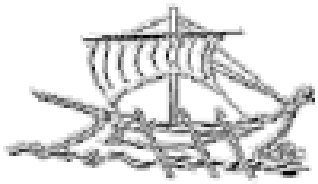


Α.Ε.Ι ΠΕΙΡΑΙΑ Τ.Τ.

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ Τ.Ε.

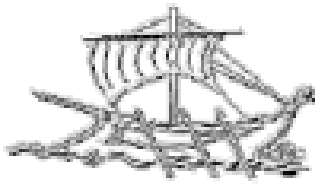
ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Ανάλυση της ασφάλειας στις υποδομές του νέφους από την σκοπιά του τελικού χρήστη και του παρόχου υπηρεσιών

Αργύρης Α. Γκιώνης

Εισηγητής: Χαράλαμπος Ζ. Πατρικάκης

ΑΘΗΝΑ
ΙΟΥΝΙΟΣ 2017



PIRAEUS UNIVERSITY OF APPLIED SCIENCES
SCHOOL OF ENGINEERING
DEPARTMENT OF COMPUTER SYSTEMS ENGINEERING

DEGREE THESIS

Security analysis on cloud infrastructures both from the end user and service provider perspective

Argiris A. Gkionis

Supervisor: Charalampos Z. Patrikakis

ATHENS
JUNE 2017

(Κενό φύλλο)

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Ανάλυση της ασφάλειας στις υποδομές του νέφους τόσο από τη σκοπιά του τελικού χρήστη και του παρόχου υπηρεσιών

Αργύρης Α. Γκιώνης
Α.Μ. 42624

Εισηγητής:

Χαράλαμπος Ζ. Πατρικάκης

Εξεταστική Επιτροπή:

Ημερομηνία εξέτασης

(Κενό φύλλο)

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Ο/Η κάτωθι υπογεγραμμένος/η Γκιώνης Αργύρης, του Απόστολου Γκιώνη, με αριθμό μητρώου 42624 φοιτητής/τρια του Τμήματος Μηχανικών Η/Υ Συστημάτων Τ.Ε. του Α.Ε.Ι. Πειραιά Τ.Τ. πριν αναλάβω την εκπόνηση της Πτυχιακής Εργασίας μου, δηλώνω ότι ενημερώθηκα για τα παρακάτω:

«Η Πτυχιακή Εργασία (Π.Ε.) αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο του συγγραφέα, όσο και του Ιδρύματος και θα πρέπει να έχει μοναδικό χαρακτήρα και πρωτότυπο περιεχόμενο.

Απαγορεύεται αυστηρά οποιοδήποτε κομμάτι κειμένου της να εμφανίζεται αυτούσιο ή μεταφρασμένο από κάποια άλλη δημοσιευμένη πηγή. Κάθε τέτοια πράξη αποτελεί προϊόν λογοκλοπής και εγείρει θέμα Ηθικής Τάξης για τα πνευματικά δικαιώματα του άλλου συγγραφέα. Αποκλειστικός υπεύθυνος είναι ο συγγραφέας της Π.Ε., ο οποίος φέρει και την ευθύνη των συνεπειών, ποινικών και άλλων, αυτής της πράξης.

Πέραν των όποιων ποινικών ευθυνών του συγγραφέα σε περίπτωση που το Ίδρυμα του έχει απονείμει Πτυχίο, αυτό ανακαλείται με απόφαση της Συνέλευσης του Τμήματος. Η Συνέλευση του Τμήματος με νέα απόφασης της, μετά από αίτηση του ενδιαφερόμενου, του αναθέτει εκ νέου την εκπόνηση της Π.Ε. με άλλο θέμα και διαφορετικό επιβλέποντα καθηγητή. Η εκπόνηση της εν λόγω Π.Ε. πρέπει να ολοκληρωθεί εντός τουλάχιστον ενός ημερολογιακού 6μήνου από την ημερομηνία ανάθεσης της. Κατά τα λοιπά εφαρμόζονται τα προβλεπόμενα στο άρθρο 18, παρ. 5 του ισχύοντος Εσωτερικού Κανονισμού.»

(Κενό φύλλο)

ΕΥΧΑΡΙΣΤΙΕΣ

Η παρούσα πτυχιακή εργασία ολοκληρώθηκε σε ένα ενδιαφέρον γνωστικό αντικείμενο, όπως αυτό της ασφάλειας του υπολογιστικού νέφους. Την προσπάθεια μου αυτή υποστήριξε ο επιβλέπων καθηγητής μου Χαράλαμπος Πατρικάκης, τον οποίο θα ήθελα να ευχαριστήσω.

Επιπλέον, θα ήθελα να ευχαριστήσω τον Μιχάλη Ξευγένη για τις πολύτιμες συμβουλές του και την μητέρα μου Αναστασία για την υλική και ψυχολογική υποστήριξη που μου παρείχε όλο αυτό το διάστημα των σπουδών μου.

(Κενό φύλλο)

ΠΕΡΙΛΗΨΗ

Στην σύγχρονη εποχή, η πληροφορία και ο εξοπλισμός πληροφορικής αποτελούν περιουσιακό στοιχείο για τον κάθε οργανισμό και χρήζουν προστασίας. Το αντικείμενο που διαπραγματεύεται η εργασία, είναι το θέμα που αφορά την ασφάλεια γύρο από το υπολογιστικό νέφος. Αρχικά γίνεται μια γενική επισκόπιση στο υπολογιστικό νέφος η οποία αναφέρει την ιστορική εξέλιξη, σημαντικά χαρακτηριστικά καθώς και τις υπηρεσίες που προσφέρει. Στην συνέχεια ακολουθεί μια αναφορά διαχείρισης κινδύνων στο υπολογιστικό νέφος, αναφέροντας χαρακτηριστικά ασφαλείας του νέφους, σημαντικά εργαλεία αντιμετόπισης των κινδύνων, και τις υπηρεσίες του νέφους γύρω από την σκοπιά της ασφάλειας. Θα μπορούσαμε να αναφέρουμε ότι αυτή η αναφορά είναι και ο πυρήνας της πτυχιακής εργασίας κάθως γίνεται μια σημαντική παρουσίαση σε θέματα ασφάλειας. Επιπρόσθετα γίνεται εισαγωγή στα πλαίσια ασφαλείας, και την χρησιμότητα τους προς τους οργανισμούς. Ακολούθως γίνεται επιλογή και ανάλυση του πλαισίου ασφαλείας COBIT, το οποίο θα χρησιμοποιηθεί στην συνέχεια για την περίπτωση χρήσης του υπολογιστικού νέφους από μια εταιρεία. Τέλος γίνεται παρουσίαση ενός σεναρίου για τις ανάγκες του οποίου δημιουργήθηκε μια εικονική εταιρεία με την ονομασία Z-Corp, η οποία έχει σκοπό να προσφέρει στους πελάτες της, την εφαρμογή της μέσα από το υπολογιστικό νέφος. Στην συνέχεια γίνεται ανάλυση των χαρακτηριστικών και των ευπαθειών τόσο από την πλευρά του οργανισμού όσο και από του υπολογιστικού νέφους. Μέσω του πλαισίου ασφαλείας COBIT εξετάζεται άν ο οργανισμός είναι έτοιμος να ανατεθεί στο υπολογιστικό νέφος, αναλύοντας τους κινδύνους που ενδέχεται να αντιμετωπίσει, καθώς και την εφαρμογή βέλτιστων διαδικασιών και των αντίστοιχων πρακτικών για την αντιμετώπιση των κινδύνων και των ευπαθειών.

ΕΠΙΣΤΗΜΟΝΙΚΗ ΠΕΡΙΟΧΗ: Τεχνολογίες Διαδικτύου

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: υπολογιστικό νέφος, ασφάλεια, εικονοποίηση, πρότυπα, υπηρεσίες

ABSTRACT

In modern times, the information and IT equipment are assets for every company and are in need for protection. The main theme of this thesis are the issue that is concerning the security around the cloud computing. At first, there is an overview of cloud computing, indicating its historical evolution, important characteristics and services which offers. It follows a reference of security management in cloud computing, mentioning the security characteristics of cloud, important tools for dealing with risks, and the services of cloud from a security perspective. We could say that this topic is the core of the thesis, as it takes place a presentation on security issues. Moreover there is an introduction on security frameworks and the usefulness of them to enterprises. Follows a selection and analysis of a particular security framework, which will be used for the use-case study of an enterprise using the cloud computing. In the final chapter there is a presentation of a use-case study, for the needs of which includes a virtual enterprise who wants to offer the application to the customers via cloud computing. Furthermore, analysis of characteristics and vulnerabilities from perspective, enterprise and cloud computing, is done. Through the COBIT security framework is examined if an enterprise is ready to outsource, analyzing the risks that may deal, as and adjustment of best processes and their relative practices to reduce or nihilist those risks and vulnerabilities.

SCIENTIFIC AREA: Internet Technologies
KEYWORDS: cloud computing, security, virtualization, standards, services

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

ΠΙΝΑΚΑΣ ΑΚΡΩΝΥΜΙΩΝ

VPN	Virtual Private Network
VN	Virtual Network
URL	Universal Resource Locator
LAN	Local Area Network
VM	Virtual Machine
ISMS	Information Security Management System
CIA	Confidentiality, Integrity, Availability
IDS	Intrusion Detection System
SSL	Secure Socket Layer
NIDS	Network Intrusion Detection System
HIDS	Host Intrusion Detection System
SLA	Service Level Agreement
ISACA	Information Systems Audit and Control Association
COBIT	Control Objectives for Information and Related Technologies
SOA	Service Oriented Architecture
ITL	Information Technology Laboratory
NIST	National Institute of Standards and Technology
SPI	Sensitive Personal Information
PAAS	Platform As A Service
SAAS	Software As A Service
IAAS	Infrastructure As A Service
BPAAS	Business Process As A Service
IP	Internet Protocol
DNS	Domain Name Server
DOS	Denial Of Service
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
IPX	Internet Packet eXchange
SPX	Sequential Packet eXchange
ID	Intrusion Detection
REST	Representational State Transfer
IT	Information Technology
API	Application Program Interface
ESB	Enterprise Service Bus
IPS	Intrution Prevention System
WSSP	Web Service Security Protocol
IBM	International Business Machines
CSP	Cloud Service Provider
CSM	Cisco Security Manager
AWS	Amazon Web Services
ACL	Access Control List
SIEM	Security Information and Event Management

OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
COSO	Committee of Sponsoring Organizations
PBRM	Plan, Build, Run & Monitor
EDM	Evaluate, Direct &Monitor
APO	Align, Plan & Organize
EDM	Evaluate, Direct & Monitor
DSS	Deliver, Service & Support
PII	Personally Identifiable Information
CIO	Chief Information Officer
DMZ	Demilitarized Zone
RJE	Remote Job Entry
DEC	Digital Equipment Corporation
IOT	Internet Of Things
ERP	Enterprise Resource Planning
IAM	Identity and Access Management

(Κενό φύλλο)

1. ΕΙΣΑΓΩΓΗ

Η παρούσα πτυχιακή εργασία με τίτλο «Ανάλυση της ασφάλειας στις υποδομές του νέφους από την σκοπιά του τελικού χρήστη και του παρόχου υπηρεσιών» εκπονήθηκε στα πλαίσια της υποχρεωτικής πτυχιακής εργασίας κατά την διάρκεια σπουδών μου στο Τμήμα Μηχανικών Υπολογιστικών Συστημάτων του Α.Ε.Ι ΠΕΙΡΑΙΑ Τ.Τ. το έτος 2016-2017 υπό την επίβλεψη του καθηγητή κ. Χαράλαμπου Πατρικάκη. Το πιο σημαντικό κίνητρο επιλογής αυτού του θέματος, είναι ότι το υπολογιστικό νέφος αποτελεί το μέλλον του διαδικτύου και της επιχειρηματικής τεχνολογίας, προσφέροντας εντυπωσιακά αποτελέσματα. Ζωτικής σημασίας είναι η προστασία της πληροφορίας που αποτελεί περιουσιακό στοιχείο για τον κάθε οργανισμό, καθώς και τα συστήματα και τα δίκτυα που την υποστηρίζουν από ένα μεγάλο φάσμα απειλών προκειμένου να ελαχιστοποιούνται οι κίνδυνοι. Σκοπός της εργασίας είναι να αναδειχθούν οι κίνδυνοι στο υπολογιστικό νέφος και οι τρόποι με τους οποίους να ελαχιστοποιηθούν ή ακόμη και να μηδενιστούν. Η ασφάλεια της πληροφορίας επιτυγχάνεται μέσω εφαρμογής ενός πλαισίου ασφαλείας και μιας κατάλληλης ομάδας ειδικών ασφαλείας. Είναι πολύ σημαντικό για τις επιχείρησεις και του χρήστες να μπορούν να ακολουθούν τις τελευταιές εξελίξεις της τεχνολογίας με όσο γίνεται πιο ασφαλή τρόπο, αλλά και να επωφελούνται από αυτές, ώστε να δημιουργούν αξία μέσω της πληροφορικής. Τώρα, όσο αναφορά τις εξελίξεις που υπάρχουν την τρέχουσα χρονία καθώς και προβλέψεις που αφορούν το μέλλον του υπολογιστικού νέφους, είναι οι εξής:

- Πάνω από το ¼ των εφαρμογών είναι διαθέσιμες πλέον στο «νέφος».[52]
- Επιπλέον η υπηρεσία SaaS είναι αυξημένη στην αγορά κατά 20.5%.[52]
- Πλέον το 50% των επιχειρήσεων έχει υιοθετίσει υβριδικά «νέφη». [52]
- Μία ακόμη εξέλιξη που περιμένουμε στο άμεσο μέλλον είναι ότι έξυπνες εφαρμογές θα καταφέρνουν να διαχειρίζονται δίκτυα διακομιστών, αποθήκευση στο «νέφος» και ολοκληρωμένα κέντρα δεδομένων.[51]
- Όσο αναφορά το μέλλον της ασφάλειας στο υπολογιστικό νέφος, από το 2018, το 60% των επιχειρήσεων που εφαρμόζουν τα κατάλληλα εργαλεία ελέγχου θα αντιμετοπίζουν κατά ¼ λιγότερες αποτυχίες ασφαλείας.[51]

Ωστόσο, μερικές από τις θετικές επιπτώσεις που θα έχουν οι μελλοντικές εξελίξεις του υπολογιστικού νέφους στην κοινωνία είναι ότι: [53]

- Ο κόσμος θα είναι σε θέση να παίρνει έξυπνες αποφάσεις, γιατί θα μπορεί να αναλύει αμέσως ψηφιακά κάθε πληροφορία που επιθυμεί.
- Οι περιορισμοί της γλώσσας θα πέσουν καθώς γίνεται χρήση μεταφραστικών υπηρεσιών.
- Από την πλευρά του κλάδου των επιχειρήσεων, με την χρήση του υπολογιστικού νέφους μικρομεσαίες επιχειρήσεις θα μπορούν να κλιμακωθούν σε παγκόσμιο επίπεδο.

Τέλος, η δομή της εργασίας είναι η εξής:

1. Εξώφυλλο
2. Εξώφυλλο στα αγγλικά
3. Εξεταστική επιτροπή
4. Ευχαριστίες
5. Περίληψη στα Ελληνικά και στα Αγγλικά
6. Περιεχόμενα
7. Κατάλογος Εικόνων
8. Κατάλογος Πινάκων
9. Πίνακας Ακρωνυμίων
10. Κεφάλαια
11. Παραρτήματα
12. Βιβλιογραφία

1.1 Αντικείμενο της πτυχιακής εργασίας

Η εργασία έχει στόχο να παρουσιάσει στον αναγνώστη το υπολογιστικό νέφος, τα ζητήματα ασφάλειας, καθώς και τρόπους αντιμετώπισης αυτών. Ο σκοπός της παρούσης πτυχιακής εργασίας είναι, αφού έχουν παρουσιάστει τα σημαντικότερα θέματα που αφορούν την ασφάλεια γύρω από το υπολογιστικό νέφος, ο αναγνώστης να έχει αποκτήσει μια βασική γνώση σχετικά με το υπολογιστικό νέφος, το πως να επιλέξει και να διαχείριστει μια συνεργασία με έναν πάροχο, αλλά και να είναι σε θέση να

γνωρίζει με ποιούς τρόπους αντιμετοπίζονται οι κίνδυνοι που υπάρχουν, μέσα από μια σείρα βέλτιστων πρακτικών που παρέχει το πλαίσιο ασφάλειας, για να γίνει διασφάλιση των δεδομένων του. Ο λόγος που το αντικείμενο της εργασίας είναι σημαντικό, είναι γιατι το υπολογιστικό νέφος αποτελεί μια μεγάλη εξέλιξη στο χώρο της πληροφορικής και προσφέρει τεράστια πλεονεκτήματα στους χρήστες και στις επιχειρήσεις. Πιο σημαντικό ακόμα είναι να εξασφαλιστεί μια σχέση εμπιστοσύνης μεταξύ τελικού χρήστη και παρόχου υπηρεσιών, όπου και τα δύο μέλη θα πρέπει να συνεργαστούν μαζί για την επίτευξη της ασφάλειας των πληροφοριών.

1.2 Μεθοδολογία

Η μεθοδολογία που ακολουθήθηκε για την διερεύνηση του θέματος της εργασίας είναι η ακόλουθη, αφού έχει γίνει γνωστή η δομή της πτυχιακής εργασίας και των σχετικών περιεχομένων του κάθε κεφαλαίου από τον επιβλέπων καθηγητή, έγινε συλλογή και μελέτη σχετικής βιβλιογραφίας. Εν συνεχεία έγινε διαχωρισμός της βιβλιογραφίας στα αντίστοιχα θέματα που διαπραγματεύεται το κάθε κεφάλαιο της εργασίας ξεχωριστά. Για το δεύτερο κεφάλαιο που αφορά τις βασικές πτυχές του υπολογιστικού νέφους έγινε μελέτη και διασταύρωση των αντίστοιχων πηγών και τέλος βγήκαν συμπεράσματα για την συγγραφή του. Ομοίος ο ίδιος τρόπος ακολουθήθηκε για το τρίτο κεφάλαιο που αφορά την διαχείριση της ασφάλειας στο υπολογιστικό νέφος, καθώς και για το τέταρτο κεφάλαιο που αφορά την ανάπτυξη των βασικών πτυχών του πλαισίου ασφαλείας COBIT 5. Τέλος για την παρουσίαση του σεναρίου χρήσης στο πέμπτο κεφάλαιο ο τρόπος ανάπτυξης ήταν συνδιαστική μέλετη από την βιβλιογραφία που σχετίζεται με το τέταρτο κεφάλαιο δηλαδή το πλαίσιο COBIT 5 και επιστημονικών άρθρων από τον αντίστοιχο οργανισμό ανάπτυξης του πλαισίου, που αναλύουν και παρουσιάζουν αντίστοιχα σενάρια χρήσης του υπολογιστικού νέφους από επιχειρήσεις. Έτσι έγινε καταγραφή της δομής και των χαρακτηριστικών, καθώς και μελέτη του προβλήματος και τέλος εφαρμογή της αντίστοιχης θεωρίας για την αντιμετόπιση.

1.3 Δομή

Η δομή των κεφαλαίων της πτυχιακής εργασίας είναι η εξής:

- Στο 1ο κεφάλαιο αναφέρεται η εισαγωγή της πτυχιακής εργασίας.
- Στο 2ο κεφάλαιο γίνεται μια συνολική επισκόπιση στο υπολογιστικό νέφος.
- Στο 3ο κεφάλαιο αναλύεται η έννοια της ασφάλειας, περιγράφονται επίσης χαρακτηριστικά και εργαλεία ασφαλείας στα μοντέλα ανάπτυξης και παροχής υπηρεσιών.
- Στο 4ο κεφάλαιο εξηγούνται τα πλαίσια ασφαλείας, περιγράφοντας λεπτομερώς την δομή του COBIT 5 πλαισίου.
- Στο 5ο κεφάλαιο παρουσιάζεται ένα σενάριο χρήσης μεταξύ πάροχου νέφους και επιχείρησης.
- Στο 6ο κεφάλαιο δίνεται ο επίλογος και τα συμπεράσματα της μελέτης.
- Τέλος στις ενότητες βιβλιογραφία - αναφορές & παραρτήματα, δίνονται οι πηγές και οι αναφορές της πτυχιακής εργασίας.

2. ΕΙΣΑΓΩΓΗ ΣΤΟ ΥΠΟΛΟΓΙΣΤΙΚΟ ΝΕΦΟΣ

Τα συστήματα του υπολογιστικού νέφους αποτελούν την μεγαλύτερη εξέλιξη στο χώρο των Η/Υ. Σε αυτό το κεφάλαιο γίνεται μια γενική επισκόπιση του υπολογιστικού νέφους και αναλύονται όλα τα τεχνικά χαρακτηριστικά καθώς και η ιστορική του εξέλιξη.

2.1 Τι είναι το νέφος

Ο όρος σύννεφο έχει χρησιμοποιηθεί ιστορικά ως μια αλληγορία για το διαδίκτυο. Η χρήση αυτή αρχικά προέρχεται από την κοινή απεικόνιση του σε διαγράμματα δικτύου ως ένα περίγραμμα ενός συννέφου, χρησιμοποιήθηκε για να αντιπροσωπεύσει τη μεταφορά των δεδομένων σε ένα τελικό σημείο στην άλλη πλευρά του νέφους. Αυτή η έννοια χρονολογείται ήδη από το 1961, όταν ο καθηγητής John McCarthy πρότεινε ότι η τεχνολογία των υπολογιστών θα μπορούσε να οδηγήσει σε ένα μέλλον όπου η υπολογιστική ισχύ και ειδικές εφαρμογές θα μπορούσαν να πωληθούν μέσω ενός χρήσιμου τύπου επιχειρηματικού μοντέλου. Η ιδέα έγινε πολύ δημοφιλής στα τέλη του 1960, αλλά από τα μέσα της δεκαετίας του 1970, η ιδέα άρχισε να ξεθωριάζει όταν κατέστη σαφές ότι οι τεχνολογίες που σχετίζονται με την πληροφορική δεν ήταν σε θέση να υποστηρίξουν ένα τέτοιο μελοντικό υπολογιστικό μοντέλο.[10]

2.2 Η παγκόσμια φύση του νέφους

Το σύννεφο δεν έχει όρια, οι άνθρωποι από παντού έχουν πλέον πρόσβαση σε άλλους ανθρώπους από οποιοδήποτε μέρος. Η παγκοσμιοποίηση των περιουσιακών στοιχείων των υπολογιστών μπορεί να είναι η μεγαλύτερη συμβολή που έχει προσφέρει το σύννεφο μέχρι σήμερα. Για το λόγο αυτό, το σύννεφο είναι το αντικείμενο πολλών πολύπλοκων γεωπολιτικών ζητημάτων. Οι πάροχοι του νέφους πρέπει να πληρούν μυριάδες ρυθμιστικές ανησυχίες για την παροχή των υπηρεσιών του νέφους σε μια παγκόσμια αγορά. Το υπολογιστικό νέφος είναι ακόμα στην αρχή. Υπάρχει ένα συνονθύλευμα των παρόχων, μικρών και μεγάλων, παρέχοντας ένα ευρύ φάσμα υπηρεσιών νέφους. Για παράδειγμα, υπάρχει πλήρης άνθηση σε εφαρμογές, υπηρεσίες υποστήριξης, υπηρεσίες mailfiltering, υπηρεσίες αποθήκευσης, κ.τ.λ. Οι επαγγελματίες πληροφορικής έχουν μάθει να υποστηρίζουν πολλές από τις υπηρεσίες του νέφους από ανάγκη, όπως υπαγορεύεται από τις ανάγκες των επιχειρήσεων. Η έννοια του υπολογιστικού νέφους γίνεται πολύ πιο κατανοητή, όταν αρχίζει κανείς να αντιλαμβάνεται για τις απαιτήσεις των σύγχρονων πληροφοριακών περιβάλλοντων που

πάντα θα απαιτούν τα μέσα για να αυξήσουν την χωριτηκότητα ή να προσθέσουν δυνατότητες για την υποδομή τους δυναμικά, χωρίς να επενδύουν χρήματα στην αγορά νέων υποδομών, χωρίς να χρειάζεται να διεξάγει εκπαίδευση για νέο προσωπικό και χωρίς την ανάγκη για χορήγηση αδειών για νέο λογισμικό. Λαμβάνοντας υπόψη μια λύση στις παραπάνω ανάγκες, είναι τα μοντέλα του υπολογιστικού νέφους που καλύπτουν μια συνδρομή που βασίζεται στο πρότυπο πληρωμή-ανά-χρήση (pay-per-use) παρέχοντας μια υπηρεσία που μπορεί να χρησιμοποιηθεί μέσω του διαδικτύου και επεκτείνει τις υφιστάμενες δυνατότητες μιας εταιρείας πληροφορικής.[10]

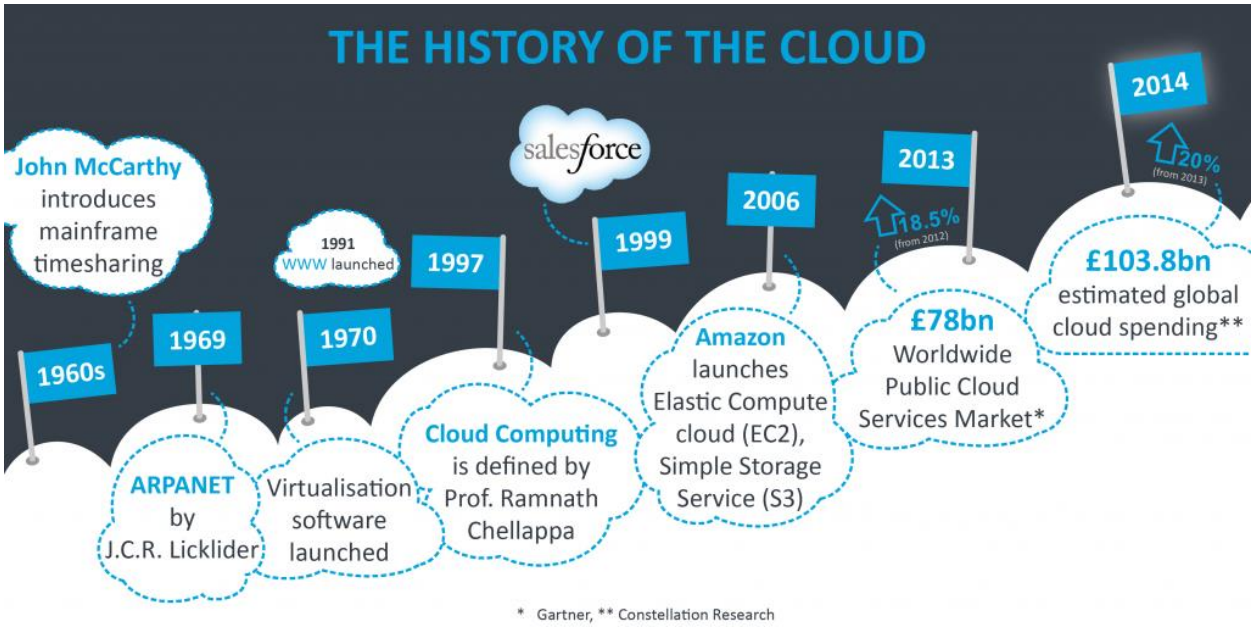
2.3 Η εμφάνιση του υπολογιστικού νέφους

Η χρησιμότητα των υπολογιστών μπορεί να οριστεί ως η παροχή υπολογιστικών και αποθηκευτικών πόρων ως μετρούμενες υπηρεσίες παρόμοιες με αυτές που παρείχαν από μια παραδοσιακή εταιρεία κοινής ωφελείας. Αυτό, φυσικά, δεν είναι μια νέα ιδέα. Αυτή η μορφή των υπολογιστών αυξάνεται σε δημοτικότητα, ωστόσο, καθώς οι εταιρείες έχουν αρχίσει να επεκτείνουν το μοντέλο σε υπολογιστικό σύννεφο παρέχωντας εικονικούς διακομιστές όπου τα τμήματα πληροφορικής και οι χρήστες μπορούν να έχουν πρόσβαση κατά απαίτηση. Οι επιχειρήσεις υιοθέτισαν και χρησιμοποίησαν την υπολογιστική χρησιμότητα κυρίως για μη-κρίσιμες ανάγκες, αλλά αυτό αλλάξε γρήγορα καθώς τα θέματα εμπιστοσύνης και αξιοπιστίας είχαν επιλυθεί. Μερικοί άνθρωποι πιστεύουν ότι το υπολογιστικό νέφος είναι το επόμενο μεγάλο βήμα στον κόσμο της πληροφορικής. Άλλοι πιστεύουν ότι είναι ακριβώς μια άλλη παραλλαγή του μοντέλου utility computing το οποίο επανακατασκευάστικε αυτή την δεκαετία σαν κάτι νέο. Ωστόσο, δεν είναι μόνο το "υπολογιστικό νέφος" που προκαλεί σύγχυση μεταξύ των μαζών. Επί του παρόντος, με τόσους λίγους παρόχους υπολογιστικού νέφους που στην πραγματικότητα ασκούν αυτή τη μορφή της τεχνολογίας, αλλά και σχεδόν κάθε αναλυτής από κάθε ερευνητικό οργανισμό καθορίζει τον ορό διαφορετικά και έτσι η έννοια του όρου έχει γίνει πολύ ασαφής. Όπως είπαμε προηγουμένως, ο όρος νέφος συχνά χρησιμοποιείται ως μεταφορά για το διαδίκτυο και έχει γίνει ένα γνωστό κλισέ. Ωστόσο, όταν «το σύννεφο» συνδυάζεται με το "υπολογιστικό", προκαλεί μεγάλη σύγχυση. Αναλυτές αγοράς και προμηθευτές τεχνολογίας ομοίος τείνουν να καθορίσουν το υπολογιστικό νέφος, ως ένα νέο τύπο utility computing που χρησιμοποιεί εικονικούς διακομιστές που έχουν γίνει διαθέσιμοι σε τρίτους μέσω του διαδικτύου. Άλλοι τείνουν

να προσδιορισθεί ο όρος χρησιμοποιώντας μια πιο ευρύ και σφαιρική εφαρμογή της εικονικής πλατφόρμας υπολογιστών.[10]

2.4 Ιστορική αναδρομή

Η προέλευση του όρου υπολογιστικό νέφος(cloud computing) στην πληροφορική είναι ασαφής. Η λέξη «σύννεφο» χρησιμοποιείται συχνά στην επιστήμη για να περιγράψει μια μεγάλη συσσώρευση αντικειμένων που εμφανίζονται οπτικά από απόσταση, όπως ένα σύννεφο, και περιγράφει κάθε σειρά πραγμάτων των οποίων τα στοιχεία δεν έχουν ακόμη ελεγχθεί σε ένα δεδομένο πλαίσιο. Κατ 'αναλογία με την παραπάνω χρήση, η λέξη «σύννεφο» χρησιμοποιήθηκε ως μια μεταφορά για το διαδίκτυο και ένα πρότυπο «σύννεφο» που μοιάζει με το σχήμα που χρησιμοποιήθηκε για να υποδηλώσει ένα δίκτυο για τις σχηματικές αναπαραστάσεις της τηλεφωνίας. Αργότερα χρησιμοποιήθηκε για να απεικονίσει το διαδίκτυο σε διαγράμματα δικτύου υπολογιστών. Το σύμβολο «σύννεφο» χρησιμοποιήθηκε για να αντιπροσωπεύσει τα δίκτυα του εξοπλισμού πληροφορικής στο αρχικό ARPANET από το 1977, και το CSNET από το 1981.[1]



Εικόνα 2. 1: Εξέλιξη του υπολογιστικού νέφους [1]

Η βασική ιδέα του υπολογιστικού νέφους προέρχεται από τη δεκαετία του 1950, με τη χρήση των mainframes, επιτρέποντας σε πολλαπλούς χρήστες να έχουν τόσο φυσική πρόσβαση στον υπολογιστή από πολλαπλά τερματικά, καθώς και κοινόχρηστο χρόνο κεντρικής μονάδας επεξεργασίας. Λόγω του μεγάλου κόστους αγοράς αλλά και συντήρησης ενός mainframe, δεν ήταν λογικό ένας οργανισμός να παρέχει ένα σε κάθε υπάλληλο. Επιπλέον, ο μέσος χρήστης δεν χρειαζόταν τον μεγάλο αποθηκευτικό χώρο και την μεγάλη υπολογιστική ισχύ ενός τέτοιου υπολογιστή. Έτσι, η βέλτιστη λύση από οικονομικής άποψης, σύμφωνα με τα παραπάνω δεδομένα, ήταν η κοινή χρήση των υπολογιστικών πόρων ενός κεντρικού mainframe από όλους τους υπάλληλους.[2] Αλλά πραγματικά δεν ήταν μέχρι την τελευταία δεκαετία ή έτσι ώστε το υπολογιστικό νέφος αρχίσει πραγματικά να εξελιχθεί στο μεγαθήριο που γνωρίζουμε σήμερα. Στις αρχές της δεκαετίας του 2000, εταιρείες όπως η e-tail, Amazon.com Inc έπαιξαν καθοριστικό ρόλο στην ανάπτυξη του cloud computing. Η σημερινή διαθεσιμότητα των δικτύων υψηλής χωρητικότητας και υπολογιστών χαμηλού κόστους, σε συνδυασμό με την ευρεία υιοθέτηση της εικονοποίησης, οδήγησαν στην έκδοση του υπολογιστικού νέφους που γνωρίζουμε σήμερα και είναι ένα μοντέλο που εξελίσσεται συνεχώς.[1]

Κατά τη διάρκεια της δεκαετίας του 1960, οι αρχικές ανησυχίες για τον χρονομετρισμό έγιναν δημοφιλείς μέσω RJE. Η ορολογία αυτή ήταν ως επί το πλείστον συνδεδεμένη με μεγάλους πωλητές όπως η IBM & DEC. Οι πλήρεις χρονομετριστικές λύσεις ήταν διαθέσιμες πλέον στις αρχές του 1970 σε πλατφόρμες όπως Multics Cambridge CTSS.[1]

Στη δεκαετία του 1990 οι εταιρείες τηλεπικοινωνιών, οι οποιες στο παρελθόν προσέφεραν δεδομένα απο σημείο σε σημείο(point to point) άρχισαν να προσφέρουν υπηρεσίες ιδιωτικών εικονικών δικτύων(VPN) με συγκρίσιμη ποιότητα των υπηρεσιών αλλά σε χαμηλότερο κόστος. Καθώς είδαν, ότι αλλάζοντας την κίνηση των δεδομένων κατάλληλα, εξισορροπεί η χρήση του εξυπηρετητή, έτσι μπορούσαν να χρησιμοποιήσουν το συνολικό εύρος ζώνης του δικτύου πιο αποτελεσματικά. Άρχισαν να χρησιμοποιούν το «σύννεφο» για να υποδηλώσει το σημείο διαχωρισμού μεταξύ αυτων που ο πάροχος ειναι υπεύθυνος και αυτών που οι χρήστες είναι υπεύθυνοι. Το υπολογιστικό νέφος επεκτάθηκε πέρα από αυτό το όριο για να καλύψει όλους τους εξυπηρετητές, καθώς και την υποδομή του δικτύου. Δεδομένου ότι οι υπολογιστές

έγιναν πιο διαδεδομένοι, επιστήμονες και τεχνολόγοι διερεύνησαν τρόπους για να κάνουν μεγάλης κλίμακας υπολογιστική ισχύ διαθέσιμη σε περισσότερους χρήστες. Πειραματίστηκαν με αλγόριθμους για να βλετιώσουν τις υποδομές, τις πλατφόρμες και τις εφαρμογές ώστε να δώσουν προτεραιότητα σε CPU και να αυξήσουν την αποδοτικότητα για τους τελικούς χρήστες.[1]

Το υπολογιστικό νέφος υπάρχει από τις αρχές του 2000, στις αρχές του 2008 το OpenNebula έγινε το πρώτο λογισμικό ανοιχτού κώδικα για την ανάπτυξη ιδιωτικών και υβριδικών υπολογιστικών νεφών. Κατά το ίδιο έτος, οι προσπάθειες επικεντρώθηκαν στην παροχή εγγυήσεων ποιότητας υπηρεσίων σε υποδομές υπολογιστικού νέφους. Η εξέλιξη του διαδικτύου και η νέα οπτική για την παροχή όλο και περισσότερων υπηρεσιών, σε συνδιασμό με τα ταχύτατα δίκτυα, το χαμηλό κόστος των υπολογιστών και των μέσων αποθήκευσης και την ευρεία υιοθέτηση υπηρεσιοστρεφών αρχιτεκτονικών(SOA) και εικονικών μηχανών, οδηγεί στην περαιτέρω ανάπτυξη του υπολογιστικού νέφους.[1]

Τον Αύγουστο του 2006 η Amazon παρουσίασε το Elastic Compute Cloud. Η Microsoft Azure είχε ανακοινωθεί ως "Azure" τον Οκτώβριο του 2008 και κυκλοφόρησε την 1η Φεβρουαρίου 2010, πριν μετονομαστεί σε Microsoft Azure στις 25 Μαρτίου 2014. Για ένα διάστημα η Azure ηταν στην λίστα με τους καλύτερους υπερυπολογιστές. Τον Ιούλιο του 2010 η RackSpase Hosting & η NASA ξεκίνησαν από κοινού μια πρωτοβουλία για ένα ανοιχτού κώδικα λογισμικό γνωστό ως OpenStack. Το έργο OpenStack προορίζεται να βοηθήσει τους οργανισμούς να προσφέρουν υπηρεσίες υπολογιστικού νέφους που λειτουργούν με το πρότυπο υλικό. Ο αρχικός κώδικας προήλθε από την πλατφόρμα Nebula της NASA, καθώς και από την πλατφόρμα Cloud Files της Rackspace. Την 1η Μαρτίου 2011, η IBM ανακοίνωσε το πλαίσιο IBM SmartCloud για την υποστήριξη της επιχειρησιακής πρωτοβουλίας Smarter Planet.[1]Την 7η Ιουνίου 2012, η Oracle ανακοίνωσε την Oracle Cloud.[1] Ενώ οι πτυχές της Oracle Cloud είναι ακόμα σε εξέλιξη, αυτή η παροχή νέφους είναι έτοιμη να είναι η πρώτη που παρέχει στους χρήστες πρόσβαση σε μια ολοκληρωμένη σειρά λύσεων πληροφορικής, συμπεριλαμβανομένων των επιπέδων SaaS, PaaS, IaaS.[1]

2.4.1 Παραβιάσεις στο νέφος

Μια παραβίαση δεδομένων είναι ένα περιστατικό που περιλαμβάνει την παράνομη προβολή, την πρόσβαση ή την ανάκτηση δεδομένων. Παρακάτω θα αναφερθούμε σε μερικές από τις πιο γνωστές παραβιάσεις δεδομένων που έχουν συμβεί:

- **Dropbox**

Μία από τις πιο πρόσφατες παραβιάσεις της ασφάλειας έχει υποστεί το Dropbox εκπλήσωντας πώς οι hackers κατάφεραν να πάρουν 7.000.000 κωδικούς πρόσβασης. Η δημοφιλής υπηρεσία αποθήκευσης αρνείται ότι έχει παραβιαστεί και ότι οι κωδικοί πρόσβασης ελήφθησαν από άγνωστες υπηρεσίες τρίτων. Γιατί λοιπόν, οι δράστες να αποσπάσουν όλους εκείνους τους κωδικούς πρόσβασης;Ο λόγος το (Bitcoin - ψηφιακό νόμισμα). Οι hackers κυκλοφόρησαν μια λίστα με 400 μηνύματα ηλεκτρονικού ταχυδρομείου και μια αντιστοιχία κωδικών πρόσβασης στις 13 Οκτωβρίου 2014 για να κάνουν το κοινό να δωρίσει Bitcoins. Όσα περισσότερα Bitcoins γίνουν δωρεά, τόσο περισσότεροι λογιαριασμοί θα δημοσιευθουν.[3]

- **Google Drive**

Τον Ιούλιο του 2014 η Google Drive για την αναγνώριση μια ευπάθειας του υπερσυνδέσμου, παρόμοια με την προηγούμενη ευπάθεια του Dropbox, το πρόβλημα είχε ως εξής. Άν έχετε μοιραστεί έναν σύνδεσμο που επέτρεπει την λειτουργία “όποιος έχει το σύνδεσμο" να το δεί οι πιθανότητες είναι άγνωστες αν ιστοσελίδες τρίτων μπορούν να δούν τα αρχεία. Ο ιδιοκτήτης των τρίτων ιστοσελίδων λαμβάνει μια διεύθυνση URL, επιτρέποντάς τους να έχουν πρόσβαση σε ευαίσθητες πληροφορίες που είναι αποθηκευμένες στην υπηρεσία Google Drive.[3]

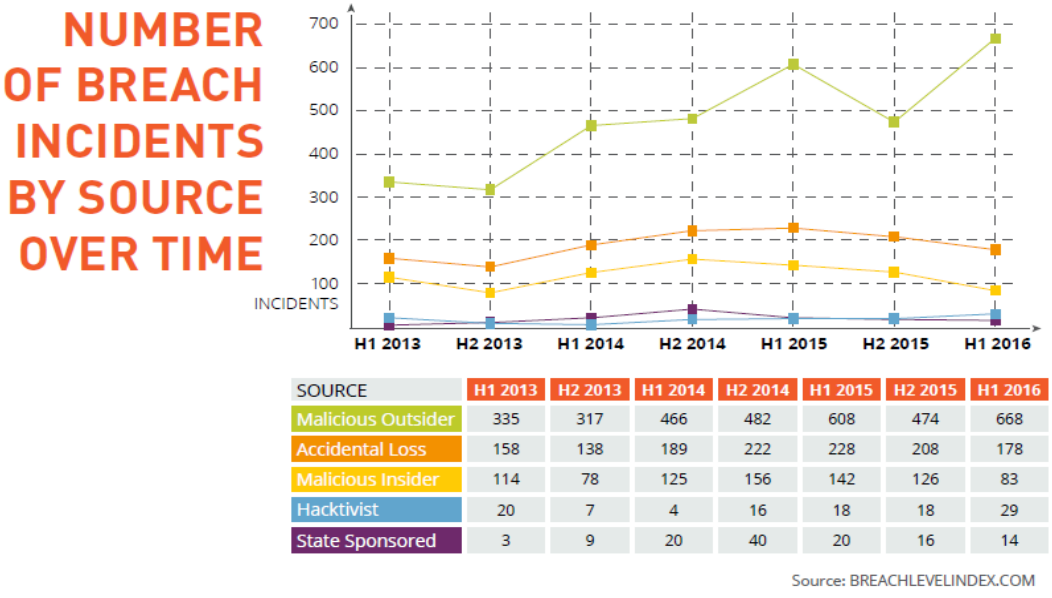
- **iCloud**

Η διαρροή φωτογραφιών διασήμων ανθρώπων το 2014 μας υπενθύμισε ότι τα αρχεία μας στο σύννεφο μπορεί να μην είναι τόσο ασφαλές όσο αρχικά νομίζαμε. Λίγο μετά την επίθεση των hacker, οι φωτογραφίες από διάφορες διασημότητες έιχαν αναρτηθεί στο Reddit. Η Apple κυκλοφόρησε μια δήλωση λέγοντας ότι το iCloud δεν παραβιάστηκε. Μάλλον, ήταν “μια πολύ στοχευμένη επίθεση σε ονόματα χρηστών, κωδικούς

πρόσβασης και τα ζητήματα της ασφάλειας, μια πρακτική που έχει γίνει πάρα πολύ κοινή στο διαδίκτυο. Τι μπορούμε να κάνουμε για να αποτρέψουμε τους κλέφτες από την πρόσβαση τους στα αρχεία μας, αν και όταν έχουν κλαπεί οι κωδικοί μας;Η κρυπτογράφηση είναι η απάντηση. Θα πρέπει να κρυπτογραφούμε τα αρχεία πριν από την αποθήκευση τους στο σύννεφο, αυτή η διαδικασία θα αποτρέψει την διαρροή πληροφοριών από κλεμμένα αρχεία. Αν οι κωδικοί πρόσβασης έχουν κλαπεί, οι κλέφτες θα έχουν ακόμα πρόσβαση στα αρχεία και στις φωτογραφίες, αλλά δεν θα είναι σε θέση να τα αποκρυπτογραφήσουν για να τα δούν.[3]

2.4.2 Στατιστική μελέτη παραβιάσεων

Παρακάτω θα δούμε μια στατιστική ανάλυση από μια παγκόσμια βάση δεδομένων που παρακολουθεί παραβιάσεις δεδομένων σε παγκόσμιο επίπεδο και μετρά τη σοβαρότητά τους με βάση πολλαπλές διαστάσεις, συμπεριλαμβανομένου του είδους των δεδομένων και την πηγή της παραβίασης. Ο Δείκτης επιπέδου παραβίασης όχι μόνο εντοπίζει παραβιάσεις δεδομένων αλλά και επιτρέπει στους οργανισμούς να κάνουν τη δική τους αξιολόγηση κινδύνου. Η **Εικόνα 2.2** μας δείχνει τον αριθμό των παραβιάσεων, αλλά και από ποιούς παράγωντες προήλθαν από το πρώτο εξάμηνο του έτους 2013 εώς και το πρώτο εξάμηνο του έτους 2016.[29]

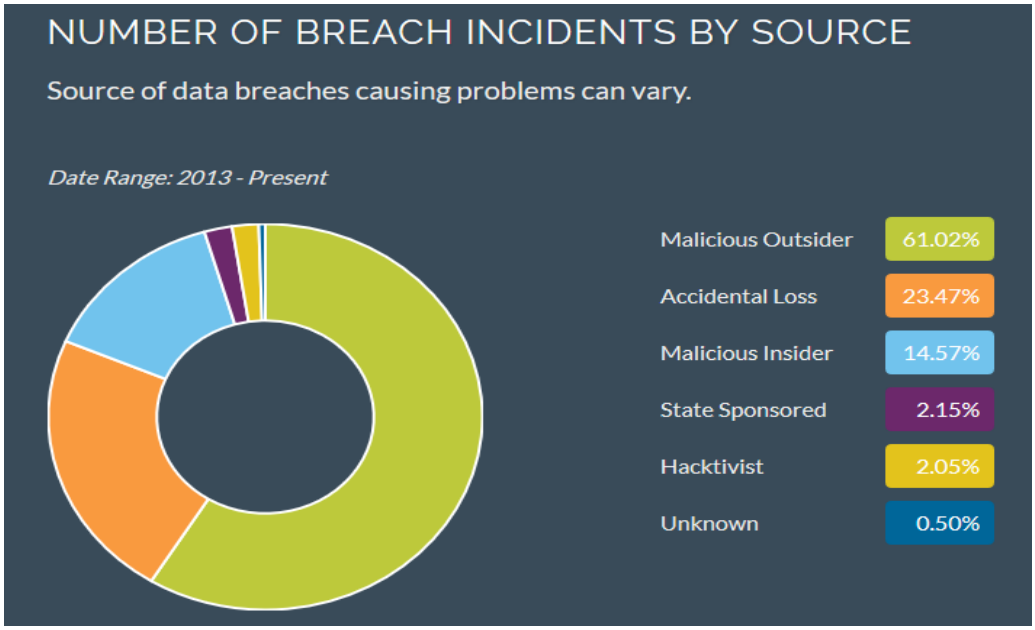


SOURCE	H1 2013	H2 2013	H1 2014	H2 2014	H1 2015	H2 2015	H1 2016
Malicious Outsider	335	317	466	482	608	474	668
Accidental Loss	158	138	189	222	228	208	178
Malicious Insider	114	78	125	156	142	126	83
Hacktivist	20	7	4	16	18	18	29
State Sponsored	3	9	20	40	20	16	14

Source: BREACHLEVELINDEX.COM

Εικόνα 2. 2: Στατιστική παραβιάσεων [2]

Σύμφωνα με την παραπάνω μελέτη το μεγαλύτερο ποσοστό όπως και στις προηγούμενες περιόδους είναι οι κακόβουλοι χρήστες(malicious Outsiders) με ποσοστό ≈61%, είναι η μεγαλύτερη πηγή παραβιάσεων. Εν συνεχεία οι απώλειες από λάθος χειρισμό(Accidental Loss) με ποσοστό ≈23.4% το οποίο είναι μειωμένο σε σχέση με τα τρία προηγούμενα εξάμηνα. Η επόμενη πηγή είναι κακόβουλοι χρήστες(Malicius Insiders) που βρίσκονται μέσα στον οργανισμό, π.χ., εργαζόμενοι, με ποσοστό ≈14.5%.Hacker ακτιβιστές με ποσοστό ≈2%, state-sponsored επιθέσεις με ποσοστό ≈2.1%, και τέλος ≈0.5% από άγνωστες πηγές (Unknown).[29]



Εικόνα 2. 3: Ποσοστά πηγών παραβιάσεων[2]

2.5 Υπολογιστικό νέφος

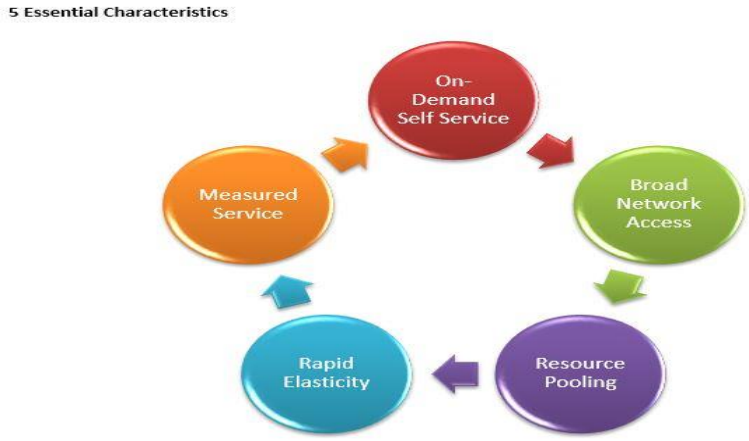
Το υπολογιστικό νέφος είναι το επόμενο στάδιο στην εξέλιξη του διαδικτύου. Το «νέφος» στο υπολογιστικό νέφος παρέχει το μέσο με το οποίο τα πάντα – από την υπολογιστική ισχύ σε υπολογιστική υποδομή, εφαρμογές, επιχειρησιακές διεργασίες σε προσωπικές συνεργασίες μπορούν να διανεμηθούν στους χρήστες ως υπηρεσία όπου και όποτε χρειαστεί. Γενικά το υπολογιστικό νέφος μπορεί έυκολα να κλιμακωθεί προς τα πάνω ή προς τα κάτω, όποτε αυτό χρειαστεί ανάλογα με τους πόρους που μπορεί να ζητήσουν οι χρήστες κατ' απαίτηση. Αυτή η εξέλιξη προς το cloud computing μπορεί να

αλλάξει εντελώς τον τρόπο που οι εταιρείες χρησιμοούν την τεχνολογία για να εξυπηρετούν τους πελάτες, τους συνεργάτες, και τους προμηθευτές.[43]

Εικόνα 2. 4: Υπολογιστικό νέφος [3]

2.6 Κύρια χαρακτηριστικά

Υπάρχουν πέντε αναγκαία χαρακτηριστικά, τα οποία είναι κοινά μεταξύ όλων των υπηρεσιών του υπολογιστικού νέφους, και είναι τα παρακάτω:[5]



Εικόνα 2. 5: Χαρακτηριστικά υπολογιστικού νέφους [4]

- **Αυτοεξυπηρέτηση κατ' απαίτηση**

Ο καταναλωτής μπορεί να προμηθευτεί υπολογιστικές δυνατότητες όπως χρόνο επεξεργασίας στον διακομιστή και χώρο αποθήκευσης στο δίκτυο, όποτε το χρειαστεί, χωρίς να απαιτείται η ανθρώπινη παρέμβαση με τον πάροχο της εκάστοτε υπηρεσίας.

- **Ευρεία πρόσβαση στο δίκτυο**

Οι δυνατότητες είναι διαθέσιμες σε όλο το δίκτυο και είναι προσβάσιμες από όλες τις συσκευές των πελατών.

- **Διαθεσιμότητα πόρων**

Οι υπολογιστικοί πόροι του παρόχου, φυσικοί και εικονικοί είναι διαθέσιμοι μέσω ενός μοντέλου μίσθωσης και διατίθενται με σκοπό να εξυπηρετήσουν παράλληλα πολλαπλούς χρήστες.

- **Γρήγορη ελαστικότητα**

Δυνατότητες που μπορούν να διανεμηθούν γρήγορα και ευέλικτα. Για τον καταναλωτή, οι διαθέσιμες δυνατότητες για παροχή υπηρεσιών φαίνονται να είναι απεριόριστες και να μπορούν να αγοραστούν σε οποιαδήποτε ποσότητα και οποιοδήποτε χρόνο.

- **Μετρήσιμη υπηρεσία**

Τα συστήματα «νέφους» ελέγχουν αυτόματα και βελτιστοποιούν την χρήση πόρων αξιοποιώντας την δυνατότητα μέτρησης. Η χρήση των πόρων μπορεί να παρακολουθηθεί, ελεγχθεί και να αναφερθεί. Με αυτόν τον τρόπο ο πελάτης μπορεί να ελέγξει την κατανάλωση και την χρέωση τους.

- **Εικονοποίηση**

Η εικονοποίηση είναι μια τεχνολογία που ξεπερνά τους περιορισμούς του φυσικού υλικού και παρέχει εικονικούς πόρους για υψηλού επιπέδου επιστημονικές εφαρμογές. Η εικονοποίηση προσφέρει έναν οικονομικά αποδοτικό και ευέλικτο τρόπο χρήσης και διαχείρισης των υπολογιστικών πόρων. Η συγκεκριμένη τεχνική χρησιμοποιείται τόσο

στο Grid computing, όσο και στο cloud computing, για την καλύτερη κατανομή των υπολογιστικών πόρων ανάλογα με τη ζήτηση. Αυτό επιτρέπει στους υφιστάμενους υπολογιστικούς πόρους να τροφοδοτηθούν δυναμικά κατά το χρόνο εκτέλεσης από τους χρήστες, με βάση τις απαιτήσεις των εφαρμογών.[27]

2.7 Πλεονεκτήματα & Μειονεκτήματα

Το cloud προσφέρει πολλά οφέλη στους χρήστες του. Ο χρήστης μπορεί να το χρησιμοποιήσει από οπουδήποτε βρίσκεται, όποτε επιθυμεί και με ασφάλεια. Κάποια από τα πλεονεκτήματα που μας παρέχει η χρήση του cloud είναι τα εξής:

- **Οικονομία**

Η οικονομία είναι από τα πιο βασικά πλεονεκτήματα του cloud computing.Καθώς η εταιρεία μειώνει το κόστος επένδυσης, το κόστος ιδιοκτησίας, το κόστος λειτουργίας και τέλος μειώνει τον επιχειρηματικό ρίσκο.[2]

- **Μεγάλος αποθηκευτικός χώρος**

Η αποθήκευση των διαφόρων πληροφοριών είναι θέμα υψίστης σημασίας. Με το cloud computing έχουμε απεριόριστο αποθηκευτικό και διαδικτυακό χώρο με ελαστικό τρόπο.[2]

- **Γρήγορη ανάπτυξη και Κλιμάκωση**

Οι εταιρείες μπορούν εύκολα να παρέχουν λογαριασμούς στους εργαζόμενους για πρόσβαση στις εφαρμογές καθώς, ολόκληρο το σύστημα μπορεί να είναι έτοιμο σε λίγα μόλις λεπτά. Επιπλέον, με τις υποδομές του cloud, μία εταιρεία μπορεί να ξεκινήσει με μία μικρή ανάπτυξη ανάλογα με τις τρέχουσες ανάγκες της και όταν χρειαστεί, μπορεί να κλιμακωθεί προς τα πάνω προκειμένου να ανταποκριθεί σε μεγαλύτερες απαιτήσεις αλλά και να κλιμακωθεί προς τα κάτω όταν αυτές οι απαιτήσεις μειωθούν ξανά. [6]

- **Ευκολία στην πρόσβαση**

Ο χρήστης μπορεί να έχει πρόσβαση στα αρχεία και στα δεδομένα από οποιαδήποτε γεωγραφικό σημείο, αρκεί να υπάρχει φυσικά πρόσβαση στο διαδίκτυο. Μπορεί επίσης να έχει πρόσβαση και να διαχειρίζεται τα δεδομένα του χρησιμοποιώντας και άλλες συσκευές, όπως iPad, netbooks και ακόμη και κινητά τηλέφωνα. Αυτό, όχι μόνο αυξάνει την αποτελεσματικότητα, αλλά ενισχύει τις υπηρεσίες που παρέχονται στους καταναλωτές.[5]

- **Διευκόλυνση της συνεργασίας**

Κάθε αρχείο που ανεβάζει ή δημιουργεί ένας χρήστης στο cloud, υπάρχει η δυνατότητα να είναι ορατό από άλλα μέλη της ομάδας ανάλογα με τα δικαιώματα που έχει ο κάθε χρήστης της ομάδας. Έτσι δεν χρειάζεται κάθε φορά που γίνεται κάποια αλλαγή σε κάποιο αρχείο αυτό να αποστέλνετε ξανά στους υπόλοιπους χρήστες της ομάδας.[27]

Εικόνα 2. 6: Πλεόνεκτήματα & Μειονεκτήματα υπολογιστικού νέφους [5]

Όπως κάθε νέα τεχνολογία έτσι και το cloud computing έχει κάποια μειονεκτήματα. Μερικά από αυτά είναι τα εξής:

- **Ασφάλεια και Μυστικότητα**

Οι δύο αυτές έννοιες μπορούν να θεωρηθούν ως μειονεκτήματα για τον λόγο ότι όλα τα στοιχεία δίνονται σε ένα τρίτο άτομο το οποίο είναι ο πάροχος, και αυτή η ανησυχία είναι ακόμη μεγαλύτερη για τις επιχειρήσεις, διότι μερικές φορές επιθυμούν να κρατήσουν τις πληροφορίες τους στα υπολογιστικά νέφη.[6]

- **Απώλεια ελέγχου**

Μπορεί να υπάρξουν προβλήματα απώλειας ελέγχου, με τους φορείς παροχής υπηρεσιών στα επίπεδα συντήρησης και συχνότητας.[6]

- **Τεχνικά θέματα & Συνδεσιμότητα**

Προβλήματα όπως τεχνικές βλάβες, και θέματα που έχουν σχέση με το δίκτυο και την συνδεσιμότητα μπορούν να καταστίσουν την πρόσβαση στο υπολογιστικό νέφος αλλά και όλες τις υπηρεσίες που προσφέρει μη διαθέσιμες.[27]

- **Κενά ασφαλείας**

Εφόσον οι πληροφορίες αποθηκεύονται στο cloud και η ανταλλαγή τους γίνεται μέσω του διαδικτύου, οι υπηρεσίες που στηρίζονται στο cloud είναι εκτεθειμένες σε κακόβουλους χρήστες. Από αυτό συμπίπτουν και νομικά θέματα ωπος όταν ένας πάροχος που θα αδυνατούσε να προστατέψει δεδομένα ή θα έπεφτε θύμα υποκλοπής δεδομένων, θα αντιμετωπίσει σοβαρά νομικά προβλήματα. Έτσι επινοήθηκε η ιδέα του private cloud για να δώσει τέλος στις σχετικές αυτές ανησυχίες.[5]

- **Κλείδωμα σε έναν πάροχο**

Ένας κοινός φόβος μεταξύ των τελικών χρηστών και εταιρειών του «νέφους» είναι να «κλειδωθούν» σε ένα συγκεκριμένο πάροχο. Ως αποτέλεσμα, η μετάβαση από τον ένα πάροχο «νέφους» στον άλλον είναι πολύπλοκη, ακριβή και πολλές φορές αδύνατη ειδικά στην υπηρεσία IaaS. Και γιαυτόν τον λόγο ο κάθε χρήστης ή εταιρεία πριν την

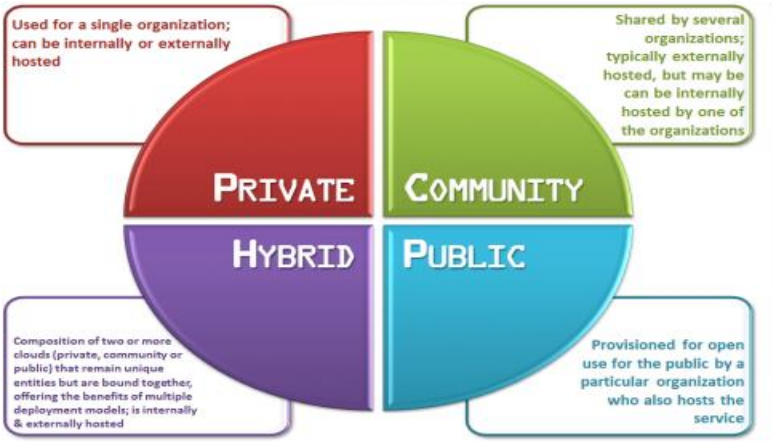
μετάβαση σε ένα πάροχο «νέφους» θα πρέπει να εξετάσει προσεκτικά τα χαρακτηριστικά αυτού.[25]

2.8 Μοντέλα ανάπτυξης νέφους

Το υπολογιστικό νέφος φιλοξενεί μοντέλα ανάπτυξης(Deployment models) που αντιπροσωπεύουν την ακριβή κατηγορία περιβάλλοντος υπολογιστικού νέφους, και διακρίνονται κυρίως από την πρόσβαση σε αυτό. Για να είναι γνωστό ποιο μοντέλο ανάπτυξης ταιριάζει στον τελικό χρήστη, πρέπει να γνωρίζει και τα τέσσερα μοντέλα ανάπτυξης.

- **Δημόσιο νέφος (Public cloud)**

Το δημόσιο νέφος αναφέρεται σε ένα μοντέλο, στο οποίο οι εγκαταστάσεις υποδομής του και οι προσφερόμενες υπηρεσίες, παρέχονται από τους παρόχους του, σύμφωνα με τον διακανονισμό που έχει γίνει μεταξύ παρόχου – πελάτη. Επίσης αυτό το μοντέλο βασίζεται σε παγκόσμια δίκτυα κέντρων πληροφοριών, προσφέροντας υπηρεσίες με πληρωμή ανά χρήση, δηλαδή οι εταιρείες ή οι χρήστες που χρησιμοποιούν τις υπηρεσίες του cloud, χρεώνονται για όσο τις χρησιμοποιούν. Από τη φύση του το δημόσιο cloud, χαρακτηρίζεται από μειωμένα κόστη εργασίας. Σε πολλές περιπτώσεις υπάρχουν και εντελώς δωρεάν προσφερόμενες υπηρεσίες, προκειμένου να προσελκύσουν νέους πελάτες. Συνδέεται στο διαδίκτυο μέσω ευρυζωνικής πρόσβασης και οι χρήστες του συνδέονται από δημόσια σημεία πρόσβασης στο διαδίκτυο, χρησιμοποιώντας διάφορα πρωτόκολλα.[6][5]



Εικόνα 2. 7: Μοντέλα ανάπτυξης υπολογιστικού νέφους [6]

- **Ιδιωτικό νέφος (Private cloud)**

Το ιδιωτικό νέφος είναι ένα κέντρο δεδομένων(data center) που ανήκει σε έναν πάροχο υπηρεσιών ο οποίος είναι υπεύθυνος για την υποδομή και τη λειτουργία της πλατφόρμας του cloud computing. Έτσι, το μοντέλο αυτό προσφέρει στους χρήστες μεγαλύτερη ευελιξία και εμπνέει περισσότερη εμπιστοσύνη μεταξύ παρόχου - πελάτη. Αυτό συμβαίνει γιατί οι επιχειρήσεις μπορούν να εφαρμόσουν τις πολιτικές εκείνες που οι ίδιες επιλέγουν σε θέματα που αφορούν την ασφάλεια και την προστασία της ιδιοτικότητας των δεδομένων τους και τους μηχανισμούς πρόσβασης τους. Το διωτικό cloud προτιμάται κυρίως από μεγάλους οργανισμούς οι οποίοι επιλέγουν να «χτίσουν» τα δικά τους ιδιωτικά cloud computing που στηρίζονται στις υποδομές και στο υλικό υπολογιστών που διαθέτουν.[6]Το ιδιωτικό cloud είναι προσβάσιμο σαν μία LAN προέκταση στους διακομιστές του κέντρου δεδομένων της επιχείρησης (μέσω ενός VPN).[5]Δεν είναι μοιραζόμενο με άλλους οργανισμούς, είτε γίνεται εσωτερική διαχείριση είτε από τρίτους, και μπορεί να φιλοξενείται εσωτερικά ή εξωτερικά.Υπάρχουν δύο παραλλαγές ιδιωτικών νεφών:

- **On-Premise ιδιωτικό νέφος**

Αυτός ο τύπος cloud είναι εγκατεστημένος σε μηχανήματα εντός των εγκαταστάσεων της επιχείρησης και χρησιμοποιείται περισσότερο για εφαρμογές στις οποίες απαιτείται πλήρης έλεγχος και παραμετροποίηση της υποδομής καθώς και ασφάλεια.[2] Παρέχει

μια πιο τυποποιημένη διαδικασία και προστασία, αλλά είναι συχνά περιορισμένο σε μέγεθος και επεκτασιμότητα. Επίσης, οι οργανισμοί θα επιβαρύνονται με το κεφάλαιουχικα και τα λειτουργικά έξοδα για το δικό τους κέντρο δεδομένων.[7]

- **Externally Hosted ιδιωτικό νέφος**

Αυτός ο τύπος cloud ειναι εγκατεστημένος σε μηχανήματα εκτός των εγκαταστάσεων της επιχείρησης, συνήθως από κάποιον τρίτο που ειδικεύεται στην υποδομή cloud. Ο πάροχος δημιουργεί ένα αποκλειστικό περιβάλλον cloud και εγγυάται πλήρως για την ιδιωτικότητά του.[2] Προτείνεται για οργανισμούς που προτιμούν να μην χρησιμοποιούν μια δημόσια υποδομή cloud, λόγω των κινδύνων που συνδέονται με την κατανομή των φυσικών πόρων.[7]

- **Υβριδικό νέφος (Hybrid cloud)**

Η υποδομή αυτού του cloud είναι ένας συνδυασμός από δύο ή περισσότερες διακριτές υποδομές νέφους (ιδιωτική, κοινοτική) οι οποίες είναι ξεχωριστές οντότητες, αλλά παραμένουν συνδεδεμένες μεταξύ τους έτσι ώστε να προσφέρουν τα πλεονεκτήματα που έχει το κάθε είδος. Η υποδομή του cloud είναι σχεδιασμένη έτσι ώστε κάποιες δραστηριότητες όπως η αποθήκευση ή εκτέλεση πολύπλοκων αλγορίθμων να μπορεί να διενεργηθεί με συμπληρωματικά ανεξάρτητα νέφη, όταν προκύπτουν συγκεκριμένες ανάγκες ή όταν ο όγκος δεδομένων ξεπερνά την χωρητικότητα της υποδομής του νέφους(cloud bursting).[5]

Μέρος των δεδομένων αποθηκεύεται στο ιδιωτικό νέφος και κάποιο άλλο στο δημόσιο. Με αυτή την τεχνική τα σημαντικά και απόρρητα δεδομένα, επιλέγονται για αποθήκευση στο ιδιωτικό μέρος του cloud computing, όπου παρέχει περισσότερη ασφάλεια και προστασία σε σχέση με το δημόσιο νέφος, και αυτό είναι που συμβάλλει στην εμπιστοσύνη των χρηστών.[5] Από την άλλη, τα δεδομένα που είναι λιγότερο σημαντικά, η αποθήκευση τους λαμβάνει χώρα στο δημόσιο μέρος του cloud computing, που αποτελεί πολύ πιο οικονομική λύση.[2]

- **Κοινοτικό νέφος (Community cloud)**

Το νέφος κοινότητας είναι ένα μοντέλο υπηρεσιών το οποίο είναι πολυ-πελατιακό και διαμοιράζεται μεταξύ διάφορων οργανισμών στο οποίο η διαχείριση, ο έλεγχος, και η ασφάλεια γίνεται είτε από κοινού από όλους τους συμμετέχοντες είτε από κάποιον τρίτο. Σε αυτού του ίδους το cloud έχουμε πολλές ομοιότητες με τα extranets. Τα νέφη κοινότητας είναι μια υβριδική μορφή ιδιωτικών νεφών που δημιουργούνται και λειτουργούν συγκεκριμένα για μια ομάδα. Αυτές οι κοινότητες έχουν παρόμοιες απαιτήσεις ως προς το νέφος και ο σκοπός τους είναι να επιτευχθούν οι επιμέρους στόχοι του καθενός μέσα από τη συνεργασία. Επιδίωξη των νεφών κοινότητας είναι να μπορέσουν οι συμμετέχοντες οργανισμοί να αξιοποιήσουν τα οφέλη ενός δημόσιου νέφους με το επίπεδο ιδιωτικότητας, ασφάλειας και συμμόρφωσης σε μια κοινή πολιτική που συνήθως σχετίζεται με τα ιδιωτικά νέφη.[2] Η βασικότερη δυσκολία του κοινωτικού νέφους είναι η συμμόρφωση όλων των χρηστών με τους κανονισμούς. Συνήθως είναι δύσκολο να επιτευχθεί συμφωνία απόψεων, στον τρόπο με τον οποίο διατίθενται και χρησιμοποιούνται οι παρεχόμενες υπηρεσίες.[6]

2.9 Υπηρεσίες μοντέλων

Ένας βασικός όρος που χρησιμοποιήται με το υπολογιστικό νέφος είναι η υπηρεσία(service). Οι δύο μεγάλες κατηγορίες μοντέλων υπηρεσιών είναι η NIST SPI και η IBM. Η πρώτη κατηγορία είναι ένα μοντέλο τριών επιπέδων υπηρεσιών, ενώ η δεύτερη κατηγορία είναι ένα μοντέλο τεσσάρων επιπέδων υπηρεσιών.[6]

2.9.1 Μοντέλο SPI

Όσο αναφορά το μοντέλο υπηρεσιών NIST SPI, η κύρια λειτουργία του είναι η ταξινόμηση των υπηρεσιών του παρόχου σε τρείς κατηγορίες:[6]

- **Υπηρεσία Infrastructure as a Service (IaaS)**

Η IaaS είναι το πρώτο επίπεδο του cloud computing και αποτελεί το θεμέλιό του και μέσω αυτού παρέχεται πρόσβαση σε υπολογιστικούς πόρους. Οι φυσικοί πόροι εικονικοποιούνται, το οποίο σημαίνει ότι μπορούν να μοιραστούν από διαφορετικά λειτουργικά συστήματα και περιβάλλοντα χρηστών. Χρησιμοποιώντας αυτό το μοντέλο

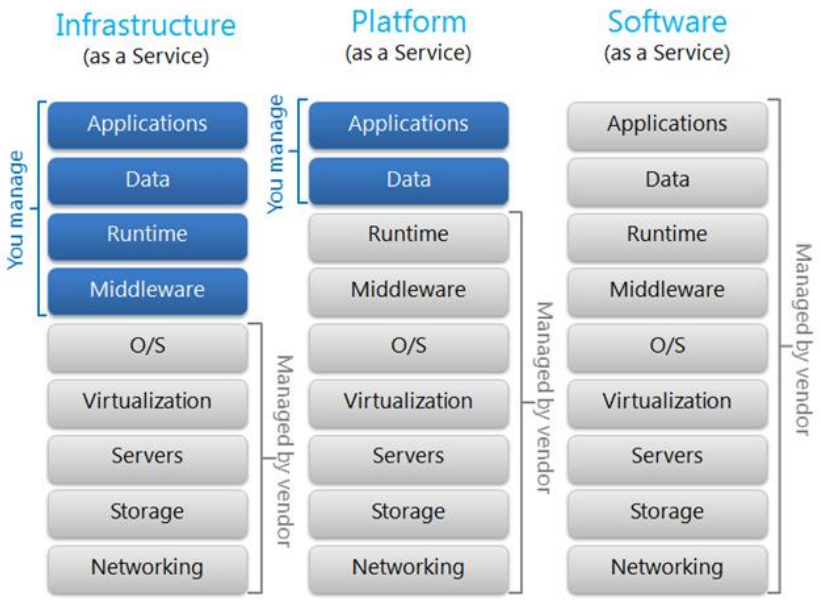
υπηρεσίας, ο χρήστης μπορεί να διαχειριστεί τις εφαρμογές, τα δεδομένα, το middleware και τον χρόνο λειτουργίας. Ο πάροχος διαχειρίζεται την εικονικοποίηση, τους servers, τη δικτύωση και την αποθήκευση. Αυτό επιτρέπει στον χρήστη να αποφύγει δαπάνες υλικού, καθώς σε αυτό το μοντέλο η χρέωση αφορά μόνο τους πόρους που χρησιμοποιούνται, και να βελτιστοποίησει και αυτοματοποιήσει την κλιμάκωση. Μερικοί γνωστοί πάροχοι IaaS είναι οι εξής: Amazon, Microsoft, VMware, Rackspace και Red Hat.[2]

- **Υπηρεσία Platform as Service (PaaS)**

Αυτή η υπηρεσία είναι το δεύτερο επίπεδο και μοιάζει πολύ με την IaaS. Το βασικό στοιχείο είναι ότι παρέχει την πλατφόρμα την οποία χρησιμοποιεί ένας χρήστης για να δημιουργήσει κάτι, για παράδειγμα μια διαδικτυακή εφαρμογή, χωρίς να εγκαταστήσει τίποτα. Επιπλέον, ο πάροχος υποστηρίζει τον χρήστη με ένα σύνολο βασικών υπηρεσιών για να βοηθήσει την επικοινωνία, την παρακολούθηση και τη χρέωση καθώς και διάφορα άλλα κομμάτια για την διευκόλυνση εκκίνησης μιας εφαρμογής, την εξασφάλιση της κλιμακωσιμότητας και ελαστικότητάς.[2]

Ο χρήστης δεν διαχειρίζεται ούτε ελέγχει το υφιστάμενο δίκτυο, τους διακομιστές, τα λειτουργικά συστήματα ή τους αποθηκευτικούς χώρους, αλλά μπορεί να ελέγξει τις ίδιες τις εφαρμογές και σε μερικές περιπτώσεις το περιβάλλον των εφαρμογών.

Το μοντέλο PaaS χρησιμοποιείται πιο πολύ για δημιουργία web interfaces, web εφαρμογών, κ.τ.λ. Μερικές δημοφιλείς PaaS υπηρεσίες είναι οι εξής: Google app Engine, Microsoft Windows Azure, Mozilla, Bespin.[2]



Εικόνα 2. 8: Μοντέλα υπηρεσιών υπολογιστικού νέφους [7]

- **Υπηρεσία Software as a Service (SaaS)**

Αυτή η υπηρεσία είναι το τρίτο και τελευταίο επίπεδο και προσφέρει πλήρεις εφαρμογές στον τελικό χρήστη του νέφους. Είναι ένα μοντέλο διανομής στο οποίο οι εφαρμογές φιλοξενούνται από τον πωλητή ή τον παροχέα υπηρεσίων και γίνεται διαθέσιμο στους πελάτες μέσω διαδικτύου. Το λογισμικό αυτό ανήκει σε κάποιον κατασκευαστή και ο τελικός χρήστης το πληρώνει ανάλογα με την χρήση που κάνει. Ο χρήστης δεν μπορεί να επηρεάσει το διαδίκτυο, τους διακομιστές, τα λειτουργικά συστήματα ή τους αποθηκευτικούς χώρους και στις περισσότερες περιπτώσεις δεν έχει καθόλου ή έχει περιορισμένο έλεγχο πάνω στην ίδια την εφαρμογή. Παράδειγμα SaaS υπηρεσιών είναι οι υπηρεσίες gmail, επιχειρηματικές εφαρμογές και υπηρεσίες περιεχομένου.[10]

2.9.2 Μοντέλο IBM

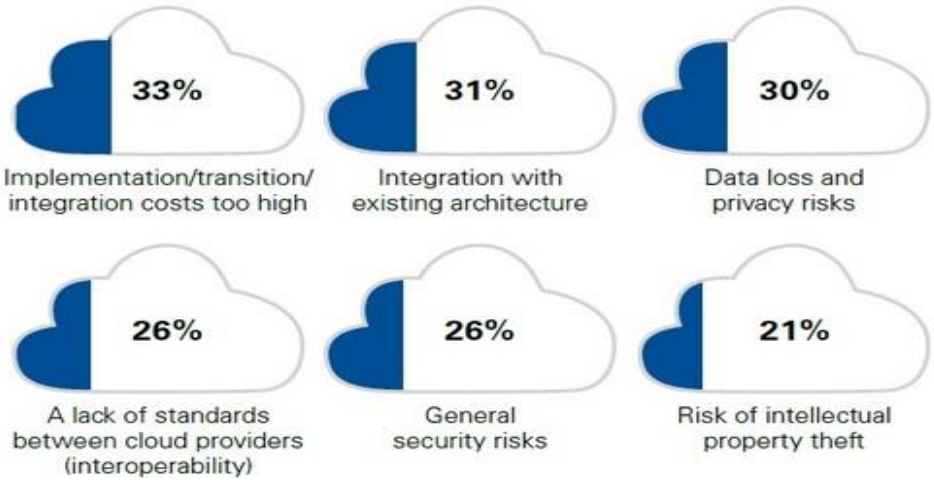
Όσο αναφορά το μοντέλο υπηρεσιών IBM αποτελείται από τέσσερα επίπεδα υπηρεσιών όπου τα τελευταία τρία επίπεδα είναι ακριβώς τα ίδια με το προηγούμενο μοντέλο. Η μόνη διαφορά που έχουν αυτά τα δύο μοντέλα, βρίσκεται στο επιπλέον επίπεδο που διαθέτει.[6]

- **Υπηρεσία Business Process as a Service (BPaaS)**

Το μοντέλο BPaaS επιτρέπει στον πελάτη, ο οποίος μπορεί να είναι ένας απλός χρήστης ή ένας διευθυντής επιχειρηματικών διαδικασιών, να σχεδιάζει, να διαχειρίζεται και να ενσωματώνει συνεργατικές δραστηριότητες, που στηρίζονται στις SaaS υπηρεσίες, έτσι ώστε να επιτευχθεί ένας επιχειρηματικός στόχος. Ο πάροχος προσφέρει εργαλεία για πρόσβαση και αξιοποίηση των πόρων στο BPaaS επίπεδο. Οι χρήστες, δεν είναι αναγκαίο να έχουν πρόσβαση στα υποκείμενα επίπεδα. Ο πάροχος είναι υπεύθυνος για τις επιχειρηματικές λειτουργίες. Αυτή η υπηρεσία βρίσκεται πάνω από τις άλλες τρείς θεμελιώδεις υπηρεσίες cloud, πρέπει να έχει καλά καθορισμένο API έτσι ώστε να μπορεί εύκολα να συνδεθεί με συναφείς υπηρεσίες, και τέλος πρέπει να είναι σε θέση να υποστηρίζει πολλαπλές γλώσσες και πολλαπλά περιβάλλοντα ανάπτυξης, διότι μια επιχείρηση δεν μπορεί να προβλέψει πώς μια επιχειρηματική διαδικασία, θα πρέπει να αξιοποιηθεί στο μέλλον. Μερικά παραδείγματα BPaaS υπηρεσιών, είναι οι διαδικασίες διαχείρισης των επιδομάτων των εργαζόμενων, ή οι διαδικασίες δοκιμής λογισμικού, συμπεριλαμβανομένων και των ελεγχών του προσωπικού, που παρέχονται μέσω των υπηρεσιών του υπολογιστικού νέφους.[6]

2.10 Ζητήματα και Προκλήσεις

Το Cloud Computing έχει ήδη αρχίσει να φέρνει την επανάσταση στον τρόπο με τον οποίο αποθηκεύουν και έχουν πρόσβαση σε δεδομένα οι χρήστες. Όπως κάθε νέα τεχνολογία, έτσι και το cloud computing δεν είναι απαλλαγμένη από προβλήματα. Οι οργανισμοί είναι όλο και περισσότερο σε επίγνωση της επιχειρηματικής αξίας που προσφέρει το cloud computing και λαμβάνουν μέτρα για τη μετάβαση στο νέφος. Μια ομαλή μετάβαση απαιτεί μια εις βάθος κατανόηση των οφελών, καθώς και των προκλήσεων που εμπλέκονται. Μερικές από τις πιο σημαντικές προκλήσεις και ανησυχίες είναι οι ακόλουθες.[8]



Εικόνα 2. 9: Ζητήματα & προκλήσεις υπολογιστικού νέφους [8]

- **Ασφάλεια και Ιδιωτικότητα**

Τα μεγαλύτερα ζητήματα στην υλοποίηση του cloud computing είναι η ασφάλεια και η αποδοτικότητα. Η κύρια πρόκληση για το cloud computing είναι το πώς θα μπορέσει να αντιμετωπίσει τις ανησυχίες για την ασφάλεια και την προστασία της ιδιωτικής ζωής των επιχειρήσεων που ενδιαφερονται να ενταχτούν στο νέφος. Το γεγονός ότι η μετακίνηση, η επεξεργασία και η αποθήκευση πολύτιμων δεδομένων θα γίνεται εκτός του εταιρικού «τοίχους προστασίας» εγγγείρει σοβαρές ανησυχίες.[8]

- **Υπηρεσία παράδοσης και Χρέωσης**

Είναι δύσκολο να εκτιμηθεί το κόστος λόγω της κατά απέτησης φύσης των υπηρεσιών. Ο προϋπολογισμος και η εκτίμηση του κόστους θα είναι πολύ δύσκολο, εκτός αν ο πάροχος έχει κάποια καλά και συγκρίσιμα κριτηρία αξιολόγησης να προσφέρει. Οι συμφωνίες επιπέδου υπηρεσιών(SLA) του παρόχου δεν είναι επαρκή για να διασφαλίζουν τη διαθεσιμότητα και την επεκτασιμότητα. Οι επιχειρήσεις θα είναι απρόθυμες να στραφούν στο «νέφος» χωρίς ισχυρή εγγύηση της ποιότητας των υπηρεσιών.[8]

- **Διαλειτουργικότητα και Φορητότητα**

Η διαλειτουργικότητα είναι η δυνατότητα να χρησιμοποιούνται τα ίδια εργαλεία ή εφαρμογές σε διαφορετικές πλατφόρμες υπηρεσίας νέφους. Οι επιχειρήσεις και οι χρήστες του νέφους θα πρέπει να έχουν τη δυνατότητα να αλλάζουν νέφος όποτε θέλουν χωρίς να υπάρχει περίοδος εξάρτησης από έναν πάροχο. Ένα από τα εμπόδια της διαλειτουργικότητας του νέφους είναι η πιθανότητα εξάρτησης απο έναν πάροχο.[8]

- **Αξιοπιστία και Διαθεσιμότητα**

Το δυνατό σημείο κάθε τεχνολογίας μετριάται από τον βαθμό αξιοπιστίας και διαθεσιμότητας. Οι πάροχοι νέφους εξακολουθούν να στερούνται σε ολοήμερες υπηρεσίες. Αυτό οδηγεί σε συχνές διακοπές, είναι σημαντικό να παρακολουθείται η υπηρεσία που παρέχεται με την χρήση εσωτερικών εργαλείων ή μέσω τρίτων.[8] Επίσης είναι ζωτικής σημασίας να διαθέτουν σχέδια για την εποπτεία της χρήσης SLAs, την απόδοση, την ευρωστία και την επιχειρηματική εξάρτηση των εν λόγω υπηρεσιών. Οι cloud υπηρεσίες μπορούν να υποστούν επιθέσεις DOS, επιβραδύνσεις απόδοσης και φυσικές καταστροφές. Προκειμένου να αντιμετωπιστούν ο φόβος, η αμφιβολία, η παραπληροφόρηση, η αξιοπιστία, η διαθεσιμότητα και η ασφάλεια είναι σημαντικά και πρωταρχικά ζητήματα για έναν οργανισμό. [2]

- **Απόδοση & Εύρος ζώνης**

Η απόδοση γενικά μετριάται από τις δυνατότητες των εφαρμογών που τρέχουν στο cloud. Κακή απόδοση μπορεί να προκύψει από έλλειψη κατάλληλων πόρων όπως χώρος αποθήκευσης, περιορισμένο εύρος ζώνης, χαμηλότερη ταχύτητα CPU, μνήμη, συνδέσεις δικτύου, κ.τ.λ. Για τις εφαρμογές που χρειάζονται να χειριστούν πολλά δεδομένα είναι πιο δύσκολο να παρασχεθούν κατάλληλοι πόροι. Η κακή απόδοση μπορεί να έχει ως αποτέλεσμα τον τερματισμό της παροχής της υπηρεσίας, την απώλεια πελατών, κ.α.[2] Τώρα όσο αναφορά το εύρος ζώνης οι επιχειρήσεις μπορούν να εξοικονομήσουν χρήματα από την αγορά υλικού, αλλά θα πρέπει να δαπανήσουν περισσότερα για το εύρος ζώνης. Από την μία πλευρά αυτό μπορεί να είναι μια χαμηλού κόστους δαπάνη για μικρότερες εφαρμογές, αλλά από την άλλη μπορεί να είναι σημαντικά υψηλό κόστος για τις εφαρμογές υψηλής έντασης δεδομένων. Εντατική

παροχή και σύνθετα δεδομένα μέσω του δικτύου απαιτούν επαρκές εύρος ζώνης. Εξαιτίας αυτού, πολλές επιχειρήσεις περιμένουν για ένα μειωμένο κόστος πριν από τη μετάβαση στο νέφος. Όλες αυτές οι προκλήσεις δεν πρέπει να θεωρηθούν ως οδοφράγματα στην επιδίωξη του cloud computing. Είναι αρκετά σημαντικό να ληφθούν σοβαρά υπόψη αυτά τα ζητήματα και τους πιθανούς τρόπους για διέξοδο από αυτά πριν από την υιοθέτηση της τεχνολογίας.[8]

- **Κλιμακωσιμότητα και Ελαστικότητα**

Ένα από τα βασικά οφέλη της χρήσης του cloud computing είναι η κλιμακωσιμότητα του. Το cloud computing επιτρέπει στην επιχείρησή να κλιμακώσει εύκολα τους πόρους πρός το πάνω ή πρός τα κάτω ανάλογα με τις απαιτήσεις, όπως και όταν απαιτείται. Για παράδειγμα, οι περισσότεροι πάροχοι υπηρεσιών cloud θα σας επιτρέψουν να αυξήσετε τους υπάρχοντες πόρους για να φιλοξενήσουν αυξημένες ανάγκες των επιχειρήσεων ή αλλαγές. Αυτό θα υποστηρίξει την ανάπτυξη της επιχείρησής χωρίς δαπανηρές αλλαγές στα υπάρχοντα συστήματα πληροφορικής. Από την άλλη πλευρά η ελαστικότητα στο cloud computing επιτρέπει στους υπαλλήλους να είναι πιο ευέλικτοι - τόσο εντός όσο και εκτός του χώρου εργασίας. Οι εργαζόμενοι μπορούν να έχουν πρόσβαση σε αρχεία χρησιμοποιώντας web-enabled συσκευές όπως smartphones, φορητούς υπολογιστές, tablets και αλλες συσκευές.[2]

- **Διαχείριση πόρων και Δρομολόγηση**

Η διαχείριση πόρων αφορά διάφορα επίπεδα όπως το λογισμικό, το υλικό, την εικονικοποίηση, την ασφάλεια και άλλες παραμέτρους που εξαρτώνται από τη διαχείριση και την προμήθεια πόρων. Επίσης περιλαμβάνει τη διαχείριση στον χώρο αποθήκευσης της μνήμης, τους επεξεργαστές, τους πυρήνες, τα νήματα, τα στιγμιότυπα των εικονικών μηχανών, τις συσκευές εισόδου/εξόδου, κ.τ.λ. Η δρομολόγηση των εργασιών είναι ένας τύπος διαμοίρασης πόρων όπου η σειρά εκτέλεσης των εργασιών αποφασίζεται με σκοπό να βελτιστοποιηθούν κάποιες παράμετροι όπως ο χρόνος ανάκαμψης, ο χρόνος απόκρισης, ο χρόνος αναμονής, η διεκπεραιωτική ικανότητα και η χρησιμοποίηση των πόρων. Τα ζητήματα δρομολόγησης στα συστήματα cloud είναι ο διαχωρισμός των εργασιών σε παράλληλες εργασίες, η διασύνδεση δικτύων μεταξύ

cloud ή επεξεργαστών, η ανάθεση προτεραιοτήτων σε εργασίες και η επιλογή των επεξεργαστών ή των cloud στα οποία θα παραχωρηθούν οι εργασίες προς εκτελεση, η ευελιξία των εργασιών, το υποστηριζόμενο επίπεδο παράκαμψης της σειράς εκτέλεσης, τα χαρακτηριστικά του φόρτου εργασίας, η παραχώρηση μνήμης, η παρακολούθηση της εκτέλεσης των επιμέρους δουλειών μιας εργασίας, οι απαιτήσεις της παραχώρησης πόρων, η τοπολογία, η φύση της εργασίας κ.τ.λ.[2]

- **Κατανάλωση ενέργειας**

Οι υποδομές των κέντρων δεδομένων για το «νέφος» φιλοξενούν από εκατοντάδες εώς και χιλιάδες εξυπηρετητές, και για να πετύχουν χαμηλές θερμοκρασίες ειδικά όταν βρίσκονται σε αυξημένο φόρτο εργασίας(workload) τους παρέχουν συστήματα ψύξης για να κατεβάσουν την θερμότητα που παράγουν. Από τα παραπάνω συμπαιρένουμε ότι καταναλώνεται ένα τεράστιο ποσοστό ηλεκτρικής ενέργειας. Σύμφωνα με έρευνες που έγιναν στις ΗΠΑ η αποδοτικότητα του cloud computing βοηθά τα κέντρα δεδομένων να μειώσουν την κατανάλωση ηλεκτρικής ενέργειας. Όπως και να έχει πέρα από τον σκοπό της μείωσης της κατανάλωσης ηλεκτρικής ενέργειας των κέντρων δεδομένων και του αντίστοιχου κόστους, σημαντικό είναι η διατήρηση των περιβαλλοντολογικών προτύπων που είναι αναγκαία για την ανθρώπινη ευημερία.[9]

3. ΔΙΑΧΕΙΡΙΣΗ ΑΣΦΑΛΕΙΑΣ

Ασφάλεια στον τομέα της πληροφορικής είναι η διαδικασία που ασχολείται με την προστασία των υπολογιστών, των δικτύων και των δεδομένων, αποτρέποντας τη μη εξουσιοδοτημένη πρόσβαση ή χρήση τους. Και στην συνέχεια η εφαρμογή μίας σειράς από μέτρα προστασίας για να μειωθεί ή να μηδενιστεί αυτή η δυνατότητα. Αυτό το κεφάλαιο ξεκινά με τις απαιτήσεις ασφαλείας, και στην συνέχεια προτείνονται μηχανισμοί για την παροχή των γενικών υπηρεσιών ασφαλείας των μοντέλων υπηρεσίων. Τέλος, εξετάζει τα πλεονεκτήματα & μειονεκτήματα των διαφόρων μοντέλων ανάπτυξης του νέφους από την «σκοπιά» της ασφάλειας.[15] [12]

3.1 Βασικές υπηρεσίες ασφαλείας

Οι βασικές υπηρεσίες για την ασφάλεια των πληροφοριών περιλαμβάνουν διασφάλιση της εμπιστευτικότητας(confidentiality), ακεραιότητας(integrity), και διαθεσημότητας(availability). Στο cloud computing το θέμα της ασφάλειας των δεδομένων γίνεται πιο περίπλοκο λόγω των χαρακτηριστικών του cloud. Πριν οι πιθανοί χρήστες του cloud είναι σε θέση να μεταφέρουν με ασφάλεια τις εφαρμογές ή τα δεδομένα τους, μια πλατφόρμα ασφάλειας πληροφοριών θα πρέπει να είναι σε θέση την οποία μπορούμε να εντοπίσουμε ως εξής:[13]

Εικόνα 3. 1: Confidentiality, Integrity, Availability (CIA) [9]

- **Εμπιστευτικότητα (Confidentiality)**

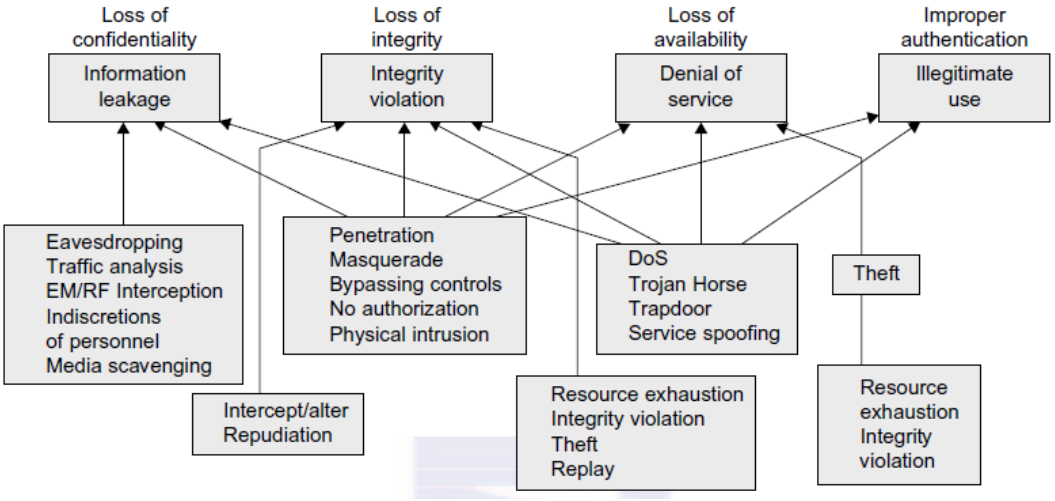
Αυτή η υπηρεσία προστατεύει τα δεδομένα από το να αποκαλυφθούν σε τρίτους. Στο cloud computing, η εμπιστευτικότητα των δεδομένων είναι μια βασική υπηρεσία ασφαλείας. Αν και διαφορετικές εφαρμογές μπορεί να έχουν διαφορετικές απαιτήσεις όσο αναφορά τον όρο της εμπιστευτικότητας αυτή η υπηρεσία θα μπορούσε να ισχύει για όλα τα αντικείμενα δεδομένων. Για παράδειγμα, η εμπιστευτικότητα των δεδομένων μπορεί να γίνει μέσω διαδικτυακών υπηρεσιών ταυτοποίησης, διαδικτυακά πρωτόκολλα ασφαλείας, και υπηρεσιών κρυπτογράφισης δεδομένων.[13][22]

- **Ακεραιότητα (Integrity)**

Αυτή η υπηρεσία προστατεύει τα δεδομένα από κακόβουλη τροποποίηση. Όταν χρήστες ή οργανισμοί έχουν αναθέσει τα δεδομένα τους σε απομακρυσμένους cloud servers πρέπει να έχουν έναν τρόπο να τα ελέγξουν κατά πόσον ή όχι τα δεδομένα τους είναι όπως ήταν, στο ακέραιο. Μια τέτοια υπηρεσία ασφάλειας είναι ο πυρήνας αξίας για τους χρήστες του cloud. Ο κύριος μηχανισμός προστασίας της ακεραιότητας των δεδομένων βρίσκεται μέσα στα ίδια τα VM. Μόνο εξουσιοδοτημένοι πελάτες έχουν πρόσβαση στις υπηρεσίες. Επιπλέον υπηρεσίες που διασφαλίζουν την ακεραιότητα είναι, υπηρεσίες τοίχους προστασίας, IDS και CSM.[13][22]

- **Διαθεσιμότητα (Availability)**

Αυτή η υπηρεσία εξασφαλίζει ότι τα δεδομένα που αποθηκεύονται στο cloud είναι διαθέσιμα σε κάθε αίτημα ανάκτησης τους από τον χρήστη. Η υπηρεσία αυτή είναι ιδιαίτερα σημαντική για τα δεδομένα και σχετικά με την εκπλήρωση του SLA. Για τις υπηρεσίες μακροχρόνιας αποθήκευσης δεδομένων, η διασφάλιση της διαθεσιμότητας των δεδομένων έχει μεγαλύτερη σημασία λόγω της αυξανόμενης δυνατότητας ζημιάς στα δεδομένα ή απώλειας κατά την πάροδο του χρόνου. Για να βελτιωθεί το πρόβλημα της μη διαθεσιμότητας των δεδομένων ο πάροχος του «νέφους» δημιουργεί αντίγραφα των δεδομένων σε διαφορετικά κέντρα δεδομένων σε πολλές χώρες, με αξιόπιστες και διαλειτουργικές διαδικασίες ασφαλείας και μηχανισμούς ασφάλειας δικτύου.[13] [22]



Εικόνα 3. 2: Απειλές CIA[10]

3.2 Ασφάλεια μοντέλων υπηρεσιών

Το κάθε μοντέλο υπηρεσιών του νέφους έχει διαφορετικές απαιτήσεις ασφαλείας. Το μοντέλο IaaS αποτελεί θεμέλιο γιατί πανώ σε αυτό έχει «χτιστεί» το PaaS και τέλος με την σειρά του το SaaS. Έτσι με τον ίδιο τρόπο που μεταφέρονται οι δυνατότητες από το ένα μοντέλο στο άλλο, μεταφέρονται και οι κίνδυνοι και τα διάφορα θέματα ασφαλείας. Γιαυτό το λόγο ο πάροχος θα πρέπει να φροντίζει για την αρχιτεκτονική ασφαλείας από τα χαμηλότερα επίπεδα.[6]

- **Ασφάλεια στο IaaS**

Διάφορα θέματα ασφαλείας στο μοντέλο υπηρεσίας IaaS:[6]

- ❖ Σε αυτό το μοντέλο ο προγραμματιστής έχει καλύτερο έλεγχο από τα άλλα μοντέλα σε θέματα ασφαλείας, υπό την προϋπόθεση ότι δεν υπάρχει κάποιο κενό ασφαλείας στην διαχείριση της εικονοποίησης.
- ❖ Το κύριο σημείο σε αυτό το μοντέλο είναι η αξιοπιστία των δεδομένων που είναι αποθηκευμένα.
- ❖ Για να επιτευχθεί καλύτερη ασφάλεια και εμπιστοσύνη πρέπει να εφαρμοστούν πρακτικές διασφάλισης.
- ❖ Ο πελάτης είναι υπεύθυνος για το κομμάτι της ασφάλειας που σχετίζεται με το σύστημα τεχνολογίας πληροφορίας.

- Ο βαθμός των ζητημάτων ασφαλείας που παρουσιάζει το μοντέλο IaaS εξαρτάται από τα μοντέλα ανάπτυξης μέσω των οποίων διατίθεται.

Παρόλα αυτά όσο και να αυξήσουμε τα μέτρα ασφαλείας, το υπολογιστικό νέφος βασίζεται πάνω στο ίδιο το διαδίκτυο. Η κρυπτογράφιση και η χρήση ασφαλών πρωτοκόλλων λειτουργούν σε κάποιο βαθμό, αλλά σίγουρα δεν είναι η λύση. Αυτό που χρειάζεται είναι ένας συνδιασμός πολιτικών και πρωτοκόλλων για την ασφαλή μετάδοση των δεδομένων.[6]

- **Ασφάλεια στο PaaS**

Διάφορα θέματα ασφαλείας στο μοντέλο υπηρεσίας PaaS:[6]

- Το μοντέλο αυτό προσφέρει στους προγραμματιστές ένα περιβάλλον για δημιουργία εφαρμογών χωρίς να έχουν γνώση για το τι συμβαίνει στο παρακάτω επίπεδο IaaS.
- Προσφέρει υπηρεσίες διαχείρισης λογισμικού από το σχεδιασμό μέχρι την δημιουργία εφαρμογών ελέγχου συντήρησης.
- Το μειονέκτημα αυτού του μοντέλου είναι ότι όλα αυτά τα πλεονεκτήματα μπορούν να φανούν χρήσιμα και σε έναν hacker που μπορεί να χρησιμοποιήσει το μοντέλο για την ανάπτυξη κακόβουλου λογισμικού, ικανού να περάσει ακόμα και στις εφαρμογές του IaaS επιπέδου.
- Στο συγκεκριμένο μοντέλο, υπάρχουν αρκετά πολύπλοκες εφαρμογές όπως ESB, στις οποίες πρέπει να παρέχεται υψηλό επίπεδο ασφαλείας, αξιοποιώντας πρωτόκολλα, όπως το πρωτόκολλο της ασφάλειας των υπηρεσιών διαδικτύου WSSP.
- Η δυνατότητα να τμηματοποιηθούν οι υπηρεσίες ESB δεν είναι διαθέσιμη στο περιβάλλον του PaaS. Γιαυτό οι πάροχοι πρέπει να είναι σε θέση, με τη χρήση μετρικών «εργαλείων», να εκτιμήσουν την αποτελεσματικότητα των προγραμμάτων ασφαλείας των εφαρμογών.

- **Ασφάλεια στο SaaS**

Διάφορα θέματα ασφαλείας στο μοντέλο υπηρεσίας SaaS:[6]

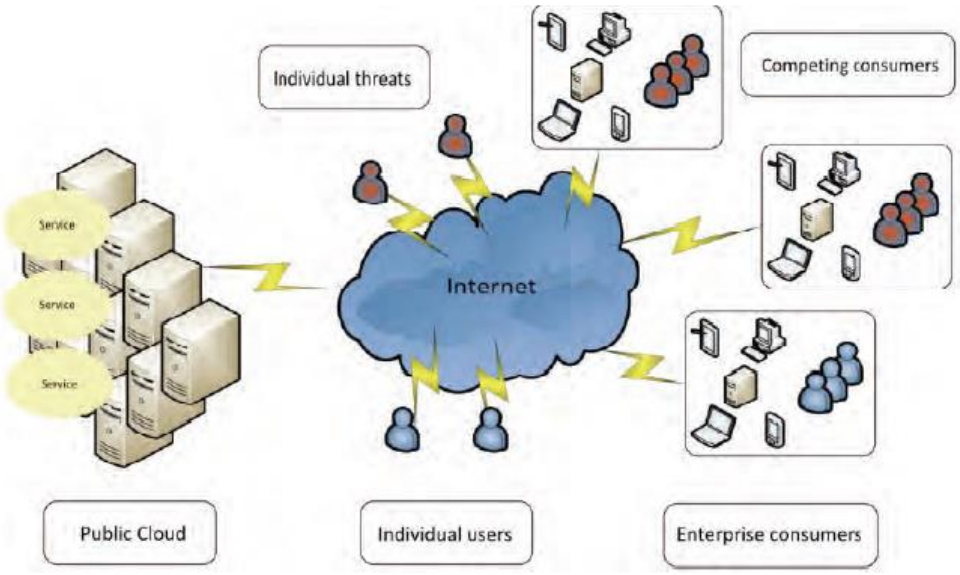
- ❖ Σε αυτό το μοντέλο ο πελάτης βασίζεται στον πάροχο για τα κατάλληλα μέτρα ασφαλείας.
- ❖ Ο πάροχος θα πρέπει να έχει φροντίσει ώστε οι χρήστες να έχουν τα κατάλληλα δικαιώματα για να μην μπορεί ο ένας να δει τα προσωπικά δεδομένα του άλλου.
- ❖ Ο πελάτης επίσης δεν γνωρίζει σίγουρα ότι η διαθεσιμότητα των δεδομένων είναι εγγυημένη.
- ❖ Επίσης όταν το μοντέλο ανάπτυξης είναι δημόσιο νέφος τα δεδομένα των επιχειρήσεων αποθηκεύονται μαζί και με άλλου είδους δεδομένα, άσχετα μεταξύ τους.

3.3 Χαρακτηριστικά ασφαλείας μοντέλων ανάπτυξης νέφους

Σε αυτήν την ενότητα θα αναφερθούμε στα χαρακτηριστικά ασφαλείας, στα πλεονεκτήματα & μειονεκτήματα των διαφόρων μοντέλων ανάπτυξης.

- **Δημόσιο νέφος**

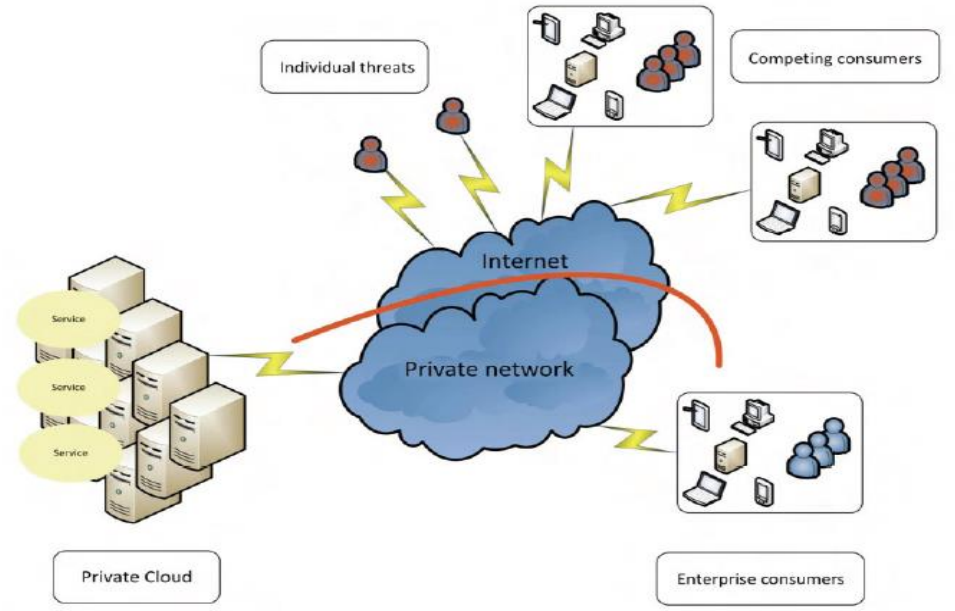
Οι διαφορετικοί πελάτες ενός CSP χωρίζονται μόνο από τους μηχανισμούς που έχουν τεθεί από τους CSPs, μια ανασφαλή υπηρεσία νέφους θα μπορούσε αποτελεσματικά να γεφυρώσει όλη την πελατειακή της βάση. Έτσι, στο μοντέλο δημοσίου νέφους, υπάρχουν κοινά δίκτυα, hypervisors, υπηρεσίες ελέγχου πρόσβασης, αποθήκευσης και κοινές πλατφόρμες και εφαρμογές (ανάλογα με το μοντέλο παροχής υπηρεσιών). Οι CSPs μεγάλων δημοσιών νεφών, λόγω τον πολλών κατανεμημένων κέντρων δεδομένων και την μεταφορά των δεδομένων μεταξύ τους, τυχαία επιτρέπουν στα δεδομένα να διαρρεύσουν από το ένα κέντρο δεδομένων στο άλλο. Αυτό συχνά οδηγεί σε έλλειψη εμπιστοσύνης των πελατων. Φυσικά το δημόσιο νέφος έχει και κάποια πλεονεκτήματα. Ένα από αυτά είναι η ευρεία προβολή των περιστατικών ασφάλειας που οι CSPs μπορεί να έχουν σε όλη την πελατειακή τους βάση.[12]



Εικόνα 3. 3: Μοντέλο ανάπτυξης δημόσιου νέφους [11]

- **Ιδιωτικό νέφος**

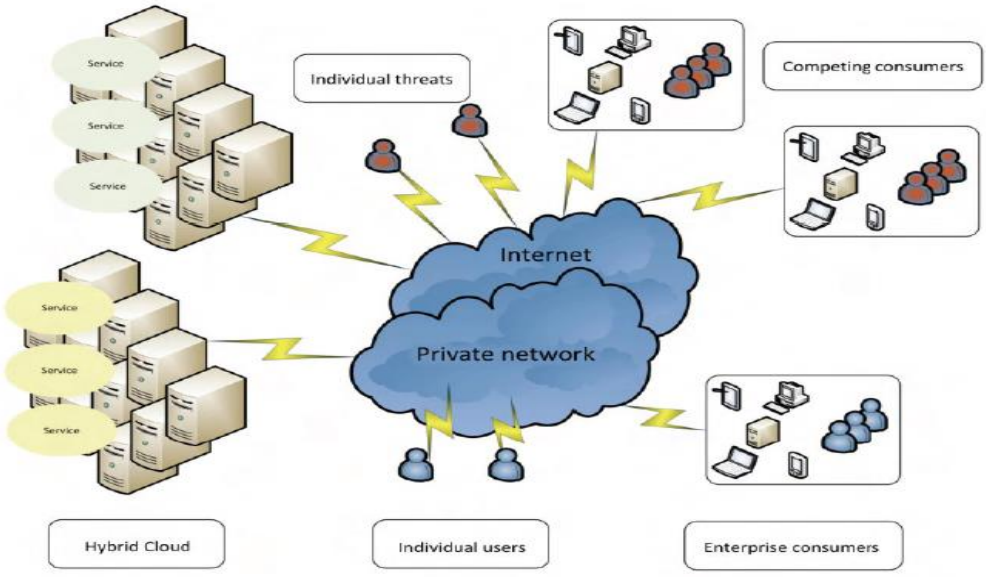
Από την άποψη της ασφάλειας, δεν υπάρχει αμφιβολία ότι το ιδιωτικό μοντέλο νέφος προσφέρει στους καταναλωτές τον περισσότερο ελέγχο. Ο καταναλωτής μπορεί να υπαγορεύσει τις δικές του απαιτήσεις σε λεπτομερή διάλογο και διαπραγμάτευση με τους υποψήφιους CSPs, ως εκ τούτου, επιτρέπει στους καταναλωτές να εφαρμόσουν τις ακριβείς λύσεις ασφάλειας που απαιτούν, υπό τους συνήθεις περιορισμούς γύρω από το κόστος. Αν ο καταναλωτής σκοπεύει να λειτουργίσει το δικό του ιδιωτικό νέφος(αντί για εξωτερική ανάθεση), τότε θα πρέπει επίσης να αποδεχθεί την ανάγκη να παρέχει τους απαραίτητους πόρους ασφαλείας. Ένα κύριο ζήτημα με τα ιδιωτικά νέφη από την προοπτική της ασφάλειας σχετίζεται με τη διαθεσιμότητα, ένα άλλο είναι ότι πρέπει να κάνει πρόβλεψεις για επαρκή εξοπλισμό πληροφορικής για να είναι σε θέση να καλύψει τις μέγιστες αιχμές χρήσης. Αυτό κατά πάσα πιθανότητα θα αφήσει την οργάνωση με το παραδοσιακό θέμα της πλεονάζουσας παραγωγικής ικανότητας, σύμφωνα με την οποία υπολογιστικοί πόροι παραμένουν απαθείς.[12]



Εικόνα 3. 4: Μοντέλο ανάπτυξης ιδιωτικού νέφους [11]

- **Υβριδικό νέφος**

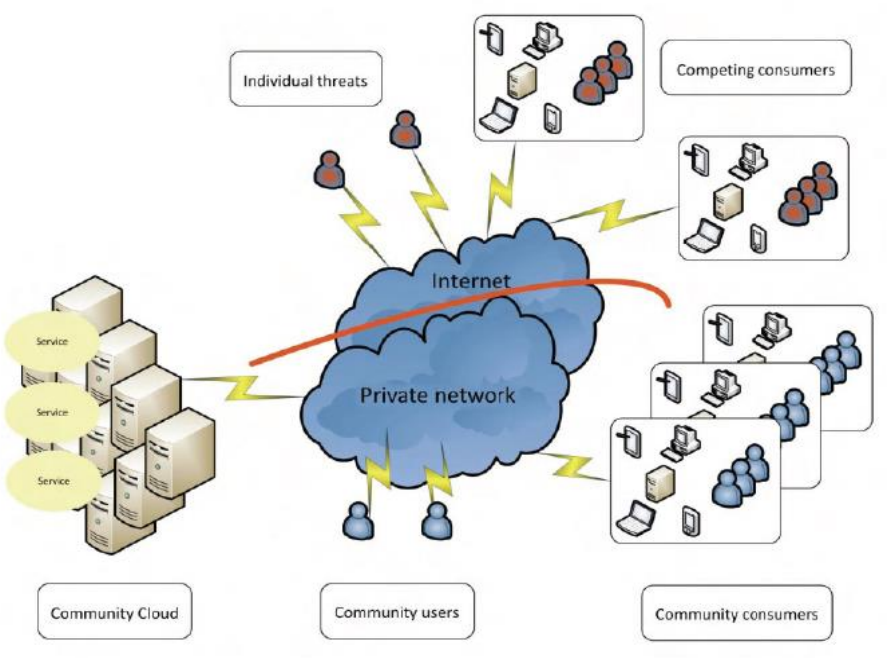
Το υβριδικό νέφος είναι το χειρότερο από την άποψη της ασφάλειας, ιδίως εάν ληφθεί υπόψη ο συνδυασμός των ιδιωτικών και δημοσίων μοντέλων νέφους. Όχι μόνο οι καταναλωτές θα πρέπει να επενδύσουν σε όλους τους πόρους της ασφάλειας που σχετίζονται με τη λειτουργία ενός ιδιωτικού (ή κοινοτικού) νέφους, αλλά θα πρέπει επίσης να εφαρμόσουν τους ελέγχους που απαιτούνται για να λειτουργήσει στο δημόσιο νέφος. Το υβριδικό μοντέλο είναι ακατάλληλο για κάθε οργανισμό που έχει επιλέξει την κατασκευή ενός ιδιωτικού νέφους, λόγω ζητημάτων συμμόρφωσης που θεωρούνται ανυπέρβλητα χρησιμοποιώντας ένα τέτοιο μοντέλο. Από την άποψη της ασφάλειας, η τοποθέτηση των δεδομένων στο δημόσιο νέφος θέτει αμέσως όλα τα ζητήματα που σχετίζονται με τη λειτουργία του δημόσιου νέφους.[12]



Εικόνα 3. 5: Μοντέλο ανάπτυξης ιβριδικού νέφους [11]

- **Κοινοτικό νέφος**

Το πλεονέκτημα με το κοινωτικό νέφος σχετικά με τα ιδιωτικά νέφη είναι ότι καθορίζουν τις δικές τους απαιτήσεις κοινής ασφάλειας και μπορούν να επιλέξουν τη θέση των κέντρων δεδομένων. Δεδομένου ότι το κοινοτικό νέφος είναι μεταξύ του ιδιωτικού και του δημοσίου, όσον αφορά την δυναμικότητα της διαθεσιμότητας. Το κοινοτικό νέφος βοηθάει τους χρήστες να καλύψουν τις ανάγκες τους με την κατανομή των πόρων που δεν έχουν διατεθεί σε άλλα μέλη της κοινότητας. Αυτό βασίζεται στην ιδέα ότι ο κάθε χρήστης έχει διαφορετικές ανάγκες από πόρους. Ένα μειονέκτημα της προσέγγισης του κοινότικου νέφους, είναι η ανάγκη για τη δημιουργία εμπιστοσύνης μεταξύ των μελών της κοινότητας, αλλά και να συμφωνήσουν σε μια κοινή δομή διακυβέρνησης. Ένα κοινοτικό νέφος απαιτεί ένα κεντρικό φορέα διακυβέρνησης για να ορίσουν τις απαιτήσεις, τις προϋποθέσεις και τα επίπεδα εξυπηρέτησης που αναμένεται από τον CSP. [12]



Εικόνα 3. 6: Μοντέλο ανάπτυξης κοινοτικού νέφους [11]

Ο Παρακάτω **Πίνακας 3.1** συνοψίζει τη συζήτηση σχετικά με τις δυνατότητες & αδυναμίες των διαφορετικών μοντέλων ανάπτυξης του νέφους από την άποψη της ασφάλειας. [12]

Πίνακας 3. 1: Περιγραφή μοντέλων ανάπτυξης [16]

Μοντέλο Ανάπτυξης	**Δυνατότητες**	**Αδυναμίες**
Δημόσιο	• Εντύπωση των απείρων πόρων. • Ευρεία προβολή των περιστατικών ασφάλειας. • Πόροι ασφάλειας παροχέα.	• Ανησυχίες συμμόρφωσης. • Multi-tenancy.

Κοινοτικό	• Μπορεί να φιλοξενηθεί από την κοινότητα ή να γίνει εξωτερική αναθέση.	• Απαιτεί ένα κεντρικό σώμα (ή επιτροπή) για τη διαχείριση της υπηρεσίας. • Απαίτηση να προμηθεύονται και να εφαρμόσουν την υπηρεσία cloud. • Απαίτηση να εμπιστεύονται τα άλλα μέλη της κοινότητας. • Ανάγκη για παροχή ασφάλειας σε κοινοτικούς πόρους.
Ιδιωτικό	• Πλήρης έλεγχος. από τον χρήστη. • Συμμόρφωση. • Κλειστή ομάδα χρηστών. • Μπορεί να φιλοξενηθεί από τον καταναλωτή ή να γίνει εξωτερική ανάθεση.	• Πρέπει να επενδύσουμε στην αρχική υλοποίηση της υπηρεσίας. • Απαίτηση οι χρήστες να παρέχουν τους δικούς τους πόρους της ασφάλειας. • Μικρότερη δυνατότητα κλιμάκωσης.
Υβριδικό	Καμία	• Multi-tenancy • Ανυσηχίες συμμόρφωσης

3.4 Υπηρεσίες ασφαλείας νέφους

Πρόσθετοι παράγοντες που επηρεάζουν άμεσα την διασφάλιση του «νέφους» συνοψίζονται παρακάτω:

- **Φυσική ασφάλεια**

Οι καταναλωτές θα πρέπει να εξασφαλίσουν ότι είναι ικανοποιημένοι με τους περιβαλλοντικούς ελέγχους που διενεργούνται από τον CSP. Για να διατηρηθεί ένα κατάλληλο περιβάλλον για τον εξοπλισμό πληροφορικής όσον αφορά την ψύξη, την ανθεκτικότητα και τα εφεδρικά συστήματα τροφοδοσίας. [12]

- **Αποθήκευση**

Είτε χρησιμοποιώντας IaaS, PaaS ή SaaS, οι καταναλωτές είναι πιθανό να χρειαστεί να αποθηκεύουν τα δεδομένα εντός του CSP, και, ως εκ τούτου, εντός των κέντρων δεδομένων του CSP. Ενώ οι καταναλωτές μπορεί να είναι σε θέση να εξασφαλίσουν τα δεδομένα τους μέσω κρυπτογράφησης (ανάλογα με την υπηρεσία νέφους), σε άλλες περιπτώσεις, οι καταναλωτές θα είναι εξαρτημένοι από την ασφάλεια της αποθήκευσης που παρέχεται από τον CSP. Όπου είναι δυνατόν, οι καταναλωτές θα πρέπει να αισθάνονται άνετα με τους μηχανισμούς που χρησιμοποιούνται από τον CSP για την ασφάλεια των δεδομένων τους, όταν είναι αποθηκευμένα εντός του νέφους. Αυτό θα πρέπει να περιλαμβάνει εξέταση των:[12]

  - Μηχανισμοί διαχωρισμού δεδομένων που ανήκουν σε διαφορετικούς καταναλωτές.
  - Μηχανισμοί στήριξης για την αποθήκευση.
  - Δυνατότητες που παρέχονται στους καταναλωτές για να αφαιρέσουν τα δεδομένα τους από τον CSP.

- **Επικοινωνίες**

Οι καταναλωτές θα πρέπει να εξασφαλίσουν ότι τα κέντρα δεδομένων του CSP έχουν πολλαπλούς συνδέσμους επικοινωνίας για να εξασφαλιστεί ότι η υπηρεσία τους παραμένει διαθέσιμη σε περίπτωση βλάβης του δικτύου. Σε περίπτωση που οι

πληροφορίες αυτές δεν είναι διαθέσιμες από τον CSP, οι καταναλωτές θα πρέπει να εξισορροπήσουν τον κίνδυνο της υπηρεσίας που δεν πληρεί τις απαιτήσεις τους, έναντι των αναμενόμενων οφελών της υπηρεσίας cloud. [12]

- **Περιβαλοντολογική ασφάλεια**

Οι χρήστες θα πρέπει να εξασφαλίσουν ότι οι μηχανισμοί φυσικής ασφάλειας του CSP είναι επαρκείς για την κάλυψη των αναγκών τους. Αυτό δεν θα πρέπει να περιορίζεται μόνο στην εξωτερική ασφάλεια άλλα και ότι οι CSPs περιλαμβάνουν, επίσης, επαρκείς μηχανισμούς εσωτερικής ασφάλειας.[12]

- **Διαχείριση κινδύνου(Risk management)**

Η αποτελεσματική διαχείριση του κινδύνου συνεπάγεται με την αναγνώριση των τεχνολογικών περιουσιακών στοιχείων, την αναγνώριση των δεδομένων και των δεσμών τους με τις επιχειρησιακές διεργασίες, εφαρμογές, και των αποθηκευμένων δεδομένων. Οι δράσεις θα πρέπει επίσης να περιλαμβάνουν τη διατήρηση ενός αποθετηρίου για τα περιουσιακά στοιχεία πληροφορικής. Οι ιδιοκτήτες έχουν την υποχρέωση λογοδοσίας για τα περιουσιακά στοιχεία πληροφορικής. Συμπεριλαμβανομένων των απαιτήσεων προστασίας και της εφαρμογής της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας. Πρέπει να δημιουργηθεί μια επίσημη διαδικασία αξιολόγησης των κινδύνων που κατανέμει τους πόρους της ασφάλειας που συνδέονται με την επιχειρηματική συνέχεια.[10]

- **Αξιολόγηση κινδύνου(Risk assessment)**

Η αξιολόγηση κινδύνου ασφαλείας είναι ζωτικής σημασίας για να βοηθήσει στην οργάνωση της ασφάλειας των πληροφοριών, να προβεί σε ενημερωμένες αποφάσεις. Η έλλειψη προσοχής για την ολοκλήρωση της αξιολόγησης κινδύνου μπορεί να συμβάλει στο να οδηγήσει σε ανεπαρκή και αναποτελεσματική επιλογή των ελέγχων ασφαλείας που δεν μπορεί να μετριάσει επαρκώς τους κινδύνους ασφάλειας των πληροφοριών σε ένα αποδεκτό επίπεδο. Μια τυπική διαδικασία διαχείρισης των κινδύνων ασφαλείας των πληροφοριών θα πρέπει προληπτικά να κάνει εκτίμηση των κινδύνων ασφάλειας των πληροφοριών, καθώς και ένα σχέδιο για την διαχείρισή τους σε περιοδική βάση. Πιο

λεπτομερές και τεχνικές αξιολόγησεις κινδύνου ασφάλειας υπό την μορφή των μοντέλων απειλής θα πρέπει επίσης να εφαρμόζεται στις αιτήσεις και τις υποδομές.[10]

- **Αυθεντικοποίηση(Authentication)**

Η αυθεντικοποίηση ελέγχει και επικυρώνει την ταυτότητα του αντικειμένου που επιζητεί πρόσβαση και χρήση. Το αντικείμενο αυτό μπορεί να είναι ένας άνθρωπος, μια εφαρμογή δικτύου ή μια συσκευή δρομολόγησης. Ο έλεγχος για την αυθεντικότητα γίνεται πριν από οποιαδήποτε συναλλαγή.[14]

- **Λογοδοσία(Accountability)**

Λογοδοσία είναι η δυνατότητα που καθορίζει τις ενέργειες και τις συμπεριφορές ενός μεμονωμένου ατόμου μέσα σε ένα σύστημα cloud και προσδιορίζει το συγκεκριμένο άτομο. Σχετίζεται με την έννοια όπου ένα άτομο δεν μπορεί να αρνηθεί με επιτυχία την απόδοση μιας δράσης. Αρχεία καταγραφής υποστηρίζουν αυτήν την δυνατότητα και μπορούν να αρθούν για ανάλυση γεγονότων και ατόμων που σχετίζονται με αυτά.[22]

- **Εξουσιοδότηση(Authorization)**

Η εξουσιοδότηση αναφέρεται σε δικαιώματα και προνόμια που χορηγούνται σε ένα άτομο ή διαδικασίες που επιτρέπουν την πρόσβαση σε πόρους του υπολογιστή και τα περιουσιακά στοιχεία των πληροφοριών. Μόλις η ταυτοποίηση ενός χρήστη εγκριθεί. Τα επίπεδα εξουσιοδότησης καθορίζουν τα δικαιώματα του συστήματος που ένας χρήστης μπορεί να έχει.[22]

3.5 Θεμελιώδεις έννοιες ασφαλείας

Η ασφάλεια πληροφοριακών συστημάτων, είναι ένα πεδίο της επιστήμης των υπολογιστικών συστημάτων, που ασχολείται με την προστασία των υπολογιστών, των δικτύων που τους διασυνδέουν και των δεδομένων σε αυτά τα συστήματα, ώστε να αποτρέψουν τη μη εξουσιοδοτημένη πρόσβαση ή χρήση τους απο άλλα άτομα.[18]

Για καλύτερη κατανόηση, δίνονται οι βασικοί ορισμοί που χρησιμοποιούνται ευρέως στην ανάλυση κινδύνων:

- **Ασφάλεια υπολογιστών(Computer security):**Είναι η διαφύλαξη υπολογιστικών πόρων από μη εξουσιοδοτημένη χρήση.[14]
- **Ασφάλεια επικοινωνιών (Communication security):** Είναι η προστασία των δεδομένων κατά τη μετάδοση τους σε δίκτυα και κατανεμημένα συστήματα.[14]
- **Απειλή(Threat):** Είναι ένα γεγονός που μπορεί να προκαλέσει μη διαθεσιμότητα του συστήματος και των υπηρεσιών, μετατροπή ή καταστροφή των δεδομένων, παραβίαση σε τμήμα ή στο σύνολο του δικτύου και τέλος αποκάλυψη ευαίσθητων πληροφοριών από μη εξουσιοδοτημένες οντότητες.[14]
- **Ευπάθεια(Vulnerability):** Είναι η αδυναμία ενός σύστηματος ή μιας εφαρμογής που μπορεί να γίνει ο λόγος για την παραβίαση της ασφάλειας και της ακεραιότητας του συστήματος.[18]
- **Κίνδυνος(Risk):** Είναι η πιθανότητα απειλής, ζημίας, απώλειας, ή οποιοδήποτε άλλο αρνητικό φαινόμενο που προκαλείται από εξωτερικούς ή εσωτερικούς παράγωντες και έχει ως στόχο την ευπάθεια.[18]
- **Αντίμετρο(Countermeasure):** Είναι μια διαδικασία, που λαμβάνεται για να αποτρέψει τις απειλές ή τις επιπτώσεις σε ένα υπολογιστικό σύστημα ή δικτύο.[14]
- **Επίθεση(Attack):** Είναι η εκμετάλλευση μιας ευπάθειας ενός συστήματος ή μιας εφαρμογής από κακόβουλους χρήστες για την πραγματοποίηση απειλής.[14]

3.6 Συστήματα ανίχνευσης εισβολής

Τα συστήματα ανίχνευσης εισβολής(Intrution detection sytems) είναι ένα βασικό στοιχείο των αμυντικών μέτρων προστασίας των ηλεκτρονικών υπολογιστικών συστημάτων και δικτύων κατά των κακόβουλων χρηστών. Παίζουν σημαντικό ρόλο στο περιβάλον του υπολογιστικού νέφους. Το κλειδί είναι να εντοπίσει, και ενδεχομένως, να εμποδίσει τις δραστηριότητες που ενδέχεται να θέσουν σε κίνδυνο την ασφάλεια του συστήματος. Υπάρχουν κυρίως δύο τύποι IDS:[16]

- **Host level (HIDS)**

Αυτό το είδος IDS περιλαμβάνει λογισμικό το οποίο εκτελείται στον εξυπηρετητή, δρομολογητή ή σε συσκευή δικτύου. Ωστόσο, μπορεί να τρέξουν μαζί στον ίδιο διακομιστή. Βασικά, το HIDS παρέχει μικρή ανταπόκριση σε πραγματικό χρόνο και δεν μπορεί να υπερασπιστεί αποτελεσματικά έναντι καταστροφικών γεγονότων. Στην

πραγματικότητα, τα HIDS είναι πολύ καλύτερα στην ανίχνευση και την αντιμετώπιση των μακροπρόθεσμων επιθέσεων, όπως η κλοπή δεδομένων.[16]

- **Network level (NIDS)**

Αυτό το είδος IDS συλλέγει πακέτα κίνησης του δικτύου, όπως το TCP, UDP και IPX / SPX), και αναλύει το περιεχόμενο ενάντια σε ένα σύνολο κανόνων ή υπογραφων για να καθοριστεί εάν ένα πιθανό γεγονός έλαβε χώρα. Τα λανθασμένα αποτελέσματα είναι ένα συχνό φαινόμενο, όταν ένα σύστημα IDS δεν έχει ρυθμιστεί ή «συντονιστεί» με την κυκλοφορία στο περιβάλλον που προσπαθεί να αναλύσει.

Ένα βασικό χαρακτηριστικό των συστημάτων ανίχνευσης εισβολής είναι η ικανότητά τους να μπορούν να καταγράψουν ασυνήθιστες δραστηριότητες και να ειδοποιούν τους διαχειριστές ή να προβούν στον αποκλεισμό μιας ύποπτης σύνδεσης. Επιπλέον, τα εργαλεία IDS είναι ικανά να διακρίνουν επιθέσεις που προέρχονται από το εσωτερικό του οργανισμού (από τους ίδιους τους υπαλλήλους ή πελάτες) και από χρήστες εκτός του οργανισμού (επιθέσεις και απειλή από hackers).[16]

Μόλις ανιχνευθεί μια εισβολή, το IDS ειδοποιεί τους διαχειριστές για αυτό το γεγονός. Το επόμενο βήμα είναι να αναληφθεί είτε από τους διαχειριστές ή από το ίδιο το IDS κάποια αντίμετρα (συγκεκριμένες λειτουργίες για να τερματίσει συνεδρίες, εφεδρικά συστήματα, συνδέσεις δρομολόγησης σε ένα σύστημα παγίδα, νομικές υποδομές, κ.τ.λ.) ακολουθώντας την πολιτική ασφάλειας του οργανισμού. Μεταξύ των διαφόρων καθηκόντων του IDS, η ταυτοποίηση εισβολέα είναι ένα από τα θεμελιώδη. Επίσης μπορεί να είναι χρήσιμο για την πρόβλεψη μελλοντικών προσπαθειών επίθεσης που μπορεί να έχουν ως στόχο συγκεκριμένους χρήστες ή πόρους.[16]

3.6.1 Λειτουργίες IDS

- Παρακολούθηση και ανάλυση τόσο των δραστηριοτήτων του χρήστη και του συστήματος.
- Αναλύοντας διαμορφώσεις του συστήματος και τα τρωτά σημεία.
- Αξιολόγηση του συστήματος και της ακεραιότητας των αρχείων.
- Δυνατότητα αναγνωρίσης των προτύπων που χαρακτηρίζουν τις επιθέσεις.
- Παρακολούθηση για παραβιάσεις της πολιτικής του χρήστη.
- Ανάλυση προτύπων για μη συνιθησμένη δραστηριότητα.[16]

3.6.2 Μέθοδοι ανίχνευσης εισβολής

Ένα σύστημα IDS αυξάνει το επίπεδο ασφάλειας ενός «νέφους» με την εφαρμογή δύο μέθοδων ανίχνευσης εισβολής:[17]

- **Η μέθοδος με βάση την συμπεριφορά (behavior - based)**

Υπαγορεύει πώς να συγκρίνουμε πρόσφατες ενέργειες του χρήστη με την συνηθή τους συμπεριφορά.

- **Η μέθοδος που βασίζεται στην γνώση (knowledge - based)**

Εντοπίζει ίχνη που άφησαν τυχών επιθέσεις ή ορισμένες ακολουθίες ενεργειών ενός χρήστη που θα μπορούσε να αντιπροσωπεύσει μια επίθεση.

3.6.3 Ανίχνευση εισβολής στα μοντέλα υπολογιστικού νέφους

Η ικανότητά του να εκτελεστεί ανίχνευση εισβολής στο νέφος εξαρτάται σε μεγάλο βαθμό από το μοντέλο του υπολογιστικού νέφους που χρησιμοποιείτε:[42]

- **Software as a Service (SaaS)**

Η πραγματικότητα είναι ότι οι χρήστες αυτού του μοντέλου πρέπει να βασίζονται σχεδόν αποκλειστικά στον πάροχο του νέφους για να εκτελέσει την ανίχνευση εισβολής (ID). Υπάρχει η δυνατότητα να ληφθούν μερικά αρχεία καταγραφής και να αναπτυχθεί μια προσαρμοσμένη παρακολούθηση και ειδοποίηση σε αυτές τις πληροφορίες.

- **Platform as a Service (PaaS)**

Λειτουργεί όπως το μοντέλο SaaS, το μεγαλύτερο μέρος της ανίχνευσης εισβολής για αυτό το επίπεδο των υπηρεσίων θα γίνει από τον πάροχο. Δεδομένου ότι τα συστήματα ανίχνευσης εισβολής είναι συνήθως έξω απο την εφαρμογή θα πρέπει ο πελάτης να βασίζεται στον πάροχο του ώστε να αναπτύξει ένα σύστημα ανίχνευσης εισβολής στο μοντέλο PaaS. Μπορεί ωστόσο να γίνει διαμόρφωση στις εφαρμογές και στις πλατφόρμες ώστε να γίνει είσοδος σε ένα κεντρικό σημείο όπου στην συναίχια μπορεί να γίνει παρακολούθηση και ειδοποίηση.

- **Infrastructure as a Service (IaaS)**

Αυτό είναι το πιο ευέλικτο μοντέλο για την ανάπτυξη ανίχνευσης εισβολής. Σε αντίθεση με τα άλλα δύο, το μοντέλο IaaS δίνει περισσότερες επιλογές στον καταναλωτή.

Πρέπει να προσδιοριστούν οι θέσεις που θα πρέπει να λαμβάνονται υπόψη όταν σκεφτόμαστε ανίχνευση εισβολής στο μοντέλο IaaS. Υπάρχουν τέσσερα κύρια σημεία:[42]

- **Στην εικονική μηχανή (VM)**

Μας επιτρέπει να παρακολουθούμε την δραστηριότητα του συστήματος, τον εντοπισμό, και την προειδοποίηση σχετικά με προβλήματα που μπορεί να προκύψουν.

- **Στα συστήματα Host και hypervisor**

Η ανάπτυξη ανίχνευσης εισβολής στο λογισμικό hypervisor επιτρέπει την παρακολούθηση όχι μόνο στο hypervisor αλλά σε οτιδήποτε περνάει μεταξύ εικονικής μηχανής στο hypervisor. Αλλά μπορεί να υπάρχουν θέματα σε ότι αφορά την επίδοση ή την απώλεια κάποιων πληροφορίων, εάν το μέγεθος των δεδομένων είναι πολύ μεγάλο.

- **Στο εικονικό δίκτυο(VN)**

Η ανάπτυξη ανίχνευσης εισβολής για να παρακολουθείτε το εικονικό δίκτυο (δηλαδή, το δίκτυο που δημιουργήθηκε μέσα στο κεντρικό υπολογιστή) δίνει την δυνατότητα παρακολούθησης της κίνησης του δικτύου μεταξύ εικονικών μηχανών στο κεντρικό υπολογιστή καθώς και την κυκλοφορία μεταξύ των εικονικών μηχανών και κεντρικού υπολογιστή.

- **Στο κανονικό δίκτυο**

Η ανάπτυξη ανίχνευσης εισβολής εδώ επιτρέπει την παρακολούθηση, την ανίχνευση, και την προειδοποίηση για την κυκλοφορία που περνά πάνω από την κανονική υποδομή του δικτύου.

4. ΠΛΑΙΣΙΟ ΑΣΦΑΛΕΙΑΣ COBIT 5

Η ασφάλεια των πληροφοριών είναι απαραίτητη για την καθημερινότητα των οργανισμών, καθώς πρέπει να διασφαλίζει την εμπιστευτικότητα, την διαθεσιμότητα και την ακεραιότητα των πληροφοριών τους. Σε αυτό το κεφάλαιο γίνεται αναφορά σε πλαίσια ασφαλείας, και στα συστήματα διαχείρισης ασφάλειας πληροφοριών. Τέλος γίνεται μια εισαγωγή στο πλαίσιο ασφαλείας COBIT, το οποίο παρέχει καθοδήγηση στους επαγκελματίες της ασφάλειας να κατανοήσουν, να χρησιμοποιήσουν, και να εφαρμόσουν τις άμεσες δραστηριότητες που αφορούν την ασφάλεια σημαντικών πληροφορίων.

4.1 Πλαίσιο ασφαλείας

Στην επιστήμη των υπολογιστών ένα πλαίσιο ασφάλειας(security framework) είναι μια σειρά τεκμηριωμένων διαδικασιών που χρησιμοποιούνται για να καθορίσουν τις πολιτικές και τις διαδικασίες γύρω από την εφαρμογή και την τρέχουσα διαχείριση των ελέγχων ασφαλείας πληροφοριών σε ένα περιβάλλον. Τα πλαίσια είναι βασικά ένα «σχεδιάγραμμα» για την οικοδόμηση ενός προγράμματος ασφάλειας πληροφοριών για να ρυθμιστεί ο κίνδυνος και να μειωθούν οι ευπάθειες. Τα πλαίσια ασφαλείας προσαρμόζονται συχνά για να λύσουν συγκεκριμένα προβλήματα ασφάλειας πληροφοριών. Υπάρχουν πλαίσια που αναπτύχθηκαν για συγκεκριμένους οργανισμούς, η επιλογή για να χρησιμοποιήθει ένα συγκεκριμένο πλαίσιο ασφάλειας μπορεί να οδηγηθεί από πολλαπλούς παράγοντες. Για παράδειγμα το είδος των απαιτήσεων του οργανισμού θα μπορούσε να είναι ενας αποφασιστικός παράγοντας.[19]

4.2 Συστήματα διαχείρισης ασφάλειας πληροφοριών

Τα συστήματα διαχείρισης ασφάλειας πληροφοριών(Information security management systems) είναι ένα σύνολο από πολιτικές που ασχολούνται με τη διαχείριση της ασφάλειας των πληροφοριών. Η βασική αρχή πίσω από ένα ISMS είναι ότι ένας οργανισμός θα πρέπει να σχεδιάσει να εφαρμόσει και να διατηρήσει μια δέσμη πολιτικών, διαδικασιών και συστημάτων για τη διαχείριση των κινδύνων, για τα περιουσιακά στοιχεία εξασφαλίζοντας έτσι τα αποδεκτά επίπεδα των κινδύνων για την ασφάλεια των πληροφοριών.[21]

Όπως συμβαίνει με όλες τις διαδικασίες διαχείρισης, ένα ISMS πρέπει να παραμείνει αποτελεσματικό και αποδοτικό μακροπρόθεσμα, προσαρμόζωντας στις αλλαγές στην εσωτερική οργάνωση και στο εξωτερικό περιβάλλον. Ως εκ τούτου, ενσωματώνεται η "Plan-Do-Check-Act" (PDCA) προσέγγιση: [21]

- Η **Plan** φάση είναι για το σχεδιασμό των ISMS, την αξιολόγηση των κινδύνων για την ασφάλεια των πληροφοριών και την επιλογή των κατάλληλων ελέγχων.
- Η φάση **Do** περιλαμβάνει την υλοποίηση και λειτουργία των ελέγχων.
- Ο στόχος στην **Check** φάση είναι να επανεξετάσει και να αξιολογήσει την απόδοση (αποδοτικότητα και αποτελεσματικότητα) των ISMS.
- Στη φάση της **Act**, γίνονται αλλαγές όπου χρειάζεται για να φέρει τα ISMS πίσω στην μέγιστη απόδοση.

4.3 Γνωστά πλαίσια ασφαλείας

Παρακάτω γίνεται μια σύντομη αναφορά σε μερικά πλαίσια ασφαλείας που υπάρχουν, αλλά και σε τι είδους επιχειρήσεις εφαρμόζονται το καθένα από αυτά, π.χ., κάποια από αυτά είναι για κάθε «μεγέθους» οργανισμό, άλλα για «μεγάλους» μόνο οργανισμούς και άλλα εφαρμόζονται σε οργανισμούς που ασχολούνται με την υγεία, κ.τ.λ. Και τέλος τα χαρακτηριστικά τους και σε ποιούς τομείς στοχεύουν.

- **Octave**

Το OCTAVE(Operationally Critical Threat, Asset, and Vulnerability Evaluation) είναι ένα πλαίσιο ασφάλειας για τον καθορισμό του επιπέδου κινδύνων και τον καθορισμό «αμυνών» εναντίον επιθέσεων. Το πλαίσιο αυτό καθορίζει μία μεθοδολογία που προορίζεται για να βοηθήσει οργανισμούς να ελαχιστοποιήσουν την έκθεση τους σε πιθανές απειλές, να καθορίσουν τις πιθανές επιπτώσεις μίας επίθεσης και να μπορούν να τις αντιμετοπίσουν. Το OCTAVE έχει σχεδιαστεί για να αξιοποιεί την εμπειρία και την τεχνογνωσία των ανθρώπων μέσα στην οργάνωση. Υπάρχουν τρείς διακριτές μεθοδολογίες OCTAVE διαθέσιμες για χρήση:[26]

- OCTAVE METHOD
- OCTAVE-S
- OCTAVE ALLEGRO

- **COSO**

Το πλαίσιο COSO(Committee Of Sponsoring Organisations of the Treadway Commission) είναι ένα πλαίσιο το οποίο ενεργοποιεί μια ολοκληρωμένη διαδικασία εσωτερικού ελέγχου. Βοηθά στην βελτίωση των μέσων ελέγχου στις επιχείρησεις μέσω της αξιολόγησης της αποτελεσματικότητας του εσωτερικού ελέγχου και αποτελείται από πέντε αλληλοσχετιζόμενες συνιστώσες εσωτερικού ελέγχου: [26]

- Περιβάλλον ελέγχου
- Εκτίμηση κινδύνου
- Ελεγτικές δραστηριότητες
- Πληροφορία και εποικηνωνία
- Παρακολούθηση και εποπτεία

- **NIST Cybersecurity**

Το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας(National Institute of Standards and Technology) είναι ένα πλαίσιο ασφαλείας στον κυβερνοχώρο. Το πλαίσιο αυτό παρέχει μια δομή για την οικονομική, την υγειονομική περίθαλψη και άλλων κρίσιμων συστημάτων για την καλύτερη προστασία των πληροφοριών τους και τα περιουσιακά στοιχεία από την επίθεση στον κυβερνοχώρο. Το NIST παρέχει μια κοινή γλώσσα για την αντιμετώπιση και τη διαχείριση του κινδύνου στον κυβερνοχώρο με οικονομικά αποδοτικό τρόπο με βάση τις ανάγκες των επιχειρήσεων, χωρίς να τοποθετήθουν πρόσθετες κανονιστικές απαιτήσεις για τις επιχειρήσεις.[41]

- **ISO/IEC 27002:2013**

Ο Διεθνής Οργανισμός Τυποποίησης(International Organization for Standardization) και της Διεθνούς Ηλεκτροτεχνικής Επιτροπής(International Electrotechnical Commission) παρέχει συστάσεις για βέλτιστες πρακτικές στην διαχείρηση ασφάλειας

πληροφοριών και στα στοιχεία του προγράμματος. Ο ISO καθορίζει την ευρύτερη δομή ενός αποτελεσματικού συνολικού προγράμματος υποστηρίζοντας την ασφάλεια των πληροφοριών ως θέμα τα συστήματα που περιλαμβάνουν την τεχνολογία, την πρακτική, και άνθρωπους, και περιγράφουν την ανάγκη για ένα επίσημο πρόγραμμα ασφαλείας.[41]

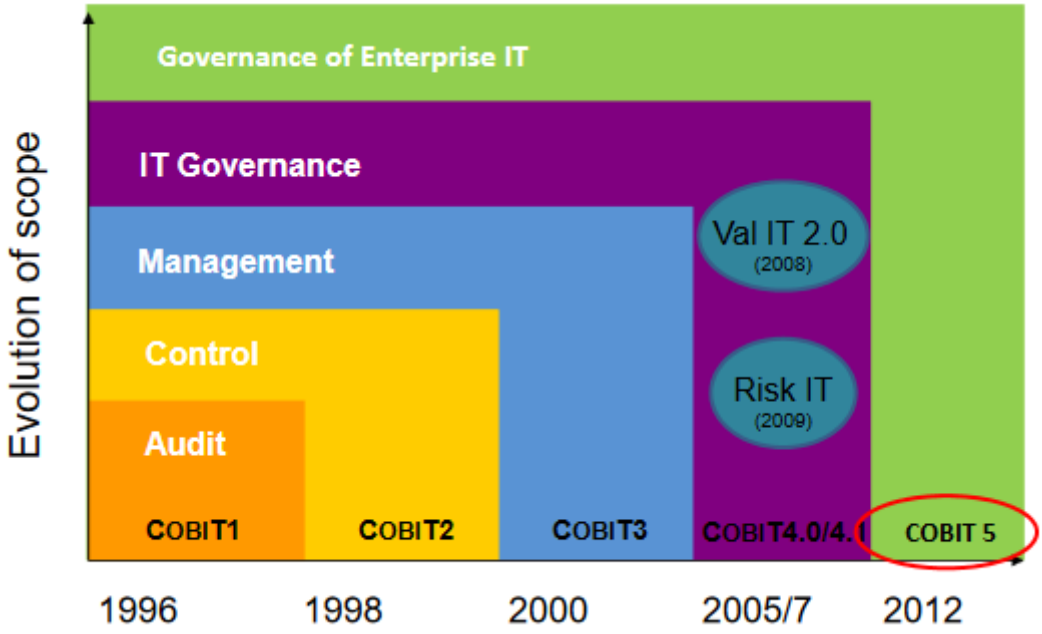
- **HITRUST CSF**

Αναπτύχθηκε σε συνεργασία με τους επαγγελματίες του τομέα της υγείας και της ασφάλειας των πληροφοριών, το κοινό πλαίσιο ασφάλειας(Common Security Framework) είναι το πρώτο πλαίσιο ασφάλειας που αναπτύχθηκε ειδικά για τις πληροφορίες υγείας. Το πρόγραμμα διασφάλισης HITRUST παρέχει απλοποιημένη αξιολόγηση της συμμόρφωσης και την υποβολή εκθέσεων για HIPAA, HITECH και των απαιτήσεων των συνεργατών των επιχειρήσεων. Αξιοποιώντας το HITRUST CSF το πρόγραμμα παρέχει στους οργανισμούς υγειονομικής περίθαλψης και τους συνεργάτες τους με μια κοινή προσέγγιση για τη διαχείριση των αξιολογήσεων ασφαλείας που βελτιώνει την αποτελεσματικότητα και περιέχει δαπάνες που συνδέονται με πολλαπλές και ποικίλες απαιτήσεις διασφάλισης.[41]

4.4 Πλαίσιο ασφαλείας COBIT

Η αρχική έκδοση του COBIT(Control Objectives for Information and Related Technologies) δημοσιεύθηκε το 1996, δημιουργήθηκε για να ερευνήσει, αναπτύξει, δημοσιεύσει και προωθήσει ένα διεθνές σύνολο γενικώς αποδεκτών προτύπων για την τεχνολογία πληροφοριακών συστημάτων. Επικεντρώθηκε σε μεγάλο βαθμό από τον έλεγχο. Η τελευταία έκδοση, που δημοσιεύθηκε το 2012 παρέχει ολοκληρωμένο πλαίσιο εργασιών για την υλοποίηση της εταιρικής διακυβέρνησης, συμπεριλαμβάνοντας επίσης στοιχεία του ITIL και ISO 27001. Το COBIT είναι ένα πλαίσιο που αφορά την αποτελεσματική διακυβέρνηση και τον έλεγχο της πληροφορικής μέσα στην επιχείρηση το οποίο έχει αναπτυχθεί από το Ινστιτούτο Διαχείρισης Πληροφορικής(IT Governance Institute) και το Ινστιτούτο Ελέγχου Συστημάτων Πληροφορικής(ISACA - Information Systems Audit & Control Association). Το πλαίσιο αυτό βασίζεται κατά ένα μέρος στο

πλαίσιο COSO. Παρέχει επίσης ένα κομμάτι συμβουλών σχετικά με τη διαχείριση του επιχειρηματικού κινδύνου. [26]



Εικόνα 4. 1: Εξέλιξη του COBIT[12]

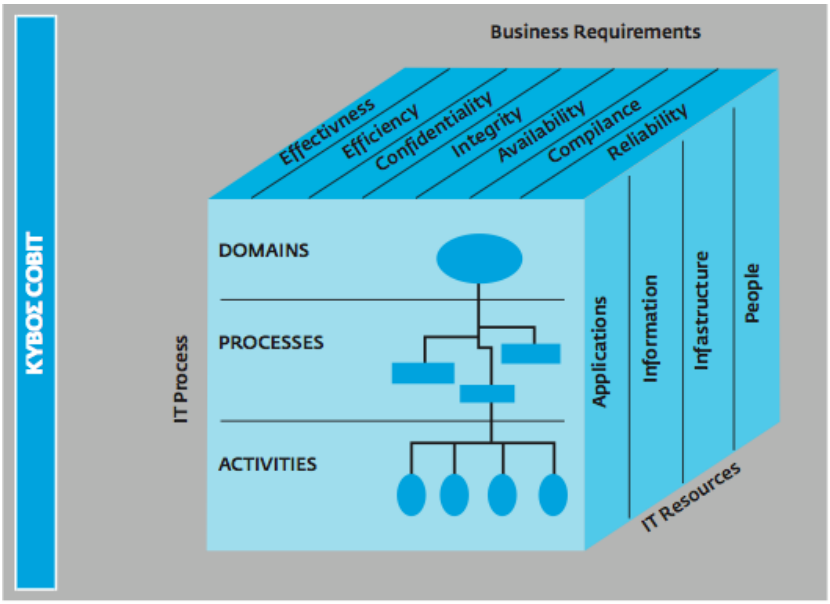
Στα πλαίσια των σημαντικότερων προτύπων που διέπουν στην αξιολόγηση της ασφάλειας των πληροφοριακών συστημάτων, το πλαίσιο COBIT παρέχει ολοκληρωμένο πλαίσιο εργασιών για την υλοποίηση της εταιρικής διακυβέρνησης. Στις μέρες μας η πληροφορία αποτελεί ένα από τα πιο σημαντικά περιουσιακά στοιχεία που μπορεί να έχει ένας οργανισμός, οπότε και η τεχνολογία που την υποστηρίζει παίζει πρωταρχικό ρόλο στην λειτουργία των οργανισμών αυτών. Το COBIT αναγνωρίζει τους σημαντικότερους πληροφοριακούς πόρους που θα πρέπει να διαχειριστούν ετσί ώστε να οριστούν οι διοικητικοί στόχοι των ελεγκτικών μηχανισμών. Άρα, η εξασφάλιση της αποδοτικότητας και της αποτελεσματικότητας του τμήματος πληροφορικής με άξονα τη στρατιγική του οργανισμού αποτελεί παράγοντα επιτυχίας.[26] Το πλαίσιο ελέγχου COBIT συμβάλει στην επιχτυχή ανταπόκριση της τεχνολογίας πληροφοριών επί των επιχειρησιακών απαιτήσεων:[26]

- 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.
- Καθορίζοντας τους στόχους του διοικητικού ελέγχου που θα πρέπει να ληφθούν υπόψη.

Το πλαίσιο COBIT βοηθά διευθυντές, ελεγκτές και χρήστες να καταλάβουν τα πληροφοριακά συστήματα της επιχείρησης τους, ώστε να αποφασίσουν ποιο είναι το κατάλληλο επίπεδο ελέγχου και ασφάλειας για την προστασία του οργανισμού τους. Οι επιχειρήσεις θα πρέπει να ικανοποιούν απαιτήσεις ποιότητας, ασφάλειας και εμπιστοσύνης των πληροφοριών τους. Η διεύθυνση θα πρέπει να ανταποκριθεί στις επιχειρησιακές απαιτήσεις τεχνολογίας πληροφοριών και πρέπει να επενδύει στους πόρους που απαιτούνται για να δημιουργηθεί τεχνική επάρκεια για την υποστήριξη μίας επιχειρησιακής ικανότητας.[26]

4.4.1 Σύνθεση πλαισίου COBIT 5

Το πλαίσιο COBIT έχει σχεδιαστεί από επαγγελματίες, ώστε να καλύπτει τις ανάγκες που προκύπτουν καθώς η τεχνολογία εξελίσσεται. Στην παρακάτω **Εικόνα 4.2** παρουσιάζεται το πλαίσιο με τα επιμέρους πεδία:



Εικόνα 4. 2: Κύβος COBIT[13]

- **Επιχειρησιακές απαιτήσεις(Business requirements)**

Μια διαχείριση με βάση το COBIT παρέχει στην επιχείρηση μια σείρα από αποτελεσματικά μέτρα για τη μέτρηση και τον έλεγχο των δραστηριοτήτων που σχετίζονται με την ανάπτυξη του νέφους ή την χρήση του. Τα επτά κριτήρια πληροφοριών του COBIT:[25]

- **Αποτελεσματικότητα** - Οι πληροφορίες είναι σχετικές και χρήσιμες για την επιχειρηματική διαδικασία και παραδίδονται έγκαιρα, σωστά και με τρόπο συνεπή και χρήσιμο.
- **Αποδοτικότητα** - Οι Πληροφορίες τροφοδοτούνται μέσω βέλτιστης χρήσης των διαθέσιμων πόρων.
- **Εμπιστευτικότητα** - Οι ευαίσθητες πληροφορίες προστατεύονται από μη εξουσιοδοτημένη αποκάλυψη.
- **Ακεραιότητα** - Οι πληροφορίες είναι ακριβείς και πλήρεις.
- **Διαθεσιμότητα** - Οι πληροφορίες είναι διαθέσιμες, όταν απαιτείται και διατηρούνται πάντα με ασφάλεια.

- **Συμμόρφωση** - Η επιχείρηση είναι σε θέση να ελέγχει τη συμμόρφωση με τους ισχύοντες νόμους, κανονισμούς και συμβατικές ρυθμίσεις.
- **Αξιοπιστία** - Ανταποκρίνεται στην πραγματικότητα και επιτρέπει την σωστή λειτουργία του οργανισμού.

- **Πόροι πληροφορικής(IT resources)**

Οι πόροι πληροφορικής, κατατάσσονται σε τέσσερεις κατηγορίες: [25]

- **Εφαρμογές(Applications)** - Είναι αυτοματοποιημένα συστήματα χρηστών και διαδικασίες που επεξεργάζονται πληροφορίες.
- **Πληροφορία(Information)** - Είναι δεδομένα που εισάγονται, επεξεργάζονται, και εξάγονται από τα πληροφοριακά συστήματα.
- **Υποδομή(Infrastructure)** - Περιλαμβάνει την τεχνολογία, τις εγκαταστάσεις (υλικό, δίκτυα και Λ.Σ) που επιτρέπουν την επεξεργασία των εφαρμογών.
- **Άνθρωπος(People)** - Είναι το προσωπικό που απαιτείται για το σχεδιασμό, την οργάνωση, την απόκτηση, την εφαρμογή, την παράδοση, την υποστήριξη, την παρακολούθηση και αξιολόγηση των υπηρεσιών και των πληροφοριακών συστημάτων.

- **Διαδικασίες πληροφορικής(IT process)**

Το COBIT αντιμετωπίζει τους κινδύνους πληροφορικής στη διάρκεια ενός ολόκληρου κύκλου ζωής του προγράμματος. Οι έλεγχοι κατηγοριοποιούνται στους ακόλουθους τέσσερεις τομείς: [25]

- **Σχεδιασμός και οργάνωση(Plan and Organize)** - Παρέχει μια κατεύθυνση προς την παροχή λύσης και την παροχή υπηρεσιών.

  - PO1 Ορίστε ένα στρατηγικό σχέδιο πληροφορικής.
  - PO2 Ορίστε την αρχιτεκτονική της πληροφορίας.
  - PO3 Καθορίστε την τεχνολογική κατεύθυνση.
  - PO4 Ορίστε τις διαδικασίες της πληροφορικής, την οργάνωση και τις σχέσεις.

- PO5 Διαχείριση στην επένδυση της πληροφορικής.
- PO6 Επικοινωνιακών στόχων και κατεύθυνση.
- PO7 Διαχείριση ανθρώπινου δυναμικού πληροφορικής.
- PO8 Διαχείριση ποιότητας.
- PO9 Αξιολόγηση και διαχείριση κινδύνων πληροφορικής.
- P10 Διαχείριση έργων.

- **Προμήθεια και υλοποίηση(Acquire and Implement)** - Παρέχει τις λύσεις και τις περνά για να μετατραπούν σε υπηρεσίες.

  - AI1 Προσδιορίσμος αυτοματοποιημένης λύσης.
  - AI2 Αποκτήση και διατήρηση λογισμικού εφαρμογής.
  - AI3 Απόκτηση και διατήρηση της τεχνολογικής υποδομής.
  - AI4 Ενεργοποίηση λειτουργίας και χρήσης.
  - AI5 Απόκτηση πόρων πληροφορικής.
  - AI6 Διαχείριση αλλαγών.
  - AI7 Εγκατάσταση και διαπίστευση λύσεων και αλλαγών.

- **Παράδοση και υποστήριξη(Deliver and Support)** - Λαμβάνει τις λύσεις, καθιστώντας τες ώστε να μπορούν να χρησιμοποιηθούν για τους τελικούς χρήστες.

  - DS1 Ορίστε και διαχειριστείτε τα επίπεδα εξυπηρέτησης.
  - DS2 Διαχείριση υπηρεσιών από τρίτους.
  - DS3 Διαχειριση της απόδοσης και την ικανότητας.
  - DS4 Διασφάλιση συνεχούς υπηρεσίας.
  - DS5 Εξασφάλιση της ασφάλειας των συστημάτων.
  - DS6 Εντοπισμός και κατανομή των δαπανών.
  - DS7 Μόρφωση και εκπαίδευση χρηστών.
  - DS8 Διαχείριση γραφείου εξυπηρέτησης και συμβάντων.
  - DS9 Διαχείριση ρυθμίσεων.

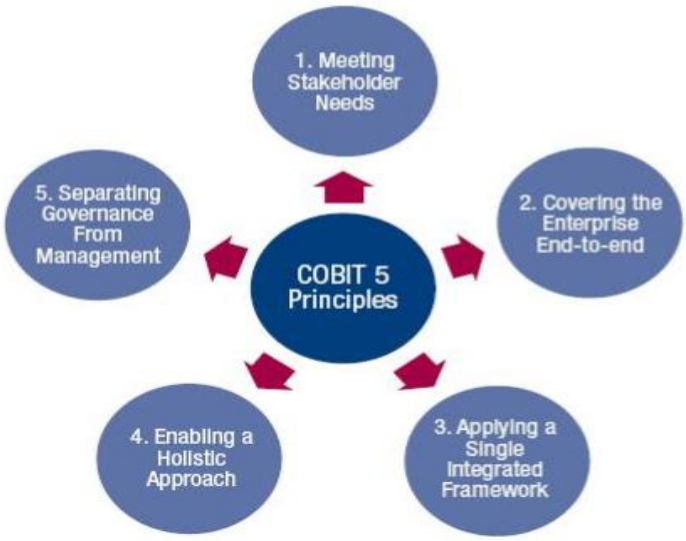
- ❖ DS10 Διαχείριση προβλημάτων.
- ❖ DS11 Διαχείριση δεδομένων.
- ❖ DS12 Διαχειριση φυσικού περιβάλλοντος.
- ❖ DS13 Διαχείριση λειτουργιών.

- ➢ **Παρακολούθηση και αξιολόγηση(Monitor and Evaluate)** - Παρακολούθηση όλων των διαδικασιών για να εξασφαλιστεί ότι η κατέφθυνση που παρέχεται ακολουθείται.

  - ❖ ME1 Παρακολούθηση και αξιολόγηση απόδοσης πληροφορικής.
  - ❖ ME2 Παρακολούθηση και αξιολόγηση του εσωτερικού ελέγχου.
  - ❖ ME3 Διασφάλιση της συμμόρφωσης με τις εξωτερικές απαιτήσεις.
  - ❖ ME4 Παρέχει διακυβέρνηση πληροφορικής.

4.4.2 Αρχές του COBIT 5

Το COBIT 5 έχει εξελιχθεί από έναν αριθμό πλαισίων και καθοδηγιών καθόλη την διάρκεια της εξέλιξης και της υιοθέτησης του από έναν μεγάλο αριθμό εταιρειών, και διαφόρων οργανισμών έγινε εμφανές ότι η χρήση των αρχών του πλαισίου μπορεί εύκολα να κατανοηθεί επιτρέπωντας στους οργανισμούς να δημιουργήσουν αξία. Αυτή η ιδέα επεκτάθηκε και στο COBIT 5, επίσης αναγνωρίζοντας τα ValIT & RiskIT πλαίσια είναι βασισμένα σε αρχές και είναι η καρδιά του COBIT 5. Είναι αξιοσημείωτο ότι και άλλα πλαίσια όπως το ITL, TOGAF, ARCHIMATE προάγουν την χρήση αρχών.[31]



Εικόνα 4. 3: Αρχές COBIT [14]

- **Ικανοποίηση αναγκών των ενδιαφερόμενων**

Οι οργανισμοί έχουν πολλούς ενδιαφερόμενους και κάθε ένας από αυτούς έχει μια δική του άποψη για το τι είναι σημαντικό. Παρόλα αυτά όλοι συμφωνούν ότι ο οργανισμός πρέπει να δημιουργήσει αξία. Αυτή η αξία μπορεί να είναι παροχή δημοσίων υπηρεσιών, κέρδος παραγωγής, φιλανθρωπικές υπηρεσίες, κ.α. Οι ανάγκες των ενδιαφερόμενων θα πρέπει να ληφθούν υπόψην όταν λαμβάνονται αποφάσεις όσο αναφορά τους πόρους, την υλοποίηση οφελών και την αξιολόγηση κινδύνου κατά την δημιουργία αξίας. Για να μας βοηθήσει να καταλάβουμε τις ανάγκες των ενδιαφερόμενων, το COBIT 5 κάνει τρία ερωτήματα, ποιος εποφελείται; ποιος παίρνει το ρίσκο; και τι πόροι χρειάζονται;Μερικές φορές υπάρχουν αντικρουόμενες ανάγκες μεταξύ των ενδιαφερόμενων και ότι οι οργανισμοί έχουν διαφορετικούς παράγωντες οργάνωσης. Επειδή κάθε οργανισμός έχει διαφορετικούς στόχους, θα πρέπει να τροποποιηθεί κατάλληλα το COBIT 5 μέσα από μια αλληλουχία στόχων. Μεταφράζοντας τους επιχειρησιακούς στόχους σε στόχους πληροφορικής και ευθυγραμμίζοντας τους σε συγκεκριμένες διαδικασίες και πρακτικές. Αυτό μας βοηθάει να ικανοποιήσουμε τις ανάγκες των ενδιαφερόμενων.[35]

- **Κάλυψη της επιχείρησης**

Η έκταση του COBIT 5 περιλαμβάνει όλες τις πληροφορίες και την σχετική τεχνολογία στον οργανισμό. Αυτό διευθυνσιοδοτήτε από την διακυβέρνηση και την διαχείριση όλης της πληροφορίας στον οργανισμό και σημαίνει κυρίως ότι το COBIT 5 ενσωματώνει την διακυβέρνηση της πληροφορικής στην διακυβέρνηση του οργανισμού. Και δεύτερον ότι όλες οι λειτουργίες και οι διαδικασίες για την διακυβέρνηση και την διαχείριση της πληροφορικής περιλαμβάνονται επίσης. Με αυτό εννοούμε κάλυψη της επιχείρησης. Η όπως το αποκαλεί το COBIT 5 προσέγγιση διακυβέρνησης. Η ενσωμάτωση της διακυβέρνησης της πληροφορικής στην διακυβέρνηση του οργανισμού επιτρέπει στο COBIT να συνδιάσει και τους δύο τύπους διακυβέρνησης και την ίδια στιγμή να λάβει υπόψη τις τελευταίες εξελίξεις. Το COBIT 5 περιλαμβάνει όλες τις εσωτερικές και εξωτερικές υπηρεσίες πληροφορικής καθώς και τις επιχειρησιακές διαδικασίες. Αυτή η προσέγγιση αποτελείται από τέσσερα στοιχεία δημιουργίας αξίας, από το διακυβερνητικό στόχο, από προϋπόθέσεις, από έκταση και το τελευταίο στοιχείο που αποτελείται από ρόλους, δραστηριότητες και σχέσεις. Είναι σημαντικό να αναφέρουμε ότι το COBIT 5 καλύπτει όλες τις λειτουργίες και τις διαδικασίες σε όλο τον οργάνισμο, και όχι μόνο στις λειτουργίες της πληροφορικής. Το COBIT χειρίζεται την πληροφορία και την τεχνολογία σαν περιουσιακά στοιχεία.[36]

- **Εφαρμογή ενιαίου ολοκληρωμένου πλαισίου**

Οι οργανισμοί έχουν μια αυξημένη προκλητική δοκιμασία της διαχείρισης και της διακυβέρνησης της πληροφορίας και της τεχνολογίας, αυτό επειδή υπάρχουν συνεχείς αλλαγές στην τεχνολογία και επίσης πίεση από πελάτες, προμηθευτές και πιο σημαντικά από ρυθμιστές και νομοθέτες. Καθιστώντας την αίσθηση όλων αυτών των διαδικασιών, απαιτείται ένα πλαίσιο που είναι προσαρμόσιμο στον οργανισμό. Το COBIT 5 είναι ικανό για τους εξής λόγους, πρώτων λαμβάνει υπόψη τα τελευταία πρότυπα και πλαίσια που το θέτει σαν μια υπερδομή που μπορεί να ευθυγραμμίσει τις διαχειρηστικές και διακυβερνητικές δραστηριότητες. Δεύτερον ως βάση για την ενσωμάτωση άλλων πλαισίων, προτύπων και πρακτικών, το COBIT 5 είναι μια ενιαία ολοκληρωμένη πηγή καθοδήγησης. Τρίτον το COBIT 5 παρέχει ένα βασικό και απλό πλαίσιο για την καθοδήγηση και υποστήριξη συνόλου του προϊόντος. Τέλος το COBIT 5

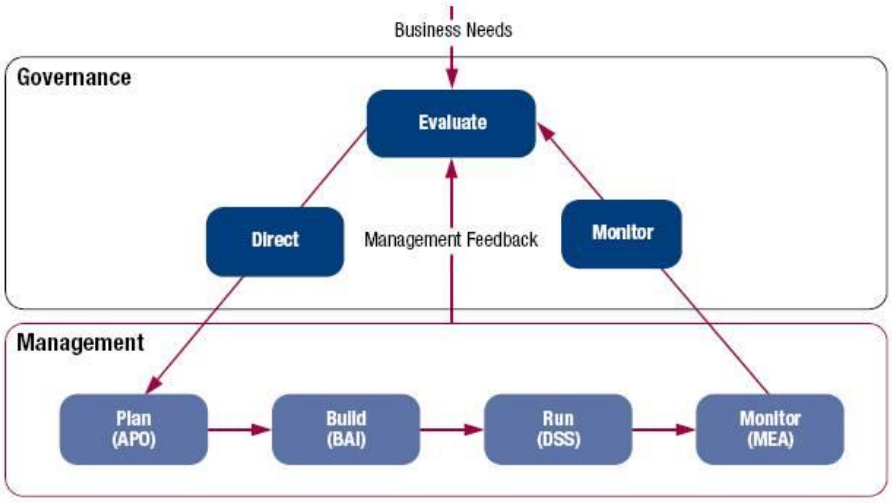
παρέχει μια ολοκληρωμένη πηγή αναφοράς της καθοδήγησης της τεχνολογίας και πληροφορίας και καλές πρακτικές διαχείρισης.[37]

- **Ολιστική προσέγγιση**

Απαιτεί να θέτουμε μια αποδοτική και αποτελεσματική διακυβέρνηση και διαχείριση της πληροφορικής σε όλη την επιχείρηση. Έτσι όταν παίρνουμε αποφάσεις είναι σημαντικό να έχουμε όσες περισσότερες πληροφορίες διεθέσιμες σε εμάς το οποίο σημαίνει ότι πρέπει να έχουμε ολοκληρωμένη εικόνα του οργανισμού. Στην περίπτωση μας, συγκεκριμένα των διακυβερνητικών και διαχειρησιακών διαδικασιών και δομών, το COBIT 5 παρέχει προϋποθέσεις οι οποίες είναι παράγοντες που επηρεάζουν τις διακυβερνητικές και διαχειρησιακές δραστηριότητες. Στην πραγματικότητα αυτές οι προϋποθέσεις μπορούν να παρθούν ξεχωριστά ή συλογικά για να μας βοηθήσουν να κατανοήσουμε μια προσέγγιση συμμόρφωσης στην διακυβέρνηση και διαχείριση της πληροφορικής στην επιχείρηση. Οι προϋποθέσεις είναι εφαρμόσιμες σε όλο τον οργανισμό και περιλαμβάνουν όλους τους πόρους, εσωτερικούς και εξωτερικούς που σχετίζονται με την διακυβέρνηση και διαχείριση της πληροφορίας και της σχετικής τεχνολογίας. Αξίζει να πούμε ότι οι προϋποθέσεις περιλαμβάνουν δραστηριότητες και ευθύνες των λειτουργιών της πληροφορικής και όχι μόνο.[38]

- **Διαχωρισμός διακυβέρνησης και διαχείρισης**

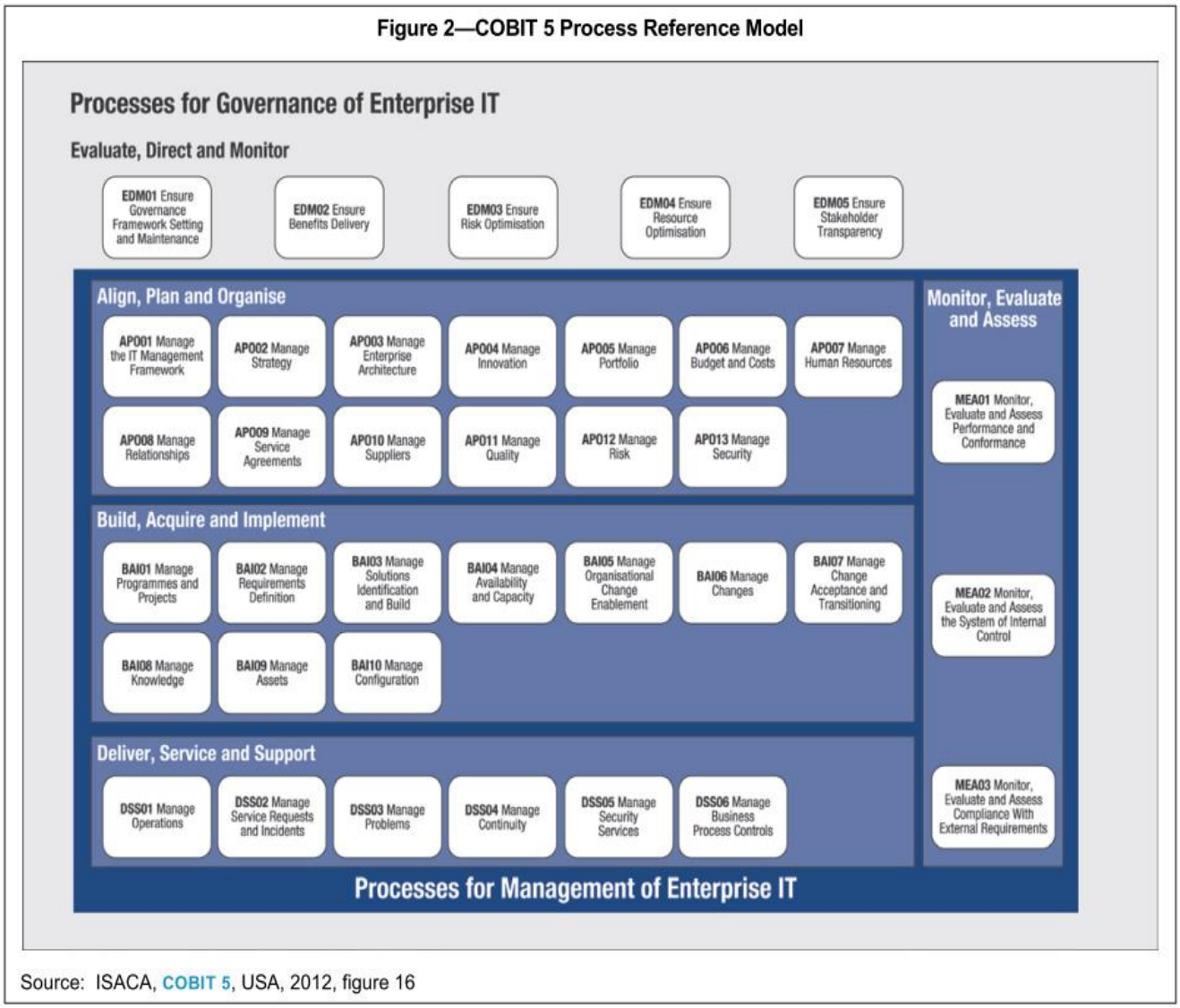
Μερικές φορές η διαφορά ανάμεσα στην διακυβέρνηση και την διαχείριση δεν είναι τόσο ξεκάθαρη όσο θα έπρεπε. Το COBIT 5 την αποσαφηνίζει αναζνωρίζοντας τους διαφορετικούς σκοπούς, ευθύνες, τύπους δραστηριοτήτων, οργανωτικές δομές υποστήριξης. Εν συντομία το COBIT 5 χρησιμοποιεί τα εξής μνημονικά, EDM(Evaluate Direct Monitor) για την διακυβέρνηση και PBRM(Plan Build Run Monitor) για την διαχείριση.[39]



Εικόνα 4. 4: Διαχωρισμός Διακυβέρνησης – Διαχείρισης [14]

Το EDM είναι για να διαβεβαιώσει ότι οι ανάγκες των ενδιαφερόμενων είναι για να εντοπίσουν και να συμφωνήσουν με τους στόχους που πρέπει να επιτευχθούν. Οδηγίες, μέσω ιεράρχησης και λήψης αποφάσεων. Και ελέγχος για τις επιδόσεις και τη συμμόρφωση προς τους στόχους. [39]

Το PBRM είναι για να διασφάλισει ότι οι δραστηριότητες που αναλαμβάνονται και επιβλέπονται, είναι σε ευθυγράμμιση με την κατεύθυνση που έχει χαραχθεί από την διακυβέρνηση. Το COBIT 5 περιλαμβάνει ένα μοντέλο αναφοράς διαδικασίας το οποίο διαιρεί τις διεργασίες της διακυβέρνησης και διαχείρισης σε δύο κύριες περιοχές EDM & PBRM το οποίο αναγνωρίζει μια σειρά από 37 διαδικασίες σε όλη την διαχείριση και διακυβέρνηση.[39]

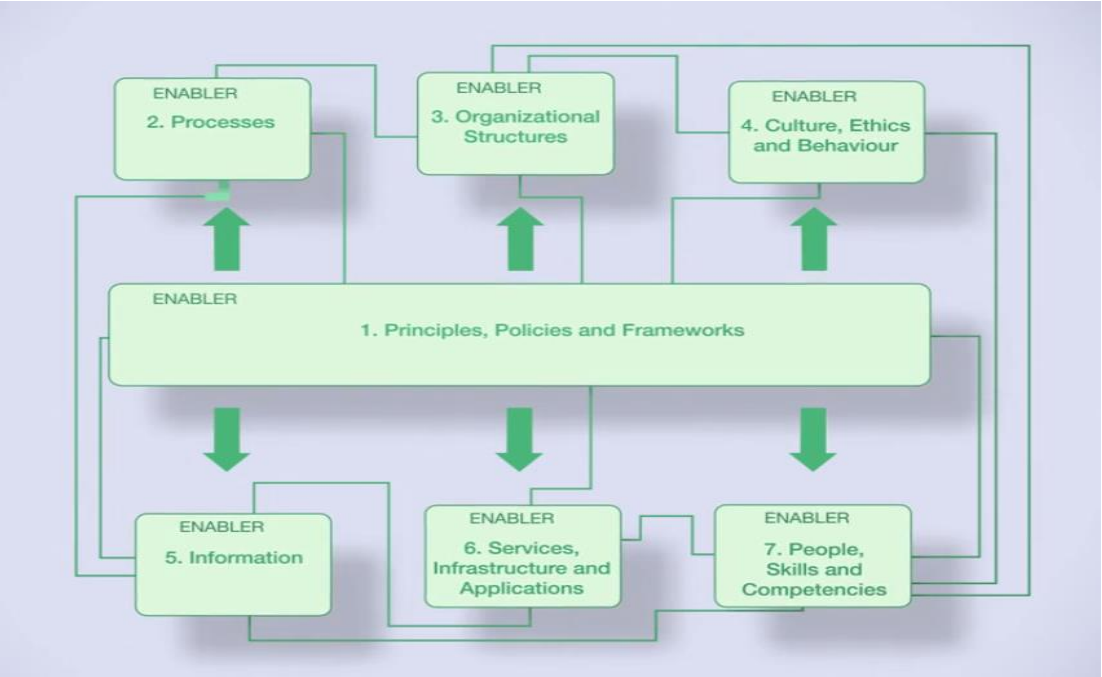


Εικόνα 4. 5: Μοντέλο αναφοράς COBIT[14]

Το COBIT 5 αναγνωρίζει ότι οι επιχειρήσεις είναι διαφορετικές σε «μέγεθος»,δομές και πολυπλοκότητα γιαυτό και οι επιχειρήσεις οργανώνουν τις διαδικασίες ανάλογα με τις ανάγκες τους.

4.4.3 Επιχειρησιακοί παράγωντες

Οι προϋποθέσεις είναι παράγωντες που ο καθένας ξεχωριστά ή μαζί επηρεάζουν την διαχείριση & διακυβέρνηση της επιχείρησης:[33]



Εικόνα 4. 6: Επιχειρησιακοί Παράγωντες [14]

1)**Principles, Policies and Frameworks(Αρχές, Πολιτικές, Πλαίσια):**Μεταφράζουν τις επιθυμητές συμπεριφορές σε πρακτική καθοδήγηση.

2)**Processes(Διαδικασίες):**Περιγράφουν πρακτικές και δραστηριότητες για να επιτευχθούν συγκεκριμένοι στόχοι. Επίσης προάγουν ένα σύνολο παραγωγής για να υποστηρίζουν τα επιτεύγματα των στόχων πληροφορικής.

3)**Organizational Structures(Οργανωτικές Δομές):**Είναι οι βασικοί φορείς λήψης αποφάσεων σε μια επιχείρηση.

4)**Culture, Ethics and Behavior(Κουλτούρα, Ηθική, Συμπεριφορά):**Των ιδιωτών και των επιχειρήσεων, είναι ένας υποτιμημένος παράγωντας επιτυχίας στις διαχειρηστικές & διακυβερνητικές δραστηριότητες.

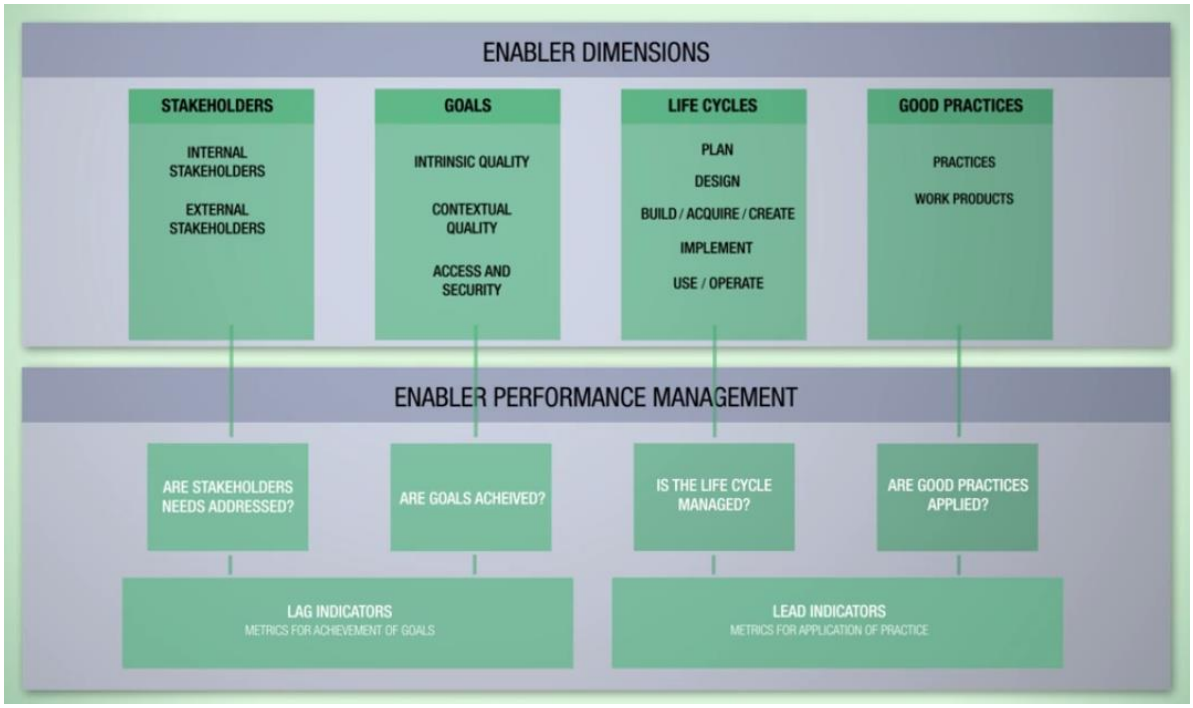
5)**Information(Πληροφορία):**Η οποία είναι διάχυτη σε όλες τις εταιρείες και περιλαμβάνει όλη την πληροφορία που παράγεται και χρησιμοποιείται από την επιχείρηση. Απαιτείται για να κρατήσει την επιχείρηση σε λειτουργία και με σωστή

διακυβέρνηση καθώς σε επιχειρηματικό επίπεδο η πληροφορία είναι το κλειδί της επιχειρήσης.

6)**Services Infrastructure Applications(Ηπηρεσίες Εφαρμογών Υποδομής):** Παρέχουν στην επιχείρηση τεχνολογία επεξεργασίας πληροφοριών και υπηρεσίες.

7)**People, skills and Competencies(Άνθρωποι, Ικανότητες, Αρμοδιότητες):** Ευθυγραμμίζονται με ανθρώπους που απαιτούνται για την επιτυχή ολοκλήρωση όλων των δραστηριοτήτων, παρέχουν σωστές αποφάσεις για την λήψη διορθωτικών μέτρων.

Κάθε προϋποθέση χρειάζεται την είσοδο μιας άλλης για να είναι πλήρης αποτελεσματική.[33] Οι επτά προϋποθέσεις του COBIT 5 περιγράφονται από μια δομή που μας βοηθάει να κατανοήσουμε τις προϋποθέσεις στην πράξη. Η κάθε δομή αποτελείται από δύο περιοχές οι οποίες περιγράφονται στην παρακάτω **Εικόνα 4.7**.[34]



Εικόνα 4. 7: Δομή προϋποθέσεων [14]

- **Διαστάσεις Προϋποθέσεων (Enabler Dimensions)** - Αποτελείται από τέσσερα μέρη. Καθένα από αυτά τα τέσσερα μέρη μπορεί να βρεθεί σε κάθε μια ξεχωριστά από τις επτά προϋποθέσεις:[34]

- **Stakeholders(Ενδιαφερόμενοι)**

Είναι άτομα που παίζουν ενεργό ρόλο σε μια προϋπόθεση, επεξεργάζοντας τις δικές τους ανάγκες ή επιθυμίες που κάποιες φορές ίσως να διαφέρουν, υπάρχουν δύο τύποι ενδιαφερόμενων στην επιχειρηση:

- Εξωτερικοί.
- Εσωτερικοί.

- **Goals(Στόχοι)**

Ένα πλήθος στόχων μπορεί να βρεθεί σε μια προϋπόθεση, αν επιτευχθούν τότε παράγουν αξία. Υπάρχουν τρείς κατηγορίες στόχων:

- Ουσιαστικής ποιότητας.
- Συνναφής ποιότητας (αποτελεσματικότητα, ενδιαφέρον).
- Προσβασιμότητας και Ασφάλειας.

- **Life Cycle(Κύκλος ζωής)**

Κάθε προϋπόθεση έχει ένα κύκλο ζωής και έχει της εξής φάσεις:

- Πλάνο.
- Σχέδιο.
- «Κτίσημο»/Απόκτηση/ Δημιουργία.
- Εφαρμογή.
- Χρήση/Λειτουργία.

- **Good Practices(Καλές Πρακτικές)**

Παρέχουν παραδείγματα/προτάσεις για την υλοποίηση των πορυποθέσεων:

- Πρακτικές διαδικασίες, δραστηριότητες, λεπτομερείς δραστηριότητες.
- Προϊόντα εργασίας.

- **Διαχείριση απόδοσης της προϋπόθεσης(Enabler Performance Management)** -

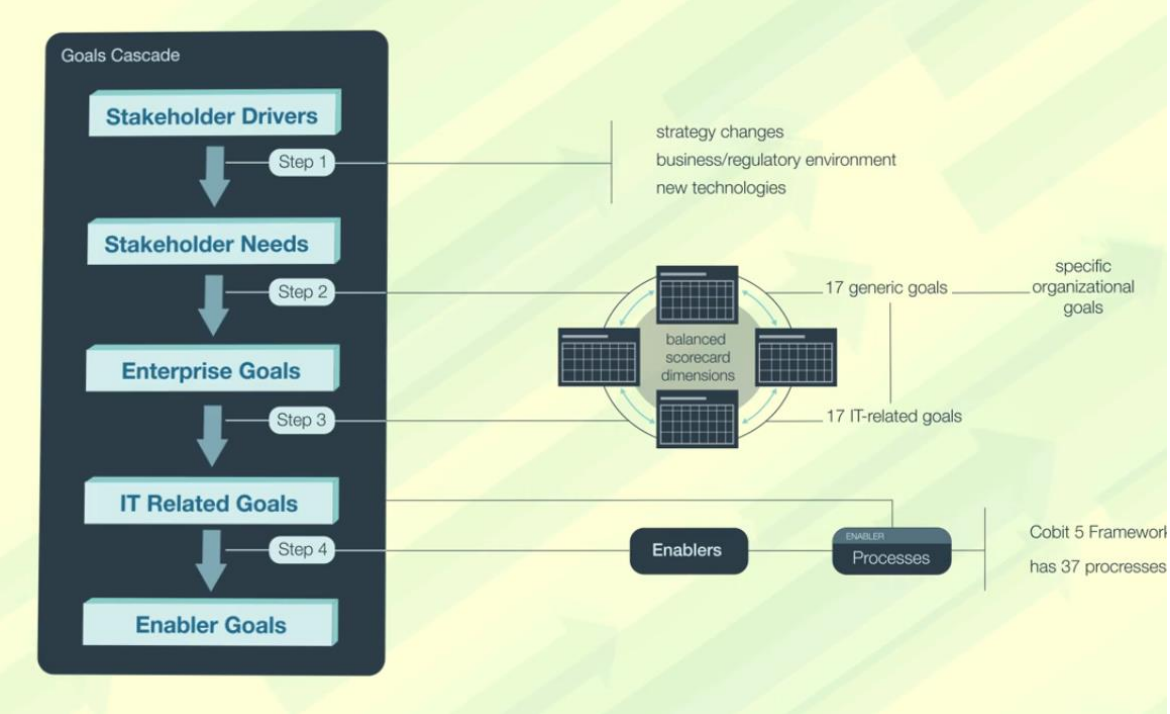
Ο παραπάνω κανόνας επίσης εφαρμόζεται και σε αυτό το πεδίο. Υποστηρίζει την πρακτική χρήση των προϋποθέσεων καθώς και τα θετικά αποτελέσματα από τις εφαρμογές, αυτό γίνεται κάνοντας τέσσερεις ερωτήσεις: [34]

- Μετρήσεις για την επίτευξη των στόχων
  - Έχουν διευθυνσιοδοτηθεί οι ανάγκες των ενδιαφερόμενων;
  - Έχουν επιτευχθεί οι στόχοι των προϋποθέσεων;

- Μετρήσεις για την εφαρμογή της πρακτικής
  - Είναι διαχειρήσιμος ο κύκλος ζωής;
  - Έχουν εφαρμοστεί οι καλές πρακτικές;

4.4.4 Αλληλουχία στόχων

Οι προϋποθέσεις οδηγούνται από μια αλληλουχία στόχων(goals cascade) και καθορίζουν ποιες προϋποθέσεις πρέπει να επιτευχθούν. Η αλληλουχία στόχων είναι μια σημαντική έννοια στο COBIT 5 καθώς μεταφράζει τις ανάγκες των ενδιαφερόμενων σε στρατηγικές. Είναι μηχανισμός που αρχικά σε πρώτο στάδιο μεταφράζει τις ανάγκες σε στόχους επιχειρήσεων, στόχους πληροφορικής, και στόχους προϋποθέσεων. Είναι κατ'ουσίαν μια Top-Down προσέγγιση. Με τον τρόπο αυτό, περνάμε μέσα από μια διαδικασία που μας επιρέπει να χρησιμοποιήσουμε το COBIT 5 αποτελεσματικά. Έτσι ο καθορισμός των αναγκών σε στόχους θέτει μια ευθυγράμμιση μεταξύ των αναγκών της επιχείρησης και τις λύσεις και υπηρεσίες της πληροφορικής και μπορεί να εφαρμοστεί σε διάφορα επίπεδα, η αλληλουχία στόχων περιλαμβάνει τέσσερα βήματα:[32]



Εικόνα 4. 8: Αλληλουχία στόχων [14]

- **Βήμα 1**

Οι ανάγκες των ενδιαφερόμενων επηρεάζονται από έναν αριθμό οδηγών, π.χ., στρατηγικές αλλαγές, το επιχειρησιακό/κανονηστικό περιβάλλον και από νέες τεχνολογίες.

- **Βήμα 2**

Οι ανάγκες των ενδιαφερόμενων είναι σε αλληλουχία με τους στόχους της επιχείρησης. Η αλληλουχία στόχων του COBIT 5 τους οργανώνει σε ένα στρατηγικό πλανό με 4 τομείς με 17 γενικούς στόχους που μπορούν εύκολα να ευθυγραμμιστούν σε συγκεκριμένους επιχειρησιακούς στόχους.

- **Βήμα 3**

Οι στόχοι της επιχείρησης είναι σε αλληλουχία με τους στόχους της πληροφορικής. Μερικές φορές οι στόχοι της επιχείρησης επιτυγχάνονται μόνο όταν συμβαδίζουν με τους στόχους της πληροφορικής. Στην αλληλουχία στόχων καθένας από τους 17

γενικούς στόχους ευθυγραμμίζεται με 17 στόχους πληροφορικής που επίσης οργανώνονται σε ένα στρατηγικό πλανό με 4 τομείς.

- **Βήμα 4**

Οι στόχοι πληροφορικής είναι σε αλληλουχία με τους στόχους των προϋποθέσεων. Για να επιτευχθούν οι στόχοι της πληροφορικής ένας αριθμός από προϋποθέσεις πρέπει να εφαρμοστεί επιτυχώς μια από αυτές τις προϋποθέσεις είναι ομοίως, όπως και στα προηγούμενα βήματα στην αλληλουχία στόχων, κάθε στόχος πληροφορικής ευθυγραμμίζεται με μια ή παραπάνω διαδικασίες. Το COBIT 5 διαθέτει 37 διαδικασίες.

Πίνακας 4. 1: COBIT 5 Επιχειρησιακοί στόχοι [23]

BSC Διάσταση	**Επιχειρησιακοί Στόχοι**
Χρηματοοικονομικά	1.Αξία από επιχειρησιακές επενδύσεις.
	2.Χαρτοφυλάκιο ανταγωνιστικών προϊόντων και υπηρεσιών.
	3.Διαχείριση επιχειρηματικών κινδύνων (διαφύλαξη των περιουσιακών στοιχείων).
	4.Συμμόρφωση με εξωτερικούς νόμους και κανονισμούς.
	5.Οικονομική διαφάνεια.
Πελατιακές σχέσεις	6.Πελατοκεντρική φιλοσοφία παροχής υπηρεσιών.
	7.Συνέχεια και διαθεσιμότητα επιχειρησιακών υπηρεσιών.
	8.Γρήγορες αποκρίσεις σε ένα μεταβαλλόμενο επιχειρηματικό περιβάλλον.
	9.Πληροφορίες που βασίζονται σε στρατηγική λήψη αποφάσεων.
	10.Βελτιστοποίηση του κόστους παροχής υπηρεσιών.
Εσωτερικές σχέσεις	11.Βελτιστοποίηση της λειτουργικότητας των επιχειρηματικών διαδικασιών.
	12.Βελτιστοποίηση του κόστους των επιχειρηματικών διαδικασιών.
	13.Διαχείριση επιχειρησιακών προγραμμάτων αλλαγής.

	14.Παραγωγικότητα επιχείρησης και προσωπικού.
	15. Συμμόρφωση με τις εσωτερικές πολιτικές.
Μαθησιακά και αναπτυξιακά	16.Άνθρωποι με ικανότητες και κίνητρα.
	17.Προϊόν και επιχειρηματική καινοτομία πολιτισμού.

Πίνακας 4. 2: COBIT 5 Στόχοι πληροφορικής [23]

IT BSC Διάσταση	**Στόχοι πληροφορικής και σχετικής τεχνολογίας**	
Χρηματοοικονομικά	1	Ευθυγράμμιση της πληροφορικής και της επιχειρηματικής στρατηγικής.
	2	Συμμόρφωση πληροφορικής και υποστήριξη για την επιχειρησιακή συμμόρφωση με εξωτερικούς νόμους και κανονισμούς.
	3	Δέσμευση της εκτελεστικής διαχείρισης για την πραγματοποίηση αποφάσεων που σχετίζονται με την πληροφορική.
	4	Διαχείριση επιχειρησιακών κινδύνων που σχετίζονται με την πληροφορική.
	5	Ολοκληρωμένα οφέλη από τις επενδύσεις στην πληροφορική και των υπηρεσιών χαρτοφυλακίου.
	6	Διαφάνεια των δαπανών πληροφορικής, των οφελών, και των κινδύνων.
Πελατιακές σχέσεις	7	Παράδοση των υπηρεσιών πληροφορικής σύμφωνα με τις απαιτήσεις των επιχειρήσεων.
	8	Κατάλληλη χρήση των εφαρμογών, των πληροφοριών, και των τεχνολογικών λύσεων.
Εσωτερικές σχέσεις	9	Ευελιξία πληροφορικής.
	10	Ασφάλεια πληροφοριών, επεξεργασίας υποδομής, και

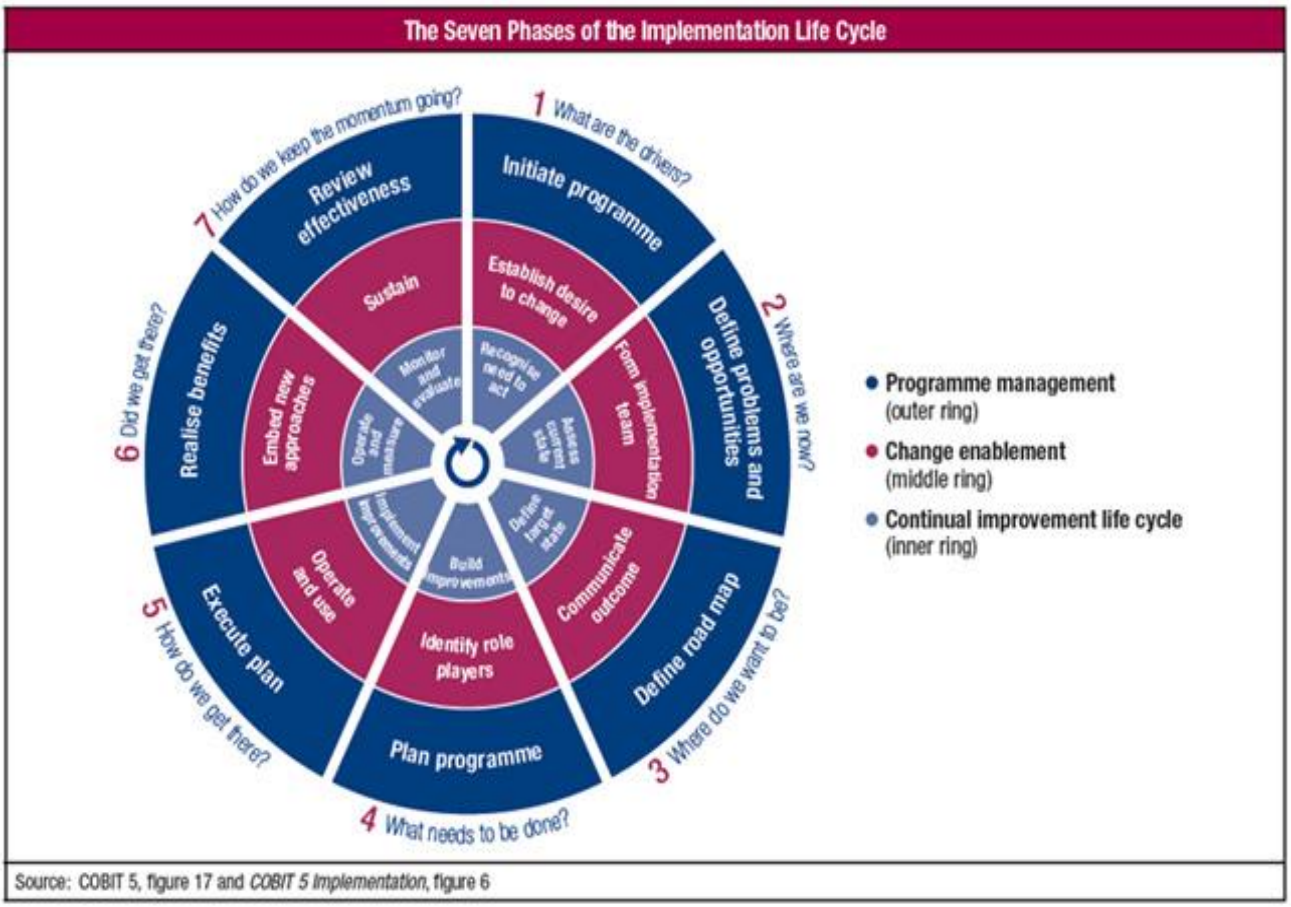
		εφαρμογών.
	11	Βελτιστοποίηση των περιουσιακών στοιχείων πληροφορικής, των πόρων, και των δυνατοτήτων.
	12	Ενεργοποίηση και υποστήριξη των επιχειρησιακών διαδικασιών με την ενσωμάτωση εφαρμογών και της τεχνολογίας στις επιχειρηματικές διαδικασίες.
	13	Παράδοση των προγραμμάτων που αποφέρουν οφέλη, στην ώρα, στον προϋπολογισμό και των απαιτήσεων και των πρότυπων ποιότητας που πληρούν.
	14	Διαθεσιμότητα αξιόπιστων και χρήσιμων πληροφοριών για τη λήψη αποφάσεων.
	15	Συμμόρφωση πληροφορικής με τις εσωτερικές πολιτικές.
Μαθησιακά και αναπτυξιακά	16	Επαρκή, και επιχειρηματικό κίνητρο και προσωπικό πληροφορικής.
	17	Γνώση, εμπειρία, και πρωτοβουλίες για την επιχειρηματική καινοτομία.

4.4.5 Φάσεις υλοποίησης κύκλου ζωής

Βέλτιστη αξία μπορεί να πραγματοποιηθεί από την χρήση του COBIT μόνο αν εφαρμοστεί αποτελεσματικά ώστε να ταιριάζει στο μοναδικό περιβάλλον της κάθε επιχείρησης. Κάθε προσέγγιση εφαρμογής θα πρέπει να αντιμετοπίσει προκλήσεις. Η εφαρμογή του COBIT βασίζεται σε μια συνεχή βελτίωση του κύκλου ζωής. Σημαντικά θέματα που αφορούν την εφαρμογή του COBIT είναι τα παρακάτω:[28]

- Κάνοντας ένα επιχειρησιακό σενάριο για την εφαρμογή και τη βελτίωση της διακυβέρνησης και της διαχείρισης της πληροφορικής.
- Αναγνωρίζοντας γεγονότα που έχουν τεθεί εις ενέργεια και ανάγκες/προβλήματα.
- Δημιουργία κατάλληλου περιβάλλοντος για την εφαρμογή.
- Αξιοποίοντας το COBIT για να εντοπίσει τα κενά και να κατευθύνει την ανάπτυξη των προϋποθέσεων, όπως πολιτικές, διαδικασίες, αρχές, οργανωτικές δομές, και τους ρόλους και τις ευθύνες.

Το COBIT προωθεί μια προσέγγιση κύκλου ζωής που παρέχει έναν τρόπο για τις επιχειρήσεις να χρησιμοποιούν το COBIT για να αντιμετωπίσουν την πολυπλοκότητα και τις προκλήσεις που συνήθως συναντώνται κατά τη διάρκεια των εφαρμογών. Οι τρείς αλληλένδετες συνιστώσες του κύκλου ζωής αποτελούν: τον πυρήνα συνεχούς βελτίωσης του κύκλου ζωής, την ενεργοποίηση αλλαγής, και τη διαχείριση του προγράμματος. Εκτός αυτού, υπάρχουν επτά φάσεις υλοποίησης του COBIT που δημιουργήθηκαν για να εξασφαλίστει η επιτυχής εφαρμογή του.[28]



Εικόνα 4. 9: Επτά φάσεις υλοποίησης του κύκλου ζωής [15]

Φάσεις υλοποίησης κύκλου ζωής:

- **Φάση 1**

Η φάση αυτή ξεκινά με την αναγνώριση και την συμφωνία με την ανάγκη για μια εφαρμογή. Προσδιορίζει τα τρέχουσα σημεία αιχμής, και θέτει εις ενέργεια και δημιουργεί μια επιθυμία να αλλάξει σε εκτελεστικό επίπεδο διαχείρισης.

- **Φάση 2**

Η φάση αυτή επικεντρώνεται στον καθορισμό του πεδίου εφαρμογής χρησιμοποιώντας τον «χάρτη» του COBIT των επιχειρησιακών στόχων σε αντίστοιχους στόχους πληροφορικής που σχετίζονται με τις διαδικασίες της πληροφορικής, και λαμβάνοντας υπόψη το πώς σενάρια κινδύνου θα μπορούσαν να αναδείξουν τις βασικές διαδικασίες στις οποίες θα επικεντρωθεί.

- **Φάση 3**

Σε αυτή τη φάση, ο στόχος βελτίωσης που έχει οριστεί, ακολουθείται από μια πιο λεπτομερή ανάλυση χρησιμοποιώντας την καθοδήγηση COBIT να εντοπίσει τα κενά και τις πιθανές λύσεις.

- **Φάση 4**

Αυτή η φάση, σχεδιάζει πρακτικές λύσεις με τον καθορισμό των σχεδίων που υποστηρίζονται από δικαιολογημένες περιπτώσεις επιχειρήσεων.Επίσης ένα σχέδιο αλλαγής για την υλοποίηση έχει αναπτυχθεί.

- **Φάση 5**

Οι προτεινόμενες λύσεις εφαρμόζονται σε καθημερινές πρακτικές σε αυτή τη φάση. Μέτρα μπορούν να οριστούν και να καθορίζονται με βάση τους στόχους και μετρήσεις του COBIT για να εξασφαλίσει ότι η ευθυγράμμιση της επιχειρήσης επιτυγχάνεται και διατηρείται, και η απόδοση μπορεί να μετρηθεί.

- **Φάση 6**

Η φάση αυτή επικεντρώνεται στη βιώσιμη λειτουργία των νέων ή βελτιωμένων προϋποθέσεων και την παρακολούθηση της επίτευξης των αναμενόμενων οφελών.

- **Φάση 7**

Σε αυτή τη φάση, η συνολική επιτυχία της πρωτοβουλίας αναθεωρείται, περαιτέρω απαιτήσεις για τη διακυβέρνηση ή τη διαχείριση της επιχείρησης προσδιορίζονται, και η ανάγκη για συνεχή βελτίωση ενισχύεται.

Με την πάροδο του χρόνου, ο κύκλος ζωής θα πρέπει να ακολουθείται επαναληπτικά καθώς δημιουργείται μια βιώσιμη προσέγγιση για τη διακυβέρνηση και την διαχείριση της επιχείρησης της πληροφορικής.[28]

4.4.5 Μοντέλο ικανότητας διαδικασίας

Αυτά τα μοντέλα χρησιμοποιούνται για την μέτρηση της τρέχουσας ωριμότητας των διεργασιών πληροφορικής μιας εταιρείας για να καθορίσουν ένα απαιτούμενο επίπεδο ωριμότητας, και να προσδιορίσουν το χάσμα μεταξύ τους, αλλά και πως μπορεί να βελτιωθεί η διαδικασία για να επιτευχθεί το επιθυμητό επίπεδο ωριμότητας. Το COBIT 5 περιλαμβάνει ένα μοντέλο ικανότητας διαδικασίας που βασίζεται στο διεθνώς αναγνωρισμένο πρότυπο ISO/IEC 15504. Αυτό θα αποτελέσει ένα μέσο για την μέτρηση της απόδοσης οποιασδήποτε από τις διεργασίες διακυβέρνησης και διαχείρισης.

Υπάρχουν 6 επίπεδα ικανότητας που μια διαδικασία μπορεί να επιτύχει συμπεριλαμβάνοντας την “ατελής διαδικασία”, εάν οι πρακτικές σε αυτήν δεν επιτυγχάνουν τον επιδιωκόμενο σκοπό της διαδικασίας:[40]

- **0 Ελλιπής διαδικασία** – Η διαδικασία δεν έχει υλοποιηθεί ή αποτυγχάνει να πετύχει τον σκοπό της. Σε αυτό το επίπεδο, υπάρχει ελάχιστη ή καμιά απόδειξη οποιασδήποτε συστηματικής επίτευξης του σκοπού της διαδικασίας.
- **1 Διαδικασία εκτελείται** (1 χαρακτηριστικό) – Η διαδικασία που έχει εφαρμοστεί επιτυγχάνει τον σκοπό της.

- **2 Διαχείριση της διαδικασίας** (2 χαρακτηριστικά) – Η προηγούμενη διαδικασία σε εκτέλεση που περιγράφηκε, εφαρμόζεται πλέον σε ένα διαχειριζόμενο τρόπο διαμόρφωσης.
- **3 Καθιερωμένη διαδικασία** (2 χαρακτηριστικά) - Η προηγούμενη διαχείριση της διαδικασίας που περιγράφηκε, τώρα εφαρμόζεται χρησιμοποιώντας μια καθορισμένη διαδικασία που είναι ικανή να επιτύχει τα αποτελέσματα της διαδικασίας της.
- **4 Προβλέψιμη διαδικασία** (2 χαρακτηριστικά) - Η προηγούμενη καθιερωμένη διαδικασία που περιγράφηκε, τώρα λειτουργεί μέσα σε καθορισμένα όρια για την επίτευξη των αποτελεσμάτων της διαδικασίας.
- **5 Βελτιστοποίηση διαδικασίας** (2 χαρακτηριστικά) - Η προηγούμενη προβλέψιμη διαδικασια που περιγράφηκε, βελτιώνεται συνεχώς για να ανταποκρίνεται στους σχετικούς και προβλεπόμενους επιχειρηματικούς στόχους.

Κάθε επίπεδο ικανότητας μπορεί να επιτευχθεί μόνο όταν το προηγούμενο επίπεδο έχει επιτευχθεί πλήρως. Υπάρχει μια σημαντική διάκριση μεταξύ του επιπέδου 1 ικανότητας διαδικασίας και τα υψηλότερα επίπεδα ικανότητας. Για την επίτευξη του επιπέδου 1 ικανότητας της διαδικασίας απαιτείται το χαρακτηριστικό απόδοσης να έχει επιτευχθεί σε μεγάλο βαθμό. Κάτι το οποίο σημαίνει ότι η διαδικασία αυτή πραγματοποιείται με επιτυχία και τα απαιτούμενα αποτελέσματα συλλέγονται από την εταιρεία.[40]

Επανεξετάζωντας τα αποτελέσματα μιας διαδικασίας όπως αυτά είχαν περιγραφεί για κάθε διαδικασία στις αναλυτικές περιγραφές της διαδικασίας, και χρησιμοποιώντας την κλίμακα διαβάθμισης του ISO/IEC 15504 για να καθορίσουμε σε τι βαθμό κάθε στόχος έχει επιτευχθεί. Αυτή η κλίμακα αποτελείται από τις ακόλουθες βαθμίδες: [40]

- **N** (Δεν έχει επιτευχθεί) - Υπάρχει μικρή ή καμιά απόδειξη της επίτευξης του καθορισμένου χαρακτηριστικού στην αξιολογημένη διαδικασία. (0% έως 15% επίτευγμα).
- **P** (Εν μέρει έχει επιτευχθεί) - Υπάρχουν κάποιες ενδείξεις μιας προσέγγισης, και κάποια επίτευξη, του καθορισμένου χαρακτηριστικού στην αξιολογημένη

διαδικασία. Μερικές πτυχές της επίτευξης του χαρακτηριστικού μπορεί να είναι μη αναμενόμενες. (15% έως 50% επίτευγμα).

- **L** (Σε μεγάλο βαθμό έχει επιτευχθεί) – Υπάρχουν στοιχεία μιας συστηματικής προσέγγισης και σημαντικού επιτεύγματος του καθορισμένου χαρακτηριστικού στην αξιολογημένη διαδικασία. Μερικές αδυναμίες που σχετίζονται με αυτό το χαρακτηριστικό μπορεί να υπάρχουν στην αξιολογημένη διαδικασία. (50% έως 85% επίτευγμα).
- **F** (Έχει πλήρως επιτευχθεί) - Υπάρχουν ενδείξεις για μια ολοκληρωμένη και συστηματική προσέγγιση, και την πλήρη επίτευξη, του καθορισμένου χαρακτηριστικού στην αξιολογημένη διαδικασία. Δεν υπάρχουν σημαντικές αδυναμίες που να σχετίζονται σε αυτό το χαρακτηριστικό στην αξιολογημένη διαδικασία. (85% έως 100% επίτευγμα).

5. ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ ΠΑΡΟΧΟΥ - ΕΤΑΙΡΕΙΑΣ

Στο παρόν κεφάλαιο αναπτύσσεται ένα σενάριο χρήσης όπου περιλαμβάνει μια εικονική εταιρεία με την ονομασία Z-Corp η οποία έχει ανατεθεί σε ένα πάροχο νέφους. Αναλύονται όλα τα τεχνικά χαρακτηριστικά του παρόχου, πιθανές ευπάθειες, απαιτήσεις της εταιρείας από τον πάροχο νέφους καθώς και ευπάθειες της εταιρείας, και τέλος γίνεται διαχείριση κινδύνου και εφαρμογή βέλτιστων πρακτικών βάση του μοντέλου αναφοράς διαδικασίας και χρήση των υπολοίπων προϋποθέσεων του πλαισίου COBIT 5 που χρησιμοποιεί η εταιρεία ώστε να αντιμετοπισθούν οι κίνδυνοι.

5.1 Πάροχος νέφους Amazon Web Services

Η AWS είναι μια ασφαλής πλατφόρμα υπηρεσιών νέφους που προσφέρει υπηρεσίες και λειτουργίες που βοηθούν τις επιχειρήσεις να αναπτυχθούν και να κλιμακωθούν.Η AWS είναι θηγατρική της Amazon που πραγματοποιήθηκε τον Ιούλιο του 2002, και προσφέρει μια σειρά από υπηρεσίες cloud computing. Αυτές οι υπηρεσίες λειτουργούν από 14 γεωγραφικές περιοχές σε όλο τον κόσμο. Περιλαμβάνουν την υπηρεσία Amazon Elastic Compute Cloud γνωστή ως “EC2” και την Amazon Simple Storage Service επίσης γνωστή ως "S3" ως την πρώτη πραγματική υπηρεσία cloud computing τον Μάρτιο του 2006. Από το 2016 η AWS έχει περισσότερες από 70 υπηρεσίες, που καλύπτουν ένα ευρύ φάσμα, συμπεριλαμβανομένου της υπολογιστικής ισχύς, αποθήκευσης, δικτύωσης, ανάπτυξης, βάσεων δεδομένων, αναλύσεων, υπηρεσιών εφαρμογής και εργαλεία για internet of things.[24] Η επιχείρηση θα χρησιμοποιήσει τις εξής υπηρεσίες:

- Υπηρεσία Amazon EC2, η οποία παρέχει μια ευρεία επιλογή τύπων εικονικών μηχανών, βελτιστοποιημένες για κάθε περίπτωση χρήσης. Οι εικονικές μηχανές περιλαμβάνουν διάφορους συνδιασμούς μνήμης, αποθήκευσης, CPU και δικτύωσης. Για το δικό μας σενάριο, όπου έχουμε μια εταιρεία η οποία προσφέρει εφαρμογές μέσω διαδικτύου, για την διαχείριση των οικονομικών των επιχείρησεων, χρησιμοποιούμε τις F1 τύπου εικονικές μηχανές γιατί είναι βελτιστοποιημένες στο να κάνουν οικονομικές αναλύσεις & αναζήτηση μεγάλου όγκου δεδομένων και ανάλυση.[47]

- Υπηρεσία Amazon simpleDB που μετρά την χρήση της εικονικής μηχανής σε κάθε αίτημα, και χρεώνει βάση στην ποσότητα που χρησιμοποιείται για να ολοκληρωθεί το αίτημα.[46]
- Υπηρεσία Identity and Access Management(I.A.M) επιτρέπει τον ασφαλή έλεγχο πρόσβασης στις υπηρεσίες της AWS και στους πόρους για τους χρήστες.Χρησιμοποιώντας την υπηρεσία I.A.M, μπορείς να δημιουργήσεις και να διαχειριστείς τους χρήστες της υπηρεσίας ή μια ομάδα χρηστών και να χρησιμοποιήσεις δικαιώματα για να επιτρέψεις ή να απαγορέυσεις την πρόσβαση στους πόρους της υπηρεσίας.[54]
- Υπηρεσία Amazon Simple Storage Service(S3) για την αποθήκευση δεδομένων με μια απλή διεπαφή υπηρεσίας διαδικτύου για την αποθήκευση και ανάκτηση οποιουδήποτε όγκου δεδομένων.[4]
- Και τέλος την υπηρεσία DNS system(Route 53) που είναι μια υψηλής διαθεσιμότητας και επεκτασιμότητας υπηρεσία DNS. Είναι σχεδιασμένη για να δώσει στους προγραμματιστές και τις επιχειρήσεις ένα εξαιρετικά αξιόπιστο και οικονομικά αποδοτικό τρόπο μεταφράζοντας ονόματα σε αριθμητικές διευθύνσεις IP, που χρησιμοποιούν οι υπολογιστές για να συνδεθούν μεταξύ τους.[48]

5.1.1 Τιμολόγηση υπηρεσιών παρόχου νέφους

Η τιμολόγηση της χρήσης των υπηρεσιών EC2, S3, DNS system(Route 53), και SimpleDB ποικίλει ανάλογα των περιφερειών και εξαρτώνται από την τοποθεσία του παρόχου της αντίστοιχης περιφέρειας. Η τιμολόγηση της υπηρεσίας S3 φαίνεται στον **Πίνακα 5.2**. Αντίστοιχα της υπηρεσία SimpleDB στον **Πίνακα 5.3** και της DNS system(Route 53) στον **Πίνακα 5.4**.

Όσο αναφορά την υπηρεσία EC2, η amazon παρέχει πολλούς τρόπους πληρωμής, ένας από αυτούς είναι η τιμολόγηση κατ’ απαίτηση. Επιτρέπει να πληρώνεις την υπολογιστική ισχύ με την ώρα. Στον **Πίνακα 5.1** αναφέρονται τα χαρακτηριστικά των F1 τύπου εικονικών μηχανών.[23] [4]

Πίνακας 5. 1: Τιμολόγηση EC2 US East (N.Virginia) [17]

Model	vCPU	FPGAs	ECU	Μνήμη (GiB)	Instance Storage (GB)	Τιμολόγηση
f1.2xlarge	8	1	26	122	480 SSD	Επικοινωνία με πάροχο
f1.16xlarge	64	8	104	976	4 x 960 SSD	Επικοινωνία με πάροχο

Πίνακας 5. 2: Τιμολόγηση S3 US East (N.Virginia) [18]

	Πρότυπο Κόστος Αποθήκευσης	Κόστος Αποθήκευσης Εφεδρείας (Χρησιμοποίουμενης)	Αποθήκευση Εφεδρείας (Παγωμένης)
Πρώτα 50 TB / Μήνα	$0.023 ανά GB	$0.0125 ανά GB	$0.004 ανά GB
Επόμενα 450 TB / Μήνα	$0.022 ανά GB	$0.0125 ανά GB	$0.004 ανά GB
Πάνω από 500 TB / Μήνα	$0.021 ανά GB	$0.0125 ανά GB	$0.004 ανά GB

Πίνακας 5. 3: Τιμολόγηση SimpleDB US East (N.Virginia) [24]

Μεταφορά δεδομένων ΕΚΤΟΣ**	Τιμολόγηση
Πρώτο 1 GB / Μήνα	$0.000 ανά GB
Μέχρι και 10 TB / Μήνα	$0.090 ανά GB
Επόμενα 40 TB / Μήνα	$0.085 ανά GB
Επόμενα 100 TB / Μήνα	$0.070 ανά GB
Επόμενα 350 TB / Μήνα	$0.050 ανά GB
>350 TB / Μήνα	Επικοινωνία με πάροχο

Πίνακας 5. 4: Τιμολόγηση DNS (Route53) US East (N.Virginia) [25]

Φιλοξενούμενες Ζώνες
$0.50 ανά φιλοξενούμενη ζώνη / μήνα για τις πρώτες 25 φιλοξενούμενες ζώνες
$0.10 ανά φιλοξενούμενη ζώνη / μήνα για τις επόμενες φιλοξενούμενες ζώνες

5.1.2 Τεχνικά χαρακτηριστικά παρόχου νέφους

Ο πάροχος AWS παρέχει τα εξής τεχνικά χαρακτηριστικά:[20]

- Δίνει την δυνατότητα δημιουργίας & διαγραφής εικονικής μηχανής ή ενός εικονικού εξυπηρετητή ή χιλιάδων εικονικών εξυπηρετητών σε ένα κέντρο δεδομένων.
- Στην κάθε εικονική μηχανή ο χρήστης ή η επιχείρηση μπορεί να επιλέξει τις ρυθμίσεις ασφαλείας και τις ρυθμίσεις δικτύωσης.
- Δίνει την δυνατότητα αυτόματης κλιμάκωσης των εικονικών μηχανών προς τα πάνω ή προς τα κάτω σε περίπτωση που ο χρήστης έχει αναγκή για περισσότερους ή λιγότερους πόρους ανάλογα την περίπτωση.
- Κάθε εικονική μηχανή αποτελείται από επεξεργαστική ισχύ, μνήμη, αποθηκευτικό χώρο και ικανότητα δικτύωσης.
- Υπάρχουν αρχεία για την δημιουργία εικονικών μηχανών με λειτουργικά συστήματα όπως Windows, Solaris και Linux καθώς μπορεί να περιέχουν προ - εγκατεστημένα πακέτα λογισμικού.
- Ο χρήστης έχει την δυνατότητα να επιλέξει πρωτόκολλα, πύλες (ports) και IP χρηστών που θα μπορούν να έχουν πρόσβαση στις εικονικές μηχανές χρησιμοποιώντας ομάδες ασφαλείας.
- Μέσω ενός χαρακτηριστικού ασφαλείας «κλειδί» γίνεται η πρόσβαση στις εικονικές μηχανές αφού δημιουργηθούν.
- Η επικοινωνία γίνεται μέσω εφαρμογής management console, οι χρήστες μπορούν εύκολα να κάνουν όποιες ρυθμίσεις/αλλαγές επιθυμούν.
- Μέσω DNS γίνεται η πρόσβαση στο σύστημα.

5.1.3 Ευπάθειες & Κίνδυνοι παρόχου νέφους

Ένας πάροχος δημοσίου νέφους ο οποίος προσφέρει υπηρεσίες IaaS σε μια επιχείρηση πιθανόν να αντιμετοπίζει τις εξής ευπάθειες και κινδύνους:

- **Κακόβουλοι χρήστες**

Η απειλή ενός κακόβουλου χρήστη εκ των έσω είναι γνωστή στους περισσότερους οργανισμούς. Αυτή η απειλή ενισχύεται για τους καταναλωτές των υπηρεσιών νέφους,

από τη σύγκλιση των υπηρεσιών πληροφορικής, και των πελατών στο πλαίσιο ενός ενιαίου τομέα διαχείρισης.[25]

- **Επιθέσεις στο Hypervisor**

Τα hypervisors είναι ζωτικής σημασίας για την εικονοποίηση στο νέφος. Παρέχουν την σύνδεση μεταξύ VMs και των υποκείμενων φυσικών πόρων που απαιτούνται για τη λειτουργία των μηχανών, χρησιμοποιώντας hypercalls. Ένας εισβολέας χρησιμοποιώντας ένα VM στο ίδιο νέφος θα μπορούσε να προσποιηθεί hypercalls για να εισάγει κακόβουλο κώδικα ή να προκαλέσει σφάλματα στο hypervisor. Αυτό θα μπορούσε πιθανόν να χρησιμοποιηθεί για την παραβίαση της εμπιστευτικότητας και της ακεραιότητας των άλλων VMs ή την συντριβή του hypervisor (δηλαδή επίθεση DDOS).[11]

- **Μη ενημερωμένη ασφάλεια στις VMs**

Μια μη ενεργή VM μπορεί εύκολα να παραβιαστεί, και σημαντικές εκδόσεις ασφαλείας μπορεί να μην έχουν εφαρμοστεί. Αυτή η μη ενημερωμένη VM μπορεί εύκολα να γίνει υποχείριο ενός κακόβουλου χρήστη όταν ενεργοποιηθεί.[11]

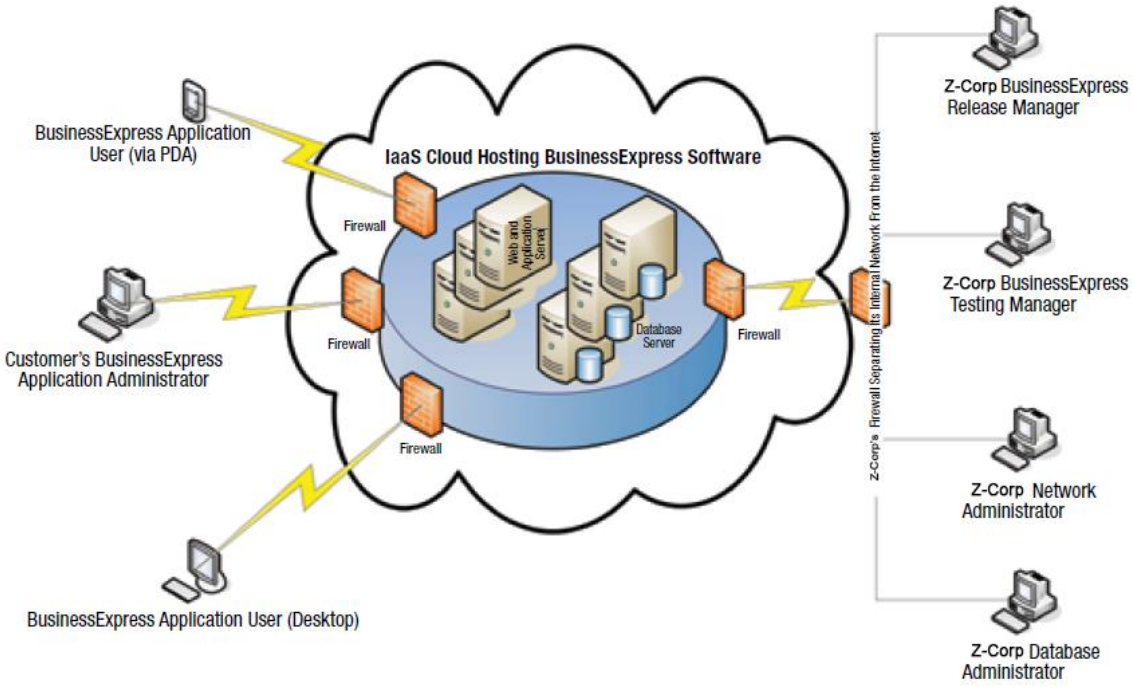
- **Multi-tenancy visibility**

Εξαιτίας της φύσης του multi-tenancy, μερικά στοιχεία όπως(πίνακες δρομολόγησης, MAC διευθύνσεις, εσωτερικές διευθύνσεις IP, κυκλοφορία LAN) μπορεί να είναι ορατά σε άλλες οντότητες μέσα στο νέφος. Κακόβουλοι χρήστες στο νέφος μπορεί να επωφεληθούν από αυτές τις πληροφορίες. Π.χ., αξιοποιώντας πίνακες δρομολόγησης για να χαρτογραφήσουν την εσωτερική τοπολογία του δικτύου μιας εταιρείας προετοιμάζοντας τον «δρόμο» για μια εσωτερική επίθεση.[11]

5.2 Εταιρεία Z-Corp

Για τις ανάγκες συγγραφής αυτού του κεφαλαίου της εργασίας επινοήθηκε μια εικονική εταιρεία παρόμοια με την εταιρεία Workday με την ονομασία Z-Corp, η οποία είναι μια νέα εταιρεία που προσφέρει επιχειρηματικές εφαρμογές μέσω διαδικτύου για την διαχείριση των οικονομικών, των ανθρωπίνων πόρων, και τις λειτουργίες και σχέσεις μεταξύ πελατών μιας επιχείρησης, με την ονομασία BusinessExpress.Είναι μια

εφαρμογή Enterprise Resource Planning(ERP) όπου ενσωματώνει όλες τις παραπάνω λειτουργίες και διαδικασίες που είναι απαραίτητες για την αποτελεσματική λειτουργία μιας επιχείρησης σε ένα ολοκληρωμένο σύστημα. Η εταιρεία Z-Corp προσφέρει το λογισμικό BusinessExpress σαν μια λύση SaaS. Η απαίτηση για SaaS λύσεις αναμένεται να αυξηθεί ραγδαία. Με την υπηρεσία SaaS οι πελάτες θα απολαμβάνουν όλα τα πλεονεκτήματα των λύσεων του νέφους.[30]



Εικόνα 5. 1: Παράδειγμα ενός IaaS CSP για το λογισμικό BusinessExpress το οποίο προσφέρεται σαν SaaS λύση [21]

Η βασική ικανότητα της εταιρείας είναι να εκτελεί ανάπτυξη λογισμικού, και όχι να παρέχει λύσεις φιλοξενίας. Οι CSP's που προσφέρουν υπηρεσίες IaaS παρέχουν λύσεις φιλοξενίας. Αξιοποιώντας έναν IaaS CSP για παροχή φιλοξενίας επέτρεψε στην εταιρεία να παραμείνει στις βασικές ικανότητες της. Υπάρχουν πολλά άλλα οφέλη από τη χρήση ενός IaaS CSP, όπως: [30]

- Η ικανότητα να προσφέρει το λογισμικό σαν λύση σε μια ποικιλία από πλατφόρμες, όπως Windows, Unix, Linux.
- Ταχεία επεκτασιμότητα.
- Διαθεσιμότητα των πόρων.

- Δυνατότητες Pay-as-you-go.

Οι πελάτες, συνεργάτες, και εργαζόμενοι χρησιμοποιούν την διαδικτυακή εφαρμογή για να συνεργαστούν ο ένας με τον άλλον χρησιμοποιόντας μια διαδικτυακή επαφή που μπορεί να προβληθεί σε οποιοδήποτε περιηγητή. Τα κίνητρα της εταιρείας για την μετάβαση στο νέφος είναι τα εξής: [30]

- Η εταιρεία επιθυμεί να αναπτύξει την διαδικτυακή εφαρμογή, και να αντιμετοπίσει την αυξανόμενη επισκεψημότητα, χωρίς να επενδύσει σε νέο εξοπλισμό υλικού.
- Να χρησιμοποιεί τις αποθηκευτικές μονάδες του νέφους για τη δημιουργία αντιγράφων ασφαλείας.
- Να χρησιμοποιεί εφαρμογές στο νέφος (SaaS) για ορισμένες λειτουργίες της επιχείρησης (E-mail, ημερολόγιο κ.τ.λ.).
- Να χρησιμοποιεί βάσεις δεδομένων του νέφους ως μέρος της επεξεργασίας των εφαρμογών.
- Να χρησιμοποιεί VM για να φέρει επιπλέον επεξεργαστές σε απευθείας σύνδεση, για να χειριστεί φορτία αιχμής. Και φυσικά την απενεργοποίηση των VM όταν πλέον δεν χρειάζονται.

5.2.1 Απαιτήσεις από τον πάροχο νέφους

Οι βασικές απαιτήσεις για την περίπτωση χρήσης της επιχείρησης στο νέφος, είναι οι παρακάτω: [50]

- **Ταυτότητα**

Η υπηρεσία νέφους πρέπει να κάνει έλεγχο ταυτότητας στον τελικό χρήστη.

- **Open Client**

Η πρόσβαση στην υπηρεσία νέφους δεν θα πρέπει να απαιτεί μια συγκεκριμένη πλατφόρμα ή τεχνολογία.

- **Ενιαία ταυτότητα**

Εκτός από τη βασική ταυτότητα που απαιτείται από τον τελικό χρήστη, ο χρήστης της επιχείρησης είναι πιθανό να έχει μια ταυτότητα με την επιχείρηση. Το ιδανικό είναι ότι ο

χρήστης της επιχείρησης διαχειρίζεται μια ενιαία ταυτότητα, με μια υποδομή συνένωσης άλλων ταυτότητων που ενδέχεται να απαιτούνται από τις υπηρεσίες νέφους.

- **Επίγνωση της τοποθεσίας**

Ανάλογα με το είδος των δεδομένων που η επιχείρηση διαχειρίζεται για λογαριασμό του χρήστη, θα μπορούσαν να υπάρχουν νομικοί περιορισμοί σχετικά με τη θέση του φυσικού server, όπου αποθηκεύονται τα δεδομένα. Παρά το γεγονός ότι αυτό παραβιάζει τα ιδεώδει του υπολογιστικού νέφους, ο χρήστης δεν θα πρέπει να γνωρίζει τις λεπτομέρειες της φυσικής υποδομής, η απαίτηση αυτή είναι απαραίτητη. Πολλές εφαρμογές δεν μπορούν να μετακινηθούν στο νέφος μέχρι οι πάροχοι του νέφους να παρέχουν ένα API για τον προσδιορισμό της θέσης του φυσικού υλικού που παρέχει η υπηρεσία νέφους.

- **Μέτρηση και παρακολούθηση**

Όλες οι υπηρεσίες του νέφους θα πρέπει να μετρώνται και να παρακολουθούνται για τον έλεγχο του κόστους.

- **Διαχείριση και Διακυβέρνηση**

Δημόσιοι πάροχοι νέφους κάνουν να είναι πολύ εύκολο να ανοίξει ένας λογαριασμός και να αρχίσει να χρησιμοποιεί τις υπηρεσίες του νέφους, αυτή η ευκολία στη χρήση, δημιουργεί τον κίνδυνο ότι άτομα σε μια επιχείρηση θα χρησιμοποιούν τις υπηρεσίες νέφους με δική τους πρωτοβουλία. Η διαχείριση των VMs και των υπηρεσιών όπως η αποθήκευση, οι βάσεις δεδομένων, και ουρές μηνυμάτων είναι απαραίτητη για να παρακολουθείτε ποιες υπηρεσίες χρησιμοποιούνται. Η διακυβέρνηση είναι ζωτικής σημασίας για να εξασφαλιστεί ότι οι πολιτικές και οι κανονισμοί της διακυβέρνησης ακολουθούνται, όπου χρησιμοποιείται το υπολογιστικό νέφος.

- **Ασφάλεια**

Κάθε περίπτωση χρήσης που αφορά μια επιχείρηση θα έχει πιο εξελιγμένες απαιτήσεις ασφαλείας από κάποια που αφορά ένα μόνο τελικό χρήστη.

- **Κοινό αρχείο δημιουργίας για τις VM**

Μια VM που δημιουργήθηκε για την πλατφόρμα ενός παρόχου νέφους πρέπει να είναι φορητή σε πλατφόρμα άλλου παρόχου. Οποιαδήποτε λύση στην απαίτηση αυτή

πρέπει να ληφθεί υπόψη για διαφορές στους τρόπους που οι πάροχοι νέφους αποδίδουν αποθήκευση σε VM.

- **Κοινά APIs για την αποθήκευση στο νέφος και middleware**

Οι περιπτώσεις χρήσης των επιχειρήσεων απαιτούν κοινό API για την πρόσβαση σε υπηρεσίες αποθήκευσης στο σύννεφο, βάσεις δεδομένων του νέφους, και άλλες middleware υπηρεσίες νέφους όπως ουρές μηνυμάτων. Γράφοντας προσαρμοσμένο κώδικα που λειτουργεί μόνο για συγκεκριμένη υπηρεσία ενός προμηθευτή νέφους, κλειδώνει την επιχείρηση στο σύστημα αυτού του ενός προμηθευτή και εξαλείφει κάποια από τα οικονομικά οφέλη και την ευελιξία που προσφέρει το υπολογιστικό νέφος.

- **Δεδομένα και εφαρμογές**

Επιχειρηματικές εφαρμογές πρέπει να συνδυάζουν δεδομένα από πολλαπλές πηγές που βασίζονται στο σύννεφο, και πρέπει να συντονίζουν τις δραστηριότητες των εφαρμογών που εκτελούνται σε διαφορετικά σύννεφα.

- **SLAs**

Εκτός από τα βασικα SLAs που απαιτούνται από τους τελικούς χρήστες, επιχειρήσεις που υπογράφουν συμβάσεις που βασίζονται σε SLAs θα χρειαστούν ένα σίγουρο τρόπο απόδοσης συγκριτικής αξιολόγησης. Πρέπει να υπάρχει σαφής τρόπος ορισμού του τι ένας πάροχος νέφους θα παραδόσει, και πρέπει να υπάρξει σαφής τρόπος μέτρησης αυτού που πράγματι παραδόθηκε.

- **Διαχείριση του κύκλου ζωής**

Οι επιχειρήσεις πρέπει να είναι σε θέση να διαχειριστούν τον κύκλο ζωής των εφαρμογών και των εγγράφων. Η απαίτηση αυτή περιλαμβάνει εκδόσεις των εφαρμογών και διατήρηση και καταστροφή των δεδομένων.

- **Ανάπτυξη**

Θα πρέπει να είναι απλή η δημιουργία μιας VM και η ανάπτυξη της στο νέφος. Όταν η VM έχει δημιουργηθεί θα πρέπει να είναι δυνατόν να μεταφερθεί από έναν πάροχο νέφους σε έναν άλλον. Αντισταθμίζοντας τους διαφορετικούς μηχανισμούς που έχουν οι πάροχοι για την τοποθέτηση και αποθήκευση σε VMs.

- **Επιχειρησιακά πρότυπα και πρωτόκολλα**

Πολλές λύσεις υπολογιστικού νέφους μεταξύ των επιχειρήσεων θα χρησιμοποιούν υφιστάμενα πρότυπα, όπως RosettaNet ή OAGIS. Τα ισχύοντα πρότυπα θα διαφέρουν από τη μία εφαρμογή στην άλλη και από την μια επιχείρηση στην άλλη.

5.2.2 Ευπάθειες & κίνδυνοι εταιρείας

Από την στιγμή που η εταιρεία έχει ανατέθει σε έναν πάροχο δημοσίου νέφους ενδέχεται να αντιμετοπίσει τους παρακάτω κινδύνους και ευπάθειες:

- **Απώλεια διακυβέρνησης**

Οι επιχειρήσεις στρέφονται σε CSPs, αναζητώντας λύσεις που μπορούν να υλοποιηθούν εύκολα και με χαμηλό κόστος. Αυτή η ευκολία μπορεί να είναι δελεαστική, ειδικά όταν η επιχείρηση αντιμετωπίζει επείγουσες προθεσμίες που απαιτούν επείγουσα λύση (όπως η λήξη των αδειών των εφαρμογών ή η ανάγκη περισσοτέρων υπολογιστικών πόρων). Αυτό μπορεί να είναι ένα ζήτημα, επειδή οι οργανώσεις μπορούν να επικοινωνούν με εφαρμογές στο σύννεφο χωρίς κατάλληλη εποπτεία των συμβάσεων, παρακάμπτοντας έτσι την τήρηση των εσωτερικών πολιτικών.[11]

- **Έλλειψη κανονιστικής συμμόρφωσης**

Είναι η τήρηση ενός οργανισμού με τους νόμους, τους κανονισμούς, τις οδηγίες, και προδιαγραφές που αφορούν τις δραστηριότητες της. Παραβιάσεις των κανονιστικών ρυθμίσεων συμμόρφωσης συχνά οδηγούν σε νομική τιμωρία, συμπεριλαμβανομένων των ομοσπονδιακών προστίμων.[11]

- **Μη εκπαιδευμένο προσωπικό**

Το προσωπικό μιας επιχείρησης μπορεί να αποτελέσει την μεγαλύτερη ευπάθεια, όσο περισσότερο οι επιχειρήσεις επενδύουνε στις τεχνολογικές περιμέτρους, τόσο πιο ευάλωτο γίνεται το ανθρώπινο δυναμικό.[25]

- **Κακόβουλο λογισμικό**

Είναι κάθε λογισμικό που φέρνει βλάβη σε ένα υπολογιστικό σύστημα.Ένα κακόβουλο λογισμικό μπορεί να είναι με τη μορφή worms, trojans, spyware, adware, rootkits, κ.τ.λ,

τα οποία κλέβουν προστατευόμενα δεδομένα, διαγράφουν έγγραφα ή να προσθέτουν λογισμικό που δεν έχει εγκριθεί από έναν χρήστη.[25]

5.3 Εφαρμογή πλαισίου COBIT 5

Ο λόγος που η εταιρεία επέλεξε να κάνει χρήση του πλαισίου COBIT 5 είναι γιατί το COBIT 5 είναι γενικό και χρήσιμο για τις επιχειρήσεις όλων των «μεγεθών». Το COBIT 5 είναι ένα δοκιμασμένο σύνολο προτύπων και διαδικασιών που οι επιχειρήσεις μπορούν να χρησιμοποιήσουν για να εξασφαλιστεί ότι λειτουργούν όσο το δυνατόν αποτελεσματικότερα, για την ελαχιστοποίηση των κινδύνων, και να μεγιστοποιήσουν τα οφέλη του νέφους. Η έκδοση αυτή περιέχει λεπτομερή οδηγό αναφοράς με τις διαδικασίες και τις πρακτικές που ορίζονται από το μοντέλο αναφοράς διαδικασίας του COBIT 5 για να αντιμετοπισθούν πιθανές ευπάθειες και κίνδυνοι της επιχείρησης.

5.3.1 Διαδικασία αξιολόγησης κινδύνου

Η διαδικασία αξιολόγησης κινδύνου εφαρμόζεται πάντα πριν την ανάθεση της εταιρείας στο υπολογιστικό νέφος. Ο επικεφαλής του τμήματος πληροφοριών(Chief Information Officer) της εταιρείας θέτει έναν ελεγκτή συστημάτων πληροφοριών για τη διεξαγωγή μιας αξιολόγησης κινδύνου. Αυτή η διαδικασία καθορίζει τι η εταιρεία χρειάζεται να προστατέψει, προσδιορίζοντας τους κινδύνους και καθορίζοντας τις αντιδράσεις. Για την διεξαγωγή της αξιολόγησης κινδύνου στο περιβάλλον του υπολογιστικού νέφους έγινε η επιλογή του RiskIT πλαισίου το οποίο βασίζεται στο COBIT 5. Το RiskIT παρέχει μια λίστα με 36 υψηλού επιπέδου κινδύνου σενάρια που μπορούν να προσαρμοστούν στον κάθε οργανισμό. Επιπλέον, το RiskIT προσφέρει μια εκτενή σύνδεση μεταξύ των γενικών σεναρίων κινδύνου, και τους στόχους ελέγχου του COBIT 5 που είναι προσαρμόσιμοι για κάθε κατάσταση. Ο παρακάτω **Πίνακας 5.5** απεικονίζει την αντιστοίχιση μεταξύ των σεναρίων κινδύνων υψηλού επιπέδου και τους στόχους ελέγχου που αντιστοιχούν στο COBIT 5 που δημιουργήθηκαν από τον ελεγκτή πληροφοριακών συστημάτων για την διευθέτηση του υπολογιστικού νέφους.[30]

Πίνακας 5. 5: Αντιστοίχιση σεναρίων υψηλού επιπέδου κινδύνων και αντίστοιχων ελέγχων του COBIT 5[19]

RiskIT Αναφορά No.	Σενάρια κινδύνου υψηλού επιπέδου	Διαδικασίες του COBIT 5 και των αντίστοιχων στόχων ελέγχου
27	Λογικές επιθέσεις	DS5.3, DS5.10
31	Ακεραιότητα βάσης δεδομένων	DS11.6

Η χρήση του RiskIT σε συνδυασμό με μια ευρέως αποδεκτή διακυβέρνηση της πληροφορικής και ενός πλαισίου ελέγχων όπως το COBIT 5, καθιστά τον εντοπισμό των κινδύνων ισχυρό και την διαδικασία αξιολόγησης κινδύνων αποτελεσματική και αποδοτική. Αυτό οδηγεί σε ένα μοντέλο που είναι επεκτάσιμο και επαναχρησιμοποιήσιμο και μπορεί να κλιμακωθεί μέχρι τους κινδύνους πληροφορικής που επηρεάζουν το σύνολο της εταιρείας. Μόλις οριστούν οι κίνδυνοι, και οι στόχοι ελέγχου του COBIT 5, θα χρησιμοποιηθούν από τον ελεγκτή πληροφοριακών συστημάτων για να αναπτυχθεί ένα πρόγραμμα ελέγχου βασισμένο στον κίνδυνο.[30]

Στόχοι ελέγχου COBIT για No. 31

- **DS11.6 Απαιτήσεις ασφάλειας για τη διαχείριση δεδομένων**

Καθορίζει και εφαρμόζει πολιτικές και διαδικασίες, για να προσδιορίσει και να εφαρμόσει τις απαιτήσεις ασφαλείας που ισχύουν για την επεξεργασία, την αποθήκευση, και την έξοδο των δεδομένων, για την επίτευξη των επιχειρησιακών στόχων, πολιτικές ασφαλείας, και τις ρυθμιστικές απαιτήσεις του οργανισμού.[30]

- **Διαδικασία ελέγχου**

Καθορίζει πότε μια πολιτική έχει οριστεί και εφαρμοστεί για την προστασία των ευαίσθητων δεδομένων από μη εξουσιοδοτημένη πρόσβαση και εσφαλμένη μετάδοση.[30]

- **Πόρισμα**

Προσωπικά αναγνωρίσιμες πληροφορίες(Personally Identifiable Information) αποθηκεύονται σε μορφή απλού κειμένου στον CSP.[30]

Στόχοι ελέγχου COBIT για No. 27

- **DS5.3 Διαχείριση ταυτότητας**

Βεβαιώνει ότι όλοι οι χρήστες και η δραστηριότητα τους στα συστήματα πληροφορικής είναι αναγνωρισμένη. Ενεργοποίει ταυτότητες χρήστη μέσω ελέγχου μηχανισμών ταυτότητων. Επιβεβαιώνει ότι τα δικαιώματα πρόσβασης των χρηστών στα συστήματα και δεδομενα συνάδουν με καθορισμένες και τεκμηριωμένες επιχειρησιακές ανάγκες. Βεβαιώνει ότι η πρόσβαση των χρηστών ζητήται από την διαχείριση του χρήστη, εγκρίνεται από τους διαχειριστές του συστήματος, και εφαρμόζεται από άτομα που είναι υπέυθυνα για την ασφάλεια. Διατηρεί τις ταυτότητες χρηστών και τα δικαιώματα πρόσβασης σε ένα κεντρικό αποθετήριο. Αναπτύσει αποδοτικά τεχνικά και διαδικαστικά μέτρα, εφαρμόζει έλεγχο ταυτότητας, και την επιβολή των δικαιωμάτων πρόσβασης.[30]

- **Διαδικασία ελέγχου**

Προσδιορίζει αν οι μηχανισμοί πρόσβασης και ελέγχου ταυτότητας χρησιμοποιούνται για τον έλεγχο της λογικής πρόσβασης σε όλους τους χρήστες, τις διαδικασίες του συστήματος και των πόρων πληροφορικής για εσωτερική και εξ' αποστάσεως διαχειρίση των χρήστων, των διαδικασίων και των συστημάτων.[30]

- **Πόρισμα**

Γενικές ταυτότητες χρήστη χρησιμοποιούνται για την πρόσβαση στις VM του νέφους. Πολλαπλοί παράγωντες ταυτοποίησης δεν χρησιμοποιούνται για την κονσόλα διαχείρισης του νέφους.[30]

- **DS5.10 Ασφάλεια δικτύου**

Χρησιμοποιεί τεχνικές ασφαλείας που σχετίζονται με τις διαδικασίες διαχείρισης (Π.χ., τοίχοι προστασίας, συσκευές ασφαλείας, ανίχνευση εισβολής) για να επιτρέψει την πρόσβαση και τον έλεγχο ροής των πληροφοριών από και προς τα δίκτυα.[30]

- **Διαδικασία ελέγχου**

Εξετάζει και επιβεβαιώνει πότε μια πολιτική ασφαλείας του δικτύου έχει συσταθεί και διατηρείται. Εξετάζει αν, και επιβεβαιώνει ότι διαδικασίες και κατευθυντήριες γραμμές

είναι για τη διαχείριση όλων των κρίσιμων μερών δικτύωσης (Π.χ., δρομολογητές πυρήνων, DMZ, VPN) είναι εγκατεστημένα και ενημερώνονται τακτικά.[30]

- **Πόρισμα**

Οι ομάδες εφαρμογών διαχειρίζονται τη διαμόρφωση του τοίχους προστασίας του νέφους, αντί να βασίζεται στην ομάδα των μηχανικών δικτύου.[30]

Ο επόμενος **Πίνακας 5.6** αντιπροσωπεύει τους συγκεκριμένους κινδύνους και τα κενά μετά τη διενέργεια του ελέγχου.

Πίνακας 5. 6: Κίνδυνοι και κενά μετά τον έλεγχο[19]

RiskIT Αναφορά No.	**Σενάρια κινδύνου υψηλού επιπέδου**	**Ιδιαίτεροι κίνδυνοι και κενά**
27	Λογικές επιθέσεις	• Ο ιδιοκτήτης της επιχείρησης IaaS δεν έχει καθοριστεί ακόμα. • Τα τοίχοι προστασίας της υπηρεσίας IaaS τα διαχειρίζονται από την ομάδα εφαρμογών αντί από τους διαχειριστές δίκτύου. • Δεν χρησιμοποιούνται πολλαπλοί παράγωντες ταυτοποίησης για την διαχείριση στο νέφος.
31	Ακεραιότητα βάσης δεδομένων	Οι PII αποθηκεύονται σε μορφή απλού κειμένου στον CSP.

Ο έλεγχος επισήμανε ότι η εταιρεία πρέπει να μειώσει τους κινδύνους.Μόλις η εταιρεία ευθυγραμμίσει τον κίνδυνο πληροφορικής με το συνολικό επιχειρηματικό κίνδυνο, η εταιρεία είναι καλύτερα προετοιμασμένη για να αξιοποιήσει τη δύναμη του υπολογιστικού νέφους.[30]

5.3.2 Εφαρμογή βέλτιστων πρακτικών

Επιλεγμένες διαδικασίες από το πλαίσιο COBIT 5 μπορούν να βελτιώσουν την αποτελεσματικότητα της ασφάλειας των επιχειρήσεων. Ο στόχος εδώ είναι να αναπτύχθει μια στρατηγική για την ασφάλεια με τις τεχνικές διαδικασίες, τους ελέγχους και τα εργαλεία για την ασφάλεια σε μια επιχείρηση. Πρόκειται για μια στρατηγική με βάση τον κίνδυνο για την υπεράσπιση κρίσιμων πόρων της επιχείρησης ενάντια σε ένα ευρύ φάσμα απειλών και τρωτών σημείων.[44]

Χρησιμοποιώντας αυτή την προσέγγιση κινδύνου, οι προσπάθειες για την ασφάλεια μπορούν να επικεντρωθούν για να υπερασπιστούν τα δίκτυα, τα τελικά σημεία και τα δεδομένα από κακόβουλο λογισμικό και διάφορες άλλες απειλές.[44]

Το COBIT 5 παρέχει καθοδήγηση σχετικά με τις βέλτιστες πρακτικές για την ασφάλεια των επιχειρήσεων. Το COBIT 5 περιλαμβάνει ένα σύνολο επτά προϋποθέσεων για τη διακυβέρνηση και τη διαχείριση των επιχειρήσεων πληροφορικής, μια εκ των οποίων είναι οι διαδικασίες. Από τις 37 διαδικασίες του COBIT 5, θα επικεντρώθούμε σε τρείς βασικές διαδικασίες ασφαλείας:[44]

1) **APO12** Διαχείριση κινδύνων.
2) **APO13** Διαχείριση ασφάλειας.
3) **DSS05** Διαχείριση υπηρεσιών ασφαλείας.

- **Κακόβουλο λογισμικό & Κακόβουλοι χρήστες**

Η διαδικασία **Διαχείριση κινδύνου(APO12)** από τον τομέα **Align, Plan and Organize** στο πεδίο **Management** αποτελεί προϋπόθεση για οποιοδήποτε σύνολο των ελέγχων ασφαλείας και αναφέρεται από σχεδόν κάθε πλαίσιο ή πρότυπο για την ασφάλεια των πληροφοριών:[44]

Πίνακας 5. 7: Πρακτικές APO12 [22]

APO12.01	Τα δεδομένα θα πρέπει να συλλέγονται από όλες τις σχετικές πηγές (Π.χ., συστήματα, εφαρμογές, δίκτυα, βάσεις δεδομένων) σε πολλαπλές κατηγορίες (Π.χ., πρόσβαση, διαμορφώσεις) για να υποστηρίξει την κατανόηση των κινδύνων.

APO12.02	Τα δεδομένα αυτά πρέπει να εξεταστούν κατά την ανάλυση του κινδύνου, ιδίως για την ανάλυση των επιπτώσεων στις επιχειρήσεις. Εκτιμόντας την πιθανότητα διαφορετικών απειλών και τον εντοπισμό ελέγχων για την μειωσή τους.
APO12.03	Ένα προφίλ κινδύνου θα πρέπει να διατηρείται σε μια απογραφή των επιχειρηματικών διαδικασιών και των πληροφοριακών συστημάτων υποστήριξης, εφαρμογών, υποδομής, δεδομένων, εγκαταστάσεων και δυνατότητων. Η απογραφή αυτή θα πρέπει να χρησιμοποιείται για να προσδιορίσει τα στοιχεία πληροφορικής, περιουσιακά στοιχεία που είναι πιο κρίσιμα και που απαιτούν τους ισχυρότερους ελέγχους. Δείκτες κινδύνου ή παράγοντες (εσωτερικοί/εξωτερικοί) χρησιμοποιούνται για να διατηρηθεί η απογραφή, και θα πρέπει να αναθεωρούνται και να επικυρώνονται περιοδικά.
APO12.04	Βασικοί ενδιαφερόμενοι θα πρέπει να ενημερώνονται μέσω του καθεστώτος κινδύνου. Συμπεριλαμβανομένης της χειρότερης περίπτωσης και τα πλέον πιθανά σενάρια.
APO12.05	Ένα χαρτοφυλάκιο δράσης διαχείρισης κινδύνου θα πρέπει να οριστεί και να διατηρηθεί για τις δραστηριότητες διαχείρισης ελέγχου, την αποφυγή, την πρόληψη ή την μεταφορά κινδύνου.
APO12.06	Η απόκριση σε συμβάντα κινδύνου πρέπει να είναι έγκαιρη και αποτελεσματική βασιζόμενη σε επίσημα προγράμματα δοκιμών. Τα εν λόγω σχέδια πρέπει να είναι προετοιμασμένα, να συντηρούνται και ελέγχονται περιοδικά για την αντιμετώπιση σε περιστατικά που σχετίζονται με την πληροφορική τα οποία μπορεί να επηρεάσουν τις επιχειρηματικές δραστηριότητες.

Η διαδικασία **Διαχείριση ασφάλειας(APO13)** από τον τομέα **Align, Plan and Organize** στο πεδίο **Management** αποτελείται από τον ορισμό, τη λειτουργία και την παρακολούθηση ενός ISMS. Αυτός είναι ένας σημαντικός σύνδεσμος για να μεταφράσει τη διαδικασία κίνδυνου σε αποτελεσματικές υπηρεσίες ασφαλείας. Για την κατασκευή του ISMS επαγκελματίες ασφαλείας θα πρέπει να εξετάσουν και να καταγράψουν την

διάθεση ανάληψης κινδύνου, τις απαιτήσεις ασφαλείας και τις λύσεις ασφαλείας. Συγκεκριμένες πρακτικές που συνθέτουν την διαδικασία διαχείρισης ασφαλείας ακολουθούν: [44]

Πίνακας 5. 8: Πρακτικές APO13 [22]

APO13.01	Ένα ISMS θα πρέπει να καθιερωθεί ως πρότυπο, για την ασφάλεια πληροφορικής. Η προσέγγιση αυτή θα πρέπει να ευθυγραμμιστεί με τις απαιτήσεις των επιχειρήσεων και τις επιχειρηματικές διαδικασίες.
APO13.02	Για να επισημοποιήθει αυτή η προσέγγιση, ένα σχέδιο μεταχείρισης κίνδυνου για την ασφάλεια των πληροφοριών θα πρέπει να καθορίζεται με βάση ρεαλιστικές περιπτώσεις επιχειρήσεων και να εφαρμόζεται ως μέρος των στρατηγικών στόχων και της αρχιτεκτονικής της επιχείρησης.
APO13.03	Συνολικά τα ISMS θα πρέπει να παρακολουθούνται και να επανεξετάζονται τακτικά, μέσω της ανασκόπησης από τη διοίκηση και τους ελέγχους ασφαλείας. Ένα βασικό θέμα εδώ είναι μια αντίληψη για την ασφάλεια και τη συνεχή βελτίωση.

Η διαδικασία **Διαχείριση υπηρεσιών ασφαλείας(DSS)** από τον τομέα **Deliver, Service and Support** στο πεδίο **Management** καλύπτει τεχνικούς ελέγχους ασφαλείας για να υπερασπιστεί τους πιο κρίσιμους ευάλωτους και ευαίσθητους πόρους, συμπεριλαμβανομένων πληροφοριών, υποδομών δικτύου και επικοινωνιών, τελικά σημεία δικτύου (Π.χ., χρήστες, υπολογιστές) και συστήματα πρόσβασης. Συγκεκριμένες πρακτικές που αποτελούν τη διαδικασια διαχείρισης ασφαλείας πληροφοριών ακολουθούν: [44]

Πίνακας 5. 9: Πρακτικές DSS [22]

DSS05.01	Προστασία από κακόβουλο λογισμικό(Π.χ., virus, worms, spyware, κ.α) θα πρέπει να εφαρμοστούν μέσω συστημάτων ανίχνευσης απειλών(Π.χ., τοίχοι προστασίας, IDS, IPS), αποθετήρια αναζήτησης συμβάντων(Π.χ., ασφάλεια πληροφοριών και διαχείριση γεγονότων), και διαχείριση

	ενημερώσεων ασφαλείας. Τα κακόβουλα λογισμικά θα πρέπει να ανιχνεύονται, αποτρέπονται και αφαιρούνται σε όλα τα επίπεδα του πληροφοριακού περιβάλλοντος συμπεριλαμβανομένων των εφαρμογών, λειτουργικών συστημάτων, δικτύων, κοινών πόρων και υλικού.
DSS05.02	Την ασφάλεια των δικτύων θα πρέπει να διαχειρίζεται ενεργά με μια ολοκληρωμένη στρατηγική και ένα σύνολο εργαλείων σε όλα τα επίπεδα του δικτύου και τοπολογίας (Π.χ., Switch/router, λίστες ελέγχου πρόσβασης [ACL], τοίχοι προστασίας, IDS/IPS). Οι έλεγχοι πρέπει να αναπτυχθούν σε όλα τα σημεία εισόδου συμπεριλαμβανομένου του ηλεκτρονικού ταχυδρομείου, διαδικτυακές εφαρμογές, πρωτόκολλα μεταφοράς αρχείων, κοινωνικής δικτύωσης, ανταλλαγής μηνυμάτων, εφαρμογές cloud/ αποθήκευσης και υλικού (USB).
DSS05.03	Ασφάλεια καταληκτικού σημείου(antivirus, antimalware λογισμικό, ασφάλεια e-mail, τοίχοι προστασίας) πρέπει να αναπτυχθούν και να διασφαλίσουν ότι laptops, desktops, και άλλες φορητές συσκευές είναι εξασφαλισμένες.
DSS05.04	Η ταυτότητα χρήστη και η λογική πρόσβαση θα πρέπει να διαχειρίζονται με βάση την επιχειρηματική ανάγκη. Μια καλή πρακτική είναι να ενισχύθουν οι έλεγχοι γύρω από τον έλεγχο ταυτότητας(Π.χ., userID, passwords) και η παροχή εξουσιοδότησης σε ευαίσθητους πόρους. Κάποιος πρέπει να εξασφαλίσει ότι τα δικαιώματα και η πρόσβαση διαχειριστή είναι ιδιαίτερα καλά, ελέγχονται και παρακολουθούνται.
DSS05.05	Η φυσική πρόσβαση στα περιουσιακά στοιχεία της πληροφορικής θα πρέπει να διαχηρίζεται με διαδικασίες παραχώρησης, περιορισμού και ανάκλησης φυσικής πρόσβασης σε διαδικτυακούς τόπους που βασίζονται στην αναγκή των επιχειρήσεων. Η πρόσβαση θα πρέπει να αιτιολογείται, εγκρίνεται, καταγράφεται και παρακολουθείται.
DSS05.06	Ευαίσθητα έγγραφα θα πρέπει να διαφυλαχθούν με κατάλληλους ελέγχους. Συσκευές εξόδου(Π.χ., δικλείδες ασφαλείας) θα πρέπει επίσης να ελέγχονται.

DSS05.07	Η παρακολούθηση της ασφάλειας των υποδομών πληροφορικής αποτελεί βασικό συστατικό του περιβάλλοντος ελέγχου. Ένα σύνολο αυστηρών ελέγχων και εργαλειών όπως η αναζήτηση χώρου αποθήκευσης (Π.χ., σύστημα SIEM), συγκεντρωτικά και ασφαλή συστήματα καταγραφής, και ανίχνευση κακόβουλου λογισμικού θα πρέπει να ληφθούν υπόψη.Η ολοκλήρωση με την διαχείριση περιστατικών και κλιμάκωσης διαδικασιών θα πρέπει να εξασφαλιστεί.

- **Απώλεια διακυβέρνησης**

Διασφαλίζει ότι υπάρχουν εσωτερικοί έλεγχοι διακυβέρνησης εντός της επιχείρησης για την συμμετοχή των απαραιτήτων φορέων ελέγχου κατά την διαδικασία λήψης αποφάσεων για την μετάβαση στις υπηρεσίες στο νέφους.

Για την αποφυγή αυτού του κινδύνου, η διαδικασία **Εξασφάλιση & διατήρηση πλαισίου Διακυβέρνησης(EDM01)** από τον τομέα **Evaluate**, **Direct and Monitor** από το πεδίο **Governance** αναλύει και αρθρώνει τις απαιτήσεις για την διακυβέρνηση της πληροφορικής της εταιρείας και θέτει και διατηρεί αποτελεσματικές δομές, αρχές, διαδικασίες και πρακτικές, με σαφήνεια των αρμοδιοτήτων και αρχή για την επίτευξη της αποστολής της επιχείρησης. Και η διαδικασία **Παρακολούθηση, αξιολόγηση & εκτίμηση του συστήματος εσωτερικού ελέγχου(MEA02)** από τον τομέα **Monitor Evaluate and Assess** από το πεδίο **Management** όπου κάνει συνεχής αξιολόγηση του περιβάλλοντος ελέγχου, συμπεριλαμβανομένης της αυτο-αξιολόγησης. Καθιστά ικανή την διαχείριση να εντοπίσει ελλείψεις ελέγχου και ανικανότητες, και τέλος να δρομολογήσει δράσεις βελτίωσης. Το πρόγραμμα οργανώνει και διατηρεί πρότυπα για δραστηριότητες αξιολόγησης και διασφάλισης του εσωτερικού ελέγχου. Εφαρμόζοντας τις παρακάτω πρακτικές:[49]

Πίνακας 5. 10: Πρακτικές EDM [20]

EDM01.01	Συνεχώς αναγνωρίζει και απασχολεί μαζί με τους ενδιαφερόμενους του οργανισμού, καταγράφοντας μια συμφωνία των απαιτήσεων, και κάνοντας κριτική στην υπάρχουσα και μελλοντική σχεδίαση της διακυβέρνησης της πληροφορικής της επιχείρησης.

EDM01.02	Ενημερώνει τους αρμόδιους και λαμβάνει την υποστήριξη τους και τη δέσμευση τους. Καθοδηγεί διαδικασίες και πρακτικές για τη διακυβέρνηση της πληροφορικής σε ευθυγράμμιση με τις συμφωνηθείσες αρχές σχεδιασμού της διακυβέρνησης, τα μοντέλα λήψης αποφάσεων, και των επιπέδων εξουσίας.
EDM01.03	Αξιολογεί αν το σύστημα διακυβέρνησης και οι εφαρμοσμένοι μηχανισμοί λειτουργούν αποτελεσματικά.

Πίνακας 5. 11: Πρακτικές MEA02 [20]

MEA02.01	Παρακολουθεί συνεχώς τον δείκτη αναφοράς και βελτιώνει το περιβάλλον ελέγχου πληροφορικής και το πλαίσιο ελέγχου ώστε να ανταποκρίνεται στους οργανωτικούς στόχους.
MEA02.02	Επανεξετάζει την λειτουργία των ελέγχων, συμπεριλαμβανομένης της επανεξέτασης των στοιχείων παρακολούθησης και των δοκιμών, ώστε να εξασφαλίζεται ότι οι έλεγχοι μέσα στο πλαίσιο των επιχειρησιακών διαδικασιών λειτουργούν αποτελεσματικά. Περιλαμβάνει δραστηριότητες για την διατήρηση στοιχείων της αποτελεσματικής λειτουργίας των ελέγχων μέσα από μηχανισμούς, όπως περιοδικές δοκιμές ελέγχων, συνέχεις ελέγχοι παρακολούθησης, ανεξάρτητες αξιολογήσεις και κέντρα ελέγχου. Αυτό παρέχει στην επιχείρηση την διασφάλιση της αποδοτικότητας του ελέγχου, ώστε να ανταποκρίνεται στις απαιτήσεις που σχετίζονται με τις επιχειρηματικές, κανονιστικές και κοινωνικές ευθύνες.
MEA02.03	Ενθαρρύνει τους διαχειριστές να αναλάβουν την ιδιοκτησία των ελέγχων βελτίωσης, μέσω ενός συνεχούς προγράμματος αυτο-αξιολόγησης για την εκτίμηση της πληρότητας και της αποτελεσματικότητας των ελέγχων διαχείρισης διαδικασιών, των πολιτικών και των συμβάσεων.
MEA02.04	Εντοπίζει ελλείψεις ελέγχου και αναλύει τις βασικές αιτίες τους. Κλιμακώνει τις ελλείψεις ελέγχου και τις αναφέρει στους ενδιαφερόμενους.
MEA02.05	Εξασφαλίζει ότι οι φορείς που ασκούν την διασφάλιση είναι ανεξάρτητοι, από τις ομάδες ή των οργνανισμών στο πεδίο εφαρμογής. Οι φορείς αυτοί

	πρέπει επιδεικνύουν κατάλληλα χαρακτηριστικά, ικανότητες και γνώση που απαιτείται για την εκτέλεση ή την διασφάλιση και την τήρηση των κωδίκων δεοντολογίας και των επαγγελματικών προτύπων.
MEA02.06	Πρωτοβουλίες διασφάλισης προγράμματος με βάση τους στόχους των επιχειρήσεων και τις στρατηγικές προτεραιότητες, τον εγγενή κίνδυνο, τους περιορισμούς των πόρων και την επαρκή γνώση της επιχείρησης.
MEA02.07	Καθορίζει και συμφωνεί με τη διοίκηση σχετικά με το πεδίο εφαρμογής της πρωτοβουλίας διασφάλισης , με βάση τους στόχους διασφάλισης.
MEA02.08	Εκτελεί την πρωτοβουλία διασφάλισης σχεδίου, κάνει αναφορά σχετικά με τα πορίσματα που εχουν βρεθεί. Παρέχει συστάσεις για την βελτίωση σχετικά με τις προσδιορισμένες επιχειρησιακές επιδόσεις, την εξωτερική συμμόρφωση και τον υπολειπόμενο κίνδυνο του συστήματος εσωτερικού ελέγχου.

- **Έλλειψη κανονιστικής συμμόρφωσης**

Για την αποφυγή αυτού του κινδύνου, γίνεται χρήση της διαδικασίας **Παρακολούθηση, εκτίμηση & αξιολόγηση της συμμόρφωσης με εξωτερικές απαιτήσεις(MEA03)** από τον τομέα **Monitor, Evaluate and Assess** από το πεδίο **Management** η οποία διασφαλίζει ότι η διάθεση ανάληψης κινδύνου της εταιρείας και η ανοχή είναι γνωστά, και ότι ο κίνδυνος της επιχειρησιακής αξίας που σχετίζεται με την χρήση της πληροφορικής είναι αναγνωρισμένος και διαχειρίσημος. Εφαρμόζοντας τις παρακάτω πρακτικές:[49]

Πίνακας 5. 12: Πρακτικές MEA03 [20]

MEA03.01	Σε συχνή βάση, αναγνωρίζει και παρακολουθεί για αλλαγές σε τοπικούς και διεθνείς νόμους, κανονισμούς και άλλες εξωτερικές απαιτήσεις που πρέπει να εφαρμόζωνται από την σκοπιά της πληροφορικής.
MEA03.02	Επανεξέταζει και προσαρμόζει πολιτικές, αρχές, προτύπα και μεθοδολογίες για να εξασφαλιστεί η νομιμότητα, ρυθμιστικές και συμβατικές απαιτήσεις που έχουν διευθυνσιοδοτηθεί.

MEA03.03	Επιβεβαίωση συμμόρφωσης πολιτικών, προτύπων, διαδικασιών και μεθοδολογιών με τον νόμο, κανονιστικών και συμβατικών απαιτήσεων.
MEA03.04	Διασφάλιση της εξωτερικής συμμόρφωσης, και προσκόλληση με πολιτικές, αρχές, πρότυπα, διαδικασίες και μεθοδολογίες. Επιβεβαίωση ότι διορθωτικές ενέργειες για να διευθετήσουν τα κενά στην συμμόρφωση έχουν γίνει εγκαίρως.

- **Εκπαίδευση προσωπικού**

Για την αποφυγή αυτού του κινδύνου, γίνεται εφαρμογή των παρακάτω πρακτικών από την διαδικασία **Μόρφωση και εκπαίδευση χρηστών(DS7)** από τον τομέα **Delivery and Support** από το πεδίο **Management** του COBIT 5 για την εκπαίδευση του προσωπικού της εταιρείας.[49]

Πίνακας 5. 13: Πρακτικές DS [20]

DS7.1	Καταρτίζει και ενημερώνει τακτικά ένα πρόγραμμα σπουδών για κάθε ομάδα των εργαζομένων.
DS7.2	Βασισμένη στην αναγνωρισμένη εκπαίδευση και την ανάγκη κατάρτισης, αναγνωρίζει συγκεκριμένες ομάδες και τα μέλη τους , αποτελεσματικούς μηχανισμούς παράδοσης, εκπαιδευτές και συμβούλους.
DS7.3	Αξιολογεί την εκπαίδευση και την παράδοση του περιεχόμενου κατάρτισης, μετά την ολοκλήρωση για τη συνάφεια, την ποιότητα, την αποτελεσματικότητα, τη διατήρηση της γνώσης, το κόστος και την αξία.

- **Επιθέσεις στο Hypervisor**

Για την μείωση αυτού του κινδύνου η επιχείρηση απαιτεί από τον CSP εσωτερικά SLA για την διαχείριση ευπάθειας του hypervisor. Το SLA θα πρέπει να περιέχει αναλυτικές προδιαγραφές σχετικά με τις ταξινομήσεις των ευπαθειών και των μέτρων που λαμβάνονται. Από τις επτά προϋποθέσεις του COBIT 5 τίθενται σε εφαρμογή οι τρείς παρακάτω:[11]

- Εφαρμόζει: Αρχές, Πολιτικές και Πλαίσια.

Οι πολιτικές παρέχουν πιο αναλυτική καθοδήγηση για το πως οι αρχές λειτουργούν στην πράξη, και πως επηρεάζουν την λήψη αποφάσεων. Γίνεται χρήση της:[45]

- ❖ Πολιτική ασφάλειας πληροφορίας.[11]

- Εφαρμόζει: Ανθρώπινο δυναμικό, Ικανότητες, Δεξιότητες.

Για να λειτουργήσει αποτελεσματικά μια λειτουργία ασφαλείας πληροφοριών στο πλαίσιο μιας επιχείρησης άτομα με κατάλλαλες (Ικανοτητες/Δεξιοτητες) οφείλουν να ασκούν την λειτουργία:[45]

- ❖ Διαχειρίση κινδύνου πληροφοριών.[11]

- Εφαρμόζει: Διαδικασίες

Η διαδικασία **Διαχείριση των συμφωνιών παροχής υπηρεσιών(APO09)** από τον **τομέα Align, Plan and Organise** από το πεδίο **Management** διασφαλίζει ότι οι υπηρεσίες και τα επίπεδα εξυπηρέτησης ικανοποιούν τις τρέχουσες και μελλοντικές ανάγκες των επιχειρήσεων.[49]

Πίνακας 5. 14: Πρακτικές APO09 [20]

APO09.1	Ανάλυση επιχειρηματικών απαιτήσεων και τον τρόπο με τον οποίο οι υπηρεσίες πληροφορικής και των επιπέδων υπηρεσιών υποστήριξης επιχειρησιακών διαδικασιών.
APO09.2	Καθορίζει και διαχειρίζεται έναν ή περισσότερους καταλόγους υπηρεσιών για σχετικές ομάδες.
APO09.3	Καθορίζει και προετοιμάζει τα επίπεδα υπηρεσιών βάση τις επιλογές του καταλόγου υπηρεσιών. Συμπεριλαμβανομένου εσωτερικών επιχειρησιακών συμφωνιών.
APO09.4	Παρακολούθει τα επίπεδα εξυπηρέτησης, κάνει αναφορά σχετικά με τα επιτεύγματα και τον προσδιορισμό των τάσεων. Παρέχει τις κατάλληλες πληροφορίες διαχείρισης για την ενίσχυση της διαχείρισης των επιδόσεων.
APO09.5	Διεξάγει περιοδικές αξιολογήσεις των συμβάσεων παροχής υπηρεσιών και

	αναθεωρεί, όταν χρειάζεται.

- **Μη ενημερωμένη ασφάλεια στις VMs**

Για την μείωση αυτού του κινδύνου, συστήνει διαδικασίες εντός της επιχείρησης για να επιβεβαιώσει την κατάσταση ενημερώσεων ασφαλείας λογισμικού πριν από την ενεργοποίηση της κάθε VM. Εξουσιοδοτεί τον CSP να εφαρμόσει σημαντικές εκδόσεις ασφαλείας σε μη ενεργές VM. Από τις επτά προϋποθέσεις του COBIT 5 τίθενται σε εφαρμογή οι δύο παρακάτω:[11]

- Εφαρμόζει: Αρχές, Πολιτικές και Πλαίσιο.
  - Πολιτική ασφάλειας πληροφορίας.[11]

- Εφαρμόζει: Υπηρεσίες, Υποδομές και Εφαρμογές.

Οι δυνατότητες των υπηρεσιών απαιτούνται για την παροχή ασφάλειας των πληροφοριών και των σχετικών λειτουργιών με τις επιχειρήσεις.Οι υπηρεσίες δεν απαιτούν μόνο κατάλληλες υποδομές και εφαρμογές αλλά παρέχονται μέσω ενός συνδιασμού άλλων προϋποθέσεων όπως, διαδικασίες, πληροφορία και οργανωτικές δομές. Γίνεται χρήση της:[45]

- Υπηρεσία παροχής επαρκώς εξασφαλισμένων και διαμορφωμένων συστημάτων, σύμφωνα με τις απαιτήσεις της ασφάλειας και της αρχιτεκτονικής ασφάλειας.[11]

- **Multi-tenancy visibility**

Για την μείωση αυτής της ευπάθειας απαιτεί από τον CSP τεχνικές λεπτομέρειες, και απαιτεί συμπληρωματικούς ελέγχους για να διασφαλιστεί η ιδιοτικότητα των δεδομένων, όταν είναι απαραίτητο.

Η συμβατική συμφωνία είναι απαραίτητη για να διευκρινιστεί επισήμως σε ποιον επιτρέπεται να έχει πρόσβαση στις πληροφορίες της επιχείρησης, κατονομάζοντας συγκεκριμένους ρόλους για τους υπαλλήλους του CSP και εξωτερικούς συνεργάτες. Όλοι οι έλεγχοι για την προστασία των πληροφορίων πρέπει να καταγράφονται στο

SLA. Από τις επτά προϋποθέσεις του COBIT 5 τίθενται σε εφαρμογή οι τρείς παρακάτω:[11]

- Εφαρμόζει: Πληροφορία.

Έκθεση ανασκόπησης της ασφάλειας των πληροφοριών, η οποία περιλαμβάνει:[45]

- ❖ Αποτελέσματα ελέγχου ασφάλειας πληροφοριών.
- ❖ Αναφορά ωριμότητας ασφάλειας πληροφοριών.
- ❖ Διαχείριση κινδύνου σχετικά με την ασφάλεια πληροφοριών.

- Εφαρμόζει: Οργανωτικές δομές.

Μέσα σε μια τυπική εταιρεία, υπάρχουν ρόλοι της ασφάλειας των πληροφοριών και δομές. Γίνεται χρήση:

- ❖ Επικεφαλής ασφάλειας πληροφοριών (CISO) – Ολική ευθύνη του προγράμματος ασφάλειας των πληροφοριών της επιχείρησης.[11] [45]

- Εφαρμόζει:Υπηρεσίες, Υποδομές και Εφαρμογές.
  - ❖ Παρέχει υπηρεσίες παρακολούθησης και ειδοποίησης για γεγονότα που σχετίζονται με την ασφάλεια.[11][45]

(Κενό φύλλο)

6. ΕΠΙΛΟΓΟΣ & ΣΥΜΠΕΡΑΣΜΑΤΑ

Στην παρούσα πτυχιακή εργασία μελετήθηκε η υποδομή του υπολογιστικού νέφους, μια τεχνολογία με αρκετούς κινδύνους, αλλά και πολύ σημαντικά πλεονεκτήματα για τις επιχειρήσεις και τους τελικούς χρήστες. Παρόλο που το υπολογιστικό νέφος μπορεί να προσφέρει πολλαπλά οφέλη, πριν γίνει ανάθεση σε αυτό θα πρέπει να εξεταστούν πολλαπλοί παράγοντες, όπως ζητήματα ασφαλείας, συμμόρφωσης, καθώς και νομικές συνέπειες. Όσο αναφορά τα ζητήματα που αναφέραμε, εδώ έρχονται να δώσουν λύση τα πλαίσια ασφαλείας. Η εταιρεία θα πρέπει να επιλέξει το κατάλληλο πλαίσιο που της ταιρίαζει με βάση τις ανάγκες της. Με την βοήθεια του πλαισίου και ειδικών ασφαλείας, η επιχείρηση μπορεί να αναπτύξει μια αποτελεσματική στρατιγική και μια ολοκληρωμένη πολιτική ασφαλείας, ώστε να πετύχει τους επιχειρηματικούς στόχους της, και να αντιμετοπίσει τους κινδύνους στο «νέφος». Μέσα από αυτήν την μελέτη παρουσιάστηκαν οι βέλτιστες πρακτικές μέσα από το πλαίσιο COBIT για την αντιμετόπιση των κινδύνων, και την διασφάλιση των πληροφοριακών συστημάτων. Παρόλα αυτά, αυτό που πρέπει να θέσουμε σαφές είναι ότι, απόλυτα ασφαλές πληροφοριακό σύστημα δεν υπάρχει, και δεν θα υπάρξει ποτέ, όπως και απόλυτη ασφάλεια σαν έννοια. Για να μπορούμε να πούμε ότι έχουμε ένα ασφαλές πληροφοριακό σύστημα σημαίνει ότι θα πρέπει να απαιτείται ένα μεγάλο χρονικό διάστημα αλλά και υψηλό χρηματικό κόστος για να παραβιαστεί από κακόβουλους χρήστες. Ωστόσο η εταιρεία, θα πρέπει να γνωρίζει ότι όποιο πλαίσιο και αν επιλέξει, όσο σωστά και αν αυτό εφαρμοστεί, δεν θα μπορεί ποτέ να εγγυηθεί στο 100% την ασφάλεια της πληροφορίας. Γιατί καθώς η τεχνολογία του υπολογιστικού νέφους εξελλίσεται, με τον ίδιο τρόπο εξελίσσονται και οι κίνδυνοι. Έτσι τα πλαίσια ασφαλείας θα πρέπει να ενημερώνονται, και να βελτιώνονται όταν χρειάζεται. Το σίγουρο είναι ότι το υπολογιστικό νέφος έχει κάνει αισθητή την παρουσία του, και έχει έρθει στις ζωές μας για να μείνει.

ΠΑΡΑΡΤΗΜΑΤΑ

Πηγές Εικόνων, Πινάκων

[1] Εικόνα 2.1: History and Vision of Cloud Computing | Times of Cloud, URL: http://timesofcloud.com/cloud-tutorial/history-and-vision-of-cloud-computing/, προσπελάστηκε στις 15/7/16

[2] Εικόνα 2.2, 2.3: Breach-Level-Index-Report-H12016.pdf, URL: http://breachlevelindex.com/assets/Breach-Level-Index-Report-H12016.pdf, προσπελάστηκε στις 7/7/16

[3] Εικόνα 2.4: State of Cloud Computing, URL: http://www.business2community.com/tech-gadgets/state-of-cloud-computing-0381119#gRyqMTWE83KEdb3g.97, προσπελάστηκε στις 1/7/16

[4] Εικόνα 2.5: The Cloud Computing Services Primer Part 1: Erick Simpson, URL: https://blog.spc-intl.com/cloud-computing-services-primer-part-1-erick-simpson/, προσπελάστηκε στις 25/7/16

[5] Εικόνα 2.6: Pros and Cons | Cloud Computing in Business, URL: https://u.osu.edu/cloudcomputing/pros-and-cons/, προσπελάστηκε στις 30/7/16

[6] Εικόνα 2.7: Why companies are adopting #hybrid cloud | E-media, the Econocom blog, URL: https://blog.econocom.com/en/blog/why-companies-are-adopting-hybrid-cloud/, προσπελάστηκε στις 2/8/16

[7] Εικόνα 2.8: What is Cloud Computing Stack (SaaS,PaaS,IaaS) – Mazik Global Blog, URL: http://www.mazikglobal.com/blog/cloud-computing-stack-saas-paas-iaas/, προσπελάστηκε στις 10/8/16

[8] Εικόνα 2.9: Revealed:The top challenges to cloud computing – Computer Weekly Data Bank, URL: http://www.computerweekly.com/blog/Computer-Weekly-Data-Bank/Revealed-The-top-challenges-to-cloud-computing, προσπελάστηκε στις 15/8/16

[9] Εικόνα 3.1: 3 Essential Elements for Mobile App Security – AT&T Developer, URL: https://developer.att.com/blog/3-essential-elements-to-creating-highly-secure-applications-for, προσπελάστηκε στις 21/8/16

[10] Εικόνα 3.2: Kai Hwag Geoffrey C. Fox Jack J. Dongarra(2012). Distributed and Cloud Computing From Parallel Processing To Internet Of Things. China Machine Press, pp.50

[11] Εικόνα 3.3-3.6: L. Newcombe (2012). Securing Cloud Services: A pragmatic approach to security architecture in the cloud.IT Governance Publishing, pp.129-138

[12] Εικόνα 4.1: COBIT 5 versus ITIL | bit happens, URL: https://bithappenz.wordpress.com/2015/03/22/what-is-cobit-5/, προσπελάστηκε στις 11/10/16

[13] Εικόνα 4.2: COBIT | Office of Internal Audit, URL: http://www.internalaudit.iastate.edu/internal-controls/cobit, προσπελάστηκε στις 28/10/16

[14] Εικόνα 4.3-4.8: Video Library | Orbus Software, URL: http://www.orbussoftware.com/resources/videos/cobit-distilled/, προσπελάστηκε στις 6/11/16

[15] Εικόνα 4.9: ISACA Development Team (2012). COBIT Implementation.ISACA, pp.19-20

[16] Πίνακας 3.1: L.Newcombe(2012).Securing Cloud Services: A pragmatic approach to security architecture in the cloud.IT Governance Publishing, pp.140-141

[17] Πίνακας 5.1:EC2 Instance Pricing – Amazon Web Services (AWS), URL: https://aws.amazon.com/ec2/pricing/on-demand/, προσπελάστηκε στις 23/11/16

[18] Πίνακας 5.2: Cloud Storage Pricing – Amazon Simple Storage Service (S3) – AWS, URL: https://aws.amazon.com/s3/pricing/, προσπελάστηκε στις 23/11/16

[19] Πίνακας 5.5,5.6: Sailesh Gadia, ISACA Development Team.:,Cloud Computing Risk Assessment: A Case Study. ISACA (Volume 4) (2011)

[20] Πίνακας 5.10-5.14: ISACA Development Team (2013). COBIT 5 for Risk.ISACA, pp.13-112

[21] Εικόνα 5.1: Sailesh Gadia, ISACA Development Team. Cloud Computing Risk Assessment: A Case Study. ISACA(Volume 4)(2011)

[22] Πίνακας 5.7-5.9: F. Greene, Selected COBIT 5 Processes for Essential Enterprise Security. ISACA Journal volume 2 (2015) https://www.isaca.org/Journal/archives/2015/Volume-2/Pages/selected-cobit-5-processes-for-essential-enterprise-security.aspx

[23] Πίνακας 4.1,4.2: ISACA Development Team (2012). COBIT 5 A Business Fremework for the Governance and Management of Enterprise IT.ISACA, pp.19

[24] Πίνακας 5.3: Pricing, URL: https://aws.amazon.com/simpledb/pricing/, προσπελάστηκε στις 3/3/17

[25] Πίνακας 5.4: AWS | Amazon Route 53 | Pricing URL: https://aws.amazon.com/route53/pricing/, προσπελάστηκε στις 4/3/17

ΒΙΒΛΙΟΓΡΑΦΙΑ – ΑΝΑΦΟΡΕΣ

[1] Cloud Computing - Wikipedia, URL: https://en.wikipedia.org/wiki/Cloud_computing#Origin_of_the_term, προσπελάστηκε στις 15/7/16

[2] Ν. Βλαστάρα, “Διαχείριση και παρακολούθηση υποδομής νέφους”,Διπλωματική εργασία,Τμήμα Ηλεκτρολόγων Μηχανικών & Μηχανικών Υπολογιστών, Εθνικό Μετσόβιο Πολυτεχνείο, 2014

[3] Goodle Drive,Dropbox,Box and iCloud Reach The Top 5 Cloud Storgage Security Breaches List, URL: https://psg.hitachi-solutions.com/credeon/blog/google-drive-dropbox-box-and-icloud-reach-the-top-5-cloud-storage-security-breaches-list, προσπελάστηκε στις 7/7/16

[4] Cloud Storage Pricing – Amazon Simple Storage Service (S3) - AWS, URL: https://aws.amazon.com/s3/pricing/, προσπελάστηκε στις 6/1/17

[5] Κ. Γιαννάκου,Μ. Κισσούδη,Π. Μαργώνη, “Δουλεύοντας στο σύννεφο.Δυνατότητες,λύσεις,προοπτικές του υπολογιστικού νέφους στην Ελληνική επιχειρηματικότητα”,Πτυχιακή εργασία,Τμήμα Διοίκησης Επιχειρήσεων,Τεχνολογικό Εκπαιδευτικό Ίδρυμα Δυτικής Ελλάδος,2015

[6] Ανοικτά Μαθήματα Συστήματα Παράλληλης & Κατανεμημένης Επεξεργασίας Ενότητα 14: cloud computing. Δρ. Μηνάς Δασυγένης.

[7] Externally - Hosted Private Cloud | Cynosure Solutions, URL: http://www.cynosure-solutions.com/blog/tag/externally-hosted-private-cloud/, προσπελάστηκε στις 6/8/16

[8] Top Five Challenges Of Cloud Computing, URL: http://cloudtweaks.com/2012/08/top-five-challenges-of-cloud-computing/, προσπελάστηκε στις 6/8/16

[9] David Linthicum, Greenpeace was wrong: The cloud is good for the environment.InfoWorld FROM IDG (2016) http://www.infoworld.com/article/3090562/cloud-computing/greenpeace-was-wrong-the-cloud-is-good-for-the-environment.html

[10] J.W Rittinghouse, J.F Ransome (2010).Cloud Computing Implementetion,Management and Security.CRC Press Taylor & Franis Group, pp.27-204

[11] ISACA Development Team (2013).VENDOR MANAGEMENT: Using COBIT 5.ISACA, pp.76-79

[12] L.Newcombe (2012).Securing Cloud Services: A pragmatic approach to security architecture in the cloud.IT Governance Publishing, pp.119-140

[13] Shucheng Yu, Wenjing Lou, Kui Ren, (2012). Securing Cyber-Physical Critical Infrastructure, Morgan Kaufmann, pp. 389-410

[14] Γ. Καμπουράκης (2014). Εισαγωγή στην Ασφάλεια Πληροφοριακών και Επικοινωνιακων Συστημάτων. Τμήμα Μηχανικών Πληροφοριακών & Επικοινωνιακών Συστημάτων, Πανεπιστήμιο Αιγαίου

[15] Kai Hwag Geoffrey.C Fox Jack J. Dongarra (2012). Distributed and Cloud Computing From Parallel Processing To Internet Of Things. China Machine Press, pp.49-50

[16] Hassen Mohammed Alsafi, Wafaa Mustafa Abduallah, Al-Sakib Khan Pathan (2012). IDPS: An Intrigrated Intrusion Handling Model for Cloud Computing Enviroment. International Islamic University Malaysia (IIUM),Department of Computer Science

[17] S.V. Narwane, S. L. Vaikol, A Survey on Intrusion Detection System for Cloud Computing Environment. International Journal of Computer Applications (0975 - 887) Volume 109 – No. 1,(2015) http://research.ijcaonline.org/volume109/number1/pxc3900573.pdf

[18] Μ. Λέρα, “Μελέτη Ασφάλειας Πληροφοριών Και Πληροφοριακών Συστημάτων” Διπλωματική εργασία, Τμήμα Μηχανικών Πληροφορικής και Τηλεπικοινωνιών,Πανεπιστήμιο Δυτικής Μακεδονίας, 2012

[19] IT security frameworks and standards: Choosing the right one, URL: http://searchsecurity.techtarget.com/tip/IT-security-frameworks-and-standards-Choosing-the-right-one, προσπελάστηκε στις 20/9/16

[20] Introduction to amazon elastic compute cloud (EC2) – Cloud Servers on AWS, URL: https://www.youtube.com/watch?v=Px7ZPLq4AOU , προσπελάστηκε στις 20/9/16

[21] Information Security Management System - Wikipedia, URL: https://en.wikipedia.org/wiki/Information_security_management_system, προσπελάστηκε στις 5/12/16

[22] Ronald L. Krutz and Rusell Dean Vines (2010). Cloud Security A Comprehensive Guide To Secure Cloud Computing. Wiley Publishing, Inc, pp.64-67

[23] EC2 Instance Pricing – Amazon Web Services (AWS), URL: https://aws.amazon.com/ec2/pricing/on-demand/, προσπελάστηκε στις 6/1/17

[24] Amazon Web Services - Wikipedia, URL: https://en.wikipedia.org/wiki/Amazon_Web_Services , προσπελάστηκε στις 6/1/17

[25] ISACA Development Team (2011). IT CONTROL OBJECTIVES for CLOUD COMPUTING: CONTROLS AND ASSURANCE IN THE CLOUD.ISACA, pp.36-112

[26] Ε. Καραμανλή, “Προσεγγίσεις,Πρότυπα και Πλαίσια Ασφάλειας στο τραπεζικό τομέα”, Μεταπτυχιακή διατριβή, Τμήμα Πληροφορικής, Πανεπιστήμιο Πειραιά, 2012.

[27] Ι. Θεοδωρόπουλος, “Σύγκριση τεχνολογιών cloud computing”, Διπλωματική εργασία, Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο Πειραιά.

[28] ISACA Development Team (2012). COBIT Implementation.ISACA, pp.19-20

[29] Breach-Level-Index-Report-H12016.pdf, URL: http://breachlevelindex.com/assets/Breach-Level-Index-Report-H12016.pdf, προσπελάστηκε στις 3/10/16

[30] Sailesh Gadia, ISACA Development Team. Cloud Computing Risk Assessment: A Case Study. ISACA(Volume 4)(2011) https://www.isaca.org/Journal/archives/2011/Volume-4/Pages/Cloud-Computing-Risk-Assessment-A-Case-Study.aspx

[31] The Principles of COBIT 5, URL: http://www.orbussoftware.com/resources/videos/cobit-distilled/the-principles-of-cobit-5/, προσπελάστηκε στις 27/11/16

[32] COBIT 5 Goals Cascade, URL: http://www.orbussoftware.com/resources/videos/cobit-distilled/cobit-5-goals-cascade/, προσπελάστηκε στις 27/11/16

[33] COBIT 5 Enablers, URL: http://www.orbussoftware.com/resources/videos/cobit-distilled/cobit-5-enablers/, προσπελάστηκε στις 28/11/16

[34] COBIT 5 Enabler Dimensions and Performance Management, URL: http://www.orbussoftware.com/resources/videos/cobit-distilled/cobit-5-enabler-dimensions-and-performance-management/ , προσπελάστηκε στις 27/11/16

[35] COBIT 5 Principle 1: Meeting Stakeholder Needs, URL: http://www.orbussoftware.com/resources/videos/cobit-distilled/cobit-principle-1-meeting-stakeholder-needs/, προσπελάστηκε στις 25/11/16

[36] COBIT 5 Principle 2: Covering the Enterprise from End to End, URL: http://www.orbussoftware.com/resources/videos/cobit-distilled/cobit-principle-2-covering-the-enterprise-end-to-end/, προσπελάστηκε στις 25/11/16

[37] COBIT 5 Principle 3: Applying a Single Integrated Framework, URL: http://www.orbussoftware.com/resources/videos/cobit-distilled/cobit-5-principle-3-applying-single-integrated-framework/, προσπελάστηκε στις 25/11/16

[38] COBIT 5 Principle 4: Enabling a Holistic Approach, URL: http://www.orbussoftware.com/resources/videos/cobit-distilled/cobit-5-principle-4-enabling-a-holistic-approach/, προσπελάστηκε στις 25/11/16

[39] COBIT 5 Principle 5: Separating Governance from Management, URL: http://www.orbussoftware.com/resources/videos/cobit-distilled/cobit-5-principle-5-separating-governance-from-management/, προσπελάστηκε στις 25/11/16

[40] ISACA Development Team (2012). COBIT 5 A Business Fremework for the Governance and Management of Enterprise IT.ISACA, pp.41-45

[41] Security Frameworks | Solutionary, URL: https://www.solutionary.com/solutions/compliance/security-frameworks/, προσπελάστηκε στις 5/12/16

[42] Intrution detection system in cloud computing, URL: http://searchcloudcomputing.techtarget.com/tip/Intrusion-detection-in-a-cloud-computing-environment, προσπελάστηκε στις 5/10/16

[43] J. Hurwitz, R. Bloor, M. Kaufman, F. Halper (2010). Cloud Computing FOR DUMMIES. Wiley Publishing, Inc, pp.8-9

[44] F. Greene, Selected COBIT 5 Processes for Essential Enterprise Security. ISACA Journal volume 2 (2015) https://www.isaca.org/Journal/archives/2015/Volume-2/Pages/selected-cobit-5-processes-for-essential-enterprise-security.aspx

[45] ISACA Development Team (2012). COBIT 5 FOR INFORMATION SECURITY.ISACA, pp.22-52

[46] AWS | Amazon SimpleDB – Simple Database Service, URL: https://aws.amazon.com/simpledb, προσπελάστηκε στις 20/3/17

[47] EC2 Instance Types – Amazon Web Services (AWS), URL: https://aws.amazon.com/ec2/instance-types/, προσπελάστηκε στις 20/3/17

[48] Managed Cloud DNS – Domain Name System – Amazon Route 53 | AWS, URL: https://aws.amazon.com/route53/, προσπελάστηκε στις 20/3/17

[49] ISACA Development Team (2013). COBIT 5 for Risk.ISACA, pp.13-112

[50] M. Ahronovitz, D. Amrhein (2009). Cloud Computing Use Cases White Paper Version 4.0. Cloud Computing Use Case Discussion Group, pp.23-24

[51] Is The Cloud Secure? – Smarter With Gartner, URL: http://www.gartner.com/smarterwithgartner/is-the-cloud-secure/, προσπελάστηκε στις 5/3/17

[52] The future of cloud computing: 5 predictions – Cloud computing news, URL: https://www.ibm.com/blogs/cloud-computing/2014/05/future-cloud-computing-5-predictions/, προσπελάστηκε στις 5/3/17

[53] J. Mullich, 16 Ways The Cloud Will Change Our Lives. The Wall Street Journal(2011) http://online.wsj.com/ad/article/cloudcomputing-changelives

[54] Identity and Access Management (IAM) – Amazon Web Services (AWS), URL: https://aws.amazon.com/iam/, προσπελάστηκε στις 3/15/17

(Κενό φύλλο)