό να καταστήσουν τον υπολογιστή ή την υπηρεσία ανίκανη να δεχτεί άλλες συνδέσεις και έτσι να μην μπορεί να εξυπηρετήσει άλλους πιθανούς πελάτες. Υπάρχουν γενικά δύο μορφές αυτής της επίθεσης. Η μία είναι η επίθεση κατά την οποία η υπηρεσία αναγκάζεται να καταρρεύσει και να πρέπει να επανεκκινηθεί και η άλλη είναι η αποστολή υπερβολικά μεγάλου αριθμού ψεύτικων αιτήσεων για εξυπηρέτηση με αποτέλεσμα η υπηρεσία να μην μπορεί να εξυπηρετήσει αυτούς που πραγματικά θέλουν την υπηρεσία (ορισμός Wikipedia)4. Λόγω του οτι αυτή η επίθεση δεν έχει σκοπό παραβίασης ή κλοπής δεδομένων, αυτή η απειλή όπως φαίνεται και από τη φόρμα του ISF, είναι τέτοιας μορφής που επηρεάζει μόνο τη διαθεσιμότητα της πληροφορίας (Α). Βάσει της στατιστικής έρευνας του ISF η απειλή αυτή έχει εκτιμηθεί με βαθμό «Μεσαίο» (Medium). Όσον αφορά την εσωτερική πληροφόρηση, από τα συμβάντα που έχει υποστεί η τράπεζα, αν και δεν έχει δεχτεί άμεσα τέτοιου είδους επίθεση, απόπειρες έχουν γίνει και για το λόγο αυτό κρίνεται οτι είναι απειλή «μεσαίου βαθμού». Επίσης, στηριζόμενοι σε έρευνες που κυκλοφορούν από ειδικευμένες εταιρίες στο αντικείμενο και λόγω του οτι αυτές οι επιθέσεις ολοένα και αυξάνουν στην Ελλάδα και στο εξωτερικό έχοντας καταγράψει περίπου 10.000 (Hussain et al., 2003), η εκτίμηση που έγινε είναι υψηλού βαθμού. Συνολικά ο βαθμός που προκύπτει στον συγκεκριμένο τύπο απειλής είναι «μεσαίου» μεγέθους.

[4] http://el.wikipedia.org/wiki /Επιθέσεις_άρνησης_υπηρεσιών

Threat Assessment

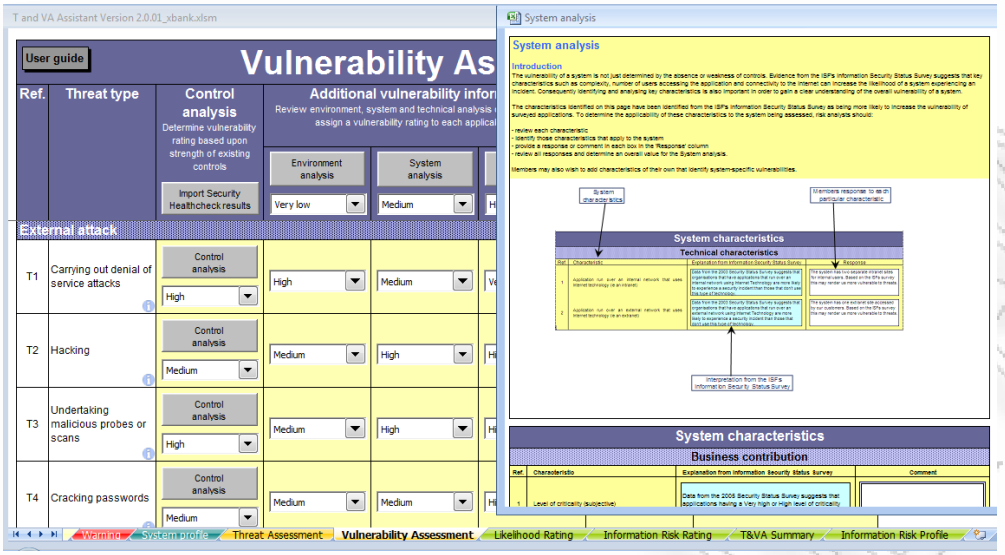
Ref.	Threat type Review the list of threat types and select those that are most applicable to the system being assessed (add additional system-specific Threat types if necessary)	Main properties of information affected			ISF threat information Review the information in the ISF's Threat Data Tool and assign a rating to each applicable threat	Additional threat information Review Internal and External sources of information on threats and assign a rating to each applicable threat		Overall threat rating Consider all threat information ratings and then determine an Overall threat rating for each Threat type	Explanatory comments
		C	I	A		Internal	External		
External attack									
T1	Carrying out denial of service attacks			X	Medium	Medium	High	Medium	
T2	Hacking	X	X		Medium	High	High	High	
T3	Undertaking malicious probes or scans	X			Very low	High	High	Very low	
T4	Cracking passwords	X			Very low	Very low	Low	Very low	
T5	Cracking keys	X			Very low	Low	Medium	Medium	
T6	Defacing web sites		X		Very low	Low	Low	Very low	
T7	Spoofing web sites	X			Very low	Medium	Medium	Medium	

IRAM 12: Εκτίμηση απειλών στην XBANK.

Εκτίμηση ευπαθειών (Vulnerability Assessment)

Σε αυτό το βήμα της διαδικασίας και αφού έχουμε επιλέξει τις απειλές που σχετίζονται με το σύστημα ηλεκτρονικής τραπεζικής στο προηγούμενο βήμα, θα γίνει η εκτίμηση/ διαβάθμιση των ευπαθειών αυτού για κάθε τύπο απειλής που έχει επιλεγεί.

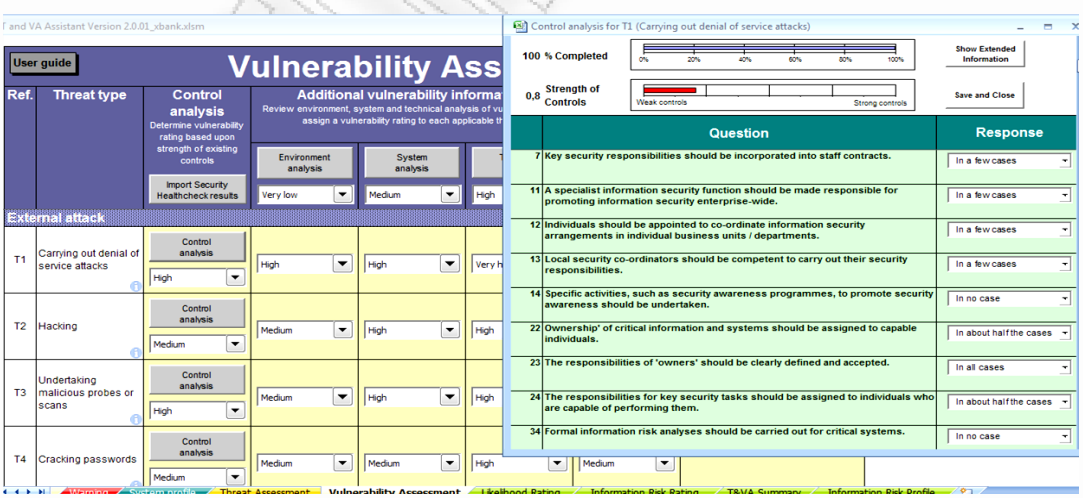
Λόγω του οτι το σύστημα ηλεκτρονικής τραπεζικής είναι περίπλοκο από την άποψη υποδομής και αριθμό συναλλαγών που εξυπηρετεί, ο προσδιορισμός του βαθμού ευπάθειάς του στους διάφορους τύπους απειλών δεν είναι εύκολο εγχείρημα. Ενώ η παρουσία ή η απουσία σημείων ελέγχου μπορεί να είναι καθοριστικός παράγοντας του βαθμού ευπάθειας ενός συστήματος απέναντι σε μια απειλή, υπάρχουν και άλλοι παράγοντες που πρέπει επίσης να θεωρηθούν για να προκύπτει ένα πιο αντικειμενικό αποτέλεσμα, όπως το επιχειρηματικό περιβάλλον, οι εγγενείς τεχνικές αδυναμίες του συστήματος και η γενικότερη υποδομή του. Στο εργαλείο IRAM και στη φόρμα της αξιολόγησης ευπάθειας του συστήματος e-banking υπάρχει επεξήγηση για τους υποπαράγοντες που πρέπει να ληφθούν υπόψη όταν βαθμολογούμε τη κάθε απειλή. Στη παρακάτω εικόνα αποτυπώνεται και η υπηρεσία αυτή από το εργαλείο.



IRAM 13: Παράγοντες που λαμβάνονται υπόψη κατα την αξιολόγηση ευπάθειας βάσει της συστημικής ανάλυσης

Για την αξιολόγηση της ευπάθειας του συστήματος στη κάθε απειλή και για να καταλήξουμε στη συνολική διαβάθμιση ανά τύπο απειλής λήφθηκαν υπόψη όλοι οι παράγοντες που αναφέρθηκαν παραπάνω. Στο πρώτο τύπο απειλής T1 «Επίθεση Denial of Service» (DoS attack) ακολουθήθηκε η εξής εργασία ανά παράγοντα:

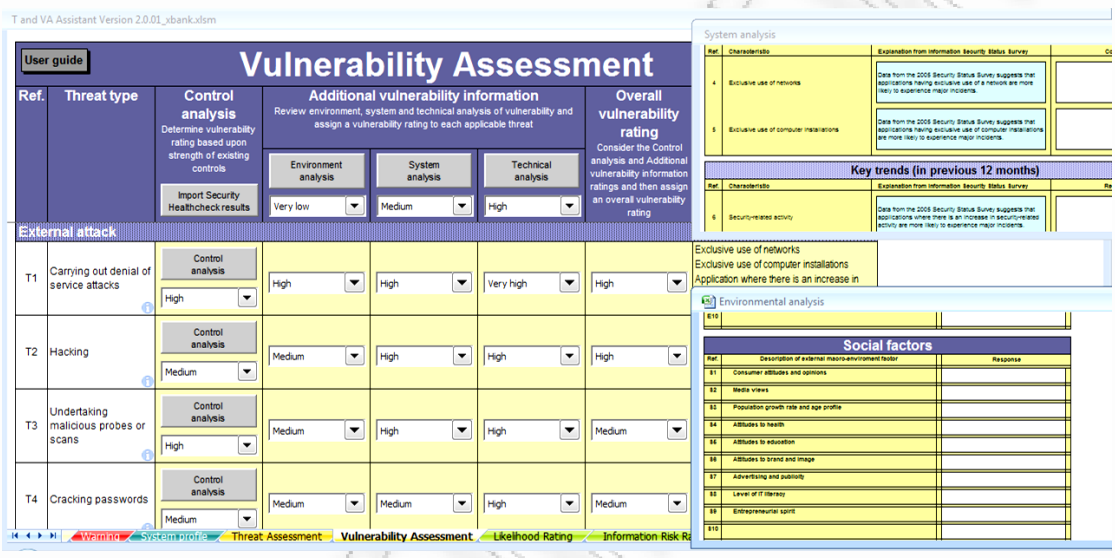
Ανάλυση σημείων ελέγχου (Controls Analysis)
Το εργαλείο παρέχει φόρμα με εξειδικευμένες ερωτήσεις οι οποίες αναφέρονται στην ύπαρξη ή οχι των συγκεκριμένων σημείων ελέγχου, τις οποίες ο αναλυτής καλείται να απαντήσει και βάσει αυτών το εργαλείο διαβαθμίζει την ευπάθεια του συστήματος στη συγκεκριμένη απειλή. Για κάθε απειλή, η ανάλυση αυτή δίνει τη πρόοδο της άσκησης (αν έχουν δηλαδή απαντηθεί όλες οι ερωτήσεις) και την ύπαρξη επαρκών ή οχι σημείων ελέγχου για την αντιμετώπιση της συγκεκριμένης απειλής. Για την απειλή T1, ένα μέρος των ερωτήσεων και των αντίστοιχα δοθέντων απαντήσεων φαίνονται στη παρακάτω εικόνα, βάσει των οποίων το IRAM υπολόγισε οτι ο βαθμός ευπάθειας του συστήματος στην απειλή μιας DoS επίθεσης είναι Υψηλός (high) βάσει της ανάλυσης στα σημεία ελέγχου. Επιπλέον φαίνεται οτι βάσει των απαντήσεων που δόθηκαν η συνολική αξιολόγηση των σημείων ελέγχου δείχνει οτι αυτά είναι ανεπαρκή.



IRAM 14: Διαβάθμιση ευπάθειας στην επίθεση DoS βάσει της ανάλυσης στα σημεία ελέγχου.

Ανάλυση περιβάλλοντος, συστημική ανάλυση και ανάλυση τεχνικού επιπέδου

Όσον αφορά την ανάλυση στο περιβάλλον, κρίθηκε οτι η εκπαίδευση στη τεχνολογία (σαν κοινωνικός παράγοντας), ο ανταγωνισμός και η μη ύπαρξη ισχυρού νομικού πλαισίου που να αποτρέπει τέτοιου είδους ενέργειες καθιστά το σύστημα ευπαθές σε μια τέτοια επίθεση. Βάσει των κριτηρίων του ISF που φαίνοντα στην εκόνα παρακάτω για τη συστημική ανάλυση (system analysis), το σύστημα ηλεκτρονικής τραπεζικής και η χρήση αυτού βασίζεται καθαρά στη δικτύωση και στο internet και συνεπώς και από αυτή την άποψη είναι επιρρεπές σε βαθμό υψηλό (high) σε μια επίθεση DoS. Τέλος, από τεχνικής πλευράς, και βάσει των αποτελεσμάτων από τη χρήση ειδικών προγραμμάτων ελέγχου στο λειτουργικό σύστημα και στη βάση δεδομένων, το σύστημα έχει αρκετές αδυναμίες σε παραμετροποίηση της υποδομής και της δικτύωσης και λόγω αυτών των παραγόντων είναι σε πολύ υψηλό βαθμό επιρρεπές (very high) σε τέτοιου είδους απειλή. Στη παρακάτω εικόνα φαίνεται η διαβάθμιση για όλους τους παράγοντες και η συνολική που υπολογίζεται για την απειλή T1.



IRAM 15: Διαβάθμιση ευπάθειας στην επίθεση DoS βάσει της ανάλυσης περιβάλλοντος και τεχνικών στοιχείων.

Μετά από την αξιολόγηση των απειλών και την άσκηση διαβάθμισης της ευπάθειας του συστήματος ηλεκτρονικής τραπεζικής ανά τύπο απειλής, το IRAM αυτόματα παράγει τα αποτελέσματα διαβάθμισης της πιθανοφάνειας ανά απειλή και την τελική αποτίμηση επικινδυνότητας ανά τύπο απειλης. Η διαβάθμιση της πιθανότητας συμβάντος (Likelihood rating) όπως φαίνεται και στον ακόλουθο πίνακα προκύπτει από το συνολικό αποτέλεσμα της αποτίμησης απειλών και το συνολικό αποτέλεσμα της αποτίμησης ευπαθειών. Για τον τύπο απειλής T1 «Επίθεση Denial of Service» (DoS attack) η συνολική διαβάθμιση για την αποτίμηση της απειλής ήταν μεσαίου βαθμού ενώ η συνολική διαβάθμιση της ευπάθειας του συστήματος ήταν υψηλού βαθμού. Συνεπώς, βάσει του IRAM η πιθανότητα ενός περιστατικού ασφάλειας είναι Υψηλή (High) όπως φαίνεται και στην επόμενη εικόνα από το εργαλείο.

Likelihood Rating

Ref.	Threat type	Overall threat rating From Threat Assessment form	Overall vulnerability rating From Vulnerability Assessment form	Likelihood rating The likelihood of an information incident occurring (automatically determined using the Likelihood reference table)	Explanatory comments
T1	Carrying out denial of service attacks	Medium	High	High	
T2	Hacking	High	High	Very high	
T3	Undertaking malicious probes or scans	Medium	Medium	Medium	
T4	Cracking passwords	Very low	Medium	Very low	
T5	Cracking keys	Medium	Medium	Medium	
T6	Defacing web sites	Very low	High	Very low	
T7	Spoofing web sites	Medium	High	High	
T8	Spoofing user identities	Very high	Medium	Very high	
T9	Modifying network traffic	Medium	Medium	Medium	

Συνολική αποτίμηση απειλής: «Μεσαία»

Συνολική αποτίμηση ευπάθειας: «Υψηλή»

Πιθανότητα περιστατικού: «Υψηλή»

IRAM 16: Πιθανότητα περιστατικού ανά τύπο απειλής (Εκτίμηση Πιθανοφάνειας)

Η τελική φάση της Αποτίμησης Απειλών και ευπαθειών, δηλαδή η ανάλυση της επικινδυνότητας ανά τύπο απειλής απορρέει επίσης αυτόματα από το IRAM, αφού συνυπολογιστούν α) η διαβάθμιση που έχει προκύψει από την εκτίμηση επιχειρησιακού αντίκτυπου αντίστοιχα για την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα της πληροφορίας που επηρεάζεται από κάθε απειλή (και σύμφωνα με τα αποτελέσματά της παρούσας ανάλυσης είναι για όλα τα σενάρια υψηλή), και β) η διαβάθμιση της πιθανότητας του συμβάντος (πιθανοφάνεια) αντίστοιχα και πάλι ως προς την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα. Η ανάλυση επικινδυνότητας προκύπτει όπως ειπώθηκε και πριν με βάση τον ακόλουθο πίνακα ο οποίος μπορεί και να τροποποιηθεί με βάση τις απαιτήσεις του οργανισμού και τη κρίση του εκάστοτε αναλυτή. Στη παρούσα εργασία χρησιμοποιήθηκε ο δεδομένος πίνακας χωρίς να γίνουν άλλες παρεμβολές.

Information Risk Reference Table

Using the Information Risk Reference Table

The **Overall Information Risk Rating** for a particular threat (ie the likelihood of an information incident occurring that could cause harm to an organisation) can be determined by looking up the value in the **Information Risk Reference Table** (below) that corresponds to the **Business Impact Rating** for the appropriate property of information being considered (from the Overall Business Impact Rating values for C, I or A in the Business Impact Assessment Summary form) and the **Likelihood Rating** (from the Likelihood Rating Form).

Business Impact Rating		Likelihood Rating: E (Very Low)	D (Low)	C (Medium)	B (High)	A (Very High)
Very High	A	C	B	A	A	A
High	B	C	C	B	A	A
Medium	C	D	D	C	B	A
Low	D	E	E	D	C	C
Very Low	E	E	E	E	D	D

Save table Save as...

IRAM 17: Πίνακας αναφοράς για τη συνολική εκτίμηση της επικινδυνότητας με βάση την εκτίμηση Πιθανοφάνειας και την εκτίμηση επιχειρησιακού αντίκτυπου.

Συνεχίζοντας με τη περίπτωση μιας Denial of Service επίθεσης η οποία σε αυτό το βήμα είναι ο κίνδυνος που πρέπει να εκτιμήσουμε (ή ρίσκο) R1, είναι φανερό οτι α) βάσει του υψηλού επιχειρησιακού αντίκτυπου (Business Impact Rating) που θα έχει η απώλεια στην διαθεσιμότητα του συστήματος ηλεκτρονικής τραπεζικής και συνεπώς στη διαθεσιμότητα της πληροφορίας που αυτό φέρει και β) βάσει της υψηλής πιθανότητας (Likelihood Rating) ενός τέτοιου περιστατικού να συμβεί, η αποτίμηση κινδύνου μιας επίθεσης DoS στη διαθεσιμότητα της πληροφορίας είναι αρκετά υψηλή (Very high). Συνεπώς, και η συνολική αποτίμηση του συγκεκριμένου κινδύνου είναι Αρκετά Υψηλή.

Information Risk Rating

Ref.	Threat type	Likelihood rating	Business Impact Assessment (BIA) Transfer the appropriate Business Security Requirements Ratings from the Business Impact Assessment Summary form			Information risk rating The likelihood of an information incident occurring (automatically determined using the Likelihood reference table)			Overall information risk rating Consider the information risk ratings for C, I and A and then assign an Overall information risk rating (this would normally be as high as the highest individual rating)
			C	I	A	C	I	A	
			High	High	High				
External attack									
R1	Carrying out denial of service attacks	High			High			Very high	Very high (As calculated)
R2	Hacking	Very high	High	High		Very high	Very high		Very high (As calculated)
R3	Undertaking malicious probes or scans	Medium	High			High			High (As calculated)
R4	Cracking passwords	Very low	High			Medium			Medium (As calculated)
R5	Cracking keys	Medium	High			High			High (As calculated)
R6	Defacing web sites	Very low		High			Medium		Medium (As calculated)

IRAM 18: Πίνακας συνολικής αποτίμησης της επικινδυνότητας ανά τύπο απειλής και πλέον κινδύνου.

Αποτελέσματα Αποτίμησης Απειλών και ευπαθειών

Η συνολική εκτίμηση του συστήματος ηλεκτρονικής τραπεζικής σε επίπεδο κινδύνου είναι Υψηλή. Η συνολική αποτίμηση των κινδύνων προκύπτει ανά ομάδα απειλών στο IRAM και αποτυπώνεται στον ακόλουθο πίνακα.

Information Risk Profile

Information Risk Rating Summary

Threat categories	A	B	C	D	E
External attack	4	7	4		
Internal misuse and abuse	2	3	5		
Theft		2			
System malfunction	3				
Service interruption	3	2	1		
Human error	1				
Unforeseen effects of changes	3		2		

Detailed Security Requirements

H	M	L
X		
X		
X		
X		
		X
X		
	X	

Information risk ratings:
A - Very high, B - High, C - Medium, D - Low, E - Very low

Detailed security requirements ratings:
H - High, M - Medium, L - Low

IRAM 19: Πίνακας συνολικής αποτίμησης της επικινδυνότητας ανά τύπο απειλής και πλέον κινδύνου.

Αναφορικά με το παραπάνω πίνακα, από τις κατηγορίες κινδύνων (απειλών) βγαίνει μια συνολική διαβάθμιση ανά κατηγορία και προκύπτουν και οι απαιτήσεις ασφαλείας ανάλογα με το βαθμό κινδύνου. Έτσι από τις εξωτερικές απειλές (στις οποίες συμπεριλαμβάνεται και η επίθεση DoS που αναλύθηκε προηγουμένως) 4 έχουν αξιολογηθεί ώς πολύ υψηλού (Very High) κινδύνου, 7 από το σύνολό τους έχουν αξιολογηθεί ως υψηλού κινδύνου (High) και 4 από αυτές μεσαίου κινδύνου. Συνολικά βάσει των υπολογισμών του IRAM οι απαιτήσεις σε ασφάλεια για τη συγκεκριμένη κατηγορία είναι Υψηλές (High).

Το IRAM παράγει αναφορά με τους υψηλότερους πληροφοριακούς κινδύνους (information risks) οι οποίοι στο σύνολό τους είναι είκοσι (20) και φαίνονται στον επόμενο πίνακα.

Top information risks

No.	Threat type	Risk rating	Comments
1	R1 Carrying out denial of service attacks	Very high	
2	R2 Hacking	Very high	
3	R7 Spoofing web sites	Very high	
4	R8 Spoofing user identities	Very high	
5	R17 Changing system privileges without authorisation	Very high	
6	R19 Modifying or inserting transactions, files or databases without authorisation	Very high	
7	R33 Malfunction of business application software acquired from a third party	Very high	
8	R34 Malfunction of system software	Very high	
9	R35 Malfunction of computer/network equipment	Very high	
10	R37 Damage to or loss of communications links/services.	Very high	
11	R38 Loss of power	Very high	
12	R41 System overload	Very high	
13	R43 IT/network staff errors	Very high	
14	R45 Unforeseen effect of changes to software	Very high	
15	R46 Unforeseen effect of changes to business information	Very high	
16	R47 Unforeseen effect of changes to computer / communications equipment	Very high	
17	R3 Undertaking malicious probes or scans	High	
18	R5 Cracking keys	High	
19	R9 Modifying network traffic	High	
20	R11 Distributing computer viruses (including worms)	High	

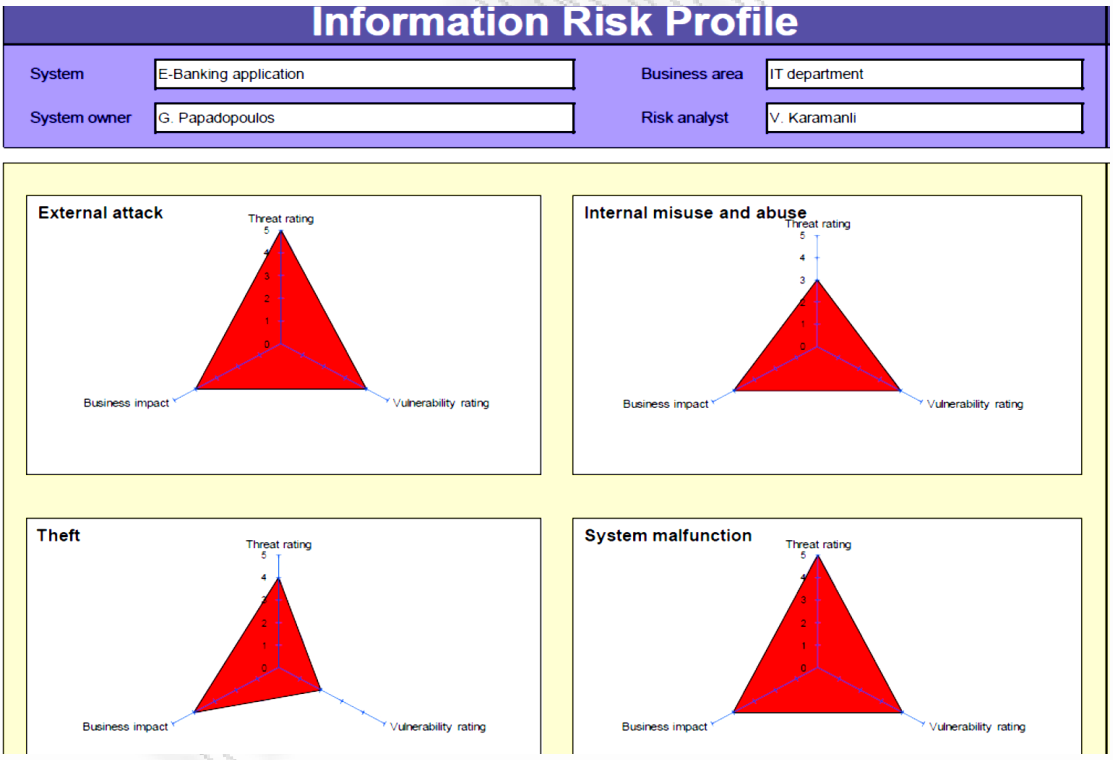
IRAM 20: Πίνακας με απειλές υψηλής ή πολύ υψηλής αποτίμησης της επικινδυνότητας.

Βάσει των στατιστικών αποτελεσμάτων από στο IRAM προκύπτει οτι το επόμενο βήμα θα πρέπει να είναι η διενέργεια μιας αναλυτικής άσκησης για την επιλογή των κατάλληλων σημείων

ελέγχου επικεντρώνοντας την ανάλυση στους 10 επικρατέστερους κινδύνους και καθορίζοντας τις απαιτήσεις ασφάλειας σύμφωνα με αυτούς.

Επιπρόσθετα, το IRAM παράγει κάποιες ενδιαφέρουσες αναφορές οι οποίες σχηματοποιούν το προφίλ του κινδύνου και βοηθούν τον αναλυτή και την ομάδα εργασίας να δουν τα αποτελέσματα συνολικά. Το σημαντικό είναι οτι βοηθά τους συμμετέχοντες στην άσκηση να βγάλουν κάποια ενδιαφέροντα συμπεράσματα για την πηγή των απειλών (threat rating) στις οποίες το σύστημα υπόκειται στον υψηλότερο κίνδυνο (αφού το IRAM τις κρατά ομαδοποιημένες) και να επικεντρώσουν την επιλογή των κατάλληλων σημείων ελέγχου στα σημεία και τις διαδικασίες που είναι πιο τρωτές σε επιθέσεις και κινδύνους (vulnerability rating) γενικότερα έτσι ώστε να μειωθεί το επίπεδο κινδύνου και συνεπώς, η πιθανότητα εμφάνισης περιστατικού ασφάλειας. Μέρος της τελικής αναφοράς για το προφίλ του πληροφοριακού κινδύνου του συστήματος ηλεκτρονικής τραπεζικής, όπως προκύπτει από το εργαλείο IRAM, παρατίθεται παρακάτω. Η συνολική αναφορά παρατίθεται στο παράρτημα σαν τελικό μέρος της άσκησης Αποτίμησης Απειλών και ευπαθειών.

Στην παρακάτω εικόνα φαίνεται οτι ο κίνδυνος της εξωτερικής απειλής (External attack) είναι πολύ υψηλός (threat rating: 5), με υψηλό επιχειρησιακό αντίκτυπο (Business impact: 4) και επίσης υψηλό βαθμό ευπάθειας (Vulnerability rating: 4). Αντίθετα, ο κίνδυνος της εσωτερικής απειλής (internal misuse and abuse) είτε αυτή προέρχεται από κακή χρήση ή κατάχρηση του συστήματος ηλεκτρονικής τραπεζικής είναι πολύ χαμηλός. Έχει όμως υψηλό το βαθμό επιχειρησιακού αντίκτυπου και το βαθμό ευπάθειας. Συμπερασματικά, βλέποντας αυτά τα αποτελέσματα συνολικά, η διοίκηση θα πρέπει να επικεντρωθεί στην υλοποίηση σημείων ελέγχου που θα καταστήσουν το δίκτυο της τράπεζας πιο ισχυρό και ασφαλές ώστε είτε να μπορούν να ανιχνευτούν εξωτερικές επιθέσεις με την υλοποίηση για παράδειγμα ενός συστήματος ανίχνευσης εισβολών (Intrusion Detection Systems) είτε να μπορούν να αντιμετωπιστούν αφού γίνουν.



IRAM 21: Διαγράμματα αποτίμησης προφίλ κινδύνου ανά κατηγορία απειλών

Στο τρίτο διάγραμμα ο κίνδυνος κλοπής των προσωπικών δεδομένων κατα την αυθεντικοποίηση παρατηρούμε οτι είναι υψηλός, αλλά το σύστημα ηλεκτρονικής τραπεζικής δεν είναι τρωτό (έχει χαμηλό βαθμό ευπάθειας), γιατί έχει ισχυρά και κατάλληλα σημεία ελέγχου που μπορούν να αποτρέψουν κλοπή των προσωπικών δεδομένων των πελατών κατά την

αυθεντικοποίηση. Συνεπώς, αυτός ο κίνδυνος αν και υψηλός δεν θα πρέπει να είναι ο πρώτος που η διοίκηση θα λάβει υπόψη για να υλοποιήσει άμεσα τα σημεία ελέγχου.

Συμπερασματικά, οι αναφορές αυτές που μας παράγει το εργαλείο IRAM είναι αρκετά αποτελεσματικές γιατί σε μια τέτοια εργασία γύρω από ένα τόσο κρίσιμο σύστημα με αρκετά τρωτά σημεία και για ένα τόσο μεγάλο οργανισμό όπως είναι η τράπεζα XBANK χωρίς ιδιαίτερη οργάνωση και ελεγχόμενο περιβάλλον πληροφορικής, όπως άλλωστε προκύπτει από την άσκηση, βοηθούν τον αναλυτή και την διοίκηση να θέσουν προτεραιότητες και να διαθέσουν χρήματα σε συγκεκριμένη κατεύθυνση για την ανεύρεση και επιλογή των καταλληλότερων σημείων ελέγχου για ένα πιο αποτελεσματικό και ισχυρό περιβάλλον εσωτερικού ελέγχου.

4.4.3 Φάση 3η: Επιλογή σημείων ελέγχου στην XBANK

Στη διαδικασία επιλογής των κατάλληλων σημείων ελέγχου στη συνέχεια της παρούσας μελέτης περίπτωσης χρησιμοποιήθηκε το εργαλείο IRAM Control Solution Assistant. Σαν πρώτο βήμα στη διαδικασία είναι η κατασκευή και η σύσταση της βάσης δεδομένων των σημείων ελέγχου βάσει των πληροφοριών που υπάρχουν από τον τραπεζικό οργανισμό. Η βάση δεδομένων αποτελείται από 179 σημεία ελέγχου ή πιθανούς ελεγκτικούς μηχανισμούς που πρέπει να ενημερωθούν με βάση τις πληροφορίες που παρέχονται από τους εκάστοτε υπεύθυνους της XBANK. Η ενημέρωση που απαιτείται να διεξαχθεί στη βάση δεδομένων αυτή σχετίζεται με την αντιμετώπιση των επιλεγμένων σημείου ελέγχου από τον οργανισμό και την δυνατότητα εφαρμογής τους σε αυτόν έτσι ώστε να ξεκινήσει η διαδικασία υλοποποίησης. Υπάρχουν τέσσερα τμήματα που αναγνωρίζουν και επεξηγούν το εκάστοτε σημείο ελέγχου:

A. Περιγραφή του σημείου ελέγχου και αντιστοίχηση με τα αντίστοιχα πρότυπα που υλοποιεί (ISO 27002 και Cobit 4) με συγκεκριμένη αναφορά σε αυτά.

B. Κατηγοριοποίηση του σημείου ελέγχου (fundamental, advanced, specialized, preventative, detective) και ανάλογα με την ή τις ιδιότητες της πληροφορίας εξυπηρετεί.

C. Πληροφορίες σχετικά με το σημείο ελέγχου και με τον οργανισμό που το υιοθετεί (αν υπάρχει εσωτερικά διαδικασία, αν χρησιμοποιείται ήδη, διαβάθμιση απαιτούμενων πόρων για υλοποίηση).

D. Αρμοδιότητες και υπεύθυνο τμήμα υλοποίησης/ συντήρησης του ελεγκτικού μηχανισμού.

Η πληροφόρηση στα δύο πρώτα τμήματα παρέχεται από το εργαλείο μιας και η εργασία αντιστίχησης με τα αντίστοιχα πρότυπα έχει ήδη διεξαχθεί από τον οργανισμό ISF και τα χαρακτηριστικά κατηγοριοποίησης του σημείου ελέγχου είναι από τα χαρακτηριστικά του ίδιου του σημείου ελέγχου και δεν προσαρμόζονται. Ο αναλυτής και η ομάδα εργασίας κλήθηκαν να συμπληρώσουν τα δυο τελευταία τμήματα.

Το πρώτο σημείο ελέγχου κατά σειρά στο εργαλείο (C1) είναι οτι «ο οργανισμός που χρησιμοποιεί το σύστημα υπό αξιολόγηση έχει ορίσει τη στάση του και τη στρατηγική του απέναντι στην ασφάλεια των πληροφοριών με την ύπαρξη και τη θέσπιση πολιτικής ασφαλείας». Αυτό το σημείο ελέγχου συγκαταλέγεται σε αυτά που είναι της κατηγορίας «διοικητικά σημεία ελέγχου» (entity level controls, Management Commitment) λόγω του οτι αντικατοπτρίζει τη στάση του τραπεζικού οργανισμού απέναντι στην ασφάλεια της πληροφορίας και αποτυπώνει την γενικότερη οδηγία προκειμένου να επιτευχθεί ο στόχος προς την ασφάλεια των δεδομένων που διαχειρίζεται. Στην παρούσα μελέτη περίπτωσης είναι το πρώτο που πρέπει να εξετασθεί και να υλοποιηθεί βάσει της ανάλυσης κινδύνου λόγω του οτι σχετίζεται άμεσα με τη γενικότερη πρακτική ενός οργανισμού ως προς την ασφάλεια της πληροφορίας και τη δέσμευσή του στη πολιτική αυτή. Το σημείο ελέγχου C1 είναι πολύ περιορισμένο στη στάση της διοίκησης, και δεν αναφέρεται άμεσα στην καθιερωμένη πολιτικής ασφάλειας, ενός δηλαδή επίσημου εγγράφου με συγκεκριμένες θέσεις. Συμπληρώνεται για αυτό το λόγο από τα επόμενα δύο (C2, C3) στη σειρά της κατηγορίας «Management Commitment» και τα C4, C5 της κατηγορίας «Πολιτική Ασφάλειας» (Security Policy). Μια σύντομη απόδοση στην ελληνική γλώσσα των τεσσάρων αυτών σημείων ελέγχου από το εργαλείο, ακολουθεί.

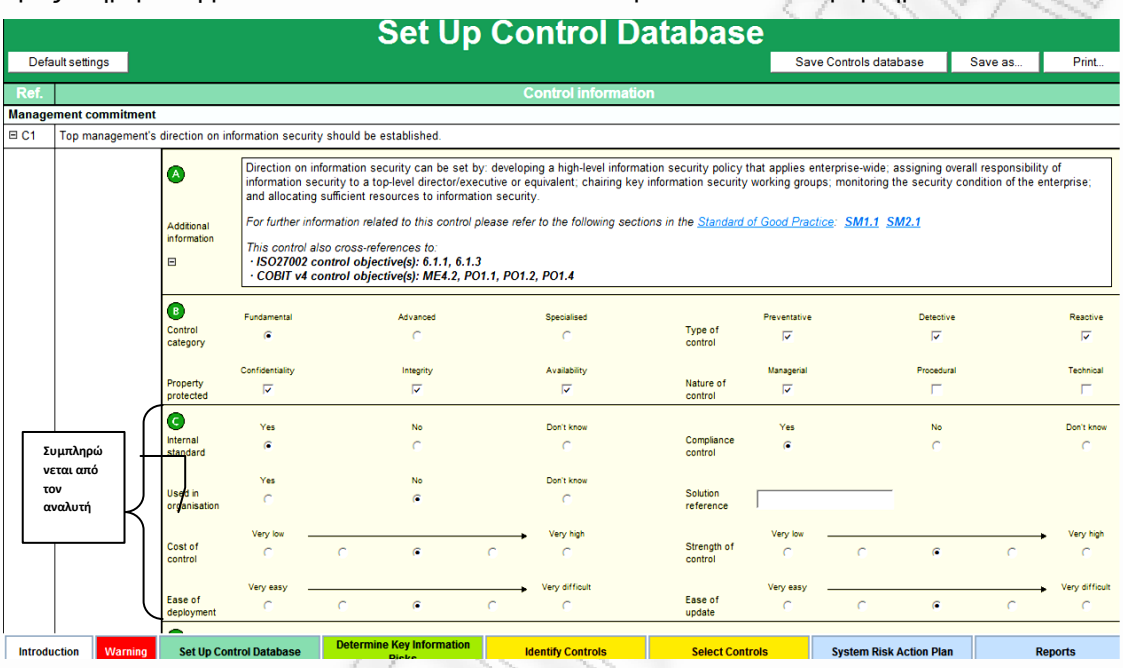
C2: Η δέσμευση της διοίκησης πρέπει να είναι εμφανής και να αποδεικνύεται (π.χ. με τον ορισμό υπεύθυνου ασφαλείας και την ανάθεση ανάλογων αρμοδιοτήτων κλπ.).

C3: Ο έλεγχος ως προς την ασφάλεια των πληροφοριών θα πρέπει να επιβάλλεται από επιτροπή που απαρτίζεται από υψηλόβαθμα στελέχη της ανώτατης διοίκησης.

C4: Θα πρέπει να υπάρχει μια γενική, συνολική και επίσημα καταγεγραμμένη πολιτική ασφαλείας.

C5: Η πολιτική ασφαλείας θα πρέπει να έχει επικοινωνηθεί σε όλους όσους έχουν πρόσβαση στις πληροφορίες και τα πληροφοριακά συστήματα του οργανισμού.

Στην εικόνα που ακολουθεί παρουσιάζεται μέρος της εργασίας κατασκευής και ενημέρωσης της βάσης αυτής ενώ το σύνολο των σημείων ελέγχου που περιέχει η βάση δεδομένων του IRAM προς ενημέρωση βάσει του ISO 27002 και Cobit 4 παρατίθεται στο παράρτημα.



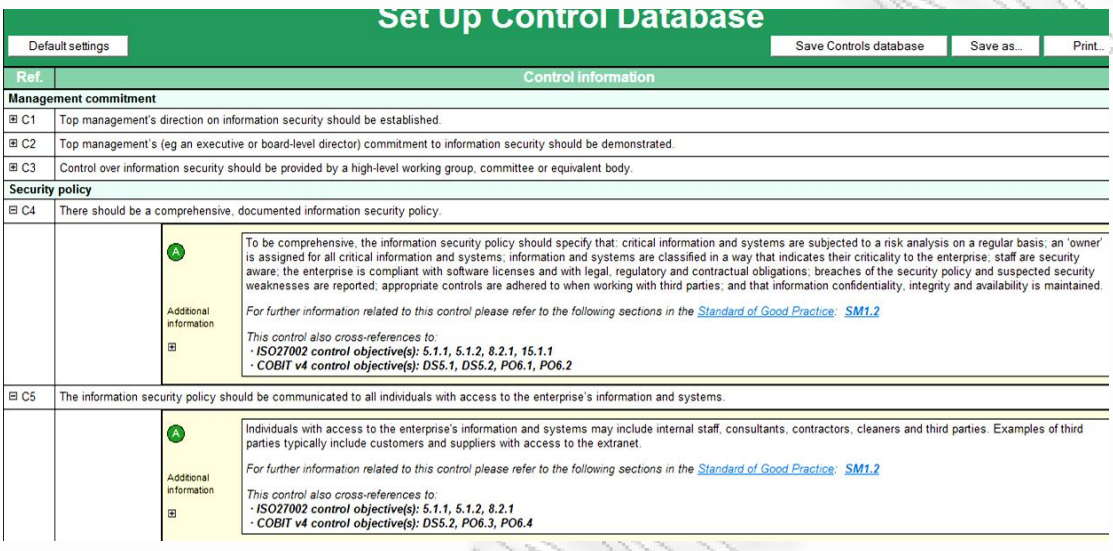
IRAM 22: Κατασκευή βάσης δεδομένων με τα σημεία ελέγχου που σχετίζονται άμεσα με τις απαιτήσεις ασφάλειας του οργανισμού. Σημείο ελέγχου C1.

Το σημείο ελέγχου C1 στο IRAM, «Η στάση της διοίκησης ως προς την ασφάλεια των πληροφοριών θα πρέπει να καθορίζεται μέσω της υλοποίησης και καθιέρωσης μιας Πολιτικής Ασφάλειας», αναφέρεται πρωτίστως στο πρότυπο του ISF (Standard of Good Practice) με κωδικό αναφοράς SM1.1 και SM2.1 όπως φαίνεται και παραπάνω. Στο εργαλείο IRAM, το συγκεκριμένο σημείο ελέγχου έχει αντιστοιχηθεί επίσης με το σημείο ελέγχου 6.1.1 και 6.1.3 του προτύπου ISO 27002/2005. Η διατύπωση είναι λίγο διαφορετική αλλά συνολικά ο στόχος και ο ελεγκτικός μηχανισμός που θεσπίζει είναι πλήρως αντίστοιχοι. Επιπλέον, το C1 αναφέρεται και στην υλοποίησή του, μέσω των διαδικασιών από το πλαίσιο Cobit 4 με κωδικούς αναφοράς ME4.2, PO1.1, PO1.2 και PO1.4**.** Όπως ήδη έχει παρουσιαστεί και στην ανάλυση του πλαισίου Cobit, στη κατηγορία PO1 ανήκουν οι διαδικασίες και οι πρακτικές του οργανισμού που έχουν να κάνουν με το καθορισμό της στρατηγικής της εταιρίας σε σχέση με τη Τεχνολογία της Πληροφορίας.

Όσον αφορά στο δεύτερο τμήμα που είναι τα χαρακτηριστικά του εν λόγω σημείου ελέγχου όπως είπαμε είναι ήδη καταγεγραμμένα στο εργαλείο IRAM (Fundamental, preventative, detective, reactive, managerial, applicable for all three properties of information: availability, confidentiality and integrity). Στο τρίτο τμήμα είναι οι πληροφορίες που συμπληρώθηκαν από τον αναλυτή. Η τράπεζα έχει καθιερώσει εσωτερικά αυτή τη πολιτική παρόλα αυτά δεν εφαρμόζεται σε όλα τα επίπεδα και έτσι επιλέχθηκε οτι είναι ναι μεν εσωτερικό πρότυπο (internal standard) αλλά δεν χρησιμοποιείται στον οργανισμό (not used in organization). Θεωρήθηκε οτι οι χρηματικοί πόροι για την υλοποίησή του είναι μεσαίου μεγέθους καθώς επίσης και οτι είναι σχετικά εύκολο στην υλοποίησή του αφού αρκεί η δέσμευση της διοίκησης (cost of control, ease of deployment). Σαν σημείο ελέγχου κρίθηκε οτι δεν είναι αρκετό για να

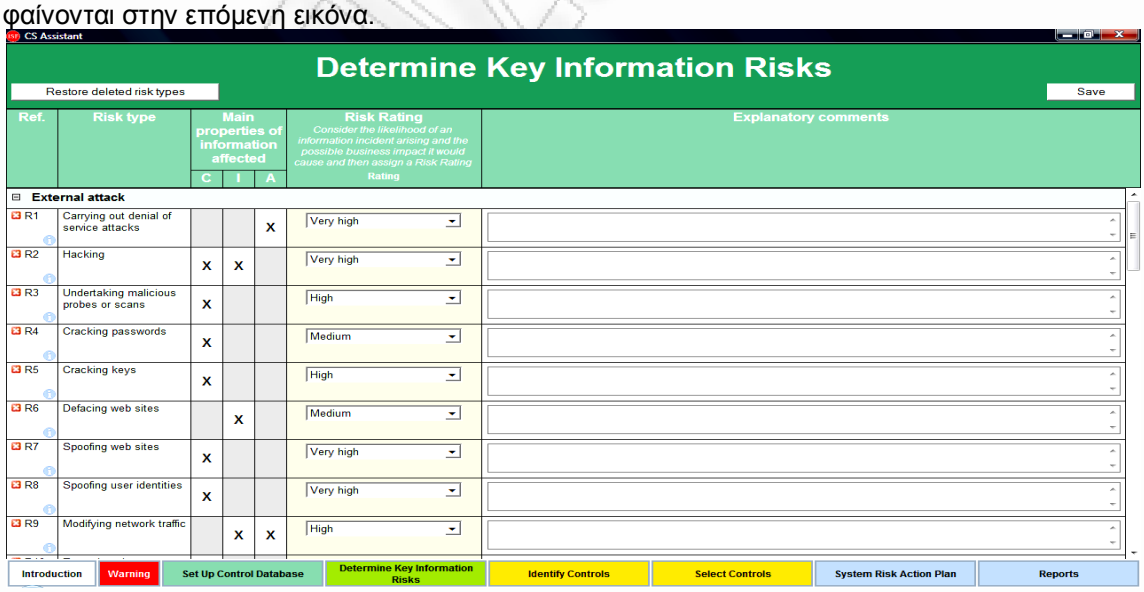
καλύψει τις ανάγκες ασφάλειας αλλά είναι ικανό να θεσπίσει το πλαίσιο και τα θεμέλια για τις απαιτήσεις του τραπεζικού οργανισμού σε θέματα ασφάλειας (strength of control). Τέλος υπεύθυνο τμήμα για την υλοποίησή του είναι η ίδια η διοίκηση δηλαδή το διοικητικό συμβούλιο.

Στην επόμενη εικόνα παρουσιάζονται τα πέντε σημεία ελέγχου που θα εξασφαλίσουν με την υλοποίησή τους οτι θα υπάρχει μια καταγεγραμμένη και εγκεκριμένη από το διοικητικό συμβούλιο πολιτική ασφαλείας για τη διαχείριση σύμφωνα με το πρότυπο ISO27002 της ασφάλειας των πληροφοριών.



IRAM 23: Σημεία ελέγχου (C1, C2, C3, C4, C5) σχετικά με τη καθιέρωση καταγεγραμμένης πολιτικής ασφάλειας

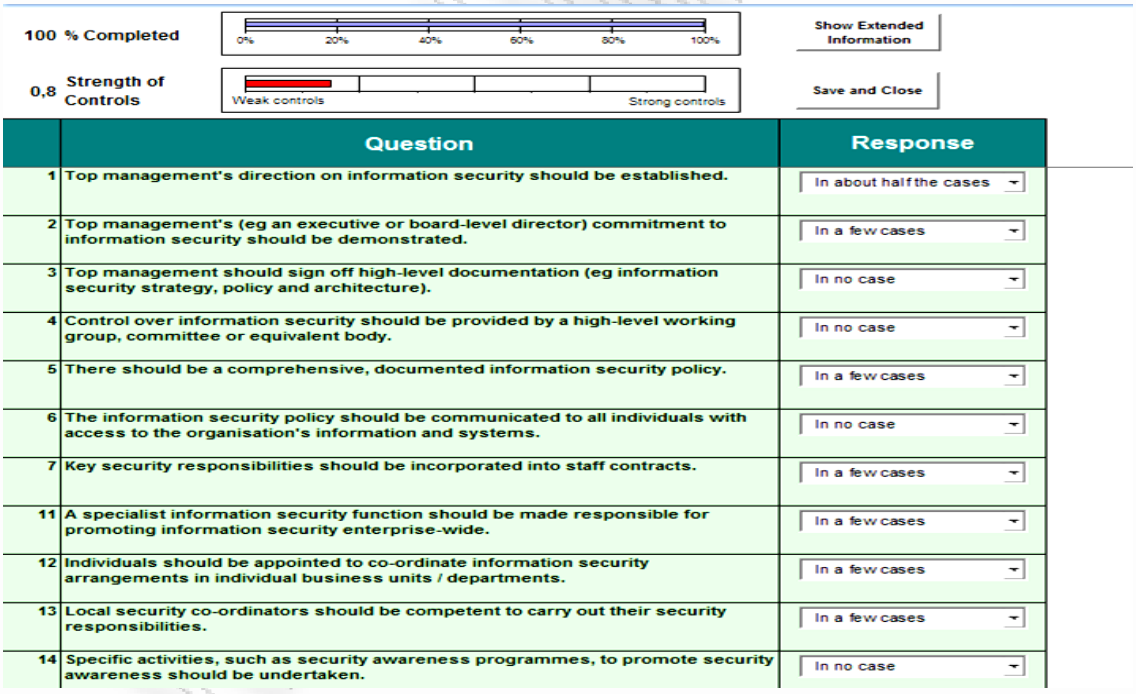
Εφόσον η εργασία που αφορά στην κατασκευή της βάσης δεδομένων ολοκληρώθηκε και ενημερώθηκε καταλλήλως με τα στοιχεία από τον τραπεζικό οργανισμό XBANK, η διαδικασία προχωρά στο επόμενο στάδιο που είναι ο καθορισμός των κυριότερων πληροφοριακών κινδύνων η οποία στην περίπτωσή μας έχει ολοκληρωθεί στην προηγούμενη φάση της μελέτης που είναι η Αποτίμηση των Απειλών και Ευπαθειών του συστήματος ηλεκτρονικής τραπεζικής. Τα αποτελέσματα από την προηγούμενη φάση αποτυπώθηκαν στο IRAM CS Assistant και φαίνονται στην επόμενη εικόνα.



IRAM 24: Εισαγωγή αποτελεσμάτων από την άσκηση αναγνώρισης κινδύνων.

Προχωρώντας στο επόμενο στάδιο της επιλογής σημείων ελέγχου, σε αυτό το σημείο κρίνεται απαραίτητο να αναφερθούμε στη προηγούμενη φάση και συγκεκριμένα στο στάδιο της εκτίμησης των ευπαθειών του συστήματος και τη συλλογή της πληροφορίας από τα ήδη υπάρχοντα σημεία ελέγχου του οργανισμού για την εξαγωγή μιας πρώτης διαβάθμισης. Συνεχίζοντας το παράδειγμά μας με την απειλή μιας επίθεσης Denial of Service (κωδικό όνομα στο IRAM CS Assistant: R1), στη προηγούμενη φάση είχε εκτιμηθεί οτι τα ήδη υπάρχοντα σημεία ελέγχου και η εφαρμογή βεβαίως αυτών δεν είναι αρκετά ώστε να αποτρέψουν τον επικείμενο κίνδυνο. Παραθέτουμε στην εικόνα που ακολουθεί εδώ, μέρος από το ερωτηματολόγιο, του οποίου οι απαντήσεις ενσωματώθηκαν αυτόματα στο εργαλείο IRAM Vulnerability Assessment και με βάση την αποτίμηση το σύστημα κρίθηκε με υψηλό (High) βαθμό ευπάθειας.

Σε αυτό το σημείο θα πρέπει να παρατηρήσουμε οτι οι πρώτες ερωτήσεις είναι σχετικές με την ύπαρξη πολιτικής ασφάλειας και τη στάση του οργανισμού απέναντι στην ασφάλεια της πληροφορίας. Οι απαντήσεις σε αυτό (αναδιπλώμενο μενού) έχουν να κάνουν με την εφαρμογή κάποιων ελεγκτικών πρακτικών και οχι αν έχουν θεσπιστεί στη τράπεζα. Η θέσπιση και καθιέρωση επίσημα καταγεγραμμένης πολιτικής ασφάλειας μπορεί να μην έχει άμεση σχέση και να είναι σημείο ελέγχου που να είναι ικανό από μόνο του να αποτρέψει μια επίθεση DoS, αλλά θέτει τη πολιτική και συνεπώς την πρόθεση του τραπεζικού οργανισμού να επιβάλλει επιπλέον ελεγκτικούς μηχανισμούς οι οποίοι θα συμμορφώνονται με τη πολιτική ασφάλειας και θα εξασφαλίζουν τη διαθεσιμότητα της πληροφορίας η οποία πλήττεται από μια τέτοια επίθεση. Προχωρώντας στο επόμενο στάδιο που είναι η επιλογή των συγκεκριμένων ελέγχων θα δούμε ποιοί είναι οι πιο συγκεκριμένοι ελεγκτικοί μηχανισμοί που εφαρμόζοντάς τους και υλοποιώντας τους θα μπορέσουμε να μειώσουμε το κίνδυνο μιας τέτοιας απειλής. Από τις απαντήσεις στις εν λόγω ερωτήσεις, παρατηρούμε, όπως ειπώθηκε και προηγουμένως, οτι ενώ ο οργανισμός έχει θεσπίσει μια πολιτική ασφάλειας και εμμέσως έχει δηλώσει τη στάση του ως προς την ασφάλεια, αυτή δεν εφαρμόζεται σε καμία περίπτωση και για αυτό το λόγο το σύστημα ηλεκτρονικής κρίθηκε ως τρωτό με υψηλό βαθμό ευπάθειας.



	Question	Response
1	Top management's direction on information security should be established.	In about half the cases
2	Top management's (eg an executive or board-level director) commitment to information security should be demonstrated.	In a few cases
3	Top management should sign off high-level documentation (eg information security strategy, policy and architecture).	In no case
4	Control over information security should be provided by a high-level working group, committee or equivalent body.	In no case
5	There should be a comprehensive, documented information security policy.	In a few cases
6	The information security policy should be communicated to all individuals with access to the organisation's information and systems.	In no case
7	Key security responsibilities should be incorporated into staff contracts.	In a few cases
11	A specialist information security function should be made responsible for promoting information security enterprise-wide.	In a few cases
12	Individuals should be appointed to co-ordinate information security arrangements in individual business units / departments.	In a few cases
13	Local security co-ordinators should be competent to carry out their security responsibilities.	In a few cases
14	Specific activities, such as security awareness programmes, to promote security awareness should be undertaken.	In no case

IRAM 25: Διαβάθμιση ευπάθειας στην επίθεση DoS βάσει της ανάλυσης στα σημεία ελέγχου.

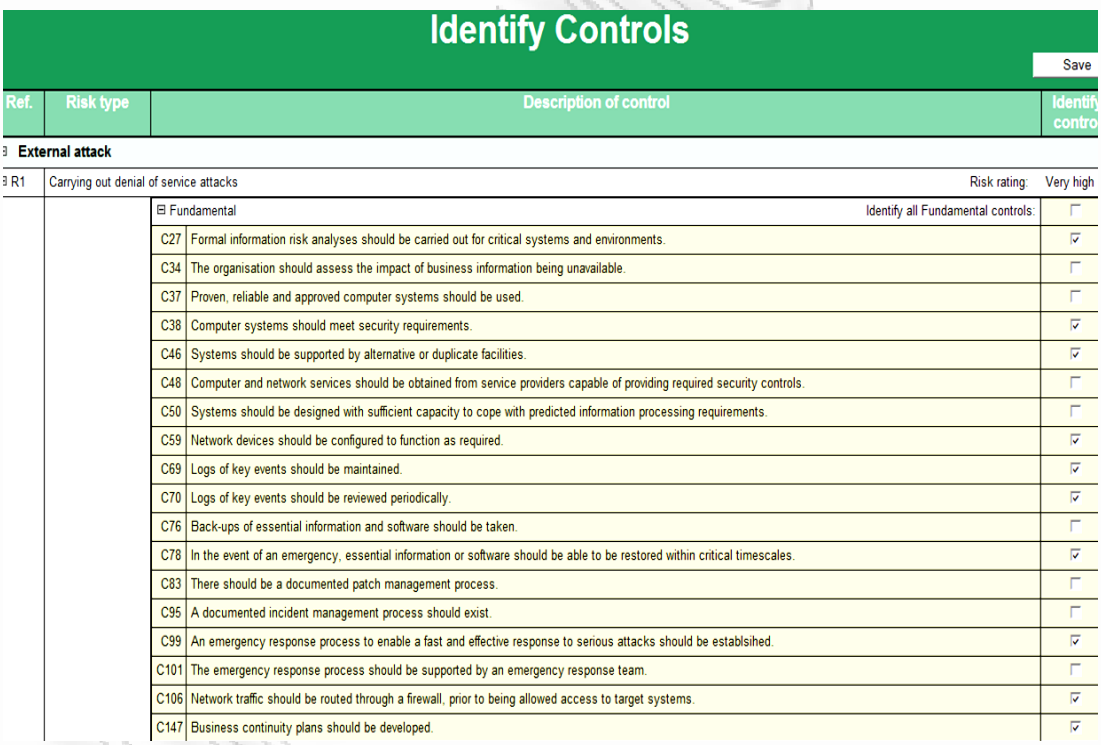
Αναγνώριση και Επιλογή Σημείων Ελέγχου

Στο στάδιο αυτό, που είναι και το τελευταίο της συνολικής άσκησης αποτίμησης επικινδυνότητας, γίνεται η αναγνώριση των σημείων ελέγχου που είναι σχετικά και ελαχιστοποιούν τους κινδύνους που έχουμε αναγνωρίσει και η τελική επιλογή αυτών για να

προσαρμοστεί και το πλάνο δράσης της τράπεζας. Για κάθε τύπο κινδύνου που έχουμε αναγνωρίσει, η εφορμογή IRAM CS Assistant έχει αντιστοιχήσει τα σημεία ελέγχου από τη βάση δεδομένων, που είναι σχετικά και μπορούν με την εφαρογή τους να ελαχιστοποιήσουν τη πιθανότητα του εκάστοτε κινδύνου. Όπως γίνεται αντιληπτό η εργασία αυτή είναι αρκετά χρονοβόρα και αρκετά εκτενής γιατί πρέπει να γίνει για κάθε τύπο απειλής που έχει αναγνωριστεί και ο αριθμός των σημείων ελέγχου που είναι σχετικά και εφαρμόσιμα στον κάθε ένα από αυτούς τους τύπους είναι σχετικά υψηλός. Συνεπώς, στα πλαίσια αυτής της εργασίας παρουσιάζεται η ανάλυση μόνο για το πρώτο τύπο απειλής που έχουμε αναλύσει και στις προηγούμενες φάσεις αυτής της μελέτης R1: Κίνδυνος Επίθεσης Denial of Service (DoS).

Στη φόρμα επιλογής των σημείων ελέγχου προτείνονται 23 σημεία ελέγχου τα οποία ο αναλυτής καλείται να αξιολογήσει και βάσει όλης της προηγούμενης ανάλυσης που έχει προηγηθεί να επιλέξει αν θα τα προτείνει προς υλοποίηση προκειμένου να ελαχιστοποιηθεί ο κίνδυνος μιας επίθεσης DoS. Όπως μπορούμε να παρατηρήσουμε στην ακόλουθη εικόνα, που απεικονίζεται μέρος από την εργασία στο IRAM, τα σημεία ελέγχου C1, C2, C3, C4 και C5 που σχετίζονται με τη πολιτική ασφάλειας δεν έχουν αντιστοιχιστεί με αυτό το τύπο απειλής, ακριβώς γιατί όπως εξηγήθηκε η πολιτική ασφάλειας δεν είναι άμμεσος ελεγκτικός μηχανισμός που εφαρμόζοντάς τον θα μπορέσει να αποτραπεί μια απειλή DoS ή να προστατευθεί το σύστημα ηλεκτρονικής τραπεζικής συγκεκριμένα από αυτή.

Από τα προτεινόμενα σημεία ελέγχου και ελεγκτικούς μηχανισμούς επιλέχθηκαν 10 οι οποιοι πρέπει να υλοποιηθούν άμεσα με στόχο την ελαχιστοποίηση αυτού του πολύ πιθανού κινδύνου να προκαλέσει απώλεια στη διαθεσιμότητα του συστήματος ηλεκτρονικής τραπεζικής με σοβαρές συνέπειες στην επιχειρησιακή δραστηριότητα. Τα 10 αυτά σημεία ελέγχου παρατίθενται και στην συνέχεια στην ελληνική.

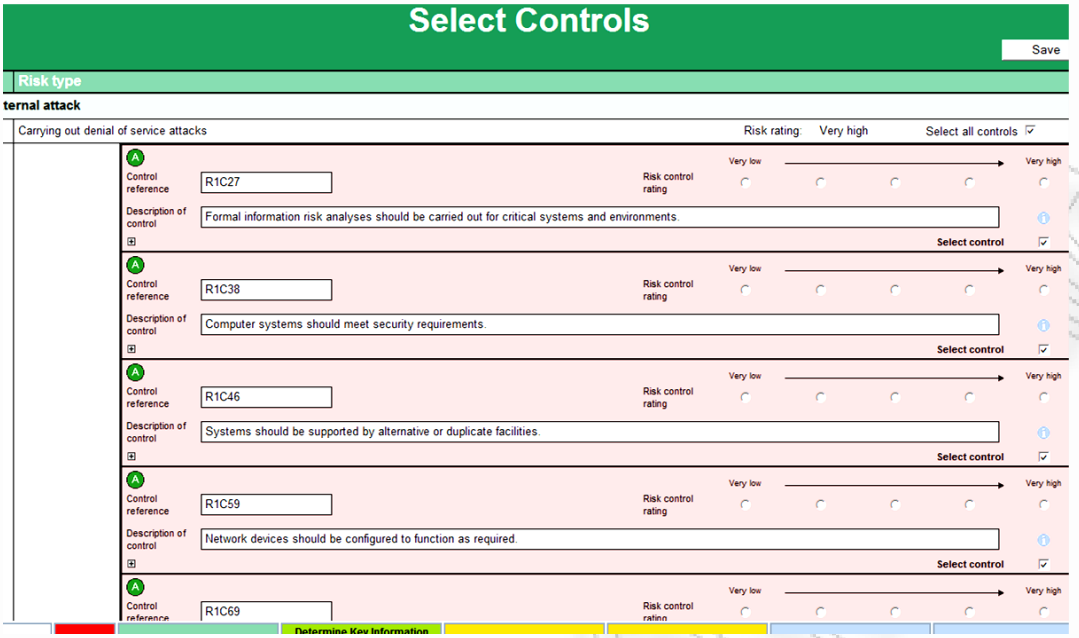


Identify Controls

Save

Ref.	Risk type	Description of control		Identify control
External attack				
R1	Carrying out denial of service attacks		Risk rating:	Very high
		⊟ Fundamental	Identify all Fundamental controls:	☐
		C27	Formal information risk analyses should be carried out for critical systems and environments.	☑
		C34	The organisation should assess the impact of business information being unavailable.	☐
		C37	Proven, reliable and approved computer systems should be used.	☐
		C38	Computer systems should meet security requirements.	☑
		C46	Systems should be supported by alternative or duplicate facilities.	☑
		C48	Computer and network services should be obtained from service providers capable of providing required security controls.	☐
		C50	Systems should be designed with sufficient capacity to cope with predicted information processing requirements.	☐
		C59	Network devices should be configured to function as required.	☑
		C69	Logs of key events should be maintained.	☑
		C70	Logs of key events should be reviewed periodically.	☑
		C76	Back-ups of essential information and software should be taken.	☐
		C78	In the event of an emergency, essential information or software should be able to be restored within critical timescales.	☑
		C83	There should be a documented patch management process.	☐
		C95	A documented incident management process should exist.	☐
		C99	An emergency response process to enable a fast and effective response to serious attacks should be establsihed.	☑
		C101	The emergency response process should be supported by an emergency response team.	☐
		C106	Network traffic should be routed through a firewall, prior to being allowed access to target systems.	☑
		C147	Business continuity plans should be developed.	☑

IRAM 26: Αναγνώριση σχετικών ελεγκτικών μηχανισμών με την αντιμετώπιση DoS Επιθέσεων.



IRAM 27: Επιλογή ελεγκτικών μηχανισμών για την αντιμετώπιση DoS Επιθέσεων.

Τα αποτελέσματα της ανάλυσης και συνεπώς τα σημεία ελέγχου που επιλέχθηκαν καθώς και μια μικρή επεξήγηση παρουσιάζονται εδώ.

R1C27 «Formal information risk analyses should be carried out for critical systems and environments».

«Θα πρέπει να διεξαχθεί επίσημα ανάλυση επικινδυνότητας για όλα τα κρίσιμα συστήματα και περιβάλλοντα της τράπεζας».

Αυτό το σημείο ελέγχου είναι από τα βασικότερα πέρα από τη πολιτική ασφάλειας εφόσον μόνο μετά από μια τέτοια άσκηση μπορεί η διοίκηση να έχει μια σαφή εικόνα των πληροφοριών και συνεπώς συστημάτων που πρέπει να προστατέψει. Στη παρούσα εργασία και για το συγκεκριμένο οργανισμό η άσκηση αυτή πραγματοποιήθηκε μόνο όμως για το σύστημα ηλεκτρονικής τραπεζικής που κρίθηκε το πιο κρίσιμο. Αυτή η άσκηση θα πρέπει να επαναλαμβάνεται κάθε φορά που το σύστημα υπόκειται σε σημαντικές αλλαγές στην υποδομή ή στην αρχιτεκτονική του δικτύου.

R1C38 «Computer systems should meet security requirements».

«Τα συστήματα πληροφορικής θα πρέπει να τηρούν τις απαιτήσεις και τις προδιαγραφές της ασφάλειας»

Με βάση αυτό το σημείο ελέγχου θα πρέπει να εξασφαλίζεται εμμέσως και η ύπαρξη πολιτικής ασφάλειας αφού οι απαιτήσεις ασφάλειας καθορίζονται από αυτή.

R1C46 «Systems should be supported by alternative or duplicate facilities».

«Τα κρίσιμα συστήματα θα πρέπει να υποστηρίζονται από εναλλακτικές ή εφεδρικές υποδομές»

Το σημείο ελέγχου αυτό έχει σαν στόχο να υποστηρίξει τη διαθεσιμότητα της πληροφορίας και τη συνέχεια των εργασιών σε περίπτωση που το περιστατικό ασφάλειας συμβεί.

R1C59 «Network devices should be configured to function as required».

«Οι συσκευές και ο εξοπλισμός δικτύου θα πρέπει να είναι ρυθμισμένα για να λειτουργούν με βάση τις απαιτήσεις ασφάλειας του οργανισμού».

Με αυτή την ελεγκτική διαδικασία η τράπεζα θα πρέπει να θεσπίσει ποιές είναι οι απαραίτητες ρυθμίσεις στο δίκτυο έτσι ώστε τυχόν επιθέσεις να μπορούν να αποτραπούν ή να ανιχνευτούν εγκαίρως.

R1C69 «Logs of key events should be maintained».

«Θα πρέπει να τηρείται αρχείο καταγραφής κινήσεων και περιστατικών ασφαλείας»

Σκοπός αυτού του ελέγχου είναι να υπάρχει μιας μορφής καταγραφή κινήσεων στα συστήματα έτσι ώστε ύποπτες επαναλαμβανόμενες και αποτυχημένες προσπάθειες πρόσβασης να μπορούν να προληφθούν εγκαίρως.

R1C70 Logs of key events should be reviewed periodically.

«Το αρχείο καταγραφής κινήσεων και περιστατικών ασφαλείας θα πρέπει περιοδικά να παρακολουθείται»

Το R1C70 είναι συμπληρωματικό του R1C69 μιας και ένα αρχείο καταγραφής κινήσεων από μόνο του δεν είναι αποτελεσματικό σημείο ελέγχου αν κάποιος δεν είναι υπεύθυνος να το παρακολουθεί.

R1C73 «System monitoring should include scanning host systems for known vulnerabilities».

«Η παρακολούθηση των συστημάτων θα πρέπει να περιλαμβάνει την ηλεκτρονική σάρωση των συστημάτων για τυχόν τρωτά σημεία»

Ο έλεγχος αυτός γίνεται με ειδικά προγράμματα και είναι αυτοματοποιημένος έτσι ώστε τυχόν αλλαγές στις ρυθμίσεις του εξοπλισμού και των υποδομών που εκθέτουν την ασφάλεια τους να μπορούν να γίνουν εγκαίρως γνωστά και να προληφθούν περεταίρω περιστατικά ασφάλειας.

R1C78 In the event of an emergency, essential information or software should be able to be restored within critical timescales.

«Σε περίπτωση ανάγκης, σημαντικά μέρη από τις κρίσιμες εφαρμογές (εδώ σύστημα ηλεκτρονικής τραπεζικής) θα πρέπει να μπορούν να λειτουργήσουν μέσα στα κρίσιμα χρονικά πλαίσια».

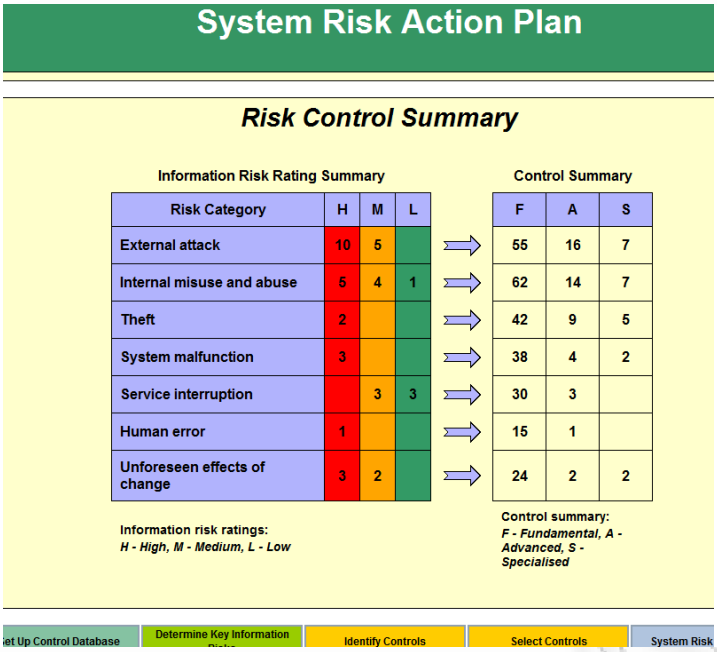
R1C93 Intrusion detection mechanisms should be applied to critical systems.

«Συστήματα ανίχνευσης παρείσφρησης θα πρέπει να υπάρχουν σε όλα τα κρίσιμα συστήματα και εφαρμογές»

Το **R1C93** ανήκει στη κατηγορία εξειδικευμένων σημείων ελέγχου (advanced) με την έννοια οτι σχετίζεται άμεσα με το καθεστώς κινδύνου και απειλής που ο τραπεζικός οργανισμός θέλει να καλύψει. Πράγματι, ένας μηχανισμός ανίχνευσης πιθανών εισβολών, που βεβαίως θα είχε ρυθμιστεί κατάλληλα θα μπορούσε να αποτρέψει μια DoS επίθεση στα συστήματα της τράπεζας άμεσα.

Αποτελέσματα της άσκησης αναγνώρισης και επιλογής σημείων ελέγχου

Εφόσον η επιλογή όλων των σημείων ελέγχου που μετριάζουν τα επίπεδα κινδύνου που αναγνωρίστηκαν ως τα υψηλότερα για το σύστημα ηλεκτρονικής τραπεζικής, έχει πλέον ολοκληρωθεί ακολουθώντας τη πρακτική που περιγράφηκε σε προηγούμενη παράγραφο, η εφαρμογή IRAM παραθέτει συνολική αναφορά της άσκησης αυτής. Παρακάτω στην εικόνα (IRAM 28) παρατηρούμε ότι για τη κάθε κατηγορία κινδύνων έχουν υπολογιστεί το σύνολο των θεμελιωδών, των πιο προηγμένων και των πιο εξειδικευμένων σημείων ελέγχου. Για όλους του κινδύνους που σχετίζονται με εξωτερική απειλή του συστήματος ηλεκτρονικής τραπεζικής έχουν αναγνωριστεί δέκα ως πολύ υψηλοί και 5 μέτριου βαθμού. Με την ανάλυση που προηγήθηκε επιλέχθηκαν 55 τύποι ελεγκτικών μηχανισμών που είναι βασικοί (θεμελιώδεις), 16 πιο προηγμένοι και 7 σημεία ελέγχου που είναι εξειδικευμένα για την αντιμετώπιση των εκάστοτε κινδύνων.



IRAM 28: Αποτελέσματα του σταδίου επιλογής σημείων ελέγχου

4.5 Συμπεράσματα από τη μελέτη περίπτωσης και περιορισμοί

Από την παρούσα μελέτη περίπτωσης για την Ανάλυση και Εκτίμηση της Επικινδυνότητας που διεξήχθη στο σύστημα ηλεκτρονικής τραπεζικής της XBANK προέκυψαν τα εξής συμπεράσματα:

Το εργαλείο του ISF IRAM παρέχει ένα ολοκληρωμένο σετ από εφαρμογές οι οποίες μπορούν να βοηθήσουν οχι μόνο τον οργανισμό, που για λογαριασμό του γίνεται η άσκηση εκτίμησης επικινδυνότητας, αλλά πολύ περισσότερο και την ομάδα αναλυτών που συμμετέχουν στην εργασία αυτή να εξάγουν αποτελεσματικά και ακριβή συμπεράσματα τόσο για τους κυριότερους κινδύνους και απειλές που περιστοιχίζουν τα πληροφοριακά συστήματα αλλά και να επιλέξουν τα σωστά σημεία και μέτρα ελέγχου ή να θεσπίσουν τους σωστούς ελεγκτικούς μηχανισμούς έτσι ώστε να μειωθούν στο ελάχιστο τα επίπεδα επικινδυνότητας και η πιθανότητα περιστατικών ασφάλειας που μπορεί αυτοί να προκαλέσουν.

Βάσει της έρευνας που διεξήχθη, το IRAM σαν μεθοδολογία αποτίμησης επικινδυνότητας και υλοποίηση μέτρων ασφάλειας είναι από τις πλέον κατάλληλες για να εφαρμόσει κανείς σε ένα τραπεζικό οργανισμό. Μπορεί να βασίζεται στο πρότυπο 2011 του ISF, αλλά και το τελευταίο προέκυψε από τα διεθνή πρότυπα βέλτιστων πρακτικών και μέσα στο πρότυπο του 2011 γίνεται πλήρης αντιστοίχηση με αυτά. Δικαίως λοιπόν θεωρούμε οτι το IRAM σαν μεθοδολογία είναι από τις καταλληλότερες αν όχι η καταλληλότερη, αφού σε πρώτη φάση υλοποιεί και είναι πλήρως εναρμονισμένη και με το διεθνές πρότυπο διαχείρισης ασφάλειας ISO27001:2005 και τις απαιτήσεις αυτού, μέσω του ISO27002:2006, αλλά και με το πλαίσιο Cobit που αναγάγει την όλη διαχείριση της ασφάλειας από τον οργανισμό στα πλαίσια των επιχειρησιακών διαδικασιών. Υπάρχει πλήρης αντιπαραβολή των μέτρων που επιλέγονται στο IRAM με το πρότυπο 2011 του ISF, με τις απαιτήσεις του προτύπου ISO 27001, τα σημεία ελέγχου βάσει ISO 27002 και το πλαίσιο Cobit. Συνεπώς ο οργανισμός στη πορεία προς την υλοποίηση ενός από τα προαναφερθέντα πρότυπα και στη πιστοποίησή του από αυτά, μπορεί ανά πάσα στιγμή να έχει γνώση σε ποιό σημείο της πορείας της διαδικασίας αυτής βρίσκεται.

Επιπλέον, ένα ακόμη συγκριτικό πλεονέκτημα που παρατηρήθηκε χρησιμοποιώντας τη μεθοδολογία του ISF, είναι ότι παρέχει τη μέθοδο και το τρόπο σε ένα οργανισμό για να αποτιμήσει ποιό από τα συστήματά του/ εφαρμογές του είναι το πιο κρίσιμο. Αυτό γίνεται με τη βοήθεια του «εργαλείου» εκτίμησης κρισιμότητας Information Risk Scorecard της μεθοδολογίας του ISF και στην συγκεκριμένη μελέτη περίπτωσης κρίθηκε οτι προτεραιότητα στην άσκηση αποτίμησης επιχειρησιακού αντίκτυπου είχε το σύστημα ηλεκτρονικής τραπεζικής. Σε όλες τις

περιπτώσεις ο οργανισμός XBANK θα υφίσταντο μεγαλύτερες βλάβες από το σύστημα ηλεκτρονικής τραπεζικής και άρα αποτιμήθηκε ως το πιο κρίσιμο.

Το εργαλείο και η εφαρμογή IRAM που παρέχει ο ISF για να υποστηρίξει όλη αυτή τη διαδικασία είναι πολύ απλό στη χρήση και μπορεί να το χρησιμοποιήσει ένας αναλυτής ανεξάρτητα από τη συνεργασία με το υπόλοιπο προσωπικό του οργανισμού, φυσικά αν έχει τις απαντήσεις και μπορεί να κρίνει και να αποτιμήσει τους σχετικούς τύπους επιχειρησιακού αντίκτυπου και τις σχετικές απειλές. Αποτελείται από τρεις υπό εφαρμογές και τα αποτελέσματα της μιας είναι ροή εισόδου προς την επόμενη. Τα δεδομένα όπως οι τύποι του επιχειρησιακού αντίκτυπου, οι τύποι των απειλών και τα σημεία ελέγχου προς επιλογή στο τέλος της διαδικασίας υπάρχουν μέσα στο εργαλείο και ο αναλυτής το μόνο που έχει να κάνει είναι να επιλέξει ποιά από αυτά είναι σχετικά με τον οργανισμό στον οποίο γίνεται η ανάλυση και ποιά από όλα τα μέτρα είναι σχετικά με τη λειτουργία της πληροφορικής στον οργανισμό.

Περνώντας στην πράξη και στη διαδικασία, η άσκηση Εκτίμησης Απειλών και Ευπαθειών, δηλαδή η δεύτερη φάση της συνολικής εργασίας, αν και μπορεί να εφαρμοστεί αυτόνομα, κρίνεται οτι η Ανάλυση Επιχειρησιακού Αντίκτυπου έχει πολύ σημαντικό ρόλο στην επιλογή τελικά των τύπων κινδύνου που θα επιλέξουμε για να καλύψουμε με τα αντίστοιχα μέτρα. Στο τέλος της δεύτερης φάσης της ανάλυσης, και συγκεκριμένα στο πίνακα (IRAM 18) οι αναφορές που εξάγαμε από το IRAM βοήθησαν πάρα πολύ την άσκηση μας, διότι η διοίκηση επέλεξε σωστά να δώσει περισσότερη βαρύτητα στους κινδύνους που έχουν συνολικά τον υψηλότερο επιχειρησιακό αντίκτυπο. Συνεπώς, η πρώτη φάση ενός έργου Αποτίμησης της Επικινδυνότητας θα πρέπει σίγουρα να περιλαμβάνει αποτελέσματα της αποτίμησης των επιπτώσεων στην επιχειρησιακή δραστηριότητα, αφού αυτό το βήμα διευκολύνει και εξομαλύνει τη διαδικασία επιλογής των κατάλληλων μέτρων ασφάλειας.

Έχοντας αυτό σαν τελικό συμπέρασμα, συμπεραίνουμε οτι το πρότυπο ISO 27001 είναι το καταλληλότερο για καλύψει και σε ένα τραπεζικό οργανισμό τις ανάγκες πιστοποίησης και συμμόρφωσης ταυτόχρονα με τη πράξη Διοικητή της Τράπεζας της Ελλάδος αριθ. 2577/9.3.2006. Το πλαίσιο Cobit από την άλλη είναι απαραίτητο για να πλαισιώσει μια τέτοια άσκηση υλοποίησης προτύπου ασφάλειας, εφόσον είναι άρρητα συνυφασμένο με την υλοποίηση σημείων ελέγχου για την ασφάλεια ως προς τις επιχειρησιακές διαδικασίες και κάνει σύνδεση με αυτές. Τέλος η μέθοδος IRAM αποδείχθηκε ως άκρως αποτελεσματική για να βοηθήσει έναν οργανισμό και δη τραπεζικό, στην υλοποίηση και τεκμηρίωση σημείων ελέγχου και μέτρων ασφάλειας. Θα πρέπει να σημειωθεί όμως οτι η έκταση της παρούσας εργασίας δεν είναι αρκετή για να φιλοξενήσει ολόκληρη την άσκηση υλοποίησης ενός πλαισίου για την ασφάλεια της πληροφορίας στο τραπεζικό οργανισμό XBANK, δηλαδή την παρουσίαση και τεκμηρίωση όλων των μέτρων ασφάλειας που πρέπει να ληφθούν για να ελαχιστοποιηθεί η πιθανότητα ενός περιστατικού ασφάλειας προερχόμενο από τους αναγνωρισμένους κινδύνους.

Βιβλιογραφικές Αναφορές

- Καλαμάκι, Α., (2008) «Συστήματα Εσωτερικών Ελέγχων και Εφαρμογή Μεθοδολογίας Sarbanes – Oxley στη σύγχρονη επιχείρηση :Ο ρόλος του Μηχανικού Παραγωγής», Διπλωματική Εργασία, Εθνικό Μετσόβιο Πολυτεχνείο, Αθήνα, Ιούλιος 2008.

- Κατσίκας, Σ., «Ελεγκτική Πληροφοριακών Συστημάτων», Σημειώσεις μαθήματος 'Πληροφοριακά Συστήματα', Πανεπιστήμιο Πειραιώς, Αθήνα.

- Pennathur, A., (2001), "Clicks and bricks": e-Risk Management for banks in the age of the Internet. *Journal of Banking and Finance.* (25) p.2103-2123.

- Tuttle, B., Vandervelde, S., (2007) "An empirical examination of CobiT as an internal controlframework for information technology", International Journal of Accounting Information Systems, Volume 8, Issue 4, Pages 240–263.

- Chen, H., Corriveau, J.,P., (2009), "Security Testing and Compliance for Online Banking in Real-World", *Proceedings of the International MultiConference of Engineers and Computer Scientists* 2009 Vol I, IMECS 2009, March 18 - 20, 2009, Hong Kong.

- Ridley,G., Young, J. ; Carroll, P., (2004) «COBIT and its utilization: a framework from the literature», Proceedings of the 37th Annual Hawaii International Conference on System Sciences, 5-8 Jan. 2004.

- Hussain, A., Heidemann, J., Papadopoulos, C., (2003) "A Framework for Classifying Denial of Service Attacks" Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications. SIGCOMM 2003.

- Bank van de Nederlandse Antillen, (2007), "Provisions and Guidelines for Safe and Sound Electronic Banking", Willemstad, [Online]. Διαθέσιμο: http://www.centralbank.an/docs/Electronic%20Banking.pdf, επίσκεψη ιστότοπου 05 Δεκεμβρίου 2009.

- ΕΕΔΕ, ΕΙΠ (2008), "CobiT Awareness & Overview: Principles and Core Elements - high level insight in CobiT as an IT Governance Framework", Athens.

- "The ISO 27000 Directory", [Online]. Διαθέσιμο: http://www.27000.org/, [επίσκεψη ιστότοπου 06 Δεκεμβρίου 2011].

- ISO/IEC 27001 (2005), "Information Technology - Security techniques – Information Security Management Systems - Requirements" BS 7799-2:2005.

- ISO/IEC 27000 (2009), "INTERNATIONAL STANDARD ISO/IEC 27000: Information technology — Security techniques — Information security management systems — Overview and vocabulary ", First Edition, 2009-05-01

- ISO/IEC 27002 (2005), "Information Technology - Security techniques – Code of Practice for Information Security Management".

- Cobit 4.1 (2007), "Control Objectives for Information and related Technology", [Online], Διαθέσιμο: http://www.isaca.org/Knowledge-Center/cobit/Documents/CobiT_4.1.pdf, [επίσκεψη ιστότοπου 12 Απριλίου 2012].

- Tripp, R., (2006) "SEPA", [Online]. Διαθέσιμο: http://www.howbankswork.com/13.html#sepa6, [επίσκεψη ιστότοπου 03 Ιανουαρίου 2012].
- ITGI (2008), "Aligning CobiT® 4.1,ITIL® V3 and ISO/IEC 27002 for Business Benefit", [Online], Διαθέσιμο: http://www.best-management-practice.com/gempdf/Aligning_COBITITILV3ISO27002_Bus_Benefit_9Nov08_Research.pdf, [επίσκεψη ιστότοπου 12 Απριλίου 2012].
- Robertson, W., Vigna, G., Kruegel, C., Kemmerer, R., (2006), "Using Generalization and Characterization Techniques in the Anomaly-based Detection of Web Attacks", The 13th Annual Network and Distributed System Security Symposium, 2-3 February 2006[Online], Διαθέσιμο: http://iseclab.org/papers/webfuzzing.pdf, [επίσκεψη ιστότοπου 12 Απριλίου 2012].
- Beasley, M., Branson, B., Hancock, B., (2010), "COSO's 2010 report on ERP", Committee of Sponsoring Organizations of the Treadway Commission. [Online], Διαθέσιμο: http://www.coso.org/documents/COSOSurveyReportFULL-Web-R6FINALforWEBPOSTING111710.pdf, [επίσκεψη ιστότοπου 15 Απριλίου 2012].
- Shaw, H., (2006) "The Trouble with COSO", CFO Magazine, March 15, 2006. [Online], Διαθέσιμο: http://www.cfo.com/article.cfm/5598405, [επίσκεψη ιστότοπου 15 Απριλίου 2012].
- Federal Deposit Insurance Corporation, Electronic Banking - Safety and Soundness Procedures, USA, 1998.
- Nowack, D., Samson, F., (2008), "The German Federal Government's Key Requirements on 'Trusted Computing'". ENISA Quarterly Review, Oct-Dec,. 4(4), p. 7. [Online],Διαθέσιμο: http://www.enisa.europa.eu/publications/eqr/issues [επίσκεψη ιστότοπου 19 Δεκεμβρίου 2011].
- Robertson, W., (2009), "Detecting and Preventing Attacks Against Web Applications", University of California, Doctor of Philosophy in Computer Science.
- The Open Group, (2011), Open Information Security Management Maturity Model (O-Ism3), [Online], Διαθέσιμο: http://www.google.gr/books?hl=el&lr=&id=67tozXY6U-kC&oi=fnd&pg=PR9&dq=MEHARI+(Information+risk+analysis+and+management+methodology)+V3,+Concepts+and+Mechanisms&ots=-Mk02C-TzL&sig=D1TnSjT005JqOdmLTQSsy9YW24U&redir_esc=y#v=onepage&q&f=false, [επίσκεψη ιστότοπου 13 Απριλίου 2012].
- Conclin, A., (2008), " Why FISMA Falls short: The need for security metrics", WISP 2008, Montreal, Quebec, Canada, December 7-9 2007.
- ISF, (2004), "The 2011 Standard of Good Practice", June 2011.
- ISF, (2004), "Understanding and using the ISF's Information Risk Mgmt Tools v2, March 2008.
- ΕΕΤ (2009)), «Ελληνική Ένωση Τραπεζών – Τομείς Δραστηριότητας – Συστήματα πληρωμών», Ανακοίνωση: Νοέμβριος 2009. [Online], Διαθέσιμο:

http://www.hba.gr/2Tomeis/2TomeisDetails.asp?Mpage=7&Id=182, [επίσκεψη ιστότοπου 29 Δεκεμβρίου 2011].

- Πενταφρόνημος Γ., «Πρότυπα και πολιτικές Ασφάλειας Πληροφοριακών Συστημάτων», Σημειώσεις Διαλέξεων, 2009.
- ISF (2004) "Information Risk Analysis Methodologies (IRAM) Project: Business Impact Assessment Methodology", June 2004, Information Security Forum.
- Write, S., (2007) "Using ISO 27001 for PCI DSS Compliance" White Paper, Siemens Insight Consulting, [Online], Διαθέσιμο: http://www.insight.co.uk/files/whitepapers/Using%20ISO%2027001%20for%20PCI%20DSS%20Compliance%20(White%20paper).pdf.
- ΤτΕ, (2009) «Οι Αρμοδιότητες της Τράπεζας της Ελλάδος», [Online] Διαθέσιμο: http://www.bankofgreece.gr/Pages/el/Bank/responsibilities.aspx#tel, [επίσκεψη ιστότοπου 29 Δεκεμβρίου 2011].
- ISF (2005) "Information Risk Analysis Methodologies (IRAM) Project: Threat and Vulnerability Assessment Methodology", June 2005, Information Security Forum.
- Κασσάρας Γ., (2008) «Επισκόπηση PCI DSS», Open Web Application Security Project, 25 Νοεμβρίου 2008. [Online], Διαθέσιμο: http://owasp.wordpress.com/2008/11/25/pci-dss-%CF%80%CF%81%CE%BF-%CE%B5%CF%80%CE%B9%CF%83%CE%BA%CF%8C%CF%80%CE%B7%CF%83%CE%B7-%CE%BC%CE%AD%CF%81%CE%BF%CF%82-1%CE%BF/, [επίσκεψη ιστότοπου 15 Απριλίου 2012].
- Aceituno, V., (2006), "ISM3: A Standard for Information Security Management", ISSA The Global Voice for Information Security
- Aceituno, C., (2008), «Usefulness of an Information Security Maturity Model», Information Systems Control Journal, Vol. 2, 2008.
- Παληογιάννη, Π., (2008) «Ο Εσωτερικός Έλεγχος στα πλαίσια των Πληροφοριακών Συστημάτων», Διπλωματική Εργασία, Μεταπτυχιακό Πρόγραμμα στη Λογιστική και Χρηματοοικονομική, Πανεπιστήμιο Μακεδονίας, Θεσσαλονίκη, 2008.
- ICAP Group: Τραπεζικοί Οργανισμοί και Επιχειρησιακοί - Λειτουργικοί κίνδυνοι [Online], Διαθέσιμο: http://dir.icap.gr/news/index_gr_6996.asp, [επίσκεψη ιστότοπου 31 Δεκεμβρίου 2012].
- ΕΚΤ (2008) «Ευρωσύστημα: Ενιαίος Χώρος Πληρωμών σε Ευρώ», Έκτη Έκθεση Προόδου, Ευρωπαϊκή Κεντρική Τράπεζα, Νοέμβριος 2008. [Online], Διαθέσιμο: http://www.ecb.int/pub/pdf/other/singleeuropaymentsarea200811el.pdf, [επίσκεψη ιστότοπου 29 Δεκεμβρίου 2011].
- Insight Consulting, (2005) «CRAMM User Guide Issue», έκδοση 5.1 σε Πολέμη Δ., (2011) «S - P o r t : Ένα ασφαλές, αυτοματοποιημένο, συνεργατικό περιβάλλον για την δημιουργία μεθοδολογιών Αποτίμησης Επικινδυνότητας, Σχεδίου Επιχειρησιακής Συνέχειας και Κέντρων Αποκατάστασης Καταστροφών για Πληροφοριακά Συστήματα Λιμένων-Υφιστάμενη Κατάσταση και ελλείψεις υπαρχουσών μεθοδολογιών», Μάρτιος 2011, Πανεπιστήμιο Πειραιώς.

- ISACA, Document G24 (2003) "IS Auditing Guideline: Internet Banking, Document G24". [Online], Διαθέσιμο: http://www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=18637, [επίσκεψη ιστότοπου 29 Δεκεμβρίου 2011].

- ISF (2006) "Information Risk Analysis Methodologies (IRAM) Project: Control Selection Methodology", January 2006, Information Security Forum. [Online], Διαθέσιμο: http://www.eede.gr/pdf/eip_cobit_250608_br.pdf, [επίσκεψη ιστότοπου 29 Δεκεμβρίου 2011].

- ENISA, (2006), "Risk Management - Principles and Inventories for Risk Management / Risk Assessment methods and tools". [Online]. Διαθέσιμο: http://www.enisa.europa.eu/act/rm/cr/risk-management-inventory/files/deliverables/risk-management-principles-and-inventories-for-risk-management-risk-assessment-methods-and-tools, [επίσκεψη ιστότοπου 12 Δεκεμβρίου 2011].

- "Comparison between ITIL, Cobit and ISO27001" (2010), Security Procedures, Information System Auditing Resources, [Online]. Διαθέσιμο: http://www.securityprocedure.com/comparison-between-cobit-itil-and-iso-27001, [επίσκεψη ιστότοπου 25 Ιανουαρίου 2012].

- ISF, (2004) "Information Security Status Survey 2003: Consolidated Reports" https://www.securityforum.org/downloads/documentview/665, [επίσκεψη ιστότοπου 25 Ιανουαρίου 2012].

- **CIS Benchmarks**
  http://holisticinfosec.org/toolsmith/docs/august2007.pdf
  http://www.cisecurity.org/

- **FISMA**
  http://csrc.nist.gov/groups/SMA/fisma/overview.html

- **BS ISO/IEC 20000-1**
  http://shop.bsigroup.com/ProductDetail/?pid=000000000030126227

- **ITIL**
  http://www.itil-officialsite.com
  http://www.netweek.gr/_branded_content/hp/pdf/4AA1-4406ENW.pdf
  http://www.best-management-practice.com/gempdf/itSMF_An_Introductory_Overview_of_ITIL_V3.pdf

- **Common Criteria for Information Technology Security Evaluation**
  http://en.wikipedia.org/wiki/Common_Criteria
  http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R3.pdf
  http://www.commoncriteriaportal.org/cc/

- **ENISA**
  http://www.enisa.europa.eu/act/rm/cr/risk-management-inventory

Παράρτημα

IRAM: Βάση Δεδομένων από σημεία ελέγχου/ Μέτρα ασφάλειας

Set Up Control Database

Ref.	Control information
Management commitment	
⊞ C1	Top management's direction on information security should be established.
⊞ C2	Top management's (eg an executive or board-level director) commitment to information security should be demonstrated.
⊞ C3	Control over information security should be provided by a high-level working group, committee or equivalent body.
Security policy	
⊞ C4	There should be a comprehensive, documented information security policy.
⊞ C5	The information security policy should be communicated to all individuals with access to the enterprise's information and systems.
Staff agreements	
⊞ C6	Staff agreements should be established, which specify information security responsibilities.
⊞ C7	Key security responsibilities should be incorporated into staff contracts.
⊞ C8	Information security responsibilities should be taken into account when applicants are screened for employment.
Information security function	
⊞ C9	There should be a specialist information security function.
⊞ C10	A specialist information security function should be made responsible for managing information security enterprise-wide.
Local security co-ordination	
⊞ C11	Individuals should be appointed to co-ordinate information security arrangements locally.
⊞ C12	Local security co-ordinators should be competent to carry out their security responsibilities.
Security awareness	
⊞ C13	Staff should be made aware of the key elements of information security and why it is needed.
⊞ C14	Personal information security responsibilities should be understood.
⊞ C15	Specific activities, such as security awareness programmes, to promote security awareness should be undertaken.
Security education	
⊞ C16	IT staff should be educated/trained to develop and apply security controls.
⊞ C17	Business users should be educated/trained in how to run systems correctly.
Security classification	
⊞ C18	A security classification scheme should be established.
⊞ C19	The security classification scheme should be based on the criticality of information and systems in use.
⊞ C20	The security classification scheme should be based on the sensitivity of information and systems in use.
Roles and responsibilities	
⊞ C21	'Ownership' of critical information and systems should be assigned to capable individuals.

⊞ C22	The responsibilities of 'owners' should be clearly defined and accepted.
⊞ C23	The responsibilities for key security tasks should be assigned to individuals who are capable of performing them.
⊞ C24	Users should be organised to minimise the risk of theft, fraud, error and unauthorised changes to information (eg by supervision of activities, prohibition of lone working and segregation of duties).
⊞ C25	The duties of staff running computer systems should be segregated from those developing systems.
⊞ C26	Reliance on key individuals should be minimised (eg by automating tasks, ensuring complete and accurate documentation, and arranging alternative cover for key positions).
Risk analysis/assessment	
⊞ C27	Formal information risk analyses should be carried out for critical systems and environments.
⊞ C28	Information risk analysis should determine risk by performing a business impact assessment and a threat and vulnerability assessment.
⊞ C29	The results of the risk analysis should include a clear, documented identification of key risks, an assessment of the potential business impact of each risk, and recommendations for the actions required to reduce risks to acceptable levels.
⊞ C30	The risk analysis process should help to identify special security controls (eg encryption for sensitive information), evaluate the costs of implementing security controls, and determine the limitations of security controls.
⊞ C31	The results of the risk analysis, including any residual risk, should be communicated to and signed-off by the owner.
Confidentiality requirements	
⊞ C32	The organisation should assess the impact of business information being disclosed to unauthorised individuals.
Integrity requirements	
⊞ C33	The organisation should assess the impact of business information being accidentally corrupted or deliberately manipulated.
Availability requirements	
⊞ C34	The organisation should assess the impact of business information being unavailable.
Security architecture	
⊞ C35	An 'information security architecture' should be established to implement consistent, simple-to-use security functionality across multiple computer systems.
⊞ C36	The 'information security architecture' should enable standard security controls to be applied throughout the enterprise.
Asset management	
⊞ C37	Proven, reliable and approved computer systems should be used.
⊞ C38	Computer systems should meet security requirements.
⊞ C39	Essential information about hardware and software (eg unique identifiers, version numbers and physical locations) should be recorded in inventories.
⊞ C40	Software licensing requirements should be met.
Physical protection	
⊞ C41	Buildings that house critical IT facilities should be physically protected against accident or attack.
⊞ C42	Physical access to buildings that house critical IT facilities should be restricted to authorised individuals.
⊞ C43	Critical computer equipment and documentation should be protected against theft.
Power supplies	
⊞ C44	Critical computer equipment and facilities should be protected against power outages.

Hazard protection	
⊞ C45	Computer equipment and facilities should be protected against fire, flood, environmental and other natural hazards.
Resilience	
⊞ C46	Systems should be supported by alternative or duplicate facilities.
⊞ C47	Sensitive applications should be run on dedicated systems.
Service providers	
⊞ C48	Computer and network services should be obtained from service providers capable of providing required security controls.
⊞ C49	Computer and network services should be supported by documented contracts or service level agreements.
Installation and network design	
⊞ C50	Systems should be designed with sufficient capacity to cope with predicted information processing requirements.
⊞ C51	Systems should be protected by using a range of in-built security controls.
Host system configuration	
⊞ C52	Host systems should be configured to function as required.
⊞ C53	Host systems should be configured to prevent unauthorised or incorrect updates.
Workstation configuration	
⊞ C54	Workstations should be purchased from a list of approved suppliers.
⊞ C55	Workstations should be tested prior to use.
⊞ C56	Workstations should be supported by maintenance arrangements.
⊞ C57	Workstations should be protected by physical controls.
⊞ C58	Workstations should be configured to 'time-out' after a period of inactivity.
Configuring network devices	
⊞ C59	Network devices should be configured to function as required.
⊞ C60	Network devices should be configured to prevent unauthorised or incorrect updates.
Network documentation	
⊞ C61	Networks should be supported by accurate and up-to-date documentation.
Access control	
⊞ C62	Access to information and systems should be restricted to authorised individuals.
⊞ C63	Access control arrangements should restrict access to only approved system capabilities.
User authorisation	
⊞ C64	Users should be authorised before access privileges are granted.
⊞ C65	A process should be established to ensure timely action relating to requesting, establishing, issuing, suspending and closing of user accounts.
User authentication	
⊞ C66	Users should be authenticated before access is granted to target systems.
⊞ C67	'High-risk' users should be authenticated by using strong authentication mechanisms before access is granted.
Sign-on process	

⊞ C68	Users s ould be sub ect to a rigorous sign on process before t e gain access to target s stems.
Event logging	
⊞ C69	ogs of e e ents s ould be maintained.
⊞ C70	ogs of e e ents s ould be re iewed periodicall .
⊞ C71	ogs of e e ents s ould be protected against unaut orised c ange.
System / Network monitoring	
⊞ C72	Computer s stems s ould be monitored to identif potential securit breac es.
⊞ C73	S stem monitoring s ould include scanning ost s stems for nown ulnerabilities.
⊞ C74	S stem monitoring s ould include c ec ing w et er powerful utilities/commands a e been disabled on attac ed ost s stems.
⊞ C75	S stem monitoring s ould include c ec ing for t e e istence and configuration of unaut orised wireless networ s.
Back-up	
⊞ C76	ac ups of essential information and software s ould be ta en.
⊞ C77	ac ups of essential information and software s ould be ta en on a regular basis according to a defined c cle.
⊞ C78	n t e e ent of an emergenc essential information or software s ould be able to be restored wit in critical timescales.
Change management	
⊞ C79	A documented c ange management process s ould be establis ed.
⊞ C80	C anges s ould be tested prior to being applied to t e li e en ironment.
⊞ C81	C anges s ould be re iewed to ensure t e do not compromise securit .
Patch management	
⊞ C82	ere s ould be a strateg for patc management.
⊞ C83	ere s ould be a documented patc management process.
⊞ C84	e patc management process s ould be supported b a management framewor .
Emergency fixes	
⊞ C85	mergenc fi es s ould be tested.
⊞ C86	mergenc fi es s ould be re iewed.
⊞ C87	mergenc fi es s ould be applied in accordance wit documented standards/procedures.
Virus protection	
⊞ C88	Virus protection arrangements s ould be establis ed.
⊞ C89	Virus protection arrangements s ould co er ser ers.
⊞ C90	Virus protection arrangements s ould co er wor stations including laptops .
⊞ C91	Virus protection software s ould be ept up to date.
Malicious mobile code protection	
⊞ C92	nterprise wide arrangements s ould be establis ed to protect against malicious mobile code.
Intrusion detection	
⊞ C93	ntrusion detection mec anisms s ould be applied to critical s stems eg using DS .

⊞ C94	Intrusion detection mechanisms should be applied to networks (eg using NIDS).
Incident management	
⊞ C95	A documented incident management process should exist.
⊞ C96	Incidents should be recorded.
⊞ C97	Incidents should be reviewed.
⊞ C98	The security implications of incidents - and any remedial action - should be reviewed.
⊞ C99	An emergency response process to enable a fast and effective response to serious attacks should be establsihed.
⊞ C100	The emergency response process should outline the actions to be taken in the event of a serious attack.
⊞ C101	The emergency response process should be supported by an emergency response team.
Forensic investigations	
⊞ C102	There should be a process for dealing with incidents that require forensic investigation.
⊞ C103	There should be processes to ensure that evidence is preserved.
External access/connections	
⊞ C104	External connections should be individually identified.
⊞ C105	External connections should be approved by the 'owner'.
Firewalls	
⊞ C106	Network traffic should be routed through a firewall, prior to being allowed access to target systems.
Third party access	
⊞ C107	Third parties who have access to target systems should be uniquely identified.
⊞ C108	Third party access should be subject to a risk analysis.
⊞ C109	Third party access should be approved.
⊞ C110	Third party access should be supported by contracts.
Wireless access	
⊞ C111	Wireless access should be authorised only from approved locations.
⊞ C112	Wireless access should be encrypted.
⊞ C113	Wireless access should be protected using a VPN (Virtual Private Network).
Remote working	
⊞ C114	Personal computers used by staff working in remote locations should be purchased from a list of approved suppliers.
⊞ C115	Personal computers used by staff working in remote locations should be tested prior to use.
⊞ C116	Personal computers used by staff working in remote locations should be supported by maintenance arrangements.

⊞ C11	Personal computers used b staff wor ing in remote locations s ould be protected b p sical and logical controls.
⊞ C118	Personal computers used b staff wor ing in remote locations s ould be protected from iruses and malicious mobile code.
Remote maintenance	
⊞ C11	emote maintenance s ould be restricted to aut orised indi iduals.
⊞ C120	emote maintenance s ould be confined to indi idual sessions.
⊞ C121	emote maintenance s ould be sub ect to re iew.
Special controls	
⊞ C122	Voice networ facilities eg telep one e c anges s ould be monitored regularl .
⊞ C123	Access to oice networ facilities s ould be restricted.
Information privacy	
⊞ C124	esponsibilit for managing information pri ac s ould be establis ed.
⊞ C12	Securit controls for andling personall identifiable information s ould be applied.
⊞ C12	e organisation s ould compl wit legal and regulator re uirements for information pri ac .
Cryptography	
⊞ C12	Cr ptograp ic solutions s ould be used to protect t e confidentialit of sensiti e information.
⊞ C128	Cr ptograp ic solutions s ould be used to preser e t e integrit of critical information.
⊞ C12	Cr ptograp ic solutions s ould be used to confirm t e identit of t e originator of information.
⊞ C130	Cr ptograp ic solutions s ould be appro ed and documented.
⊞ C131	Cr ptograp ic e s s ould be managed tig tl eg to protect t em against unaut orised access or destruction .
Public key infrastructure	
⊞ C132	ere a Public e nfrastructure P is used it s ould be protected b ardening t e underl ing operating s stem s .
⊞ C133	ere a public e infrastructure P is used it s ould be protected b restricting access to Certification Aut orities.
E-mail	
⊞ C134	mail s stems s ould be supported b a securit polic .
⊞ C13	mail s stems s ould be supported b securit awareness acti ities.
⊞ C13	Standards/procedures s ould be establis ed for t e protection of e mail s stems.
⊞ C13	mail s stems s ould be protected b tec nical securit controls.
Instant messaging	
⊞ C138	ere s ould be a polic go erning t e use of instant messaging.

⊞ C139	The security features of instant messaging applications should be deployed.
⊞ C140	The security elements of instant messaging infrastructure should be configured.
Web-enabled applications	
⊞ C141	Specialised technical controls should be applied to web-enabled applications.
Electronic commerce	
⊞ C142	A process to ensure that information security is incorporated into electronic commerce initiatives should be established.
⊞ C143	The security risks of electronic commerce systems should be assessed.
⊞ C144	Processes should be in place to ensure security is not sacrificed for the sake of speed.
Outsourcing	
⊞ C145	A process to govern the selection and management of outsource contractors should be established.
⊞ C146	Outsourcing arrangements should be supported by documented agreements specifying security requirements.
Business continuity	
⊞ C147	Business continuity plans should be developed.
⊞ C148	Business continuity plans should be supported by contingency arrangements.
⊞ C149	Business continuity plans should be tested periodically.
Security audit/review	
⊞ C150	Security audits/reviews should provide the system 'owner', and top management, with an independent assessment of the security status of the system.
⊞ C151	Security audits/reviews should be performed on a regular basis.
⊞ C152	Security audits/reviews should be independent.
Security monitoring	
⊞ C153	The condition of the information security of the enterprise should be monitored periodically.
⊞ C154	The condition of the information security of the enterprise should periodically be reported to top management.
Development methodologies and environment	
⊞ C155	Development activities should be carried out in accordance with a documented system development methodology.
⊞ C156	System development activities should be performed in specialised development environments, isolated from the live environment.
⊞ C157	System development activities should be protected against disruption and disclosure of information.
Quality assurance	
⊞ C158	Quality assurance of key security activities should be performed during the development lifecycle.
Specifications of requirements	
⊞ C159	Business requirements (including those for information security) should be agreed and documented before commencing detailed design.

⊞ C160	usiness re uirements s ould be signed off b t e rele ant business and Securit anagers.
General security controls	
⊞ C161	e full range of general securit controls s ould be considered w en designing t e s stem under de elopment.
Application controls	
⊞ C162	e full range of application controls eg control o er input processing and output s ould be considered w en designing t e s stem under de elopment.
⊞ C16	e uired securit controls s ould be identified.
Handling information	
⊞ C164	Additional protection s ould be pro ided for applications t at in ol e andling sensiti e material or transferring sensiti e information.
⊞ C16	Sensiti e information eld on data storage media including magnetic tapes dis s printed results and stationer s ould be protected against corruption loss or disclosure.
System design/build	
⊞ C166	nformation securit re uirements for t e s stem under de elopment s ould be considered w en designing t e s stem.
⊞ C16	S stem build acti ities including coding and pac age customisation s ould be carried out in accordance wit industr good practice.
⊞ C168	S stem build acti ities s ould be performed b indi iduals wit ade uate s ills/tools.
⊞ C16	S stem build acti ities s ould be inspected to identif unaut orised modifications or c anges w ic ma compromise securit controls.
Acquisition	
⊞ C1 0	Securit re uirements s ould be considered w en ac uiring computer s stems.
⊞ C1 1	Securit deficiencies in computer s stems s ould be identified.
⊞ C1 2	obust and reliable computer s stems s ould be ac uired.
⊞ C1	Ade uate software licenses s ould be a uired for planned use.
Testing	
⊞ C1 4	All elements of a s stem s ould be tested before it is promoted to t e li e en ironment.
⊞ C1	Acceptance tests s ould be conducted in an isolated area t at simulates t e li e en ironment.
⊞ C1 6	est results s ould be documented c ec ed against e pected results appro ed b users and signed off b t e owner.
System promotion criteria	
⊞ C1	igorous criteria s ould be met before new s stems are promoted into t e li e en ironment.
Installation process	
⊞ C1 8	ew s stems s ould be installed in t e li e en ironment in accordance wit a documented installation process.
Post-implementation review	
⊞ C1	Post implementation re iews s ould be conducted for all new s stems.