Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή
στα Πληροφοριακά και Επικοινωνιακά Συστήματα

Πλάνο Ανάκαμψης από Καταστροφή με Χρήση Διεθνών Προτύπων και Συγκριτική Αξιολόγηση Δωρεάν Εργαλείων Αποκατάστασης Λειτουργικότητας Εικονικών Υποδομών

Κωνσταντίνος Τσιαγάς

Επιβλέπων Καθηγητής
Δρ. Σταύρος Σιαηλής

Σεπτέμβριος 2015

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Πλάνο Ανάκαμψης από Καταστροφή με Χρήση Διεθνών Προτύπων και Συγκριτική Αξιολόγηση Δωρεάν Εργαλείων Αποκατάστασης Λειτουργικότητας Εικονικών Υποδομών

Κωνσταντίνος Τσιαγάς

Επιβλέπων Καθηγητής
Δρ. Σταύρος Σιαηλής

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση

μεταπτυχιακού τίτλου σπουδών
στα Πληροφοριακά Συστήματα

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

Σεπτέμβριος 2015

Περίληψη

Η εξάρτηση των σύγχρονων επιχειρήσεων από το Πληροφοριακό τους Σύστημα αυξάνεται με ταχείς ρυθμούς την τελευταία δεκαετία. Εν τούτοις έρευνες δείχνουν ότι η ασφάλεια των δεδομένων εξακολουθεί να μην θεωρείται από πολλούς ως αναγκαιότητα. Αρκετά συχνά, τα επίπεδα ασφάλειας είναι μηδαμινά έως ανύπαρκτα, αν αναλογιστούμε τις συνέπειες από μια καταστροφή.

Τα προηγούμενα χρόνια οι εταιρίες συνήθιζαν να διαχειρίζονται μια καταστροφή όταν αυτή συνέβαινε και δεν ενδιαφέρονταν για κάποιο είδος πρόληψης. Αυτό φαίνεται να αλλάζει πλέον, με μια τάση στις εταιρίες να καταστρώνουν πολύπλοκα σχέδια διαχείρισης καταστροφών έτσι ώστε να εξασφαλίσουν επιχειρησιακή συνέχεια των Πληροφοριακών Συστημάτων τους. Ο λόγος που τα Disaster Recovery Plans (DRPs) δεν είναι ακόμα αναπόσπαστα κομμάτια των διαδικασιών των εταιριών, είναι γιατί ακόμα δεν έχουν αντιληφθεί πλήρως το μέγεθος του ρίσκου και σε πολλές περιπτώσεις υπάρχει ασαφή εικόνα σχετικά με την ευθύνη της ασφάλειας των δεδομένων τους αν αναλογιστεί κανείς το κόστος για κάθε ώρα μη διαθεσιμότητας των υπηρεσιών μιας επιχείρησης.

Ένα σχέδιο ανάκαμψης από καταστροφή είναι ένα πλάνο ενεργειών και βημάτων που υιοθετεί μια εταιρία, με σκοπό την πρόληψη πιθανού σεναρίου καταστροφής το οποίο θα την καθιστούσε μη λειτουργική. Είναι ένα πλάνο – οδηγός για την γρηγορότερη ανάκαμψη σε περίπτωση καταστροφής. Ίσως επειδή οι εταιρείες δεν έχουν βιώσει τέτοια κατάσταση, είναι επιφυλακτικές στη δαπάνη ενός σημαντικού χρηματικού ποσού για την δημιουργία ενός DR plan. "Ένας άλλος λόγος πάλι είναι γιατί το θεωρούν ότι είναι ένα εξαιρετικά ακραίο (απίθανο) σενάριο μη μπορώντας να καταλάβουν δεν δαπανούν μέρος του κεφαλαίου τους, αλλά επενδύουν σε αυτό!

Βασικός στόχος αυτής της διατριβής είναι η μελέτη, ο καθορισμός των ελέγχων και η υλοποίηση ενός Disaster Recovery Plan για εικονικές υποδομές με χρήση δωρεάν εργαλείων, δηλαδή πρακτικά με μηδενικό κόστος. Αφορά κυρίως τηλεπικοινωνιακούς παρόχους με απώτερο σκοπό να επιτευχθεί επιχειρησιακή συνέχεια στις υποδομές τους και να μειωθεί στο ελάχιστο ο χρόνος ανάκαμψης από καταστροφή.

Summary

The reliance of modern businesses from Information Systems has grown rapidly over the last decade. Researchers show that while the technology concerning the validity and effectiveness is progressing rapidly, the safety of systems is still considered as a necessity. In addition, many companies persist to act when a disaster arrives instead of being prepared by creating a business continuity plan, which will serve as a means of prevention. Meanwhile, the gap between increased security risks and companies efforts to mitigate them continues to widen.

This seems to be transforming and now there is a tendency for companies to lay out sophisticated disaster management plans in order to ensure business continuity of their Information Systems. The reason that Disaster Recovery Plans (DRPs) are still not integral parts of corporate processes, is because companies did not realized the significance of the risk and in many cases they have vague view of data security. This is surprising if you consider the cost per hour for unavailability of a business service.

A disaster recovery plan is a plan, or lets say a guide, of actions and steps that a company adopts to prevent possible disaster and prevent it from being inoperant. Because of the fact that companies have not experienced any similar situation in the past, they are reluctant to spend such a substantial budget for disaster recovery plan creation. Additionally they are considering that this event is rather fictionary, so they don't think to invest to a DR plan that is more like an investment instead of an expense.

The main objective of this thesis is the research, the definition of controls and finally the implementation of a Disaster Recovery Plan for virtual infrastructure environments, using freeware tools, in order to achieve recovery of critical services with no expense at all. The main target of this plan is telecommunications companies, with a view to achieve business continuity in their virtual IT infrastructure and minimize the disaster recovery time, but can be also be adapted by other Companies in a different field of activity.

Ευχαριστίες

Σε αυτό το σημείο θα ήθελα να ευχαριστήσω την οικογένειά μου για την πολύτιμη βοήθεια και στήριξη που μου πρόσφερε καθ' όλη τη διάρκεια των μεταπτυχιακών μου σπουδών.

Στη συνέχεια θα ήθελα να ευχαριστήσω ιδιαιτέρως τον καθηγητή μου Δρ. Σταύρο Σιαηλή διότι η καθοδήγησή του και το αμείωτο ενδιαφέρον του βοήθησαν τα μάλλα στην εκπλήρωση του έργου μου.

Πολύτιμη συνεισφορά στο έργο μου παρείχε ο συνάδελφος μου Νίκος Φυτάς με τις πάντα εύστοχες παρατηρήσεις του κατά τη διάρκεια των πειραμάτων.

Τέλος νιώθω την υποχρέωση να ευχαριστήσω τη σύζυγό μου Ευγενία Αιμιλιανίδου για την ηθική υποστήριξη που μου παρείχε σε δύσκολες περιόδους των σπουδών μου.

Περιεχόμενα

Περιεχόμενα Εικόνων

Περιεχόμενα Πινάκων

Κεφάλαιο 1
Εισαγωγή

Η εξάρτηση των σύγχρονων επιχειρήσεων από τα Πληροφοριακά Συστήματα αυξάνεται με ταχείς ρυθμούς κατά την τελευταία δεκαετία. Εν τούτοις έρευνες δείχνουν η ασφάλεια των δεδομένων εξακολουθεί να μην θεωρείται από πολλούς ως μια αναγκαιότητα. Αρκετά συχνά, τα επίπεδα ασφάλειας είναι μηδαμινά έως ανύπαρκτα, αν αναλογιστούμε τις συνέπειες από μια καταστροφή. Με τον όρο «Πληροφοριακό Σύστημα» (Information System), εννοούμε το σύνολο των διαδικασιών και των αυτοματοποιημένων υπολογιστικών συστημάτων, τα οποία προορίζονται για τη συλλογή, εγγραφή, ανάκτηση, επεξεργασία, αποθήκευση και ανάλυση δεδομένων. Τα συστήματα αυτά περιλαμβάνουν λογισμικό (software) και υλικό μέρος (hardware) [42].

Τα προηγούμενα χρόνια οι εταιρίες συνήθιζαν περισσότερο να διαχειρίζονται μια καταστροφή όταν αυτή συνέβαινε, αντί να επενδύσουν σε κάποιο είδος πρόληψης. Αυτό όμως φαίνεται να αλλάζει και πλέον υπάρχει η τάση οι εταιρίες να καταστρώνουν πολύπλοκα σχέδια διαχείρισης μιας καταστροφής έτσι ώστε να εξασφαλίσουν επιχειρησιακή συνέχεια των Πληροφοριακών Συστημάτων τους.
Ο λόγος που τα Disaster Recovery Plans (DRPs) δεν είναι ακόμα αναπόσπαστα κομμάτια των διαδικασιών των εταιριών, είναι διότι ακόμα δεν έχουν αντιληφθεί πλήρως το μέγεθος του ρίσκου και σε πολλές περιπτώσεις έχουν ασαφή εικόνα σχετικά

με την ευθύνη της ασφάλειας των δεδομένων τους. Και αυτό είναι αξιοπερίεργο αν αναλογιστεί κανείς το κόστος για κάθε ώρα μη διαθεσιμότητας των υπηρεσιών μιας επιχείρησης.

Ένα σχέδιο ανάκαμψης από καταστροφή είναι ένα πλάνο ενεργειών και βημάτων που υιοθετεί μια εταιρία, με σκοπό να προλάβει ένα πιθανό σενάριο που θα την καθιστούσε μη λειτουργική εξαιτίας κάποιας καταστροφής. Επίσης είναι και ένα πλάνο – οδηγός για την όσο το δυνατόν γρηγορότερη ανάκαμψη από μια τέτοια κατάσταση. Οι εταιρίες δεν είναι θετικές στο ενδεχόμενο να δαπανήσουν ένα σημαντικό χρηματικό κεφάλαιο για την δημιουργία ενός DR plan, ίσως επειδή δεν έχουν βιώσει κάποια τέτοια κατάσταση ή επειδή νομίζουν ότι είναι ένα εξαιρετικά ακραίο (άρα και απίθανο) σενάριο, αγνοώντας ότι επί της ουσίας δεν δαπανούν μέρος του κεφαλαίου τους, αλλά επενδύουν πάνω σε αυτό γιατί τα δεδομένα κάθε εταιρίας είναι απείρως σημαντικότερα από το H/W.

1.1 Δομή της Διατριβής

Η παρούσα διατριβή αναπτύσσεται σε 6 κεφάλαια και 1 παράρτημα. Το πρώτο κεφάλαιο περιέχει μια σύντομη ιστορική αναδρομή της έννοιας Ανάκαμψη από Καταστροφή (Disaster Recovery), μια σύντομη παρουσίαση των εικονικών υποδομών και μια αρχιμή γνωριμία με την Επιχειρησιακή Συνέχεια (Business Continuity). Στο τέλος του κεφαλαίου αναφέρονται οι στόχοι της διατριβής και η καινοτομία της.
Στο δεύτερο κεφάλαιο ακολουθεί ανάλυση των εννοιών Επιχειρησιακής Συνέχειας (Business Continuity – BC) και Πλάνου Ανάκαμψης από καταστροφή (Disaster Recovery Plan – DRP). Επιπροσθέτως γίνεται αναφορά σε ISO σχετικά με disaster recovery, καθώς επίσης και σε προσπάθειες άλλων προτύπων. Κλείνοντας το κεφάλαιο, σχολιάζονται DR plans άλλων οργανισμών και αιτιολογούνται οι εν γένει συνήθεις λόγοι αποτυχίας ενός πλάνου.
Στο τρίτο κεφάλαιο μελετώνται τα σημεία ελέγχου (controls) των ISO του προηγούμενου κεφάλαιου και προτείνονται αυτά τα οποία πληρούν τις ανάγκες ενός τηλεπικοινωνιακού παρόχου.
Στο τέταρτο κεφάλαιο πραγματοποιείται υλοποίηση των σημείων ελέγχου του προτεινόμενου DR plan και δοκιμάζονται δωρεάν εργαλεία που προσφέρουν υπηρεσίες ανάκαμψης από καταστροφή.
Στο πέμπτο κεφάλαιο παρουσιάζονται τα χαρακτηριστικά των εργαλείων που δοκιμάστηκαν, οι συγκεντρωτικοί πίνακες και τα γραφήματα των επιδόσεών τους.

Φτάνοντας στο τέλος της διατριβής, στο έκτο κεφάλαιο αναφέρονται τα συμπεράσματα που εξάχθησαν από τις μετρήσεις του προηγούμενου κεφαλαίου και προτείνονται ιδέες για πιθανές μελλοντικές επεκτάσεις της παρούσας εργασίας.

1.2 Ιστορικό υπόβαθρο

Disaster Recovery είναι όλες οι πολιτικές και οι διαδικασίες σχετικά με την προετοιμασία ανάκαμψης ή την επιχειρησιακή συνέχεια μετά από καταστροφή της υποδομής ενός Datacenter. Η βιωσιμότητα του datacenter κρίνεται ζωτικής σημασίας για μια επιχείρηση. Για αυτόν τον λόγο χρειάζεται πλάνο όσον αφορά την υποδομή των Πληροφοριακών Συστημάτων (IT systems).

Η ανάγκη κάποιας μορφής επιχειρησιακής συνέχειας (business continuity), με χρήση πλάνου ανάκαμψης από καταστροφή (Disaster Recovery Plan – DRP), άρχισε να γίνεται αντιληπτή την δεκαετία του ’60. Από εκείνη την εποχή είχαν αρχίσει να συνειδητοποιούν ότι όσο αναπτύσσονταν οι υποδομές των Πληροφοριακών Συστημάτων, τόσο περισσότερο αυτές γίνονταν «μοναδικά σημεία αποτυχίας» (Single Point of Failure – SPOF). Διαπίστωσαν επίσης ότι ενδεχόμενη διακοπή των υπηρεσιών αυτών των συστημάτων θα είχε σημαντικές συνέπειες στην λειτουργία των εταιριών. Την δεκαετία του ’70 οι μηχανικοί συστημάτων της εποχής είχαν καταφέρει να αποκτήσουν υποτυπώδεις γνώσεις πάνω στον τομέα της επιχειρησιακής συνέχειας. Στην προσπάθειά τους να καταστήσουν τις υποδομές τους περισσότερο ανθεκτικές σε κινδύνους φτάσαμε στη δεκαετία του ’80 η IBM να κατασκευάζει mainframes με διπλό επεξεργαστή (System 360 model 67) για μεγαλύτερη αξιοπιστία. Η σημασία της Επιχειρησιακής Συνέχειας εδραιώθηκε και αναπτύχθηκε με το πέρασμα των χρόνων φτάνοντας το 1990 να αναγνωρίζεται η ανάκαμψη από καταστροφή ως αναγκαιότητα και μοναδική λύση ανάκτησης υπηρεσιών και δεδομένων στο σημείο που ήταν πριν συμβεί η καταστροφή [10].

Εκείνη τη δεκαετία υπήρχε έντονα αυτή η ανάγκη καθώς εισήλθαν στο προσκήνιο οι real-time processing υπολογιστές. Αμέσως συνειδητοποίησαν ότι αν προηγουμένως είχαν ανάγκη από DR, τώρα αυτή η ανάγκη ήταν ακόμα πιο έντονη. Επιπροσθέτως είδαν ότι η έννοια και η χρησιμότητα ενός πλάνου DR θα μπορούσε να εφαρμοσθεί όχι μόνο στον τομέα των πληροφοριακών συστημάτων, αλλά γενικότερα στον επιχειρηματικό κλάδο. Με την είσοδο του internet και την ραγδαία διάδοση και

εκμετάλλευση του, αυτή η ανάγκη έγινε προτεραιότητα. Πλέον κάθε επιχείρηση που ήθελε να πρωταγωνιστήσει σε επιχειρηματικό επίπεδο, ήταν υποχρεωμένη να θέσει ως στόχο 99% διαθεσιμότητα των υπηρεσιών της, ποσοστό το οποίο ήταν αδιανοήτο τα προηγούμενα χρόνια!

Φτάνοντας στο σήμερα, διαπιστώνουμε ότι η επιχειρησιακή συνέχεια (business continuity), είναι κάτι που κάθε εταιρία πρέπει να παρέχει στους πελάτες της. Αποτελεί διασφάλιση των υπηρεσιών της και δέσμευση προς τους πελάτες της, πως οτιδήποτε προκύψει, η εταιρία θα είναι σε θέση να παρέχει ανελλιπώς υπηρεσίες. Ο βαθμός υλοποίησης ενός άρτιου DRP, πλήρως λειτουργικού ανά πάσα στιγμή, είναι ένα μεγάλο στοίχημα τόσο λόγω σχεδίασης, όσο και επιλογής εύστοχων αποφάσεων ανάκαμψης. Προϋποθέτει επιτυχείς προβλέψεις σεναρίων μετάβασης και ανάκαμψης.

1.3 Τι είναι εικονικές υποδομές (virtual datacenters)

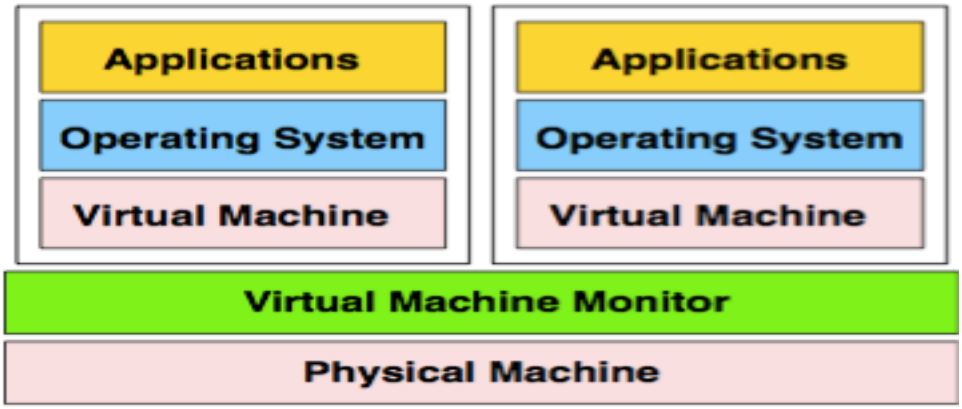
Η τεχνολογία των εικονικών μηχανών δεν είναι κάποια νέα τεχνολογία που ήρθε στο προσκήνιο ξαφνικά. Υπήρχε σε πρώιμο στάδιο από τη δεκαετία του 70 έως ότου γνωρίσει τεράστια άνθηση και κάνει αισθητή την παρουσία της στις αρχές του 2000. Ενδεικτικά να αναφέρουμε ότι πλέον οι εικονικοί εξυπηρετητές (virtual servers), παγκοσμίως ξεπερνούν σε πλήθος τους φυσικούς. Μια εικονική μηχανή (virtual machine –vm) είναι μια διεργασία (proccess) σε κάποιον φυσικό εξυπηρετητή (physical host ή αλλιώς hypervisor) η οποία αναπαριστά μια εικονική ύπαρξη (instance) ενός πραγματικού εξυπηρετητή. Κάθε εικονική μηχανή έχει το δικό της λειτουργικό σύστημα, φιλοξενεί μία ή περισσότερες εφαρμογές και συμπεριφέρεται σαν ένας εντελώς ανεξάρτητος υπολογιστής, χωρίς η μία μηχανή να γνωρίζει την ύπαρξη άλλων [37].
Κάθε εικονική μηχανή μέσω προσομείωσης έχει ένα πλήρες σύνολο εικονικών υλικών (virtual hardware) όπως επεξεργαστή (vCPU), μνήμη (vRAM), κάρτα δικτύου (vm NIC) εικονικό σκληρό δίσκο κλπ. Αυτό επιτυγχάνεται χρησιμοποιώντας ένα σύνολο οδηγών (drivers) οι οποίοι είναι συμβατοί με διαφορετικά είδη υλικού [39].

Οι οδηγοί είναι ενσωματωμένοι στην εικονική μηχανή και μπορούν να χρησιμοποιηθούν σε διαφορετικές συνθέσεις υλικού. Ολόκληρη η εικονική σύνθεση του υλικού (virtual hardware configuration), αποθηκεύεται σε αρχείο με κατάληξη .vmx έτσι ώστε ανά

πάσα στιγμή ο hypervisor να γνωρίζει τι περιέχει η κάθε εικονική μηχανή. Όταν μια εικονική μηχανή ξεκινάει, ένα συγκεκριμένο ποσοστό υπολογιστικής ισχύος (CPU), μνήμης (RAM) και χωρητικότητας δίσκου (HDD) του hypervisor ανατίθενται αυτόματα από τον hypervisor στη μηχανή και παράλληλα δημιουργείται το αντίστοιχο proccess το οποίο παραμένει ενεργό για όσο διάστημα παραμένει σε λειτουργία η εικονική μηχανή [37].

'Οπως προείπαμε κάθε μηχανή λειτουργεί σε απομονωμένο περιβάλλον. Μέσω αυτής της τεχνολογίας πετυχαίνουμε τη συγχώνευση πολλών μηχανών στο ίδιο H/W αξιοποιώντας σε μέγιστο βαθμό τους διαθέσιμους πόρους, και λόγω του ότι μπορούμε να δημιουργήσουμε κλώνους των μηχανών αυτών αυξάνουμε τη διαθεσιμότητα υπηρεσιών και εφαρμογών, συμβάλλοντας στην εξασφάλιση της υψηλής διαθεσιμότητας και επαναφοράς από καταστροφή. Το τελευταίο είναι και το ποιο σημαντικό διότι απλουστεύει τις λύσεις αποκατάστασης σε περίπτωση καταστροφής (DR), καθώς είναι πλέον ευκολότερη η εφαρμογή δοκιμών με άμεσα και αξιόπιστα αποτελέσματα δίχως να απαιτούνται τεράστιοι υπολογιστοί πόροι και υποδομές. Μέσω της υιοθέτησης της εικονικοποίησης λοιπόν προσφέρεται εξοικονόμηση πόρων, ενέργειας και κατ' επέκταση μείωση του κόστους των υποδομών [32].

Στο επόμενο σχήμα βλέπουμε μια τυπική τοπολογία δύο εικονικών μηχανών στον ίδιο Hypervisor [39]. Βλέπουμε ότι κάθε μηχανή έχει το δικό της λειτουργικό σύστημα και φιλοξενεί τις δικές της εφαρμογές. Είναι ξεκάθαρο ότι κάθε εικονική μηχανή είναι πλήρως απομονωμένη από τις υπόλοιπες.



Εικόνα 1. 1: Τυπική τοπολογία εικονικών μηχανών

1.4 Σύντομη αναφορά σε business continuity – business continuity management system

Πρόσφατες φυσικές καταστροφές, περιβαλλοντικά ατυχήματα, τεχνολογικές αστοχίες και κρίσεις προερχόμενες από ανθρώπινες ενέργειες έχουν δείξει ότι σοβαρά περιστατικά είναι δυνατό να συμβούν ανά πάσα στιγμή, επηρεάζοντας τόσο τις επιχειρήσεις του δημοσίου όσο και του ιδιωτικού τομέα. Η πρόκληση ξεφεύγει από τα στενά πλαίσια υιοθέτησης ενός πρόχειρου σχεδίου αντιμετώπισης έκτακτων αναγκών.

Οργανισμοί κάθε μεγέθους και τύπου είναι αναγκασμένοι εκ των πραγμάτων να υιοθετήσουν μια ολοκληρωμένη πολιτική για την πρόληψη, την προστασία, την ετοιμότητα, και την ανταπόκριση όσον αφορά την ανάκαμψη από καταστροφή και τελικά την επιχειρησιακή συνέχεια της εταιρίας τους. Δεν είναι πλέον αρκετό η εφαρμογή ενός πρόχειρου πλάνου αντιμετώπισης το οποίο απλώς θα ελαχιστοποιεί τις συνέπειες της διακοπής, αλλά θα πρέπει οι εταιρίες να λαμβάνουν και προληπτικά μέτρα προσαρμοσμένα στις ανάγκες τους, έτσι ώστε να ελαχιστοποιείται η πιθανότητα διακοπής. Οι σημερινοί κίνδυνοι απαιτούν τη δημιουργία συνεχώς εξελισσόμενων διαδικασιών οι οποίες θα διασφαλίζουν την επιβίωση και τη σταθερότητα των βασικών δραστηριοτήτων ενός οργανισμού, πριν, κατά τη διάρκεια, και μετά το πέρας ενός συμβάντος.

Η ικανότητα ενός οργανισμού να ανακτά τις υπηρεσίες του μετά από μια καταστροφή είναι άμεσα συνδεδεμένη με το επίπεδο σχεδιασμού της επιχειρηματικής συνέχειας μέσω του πλάνου που έχει εκπονηθεί πριν από την καταστροφή. Μελέτες δείχνουν ότι δύο στις πέντε επιχειρήσεις που έχουν βιώσει κάποιου είδους καταστροφή δεν θα μπορέσουν να ανταπεξέλθουν στη συνέχεια, και τελικά θα κλείσουν εντός πέντε ετών από το συμβάν [14].

Τα σχέδια επιχειρησιακής συνέχειας είναι ζωτικής σημασίας για την απρόσκοπτη λειτουργία κάθε επιχείρησης. Το πιο σημαντικό όμως είναι ότι τα σχέδια αυτά αποκτούν όλο και μεγαλύτερη σπουδαιότητα καθώς οι εταιρείες εξαρτώνται όλο και περισσότερο από τα πληροφοριακά τους συστήματα για την διεκπεραίωση των επιχειρηματικών διεργασιών τους.

Έρευνα της Gartner δείχνει ότι ακόμα η μικρή διάρκεια διακοπής υπηρεσιών (downtime) είναι καταστροφική [45]. Παρόλα αυτά πολλοί οργανισμοί είναι διστακτικοί στην υϊοθέτηση ενός πλήρους πλάνου ανάκαμψης από καταστροφή. Ο λόγος φαίνεται να είναι αφενός οι απαιτητικές τεχνικές γνώσεις για την υλοποίηση τέτοιων πλάνων, αφετέρου το κόστος της υλοποίησης το οποίο ίσως κρίνεται υπερβολικά υψηλό. Όλες αυτές οι ανησυχίες είναι κατανοητές και αποδεκτές αλλά υπάρχουν προτάσεις λύσεων επιχειρησιακής συνέχειας οι οποίες μπορούν να υπερκεράσουν τις όποιες ενστάσεις, προφέροντας λύσεις χαμηλού έως και μηδενικού κόστους, τεχνικά εύκολη υλοποίηση, χρησιμοποιώντας εργαλεία τα οποία διατίθενται δωρεάν.

1.5 Στόχοι διατριβής – αναφορά καινοτομίας

Έχοντας όλα τα παραπάνω υπόψη, ο στόχος αυτής της διατριβής είναι η μελέτη, ο καθορισμός συγκεκριμένων ελέγχων βασισμένων σε διεθνή πρότυπα, η κατάθεση προτεινόμενου Disaster Recovery Plan για εικονικές υποδομές τηλεπικοινωνιακών παρόχων καθώς και η υλοποίησή του με χρήση δωρεάν εργαλείων, δηλαδή πρακτικά με μηδενικό κόστος. Όσον αφορά το μηδενικό κόστος, αναφερόμαστε μόνον σε λογισμικά προϊόντα τα οποία παρέχονται δωρεάν, δηλαδή σε εργαλεία τα οποία δεν χρειάζεται να αγοραστούν από τις επιχειρήσεις. Προφανώς μια IT υποδομή (είτε είναι DR είτε όχι), δεν είναι μηδενικού κόστους end-to-end. Το κτίριο που θα χρησιμοποιηθεί, η υποδομή σε ρεύμα και κλιματισμό, οι servers, το storage, το δίκτυο, το εργατικό προσωπικό, ακόμα και τα αναλώσιμα έχουν κόστος. Το μηδενικό κόστος άπτεται μόνον στις υπηρεσίες ανάκαμψης από καταστροφή που προσφέρουν τα διάφορα λογισμικά.

Αναλογιζόμενοι το γεγονός ότι τα σύγχρονα Πληροφοριακά Συστήματα φιλοξενούν τις πιο κρίσιμες και σημαντικές υπηρεσίες μιας εταιρίας, όπως διαχείριση πελατολογίου, τιμολόγηση, cloud services, IPTV, καθίσταται σαφές ότι το κόστος σε περίπτωση καθολικής απώλειας λειτουργίας του datacenter ανέρχεται σε χιλιάδες ευρώ για κάθε ώρα μη διαθεσιμότητας. Όπως προκύπτει λοιπόν, η εκπόνηση ενός πλήρους DRP αποτελεί σημαντικότατη επένδυση.

Υπάρχουν τρία ουσιώδη ζητήματα τα οποία θα προσπαθήσουμε να αναλύσουμε. Το πρώτο σχετίζεται με το αν πρέπει οι εταιρίες να εκπονούν disaster recovery plans, και το δεύτερο σχετίζεται με τη διαπίστωση ότι κάτι τέτοιο θα βελτιώσει τους χρόνους ανάκαμψης των υποδομών των Πληροφοριακών Συστημάτων μετά από καταστροφή. Το τρίτο έχει να κάνει με τα εργαλεία που μπορούν να χρησιμοποιηθούν για το σκοπό αυτό. Ποια τα πλεονεκτήματα και μειονεκτήματα του καθενός και αν οι δωρεάν ή ανοικτού κώδικα λύσεις μπορούν να καλύψουν τις εταιρικές ανάγκες με ταυτόχρονη μείωση του κόστους.

Η υλοποίηση ενός πλήρους DRP για μεγάλους οργανισμούς και συγκεκριμένα τηλεπικοινωνιακούς παρόχους είναι αρκετά δύσκολη διαδικασία τόσο λόγω σχεδίασης, όσο και επιλογής εύστοχων αποφάσεων ανάκαμψης. Προϋποθέτει επιτυχείς προβλέψεις σεναρίων μετάβασης και ανάκαμψης. Οι τηλεπικοινωνιακοί πάροχοι πλέον εκτός από τις παραδοσιακές υπηρεσίες (τηλεφωνία, internet), παρέχουν νέες τεχνολογίες αιχμής, όπως Cloud Services, IPTV. Όλες οι νέες υπηρεσίες είναι υλοποιημένες σε εικονικές υπολογιστικές μηχανές (virtual servers). Ως εκ τούτου δεν υπάρχει Disaster Recovery σχεδιασμένο να καλύπτει εξ' ολοκλήρου αυτές τις νέας τεχνολογίας υποδομές. Η λύση που προτείνεται είναι η μελέτη και εκπόνηση ενός DR για εικονικά Πληροφοριακά Συστήματα, κάνοντας χρήση και σύγκριση δωρεάν εργαλείων κατάλληλα για Disaster Recovery. Αναλυτικότερα:

1. Για πρώτη φορά θα παρουσιαστούν συγκριτικά στοιχεία των εργαλείων DR, όσον αφορά τους χρόνους ανάκαμψης, το overhead σε υπολογιστικούς πόρους, την ευκολία εγκατάστασης και συντήρησης.
2. Μέσω των συγκεκριμένων εργαλείων θα έχουμε για πρώτη φορά την δυνατότητα προγραμματισμένου migration υπηρεσιών. Θα είναι εφικτό να μεταφέρονται υπηρεσίες στο DR site όποτε κρίνεται σκόπιμο, πχ για λόγους συντήρησης. Αυτό είναι πολύ σημαντικό διότι μέχρι τώρα κάθε DR site καθίσταται «ανενεργό» έως ότου (και αν ποτέ), εφαρμοστεί κάποιο DR plan.
3. Για πρώτη φορά δίνεται η δυνατότητα για "point-in-time" recovery. Δηλαδή για ανάκτηση δεδομένων σε μια συγκεκριμένη χρονική στιγμή στο παρελθόν.

Επιπρόσθετα δύναται να αποτελέσει οδηγό και σημείο αναφοράς για μελλοντικές επεκτάσεις ή για εκ του μηδενός υλοποιήσεις DR plans σε Virtual Datacenters άλλων εταιριών και να βοηθήσει στη μείωση κόστους των εταιριών για επιχειρησιακή συνέχεια.

Κεφάλαιο 2

Business Continuity – Disaster Recovery Plan

Η εξάρτηση των σύγχρονων επιχειρήσεων από τα Πληροφοριακά Συστήματα έχει αυξηθεί με ταχείς ρυθμούς κατά την τελευταία δεκαετία. Και όμως έρευνες συνεχίζουν να δείχνουν ότι, ενώ η τεχνολογία όσον αφορά την ισχύ και την αποτελεσματικότητα προχωρεί με γρήγορο ρυθμό, η ασφάλεια συστημάτων εξακολουθεί να μην θεωρείται από πολλούς ως μια αναγκαιότητα. Αρκετά συχνά, αυτό απέχει πολύ από τα αποδεκτά επίπεδα αν συνυπολογίσουμε τις συνέπειες που θα υπάρξουν αν τα συστήματα που αποσκοπεί να προστατεύσει εκτεθούν σε κίνδυνο.

Επιπλέον, πολλές εταιρείες εξακολουθούν μάλλον να δρουν όταν φτάσει η καταστροφή, αντί να είναι προετοιμασμένες μέσω της δημιουργίας ενός σχεδίου επιχειρησιακής συνέχειας, το οποίο θα χρησιμεύει ως μέσο πρόληψης. Υποστηρίζεται αφενός ότι αυτό οφείλεται στη χαμηλή ευαισθητοποίηση σχετικά με τους κινδύνους, αφετέρου ότι σε πολλές περιπτώσεις, η ευθύνη για την ασφάλεια είναι θολή και ασαφής. Είναι δύσκολο να κατανοήσει κανείς την προφανή έλλειψη ενδιαφέροντος, δεδομένου ότι πάνω από το

ήμισυ των επιχειρήσεων που παρέχουν δεδομένα δείχνουν ότι μία (1) ώρα διακοπής των εργασιών τους κοστίζει περισσότερα από 50 χιλιάδες δολάρια [14].
Εν τω μεταξύ, το χάσμα μεταξύ των αυξημένων κινδύνων για την ασφάλεια και το τι κάνουν οι εταιρείες για την αντιμετώπισή τους εξακολουθεί να διευρύνεται. Η πολύπλοκη και πολυεπίπεδη συνεργασία μεταξύ των εταιρειών έχει αυξηθεί σε τέτοιο βαθμό, ώστε τα ζητήματα ασφαλείας δεν επηρεάζουν πλέον μόνο μία εταιρεία, αλλά και τους επιχειρηματικούς εταίρους της.
Τώρα τελευταία φαίνεται μια στροφή στην ασφάλεια των συστημάτων δεδομένου και των περιστατικών που έχουν αναφερθεί κατά καιρούς σχετικά με ιούς και κακόβουλο λογισμικό, φυσικές καταστροφές και τρομοκρατικές επιθέσεις.

Είναι λοιπόν πασιφανές ότι η αποκατάσταση από καταστροφή καθώς και η επιχειρησιακή συνέχεια είναι τρομακτικές προκλήσεις για κάθε οργανισμό. Πόσο δε μάλλον μετά την συνεχή αύξηση του πλήθους των απειλών και των επιθέσεων και σε μια περίοδο όπου η ανταγωνιστικότητα σε επιχειρηματικό επίπεδο είναι στο μέγιστο σημείο, είναι σημαντικό ένας οργανισμός να είναι προετοιμασμένος και να έχει την ικανότητα να αντέξει σε ενδεχόμενη καταστροφή. Κάνοντας χρήση των διαδικασιών ανάκαμψης μπορούμε να επαναφέρουμε δεδομένα που έχουν καταστραφεί και να ανακτήσουμε πάλι την πρόσβαση σε υλικό και λογισμικό έτσι ώστε να μπορέσει ο οργανισμός να επιστρέψει σε κανονικές συνθήκες λειτουργίας. Μια υλοποίηση αποκατάστασης από καταστροφή με χρήση τεχνολογιών εικονικοποίησης (virtualization) η οποία προσδίδει επιπλέον ευελιξία, με παράλληλη μείωση του κόστους, ενώ επιπρόσθετα μειώνει τη χρήση του hardware κάνοντας πιο εύκολες και απλές τις διαδικασίες ανάκτησης[14].

2.1 Business Continuity

Επιχειρησιακή Συνέχεια (Business Continuity – BC), είναι η ικανότητα ενός οργανισμού να διατηρήσει ανέπαφες τις υπηρεσίες του όταν πληγεί από μια καταστροφή ή στο χειρότερο σενάριο να έχει όσο το δυνατόν πιο σύντομη διακοπή υπηρεσιών. Μέσω της Διαχείρισης Επιχειρησιακής Συνέχειας (Business Continuity Management – BCM) και εννοούμε μέσω των διαδικασιών διαχείρισης πιθανών κινδύνων, διασφαλίζεται ότι οι πιο σημαντικές υπηρεσίες θα είναι διαθέσιμες σε όλους όσοι θελήσουν να κάνουν χρήση αυτών. Επίσης συνεισφέρει και στη πρόληψη των περιστατικών εκείνων που οδηγούν

σε διακοπή υπηρεσιών και διεργασιών. Η επιχειρησιακή συνέχεια δεν είναι κάτι που υλοποιείται όταν εμφανιστεί μια καταστροφή, αλλά αφορά ενέργειες οι οποίες εκτελούνται σε καθημερινή βάση με στόχο τη διατήρηση των υπηρεσιών, την επάρκεια αυτών και την ικανότητα ανάκτησης. Τα σχέδια επιχειρησιακής Συνέχειας βοηθούν τον οργανισμό να διασφαλίσει τη διαθεσιμότητα των περισσότερο σημαντικών υπηρεσιών του και να μειώσει όσο είναι δυνατό τη ζημιά σε επιχειρηματικό επίπεδο [18].

Η διαχείριση επιχειρησιακής συνέχειας αφορά τη μείωση των ρίσκων υιοθετώντας μια σειρά από στρατηγικές και εφαρμόζοντας λεπτομερή πλάνα για αναγνώριση των κινδύνων, προτεραιοποίηση, παρακολούθηση και μείωση αυτών, για την προστασία του οργανισμού. Πολλά από αυτά (αν όχι όλα), εμπεριέχονται στο Πλάνο Επιχειρησιακής Συνέχειας (Business Continuity Plan – BCP), το οποίο περιγράφει τα βήματα που αναλαμβάνει ένας οργανισμός για την πρόληψη, ή την ανάκαμψη από μια κατάσταση, όταν δεν μπορεί να λειτουργήσει κανονικά λόγω φυσικών ή άλλων καταστροφών. Ο στόχος είναι να ελαχιστοποιηθεί η ζημιά για την εταιρεία και ενδεχομένως, ακόμη και να αποτραπεί η καταστροφή εν τη γενέσει της.

2.1.1 Τι είναι καταστροφή

Μια καταστροφή ορίζεται ως ένα ξαφνικό, απρογραμμάτιστο γεγονός το οποίο μειώνει μερικώς ή πλήρως τις δραστηριότητες του οργανισμού ή διαταράσσει κρίσιμες διαδικασίες με αποτέλεσμα να απειλείται η ομαλή λειτουργία του. Πιθανές συνέπειες μιας καταστροφής περιλαμβάνουν βλάβη και απώλειες σε ένα ευρύ φάσμα πόρων, όπως εγκαταστάσεις, εργαζόμενους, δεδομένα, έσοδα, φήμη, ή ακόμα και πλήρη απώλεια ελέγχου της εταιρείας [10, 16, 33].

Ο μεγαλύτερος κίνδυνος για κάθε επιχείρηση είναι το γεγονός ότι μια καταστροφή μπορεί να συμβεί χωρίς προειδοποίηση. Αν και μερικές φορές μπορεί να προβλεφτεί ότι κάτι πρόκειται να συμβεί που είναι πιθανό να προκαλέσει ζημιά, τα περισσότερα ατυχήματα και οι αποτυχίες δεν είναι πραγματικά προβλέψιμα.
Ωστόσο, η άποψη πως συμβάντα όπως αυτά είναι πραγματικά απρόβλεπτα, είναι διφορούμενη. Όπως έχει υποστηριχθεί από πολλούς, όλα τα συστήματα έχουν μια τάση προς την αποτυχία. Ως εκ τούτου, δεν έχει νόημα να εξετάσουμε αν τα συστήματα θα αποτύχουν, αλλά να είμαστε προετοιμασμένοι, όταν αυτό θα συμβεί. Το πιο σημαντικό είναι να αποδεχτούμε το γεγονός ότι όλοι οι οργανισμοί θα αντιμετωπίσουν μια κρίση – καταστροφή σε κάποιο σημείο της πορείας τους.

Ας πάρουμε για παράδειγμα το σενάριο μια επαπειλούμενης φυσικής καταστροφής εξαιτίας ενός επερχόμενου τυφώνα. Ακόμα και αν έχουμε προειδοποιηθεί 3 μέρες νωρίτερα, εν τούτοις θα είναι ήδη πολύ αργά. Το χρονικό περιθώριο δύο ή τριών ημερών πριν την επερχόμενη ζημιά δεν είναι αρκετό, διότι εκτός από την εκκένωση του κτιρίου για λόγους προστασίας, υπάρχουν και πολλά άλλα που πρέπει να γίνουν. Η δημιουργία αντιγράφων ασφαλείας των συστημάτων και η ασφαλής off-site μεταφορά τους απαιτεί πολύτιμο χρόνο, και ο χρόνος είναι ακριβώς ό, τι δεν έχει στη διαθεσή της μια εταιρία που αναμένεται να πληγεί από καταστροφή.

2.1.2 Αιτίες καταστροφών

Οι καταστροφές διαχωρίζονται σύμφωνα με τη φύση τους [31]. Έχουμε φυσικές καταστροφές οι οποίες οφείλονται σε περιβαλλοντικούς παράγοντες όπως είναι η φωτιά, οι πλημμύρες, τυφώνες και φυσικά οι σεισμοί. Επόμενη κατηγορία είναι οι καταστροφές που προέρχονται από σκόπιμη ανθρώπινη παρέμβαση όπως είναι η κλοπή, η απάτη, οι τρομοκρατικές ενέργειες, οι εμπρησμοί, η δολιοφθορά αλλά τα τελευταία χρόνια λόγω της ανάπτυξης του διαδικτύου έχουμε και την εμφάνιση κυβερνο-επιθέσεων (hacking) . Τελευταία κατηγορία καταστροφών είναι αυτές που οφείλονται σε τεχνικές βλάβες, ή αστοχία υλικού, όπως συνηθίζεται να λέγεται. Σε αυτή την κατηγορία εντάσσονται οι πιο συχνές καταστροφές όπως οι βλάβες του δικτύου επικοινωνίας (τηλεφωνικά κέντρα), βλάβες λόγω διακοπής ηλεκτροδοσίας, βλάβες λόγω αποτυχίας υλικού ή λογισμικού του Πληροφοριακού Συστήματος (πχ λόγω βραχυκυκλώματος).

Ωστόσο, είναι πολύ σημαντικό να συνειδητοποιήσουμε ότι δεν θα πρέπει να σχεδιάζουμε ένα πλάνο ανάκαμψης για κάθε ένα συγκεκριμένο τύπο καταστροφής, αλλά ένα πλάνο με την λογική τη συνέχισης των διεργασιών του οργανισμού ανεξαρτήτως καταστροφής. Για παράδειγμα, δεν έχει νόημα να σχεδιαστεί κάτι ειδικά για την αντιμετώπιση της πυρκαγιάς ή την αντιμετώπιση της καταστροφής από σεισμό. Αντί αυτού, καταλληλότερος είναι ο σχεδιασμός ελαχιστοποίησης της απώλειας των εγκαταστάσεων σε γενικότερο πλαίσιο, ενσωματώνοντας διαδικασίες αποτροπής απώλειας εργαζομένων, διακοπής των επικοινωνιών, ή μιας τεράστιας απώλειας δεδομένων.

2.1.3 Συνέπειες και επιπτώσεις

Χωρίς την κατάλληλη στρατηγική επιχειρησιακής συνέχειας, οι απειλές που αναφέρονται στις αιτίες καταστροφών, μπορεί να επηρεάσουν αρνητικά ζωτικής σημασίας κομμάτια του οργανισμού. Ένα σχέδιο επιχειρησιακής συνέχειας έχει ως στόχο να προστατεύσει:

- Τις κρίσιμες υπηρεσίες του οργανισμού, οι οποίες μέσω σχεδίων αντιμετώπισης κινδύνων και συνεχείς δοκιμές αυτών, εξασφαλίζεται η απρόσκοπτη λειτουργία τους.
- Την δημόσια εικόνα της εταιρείας, αφού υιοθετώντας συγκεκριμένους και σύγχρονους τρόπους διαχείρισης κινδύνων, αποπνέει αίσθηση υψηλής υπευθυνότητας και επαγγελματισμού.
- Την εξασφάλιση των εσόδων του οργανισμού, λόγω του ότι εξαλείφει όλες τις περιπτώσεις οι οποίες δύναται να προκαλέσουν διακοπή υπηρεσιών.
- Την εμπιστοσύνη των πελατών, των εργαζομένων και όλων των εμπλεκόμενων συνεργατών, διότι θα είναι σίγουροι ότι υπάρχει πρόβλεψη για καθετί απρόοπτο που μπορεί να συμβεί.
- Την διατήρηση του μεριδίου της αγοράς, αφού οι πελάτες θα είναι ευχαριστημένοι στο μέγιστο δυνατό βαθμό.

Οι παράγοντες αυτοί είναι μεγάλης σημασίας, και συχνά θεωρούνται απαραίτητοι για τους περισσότερους οργανισμούς. Παρόλα αυτά, οι διοικήσεις των εταιριών θεωρούν ότι οι προαναφερθείσες απειλές δεν αποτελούν κίνδυνο για τις επιχειρήσεις τους, καθώς είναι σπάνιο να συμβούν. Επιπρόσθετα, πιστεύουν ότι αν προχωρήσουν σε ασφαλιστική κάλυψη της εταιρίας δαπανώντας ένα μεγάλο χρηματικό ποσό, θα οχυρωθούν έναντι οποιασδήποτε ενδεχόμενης ζημιάς. Δυστυχώς, αυτές οι απόψεις δεν βασίζονται σε εμπεριστατωμένες μελέτες, αλλά σε ευσεβείς πόθους. Το γεγονός είναι ότι ένας οργανισμός πρέπει να είναι σε θέση να αντιμετωπίσει με επιτυχία οποιαδήποτε καταστροφή προκειμένου να ευημερήσει. Είναι προφανές ότι η σωστή και συστηματική πρόληψη είναι φθηνότερη και πιο αποτελεσματική από τις απροετοίμαστες και βεβιασμένες προσπάθειες ανάκαμψης.

Επίσης έχουν αναπτυχθεί λύσεις Ανοχής σε Σφάλματα (Fault Tolerance), με στόχο να αυξηθεί η διαθεσιμότητα των υπολογιστικών συστημάτων, καθώς και να μειωθεί η ζημιά που προκαλείται από μια καταστροφή. Αλλά ακόμα κι αν τα ζωτικής σημασίας δεδομένα μπορούν να αποθηκευτούν με τέτοιο τρόπο και σε κατάλληλο μέσο ώστε να

είναι διασφαλισμένα από αποτυχίες όπως διακοπή ηλεκτρικού ρεύματος ή διακοπές συστημάτων, αυτό δεν είναι αρκετό αν συμβεί μια φυσική καταστροφή (πχ μεγάλος σεισμός). Ακόμα και αν έχουμε αντίγραφα ασφάλειας σε διάφορα σημεία, θα είναι μάταιο αν αυτά βρίσκονται εντός της πληγείσας περιοχής [18, 45].

2.2 Τι είναι Disaster Recovery Plan

Ένα Πλάνο Ανάκαμψης από Καταστροφή περιλαμβάνει βήματα, διαδικασίες και μηχανισμούς ούτως ώστε να επανέλθει σε λειτουργική κατάσταση ένα σύνολο συστημάτων τα οποία εξυπηρετούν σημαντικές επιχειρηματικές διεργασίες και υπηρεσίες. Σκοπός είναι να μπορέσει η εταιρία να επαναλειτουργήσει σε φυσιολογικά επίπεδα, όσο το δυνατόν ταχύτερα, μειώνοντας στο ελάχιστο την όποια ζημιά. Όταν λέμε DRP (Disaster Recovery Plan), εννοούμε ένα πλάνο ανάκαμψης εφαρμοσμένο κυρίως σε υποδομές Πληροφοριακών Συστημάτων [15, 16].

Έχοντας καταρτίσει ένα σωστό DRP εξοικονομούμε χρόνο ανάκαμψης, διότι από πριν είναι συμφωνημένο τι πρέπει να ανακτηθεί και με ποια σειρά προτεραιότητας.

2.2.1 οφέλη και στόχοι ενός DR plan

Ο πιο σημαντικός λόγος ανάπτυξης ενός πλάνου ανάκαμψης από καταστροφή είναι η διασφάλιση της ταχείας και οικονομικά αποδοτικής ανάκτησης των κρίσιμων επιχειρηματικών διαδικασιών. Επιπλέον, ένα καλά μελετημένο και ολοκληρωμένο πλάνο προσφέρει μια σειρά από οφέλη για τον οργανισμό:

- Μειώνεται η ανάγκη για λήψη αποφάσεων υπό την πίεση του χρόνου.
- Ενημερώνεται το προσωπικό με σαφείς οδηγίες σχετικά με τις ευθύνες του σε περίπτωση καταστροφής.
- Ωθείται η εταιρεία να ικανοποιήσει τις διάφορες απαιτήσεις ασφαλείας.
- Αναδεικνύονται οι αδυναμίες μέσω ενδελεχών ελέγχων.
- Μειώνεται το ρίσκο συνολικά στον οργανισμό.
- Μειώνονται κατά πολύ οι επιπτώσεις των καταστροφών.

Το πρώτο και κύριο μέλημα ενός τέτοιου πλάνου είναι η επιβίωση του Πληροφοριακού Συστήματος στο σύνολό του. Διεργασίες κρίσιμης σημασίας για την ίδια την ύπαρξη της εταιρείας έχουν απόλυτη προτεραιότητα αποκατάστασης. Αυτό είναι λογικό αν

σκεφτούμε πως η επιβίωση του οργανισμού στηρίζεται σε αυτές τις υπηρεσίες. Θα πρέπει να σχεδιαστεί προσεκτικά λοιπόν και να προβλεφτούν όλα τα πιθανά προβλήματα καθώς και στρατηγικές ικανές να δώσουν λύσεις σε αυτά. Λαμβάνοντας υπόψη ότι σε περίπτωση συμβάντος δεν θα υπάρχει η πολυτέλεια του χρόνου και όλοι θα διακατέχονται από άγχος, το πλάνο θα πρέπει να περιέχει όσο το δυνατόν περισσότερες λεπτομέρειες, ούτως ώστε να αποφορτίσει τους εμπλεκόμενους και να καταστήσει πιο εύκολη και σύντομη τη διαδικασία ανάκτησης.

2.2.2 Ποια πρότυπα σχετίζονται με Disaster Recovery πολιτικές

Λέγοντας Disaster Recovery εννοούμε όλες τις πολιτικές και διαδικασίες σχετικά με την προετοιμασία ανάκαμψης ή την επιχειρησιακή συνέχεια μετά από καταστροφή. Υπάρχουν διάφορα και ευρέως διαδεδομένα πρότυπα (frameworks) στα οποία βρίσκουν εφαρμογή πολιτικές disaster recovery. Τέτοια είναι το παλιό ISO/IEC 17799, το «Πρακτικό εργαλείο διακυβέρνησης πληροφοριακών συστημάτων» (Control Objectives for Information Systems – COBIT), το πρότυπο του Αμερικανικού Ινστιτούτου Προτύπων και Τεχνολογίας (NIST), καθώς και το πρότυπο «ITIL» Παρακάτω παρουσιάζονται συνοπτικά τα σημαντικότερα χαρακτηριστικά του κάθε προτύπου [26].

Το πρότυπο COBIT πρωτοεκδόθηκε από το Ινστιτούτο Ελέγχου Συστημάτων Πληροφορικής (Information Systems Audit & Control Association – ISACA) το 1996 και περιγράφει αναλυτικά την εφαρμογή των δικλίδων ασφαλείας σε όλο το φάσμα της λειτουργίας και της διακυβέρνησης των Πληροφοριακών Συστημάτων. Ορίζει 34 ελέγχους ομαδοποιημένους σε 4 τομείς, του σχεδιασμού και της οργάνωσης, της υλοποίησης, της παράδοσης και υποστήριξης και της παρακολούθησης και αξιολόγησης [21].

Το πρότυπο ISO 17799 συχνά αναφέρεται ως «Πρότυπο ISO». Η σειρά 17799 αναπτύχθηκε από το πρότυπο 7799 του Βρετανικού Ινστιτούτου Προτύπων (British Standards Institute). Χωρίζει το ευρύ πεδίο της ασφάλειας σε δέκα μεγάλους τομείς οι οποίοι περιέχουν 36 ελέγχους υψηλού επιπέδου, με περίπου διακόσιες συνιστώμενες πολιτικές. Η σειρά 17799 εν τέλει έχει αντικατασταθεί από τη σειρά 27000 [22].

Το πρότυπο ITIL της Βιβλιοθήκης για Υποδομές Τεχνολογίας πληροφοριών και επικοινωνίας (Information Technology Infrastructure Library), επικεντρώνεται στο ευρύτερο φάσμα της πληροφορικής και όχι μόνο σε θέματα ασφάλειας. Ορίζει οκτώ

σύνολα υπηρεσιών πληροφορικής. Σε σύγκριση με το COBIT και το ISO, το ITIL ασχολείται περισσότερο με την παροχή υπηρεσιών και λιγότερο με την τεχνολογία όπως το ISO, ή τις διαδικασίες ελέγχου, όπως το COBIT. Επικεντρώνεται περισσότερο στις πρακτικές και τις μετρήσεις των προηγούμενων δύο προτύπων [35].

Τέλος η σειρά προτύπων NIST-800 του Αμερικανικού Ινστιτούτου Προτύπων και Τεχνολογίας (National Institute of Standards and Technology – NIST), καθορίζει υψηλού επιπέδου ελέγχους σε 17 τομείς ασφάλειας [40].

Η παρούσα διατριβή επίλεξε και επικεντρώθηκε στα ISO 27001:2005, ISO 27031:2011 και 22301:2012.

2.2.3 Σχολιασμός άλλων DR plans

Σε αυτό το κομμάτι της διατριβής μελετήθηκαν άλλα DR plans τα οποία έχουν εκπονηθεί για διάφορους οργανισμούς. Μελετώντας τα, έγινε μια προσπάθεια αξιολόγησης και καταγραφής των αρνητικών τους σημείων, πιθανολογώντας και τους λόγους αποτυχίας τους.

Το πρώτο σχέδιο από ανάκαμψη που μελετήθηκε ήταν του Πανεπιστημίου του Τορόντο [36]. Παρόλο που όπως αναφέρει το Πανεπιστήμιο του Τορόντο αυτός είναι μόνο ένας οδηγός, εντούτοις υπάρχουν μερικές σημαντικές παραλήψεις, οι οποίες έχουν μεγάλη σημασία στην κατάρτιση ενός σωστού DRP.

1. Αναφέρεται ότι προσδιορίζονται γενικώς και αορίστως αδυναμίες, κάτι το οποίο είναι λάθος. Οι κίνδυνοι πρέπει να προσδιορίζονται με σαφήνεια, μέσω του risk assessment report.
2. Αναφέρεται λανθασμένα ότι το DR planning είναι περισσότερο “business oriented” και λιγότερο σχετίζεται με ζητήματα δεδομένων. Αυτό εμπειρικά δεν ευσταθεί αν αναλογιστούμε ότι ένα σωστό DRP εμπεριέχει διαδικασίες replication (αν επιθυμούμε hot-standby DR site) ή διαδικασίες backup (αν θέλουμε απλώς recovery site). Επίσης πρέπει να λάβουμε υπόψη την ασφάλεια και ακεραιότητα των

δεδομένων υλοποιώντας μηχανισμούς και τεχνικές για data integrity και data encryption.

3. Στην μεθοδολογία της ανάπτυξης του πλάνου δεν αναφέρονται οι χρόνοι για RTO (recovery time objectives) και RPO (recovery point objectives). Είναι ιδιαιτέρως σημαντικό να οριστούν τα παραπάνω χρονικά πλαίσια έτσι ώστε να μπορέσουμε να αξιολογήσουμε το DRP στο στάδιο των δοκιμών του ή όταν τεθεί σε εφαρμογή.
4. Επίσης δεν ορίζονται ποια είναι τα εμπλεκόμενα μέρη (stakeholders) του Πανεπιστημίου (πχ οι φοιτητές, οι καθηγητές ή κάποιοι προμηθευτές), και ως εκ τούτου δεν υπάρχει πρόβλεψη για ενημέρωση αυτών σχετικά με την εκπόνηση του DR plan.
5. Στην Ανάλυση Επιχειρησιακού Αντίκτυπου (Business Impact Analysis), δεν γίνεται λόγος για προτεραιοποίηση (prioritization) υπηρεσιών, κάτι το οποίο είναι απαραίτητο στο στάδιο της ανάκαμψης των υπηρεσιών.
6. Στην φάση της δοκιμής του πλάνου δεν ορίζονται συγκεκριμένα σενάρια δοκιμών. Επίσης δεν καταγράφεται η ανάγκη για δοκιμές του πλάνου ανά τακτά χρονικά διαστήματα, παρά μόνον μια αρχική δοκιμή.
7. Στην δημιουργία των διάφορων ομάδων δεν έχει προβλεφθεί η δημιουργία μιας ομάδας επικοινωνίας υπεύθυνη για την έγκαιρη, έγκυρη και συνεχή ενημέρωση των stakeholders κατά την διάρκεια εφαρμογής του DR plan.

Οπότε πρέπει να κατατεθούν μια σειρά από προτάσεις με σκοπό την βελτίωση του πλάνου. Αναλυτικότερα:

1. Είναι σημαντικό να οριστούν οι κίνδυνοι (τα ρίσκα), και οι πιθανές “τρύπες ασφάλειας”. Να αξιολογηθούν και όσοι από αυτούς αποφασιστεί ότι πρέπει να απαλειφθούν, να οριστούν οι κατάλληλες ενέργειες.
2. Να αποφασιστεί τι είδους recovery site θα αναπτυχθεί και ανάλογα με την απόφαση αυτή να παρθούν όλα τα αναγκαία μέτρα έτσι ώστε να επιτυγχάνεται data integrity and encryption.
3. Τα χρονικά πλαίσια RTO (recovery time objectives) και RPO (recovery point objectives) καθορίζουν την πορεία των εργασιών κατά την διάρκεια που είναι σε εφαρμογή το DR πλάνο, και επιπροσθέτως μπορούμε να αξιολογήσουμε εκ των υστέρων την απόδοση και την επιτυχία (ή την αποτυχία) του πλάνου. Ως εκ τούτου είναι αναπόσπαστα κομμάτια του πλάνου, και πρέπει να οριστούν.

4. Να οριστούν επίσης οι stakeholders του Πανεπιστημίου και να πάρουν μέρος στην ανάπτυξη του πλάνου.
5. Να προτεραιοποιηθούν οι υπηρεσίες ανάλογα με την κρισιμότητα που έχει η κάθε μία, έτσι ώστε να ανακάμψουν με την αντίστοιχη σειρά.
6. Να οριστούν ακριβή σενάρια δοκιμών αναφέροντας με σαφήνεια τι θα δοκιμαστεί κάθε φορά, τι αποτελέσματα αναμένονται, και τι συμπεράσματα εξάγονται.
7. Να δημιουργηθεί ομάδα επικοινωνίας η οποία θα είναι επιφορτισμένη με την ενημέρωση όλων των εμπλεκομένων πριν, κατά την διάρκεια και μετά την διακοπή των υπηρεσιών.

Στο δεύτερο DR plan παρουσιάζεται μια πρόταση της Morgan Doyle κατάλληλη για φορείς Τοπικής Αυτοδιοίκησης [29]. Στην κατάθεση πρότασης για BC/DR plan υπάρχουν αρκετές παραλείψεις και παραδοχές. Αναλυτικότερα:

1. Δεν αναφέρεται πουθενά αν θα χρησιμοποιηθεί κατάλληλο λογισμικό ανάκαμψης.
2. Δεν έχουν οριστεί stakeholders.
3. Παρόλο που έχει διεξαχθεί ανάλυση επιχειρησιακού αντίκτυπου, εν τούτοις δεν αναφέρονται οι χρόνοι για RTO (recovery time objectives) και RPO (recovery point objectives).
4. Δεν γίνεται λόγος για capacities (κυρίως storage capacity), που θα απαιτηθούν για την DR υποδομή.
5. Δεν ορίζεται η μεθοδολογία και οι τρόποι που θα γίνεται backup.
6. Δεν αναφέρονται μηχανισμοί για data integrity και data encryption. Είναι ιδιαιτέρως σημαντικό αν σκεφτούμε ότι το πλάνο απευθύνεται σε φορείς τοπικής αυτοδιοίκησης οι οποίοι έχουν ευαίσθητα προσωπικά δεδομένα.
7. Δεν αναφέρονται διαδικασίες που θα πρέπει να ακολουθηθούν κατά την διάρκεια της διακοπής. Δεν υπάρχουν διαδικασίες χειρισμού συμβάντος.
8. Δεν έχουν οριστεί ομάδες, η καθεμία επιφορτισμένη με συγκεκριμένο ρόλο.
9. Δεν έχουν οριστεί έλεγχοι του πλάνου. Ούτε για το κάθε πότε θα γίνεται δοκιμαστική εφαρμογή του, ούτε σύνταξη κατάλληλων σεναρίων με συγκεκριμένους στόχους και καταγεγραμμένα αποτελέσματα.
10. Δεν προβλέπεται σαν διαδικασία, η αξιολόγηση του πλάνου μέσω μετρήσεων της απόδοσής του. Θα πρέπει να οριστούν κατάλληλα metrics για την αξιολόγησή του.

Σύμφωνα με το Cobit και την μελέτη που έχει γίνει, χρειάζεται να γίνουν μια σειρά από ενέργειες όπως:

1. Να οριστούν stakeholders και να λάβουν σχετική ενημέρωση για τις γενικές κατευθύνσεις του πλάνου.
2. Να οριστούν τα χρονικά πλαίσια RTO και RPO.
3. Να γίνει ξεκάθαρο η μεθοδολογία και οι τρόποι του backup λαμβάνοντας υπόψη την ακεραιότητα και ασφάλεια των δεδομένων.
4. Να δημιουργηθούν ομάδες και η κάθε μία από αυτές να αναλάβει συγκεκριμένο και διακριτό ρόλο στην εκτέλεση του πλάνου.
5. Να οριστούν διαδικασίες που θα τεθούν σε εφαρμογή κατά τη διάρκεια του συμβάντος και να κοινοποιηθούν σε όλες τις εμπλεκόμενες ομάδες.
6. Να κατασκευαστούν σενάρια δοκιμών τα οποία θα αναφέρουν επ' ακριβώς τι θα δοκιμαστεί, τι αναμένεται να συμβεί, καθώς και να υπάρξει καταγραφή των αποτελεσμάτων. Στη συνέχεια θα πρέπει να ακολουθήσει αξιολόγηση των συμπερασμάτων και αν κριθεί απαραίτητο, αναθεώρηση του DR plan.

Το τρίτο πλάνο που μελετήθηκε αφορά μια μελέτη του East London NHS Foundation Trust με σκοπό να καθορίσει και να εξαλείψει πιθανούς κινδύνους του Πληροφοριακού του Συστήματος [43]. Στην κατάθεση πρότασης για BC/DR plan για το NHS Foundation Trust λείπουν τα παρακάτω:

1. Δεν αναφέρονται οι stakeholders.
2. Δεν έχουν οριστεί ομάδες με διακριτούς ρόλους η καθεμιά.
3. Δεν έχει οριστεί RTO/RPO για κάθε critical service.
4. Δεν έχει υλοποιηθεί Risk Assessment.
5. Δεν έχουν οριστεί metrics που θα καταγραφούν κατά τους δοκιμαστικούς ελέγχους του πλάνου.

Επομένως, θα πρέπει να οριστούν οι εμπλεκόμενοι (stakeholders) και να αρχίσουν να λαβαίνουν μέρος πιο ενεργά στην υλοποίηση του πλάνου. Επίσης να δημιουργηθούν ομάδες με διακριτούς ρόλους και επιφορτισμένες με συγκεκριμένες αρμοδιότητες (πχ ομάδα επικοινωνίας με ρόλο την ενημέρωση των εμπλεκομένων κατά την διάρκεια του συμβάντος). Επιπροσθέτως να οριστούν RTOs και RPOs έτσι ώστε να γνωρίζουμε την επιτυχία ή αποτυχία του πλάνου με βάση τα χρονικά πλαίσια downtime για κάθε critical service. Συμπληρωματικά θα πρέπει να γίνει και Risk Assessment για να καθοριστούν οι

πιθανοί κίνδυνοι, να αξιολογηθούν και να αποφασιστεί για ποιους από αυτούς θα ληφθούν μέτρα πρόληψης. Τέλος, θα πρέπει να οριστούν κατάλληλα μετρικά για τους δοκιμαστικούς ελέγχους για να μπορούμε να αξιολογήσουμε τα αποτελέσματα των δοκιμών και να κρίνουμε αν χρειάζεται βελτιώσεις ή αλλαγές το DR plan.

Το τελευταίο πλάνο που μελετήθηκε αφορά το Πληροφοριακό Σύστημα του Εθνικού Πάρκου του Dartmoor [11]. Οι ελλείψεις του συγκεκριμένου πλάνου έγκειται στα εξής:

1. Δεν αναφέρονται οι stakeholders.
2. Δεν υπάρχει DR υποδομή.
3. Δεν έχουν οριστεί ομάδες με διακριτούς ρόλους η καθεμιά.
4. Δεν έχει διεξαχθεί σωστό Business Impact Analysis.
5. Δεν έχει οριστεί RTO/RPO για κάθε critical service.
6. Δεν αναφέρεται ποια μέθοδος backup χρησιμοποιείται και αν πληρεί απαιτήσεις για data integrity & encryption.

Δεδομένου των παραπάνω παραλείψεων θα πρέπει να οριστούν οι εμπλεκόμενοι (stakeholders) και να αρχίσουν να λαμβάνουν μέρος πιο ενεργά στην υλοποίηση του πλάνου. Ένα άλλο σημαντικό στοιχείο που χρήζει προσοχής είναι η μη ύπαρξη DR υποδομής. Θα πρέπει να υπάρξει έστω και για ελάχιστα services. Επίσης να δημιουργηθούν ομάδες με διακριτούς ρόλους και επιφορτισμένες με συγκεκριμένες αρμοδιότητες (πχ ομάδα επικοινωνίας με ρόλο την ενημέρωση των εμπλεκομένων κατά την διάρκεια του συμβάντος). Επιπροσθέτως να γίνει σωστή BIA και να προτεραιοποιηθούν τα critical services και η σειρά με την οποία θα γίνουν recovered. Ακόμα θα πρέπει να οριστούν RTOs και RPOs έτσι ώστε να γνωρίζουμε την επιτυχία ή αποτυχία του πλάνου με βάση τα χρονικά πλαίσια downtime για κάθε critical service. Τέλος, θα πρέπει να αποφασιστεί μια μέθοδος για backup των δεδομένων η οποία θα διασφαλίζει την ακεραιότητα και ασφάλεια αυτών.

2.2.4 Λόγοι αποτυχίας DR plan

Υπάρχουν πολλές παγίδες που θα πρέπει να ληφθούν σοβαρά υπόψη κατά τη δημιουργία ενός πλάνου ανάκαμψης [27]. Δεδομένου αφενός ότι πολλά πλάνα είναι ελλιπή με αποτέλεσμα είτε να λείπουν ολόκληρες διαδικασίες, είτε να είναι μερικώς συμπληρωμένες, και αφετέρου άλλα να είναι ανεπαρκή, με αποτέλεσμα τα επίπεδα διασφάλισης κινδύνου να μην είναι αυτά που είχαν οριστεί εξ' αρχής από τον οργανισμό

και έτσι να μην είναι αποδεκτά, θα πρέπει το πλάνο να είναι πλήρες. Ένα άλλος σημαντικός λόγος είναι η απλότητα και πρακτικότητα των διαδικασιών. Πολλές από αυτές περιέχουν περίπλοκη εφαρμογή και εκτέλεση, με αποτέλεσμα το πλάνο είτε να καθίσταται υπερεκτιμημένο για τις ανάγκες του οργανισμού, είτε να είναι ανέφικτη η πραγματοποίηση των στόχων του πχ. λόγω έλλειψης ανθρώπινου δυναμικού, διαθέσιμου χρόνου ή και διαθέσιμου χρηματικού ποσού. Η λανθασμένη πληροφόρηση σχετικά με το πλάνο είναι άλλη μια αιτία αποτυχίας του. Αν δεν ενημερωθεί σωστά και επαρκώς το προσωπικό, όλοι θα είναι επιφυλακτικοί σχετικά με την απόδοσή του και την αποτελεσματικότητά του [30]. Φυσικά δεν πρέπει να ξεχάσουμε να αναφέρουμε τις περιπτώσεις αυτές που λόγου στενών χρονικών ορίων δεν δοκιμάζεται το πλάνο για να διαπιστωθούν τυχόν κενά στις διαδικασίες. Τέλος θα πρέπει να δίνουμε ιδιαίτερη προσοχή στην ενημέρωση και επικαιροποίηση των διαδικασιών του, διότι οι εταιρίες αλλάζουν και εξελίσσονται διαρκώς, με αποτέλεσμα να δημιουργούνται νέες ανάγκες οι οποίες πρέπει να ληφθούν υπόψη και να συμπεριληφθούν στο πλάνο.

Κεφάλαιο 3

DR plan για τηλεπικοινωνιακούς παρόχους

Όπως αναφέρθηκε, τα δομικά στοιχεία ενός Πληροφοριακού Συστήματος είναι το υλικό, το λογισμικό, τα δεδομένα, οι άνθρωποι και οι διαδικασίες. Η Ασφάλεια των Πληροφοριακών Συστημάτων αφορά στην προστασία όλων αυτών των στοιχείων όπως και του Πληροφοριακού Συστήματος ως σύνολο [42].

Όταν συμβαίνει μια καταστροφή υπάρχει περιορισμένος χρόνος αντίδρασης. Όσο περισσότερο χρόνο χρειάζεται μια κρίσιμη υπηρεσία για να ανακάμψει, τόσο μεγαλύτερες είναι οι απώλειες. Είναι πολύ σημαντικό να είμαστε προετοιμασμένοι να δράσουμε άμεσα. Επομένως χρειάζεται ένα σωστό Πλάνο Ανάκαμψης από Καταστροφή, σωστά σχεδιασμένο και κατάλληλο για εικονικές υποδομές, με έμφαση τόσο στην ταχύτατη εκτέλεσή του, όσο κυρίως στην ελαχιστοποίηση των απωλειών σε δεδομένα και πληροφορίες [14].

Μελετώντας το ISO 27001:2005 [24] το οποίο αναφέρεται στην ασφάλεια των Πληροφοριακών Συστημάτων, το ISO 27031:2011 [25] και το 22301:2012 [23] τα οποία αφορούν στην ετοιμότητα και διαχείριση της Επιχειρησιακής Συνέχειας, και λαμβάνοντας υπόψη τα συνηθισμένα λάθη και παραλείψεις προηγουμένων Disaster Recovery Plans, ξεχωρίσαμε τους ελέγχους (controls) αυτούς οι οποίοι είναι κατάλληλοι και έχουν νόημα να εφαρμοστούν σε εικονικές υποδομές. Υπό αυτό το πρίσμα λοιπόν παρουσιάζουμε την μεθοδολογία που υϊοθετούν τα προαναφερθέντα πρότυπα, μια μικρή ανάλυση για κάθε ένα από αυτά, τους ελέγχους που επιλέξαμε από κάθε ISO, και στο τέλος του κεφαλαίου παρουσιάζονται συγκεντρωτικά οι έλεγχοι σε δύο λίστες. Η πρώτη λίστα περιέχει τους ελέγχους ομαδοποιημένους ανά σειρά υλοποίησης, και η δεύτερη ομαδοποιημένους ανά ISO και φάση υλοποίησης.

Όπως δηλώθηκε και στον τίτλο της διατριβής, στόχος είναι η αποκατάσταση εικονικών υποδομών με ασφάλεια και μηδενικό κόστος. Πρέπει να αναφερθεί εν τούτοις ότι το θέμα της ασφάλειας καλύπτεται από πολλές οπτικές γωνίες και με διαφορετικές υλοποιήσεις. Σε αυτή τη διατριβή επικεντρωθήκαμε στην ασφάλεια των πληροφοριών και των δεδομένων συντάσσοντας ένα πλάνο ανάκαμψης από καταστροφή με γνώμονα την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των πληροφοριών. Δεν εντάσσονται στο πεδίο μελέτης αυτής της διατριβής, τομείς που άπτονται σε ζητήματα ασφάλειας του προσωπικού της εταιρίας, των φυσικών εγκαταστάσεων και της φυσικής ασφάλειας του hardware, της ασφάλειας δικτύου ή της ασφάλειας των εφαρμογών. Θεωρείται ότι αυτά τα ζητήματα είναι εκ προοιμίου διευθετημένα έτσι ώστε να μπορούμε να μιλάμε για ασφάλεια σε ανώτερο επίπεδο εικονικών μηχανών [14].

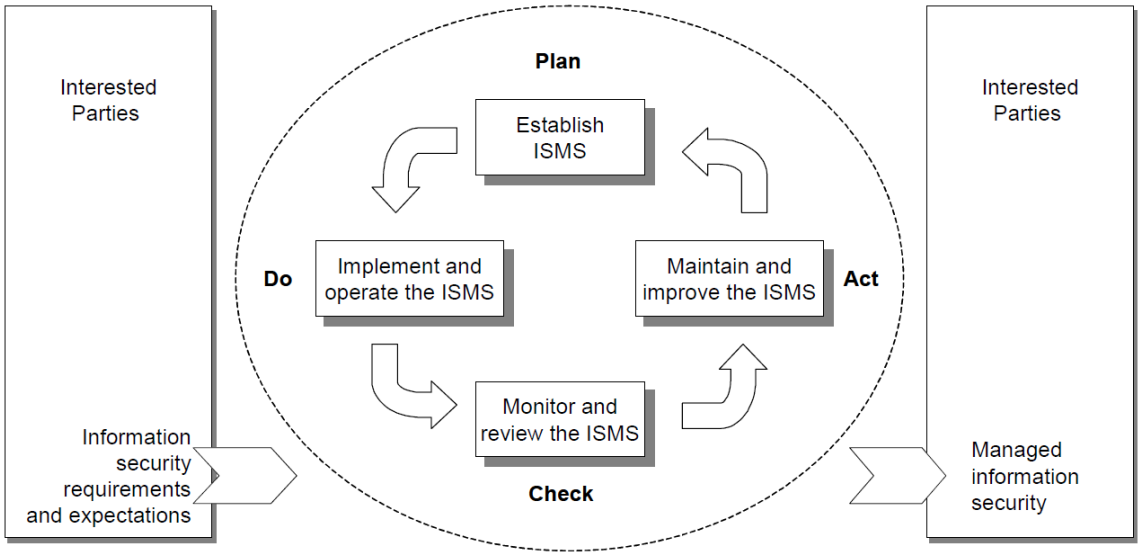
3.1 Μεθοδολογία μοντέλου PCDA

Τα πρότυπα υλοποίησης Συστήματος Διαχείρισης Ασφάλειας Πληροφοριακών Συστημάτων (Information Security Management System – ISMS), ορίζουν ένα πλαίσιο για τους οργανισμούς σχετικά με το πως να διαχειρίζονται τομείς που άπτονται της ασφάλειας των πληροφοριών της επιχείρησής τους, και να πείθουν τους πελάτες τους, τους προμηθευτές τους ή ακόμα και τους ελεγκτές τους με την ικανότητά τους να διαχειρίζονται την ασφάλεια των πληροφοριών. Προσδιορίζει ένα σύστημα διαχείρισης ασφάλειας βασισμένο στη διαχείριση των κινδύνων και αποσκοπεί στην εφαρμογή μιας

σειράς ελέγχων από πλευράς των οργανισμών με σκοπό την προστασία των πολύτιμων πληροφοριών τους. Έχουν εκδοθεί από τον Διεθνή Οργανισμό Τυποποίησης (International Organization for Standardization) και την Διεθνή Επιτροπή Ηλεκτροτεχνικής (International Electrotechnical Commission). Πάνω σε αυτή τη βάση στηρίζονται στη συνέχεια τα πλαίσια ανάπτυξης των Πλάνων Επιχειρησιακής Συνέχειας (Business Continuity Plan – BCP) και Ανάκαμψης από Καταστροφή (Disaster Recovery Plan – DRP).

Ως θεμελιώδεις αρχές της ασφάλειας των Πληροφοριακών Συστημάτων λογίζονται η Ακεραιότητα, η Διαθεσιμότητα και η Εμπιστευτικότητα. Θα αναφερθούμε και παρακάτω πιο διεξοδικά σε αυτές τις αρχές και τον τρόπο που καλύπτονται στα επιλεγμένα πρότυπα, αλλά θα ήταν χρήσιμη μια σύντομη επεξήγησή τους. Η αρχή της Εμπιστευτικότητας (Confidentiality) αποσκοπεί στην απόκρυψη ευαίσθητων πληροφοριών σε μη εξουσιοδοτημένα άτομα. Η Εμπιστευτικότητα είτε λαμβάνεται ως Ιδιωτικότητα (Privacy) και αφορά συνήθως προσωπικά δεδομένα, είτε ως Μυστικότητα (Secrecy) και αφορά ευαίσθητα δεδομένα ενός οργανισμού. Η αρχή της Ακεραιότητας (Integrity) των δεδομένων αφορά την προστασία των Πληροφοριακών Συστημάτων από ανεπιθύμητες αλλαγές, περιλαμβάνοντας ενέργειες αποτροπής μεταβολής πληροφοριών από μη εξουσιοδοτημένα άτομα, δηλαδή, πρόληψη και αποτροπή μη εξουσιοδοτημένης εγγραφής ή διαγραφής, συμπεριλαμβανομένης και της μη εξουσιοδοτημένης δημιουργίας δεδομένων. Η Διαθεσιμότητα (Availability) των Πληροφοριακών Συστημάτων είναι η εξασφάλιση ότι τα υπολογιστικά συστήματα και οι πόροι υλικού και λογισμικού βρίσκονται στη διάθεση των νόμιμων χρηστών όποτε απαιτηθεί η χρήση τους [05].

Για την ανάπτυξη ενός πλάνου ανάκαμψης από καταστροφή υιοθετείται το μοντέλο **Plan-Do-Check-Act (PCDA).** Είναι μοντέλο γενικότερης μορφής και καλύπτει την δημιουργία ολόκληρου του μηχανισμού του ISMS, και όχι μόνο ενός DR plan. Με βάση αυτό, διαμορφώνονται, αναπτύσσονται και εξελίσσονται όλες οι διαδικασίες του πλάνου. Στο σχήμα που ακολουθεί (εικ. 3.1), επεξηγείται ο τρόπος που αναπτύσσεται το μοντέλο με αποτέλεσμα να λαμβάνονται υπόψη οι απαιτήσεις ασφάλειας των πληροφοριών και των προσδοκιών των ενδιαφερόμενων μερών και, μέσα από τις απαραίτητες ενέργειες και διαδικασίες, να παράγονται αποτελέσματα τα οποία να πληρούν αυτές τις απαιτήσεις και τις προσδοκίες [24].



Εικόνα 3. 1: PCDA plan

Ακολουθώντας το μοντέλο στη γενική του μορφή βλέπουμε τις παρακάτω φάσεις:

1. Καθορισμός (PLAN) του ISMS. Γνωρίζουμε το περιβάλλον στο οποίο θα εφαρμοστεί το μοντέλο. Ορίζουμε τις πολιτικές, τους στόχους και τις διαδικασίες που θα διέπουν το μοντέλο. Αναδεικνύουμε τους πιθανούς κινδύνους και αποφασίζουμε τι είδους μέτρα προστασίας θα πάρουμε.
2. Εφαρμόγή (DO) του ISMS. Εκτελούμε όσα αποφασίσαμε και προδιαγράψαμε στην προηγούμενη φάση.
3. Έλεγχος (CHECK) του ISMS. Συγκεντρώνουμε τα αποτελέσματα του μοντέλου κατόπιν της εφαρμογής του.
4. Βελτίωση (ACT) του ISMS. Με βάση τα αποτελέσματα που έχουμε συλλέξει προχωρούμε σε βελτιωτικές ενέργειες του μοντέλου.

Καλό θα ήταν να εξηγήσουμε την εννοια του συμβάντος και του κινδύνου στα Πληροφοριακά Συστήματα. Ως Συμβάν ή Περιστατικό (Incident), ορίζεται κάτι το οποίο δύναται να προκαλέσει πιθανές απώλειες σε έναν οργανισμό, είτε αυτές είναι σε επιχειρηματικό, είτε σε επιχειρησιακό επίπεδο. Ο Κίνδυνος ή διαφορετικά Ρίσκο (Risk) είναι η πιθανότητα να συμβεί κάποιο δυσάρεστο συμβάν το οποίο θα επιφέρει σημαντικά αρνητικές επιπτώσεις σε έναν οργανισμό [33].

Το μέγεθος του ρίσκου περιλαμβάνει την πιθανότητα βλάβης ή απώλειας υπηρεσιών και αναφέρεται στην αβεβαιότητα των μελλοντικών γεγονότων και των πιθανών

αποτελεσμάτων που θα μπορούσαν να έχουν ένα ανεπιθύμητο αποτέλεσμα σε έναν οργανισμό. Ορίζεται ως η πιθανότητα ενός ανεπιθύμητου αποτελέσματος σε μια κατάσταση με αβέβαιο αποτέλεσμα. Η διαχείριση του κινδύνου είναι το αντικείμενο της ασφάλειας, το οποίο αποτελεί και σκοπό του μοντέλου PCDA. Ο κίνδυνος εξ' ορισμού αυξάνεται όσο αυξάνεται η αξία των παγίων για έναν οργανισμό. Εάν θεωρήσουμε ως πάγια τα Πληροφοριακά Συστήματα, τότε όσο μεγαλύτερη είναι η αξία τους, τόσο μεγαλύτερη είναι και η κρισιμότητά τους, άρα ενέχουν και μεγαλύτερο κίνδυνο [44].

Τα παραπάνω εκφράζονται και μαθηματικά από την παρακάτω εξίσωση [19, 20]:

R = V * P * S, όπου :

- R ορίζεται το ρίσκο (Risk).
- V είναι η αξία του παγίου (Value of asset).
- P είναι η πιθανότητα απειλής (Probability of threat).
- S είναι το μέγεθος έκθεσης του παγίου στον κίνδυνο (vulnerability exposure).

Το προτεινόμενο πλάνο Ανάκαμψης από Καταστροφή, αξιοποιεί συνδυαστικά τρία πρότυπα ISO, τα ISO/IEC 27001:2005, 27031:2011 και 22301:2012.

3.2 ISO/IEC 27001:2005

Ο Διεθνής Οργανισμός Τυποποίησης (International Organization for Standardization) και η Διεθνής Επιτροπή Ηλεκτροτεχνικής (International Electrotechnical Commission) έχουν εκδώσει μια σειρά από πρότυπα σχετικά με την Ασφάλεια Πληροφοριακών Συστημάτων. Το πρώτο κατά σειρά ISO που θα χρησιμοποιηθεί είναι το ISO/IEC 27001:2005 από την σειρά ISO/IEC 27000 [24].

Το ISO/IEC 27001:2005 «Information Technology – Security techniques – Information Security Management Systems – Requirements», είναι θεμελιώδες πρότυπο και μοντέλο εφαρμόσιμο σε όλους τους τύπους των οργανισμών και σε όλες τις μορφές εταιριών ανεξαρτήτως μεγέθους. Καλύπτει τις ανάγκες για σχεδιασμό, υλοποίηση και παρακολούθηση ενός ISMS.

3.2.1 Επισκόπηση ISO/IEC 27001:2005

Περιέχει 11 ενότητες ελέγχου, 39 ελεγκτικούς στόχους και 133 σημεία τελικού ελέγχου έτσι ώστε να είναι σε θέση να ορίζει τις απαιτήσεις για τον καθορισμό, την εφαρμογή και την τεκμηρίωση των συστημάτων διαχείρισης ασφάλειας πληροφοριών (ISMS), να προσφέρει διεθνώς αναγνωρισμένη μεθοδολογία σχετικά με την Ασφάλεια Πληροφοριών, να αξιολογεί και να συντηρεί ένα σύστημα διαχείρισης ασφάλειας πληροφοριών (ISMS), και τέλος να παρέχει ένα ολιστικό μοντέλο για κατάρτιση, υλοποίηση, λειτουργία, παρακολούθηση, αναθεώρηση, διατήρηση και βελτίωση ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ISMS). Παρέχει ένα ολοκληρωμένο σύνολο ελέγχων που αποτελείται από τις βέλτιστες πρακτικές στον τομέα της ασφάλειας των πληροφοριών εφαρμόσιμων σε όλους τους τομείς της βιομηχανίας δίνοντας έμφαση στην πρόληψη. Δίνοντας δηλαδή σημασία στο γεγονός ότι η Ασφάλεια Πληροφοριών είναι περισσότερο θέμα διαδικασιών διαχείρισης ρίσκου, παρά τεχνολογικών απαιτήσεων. Επίσης δίνεται έμφαση στο γεγονός ότι η ασφάλεια των πληροφοριών και η υιοθέτηση ενός ISMS, είναι στρατηγική απόφαση του εκάστοτε οργανισμού λαμβάνοντας υπόψη τις ανάγκες τους στόχους, το μέγεθος και τη δομή του οργανισμού. Τέλος, αποσκοπεί στην κατανόηση και εφαρμογή βασικών εννοιών του πρότυπου όπως εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα.

Εμπιστευτικότητα (Confidentiality)

Ορίζεται ως η απόκρυψη των πληροφοριών της εταιρίας από μη εξουσιοδοτημένα πρόσωπα. Μέσω της εμπιστευτικότητας εξασφαλίζεται η ιδιωτικότητα και το απόρρητο των πληροφοριών για όσο χρόνο παραμένουν διαθέσιμα και αξιοποιήσιμα.

Ακεραιότητα (Integrity)

Η ακεραιότητα των δεδομένων εξασφαλίζει την χωρίς λόγο μεταβολή των πληροφοριών και μάλιστα χωρίς αυτή η μεταβολή να καταγράφεται κάπου. Είναι δηλαδή η πρόληψη κάποιας αυθαίρετης αλλαγής (εισαγωγής ή διαγραφής) δεδομένων από μη εξουσιοδοτημένα πρόσωπα.

Διαθεσιμότητα (Availability)

Σημαίνει την δυνατότητα (ή και την ικανότητα) διάθεσης των δεδομένων χωρίς καθυστερήσεις και χωρίς να υπάρχουν απώλειες μέρους της πληροφορίας.

3.2.2 Οφέλη από το ISO/IEC 27001:2005

Μερικά από τα οφέλη του πρότυπου είναι:

- Βελτιώνεται η αποτελεσματικότητα της Ασφάλειας Πληροφοριών.
- Παρέχεται αίσθημα εμπιστοσύνης στους εμπορικούς εταίρους, στους ενδιαφερόμενους και στους εν δυνάμει πελάτες.
- Είναι πρότυπο παγκόσμιας αποδοχής.
- Η εφαρμογή του συμβάλει στη συμμόρφωση των εταιριών με τις διεθνείς εντολές και νόμους (π.χ. Νόμος περί Προστασίας Δεδομένων).
- Καλύπτει όχι μόνο τον τομέα Πληροφορικής αλλά και τις εγκαταστάσεις καθώς και το εργατικό δυναμικό.
- Ορίζει συγκεκριμένες αρμοδιότητες και ευθύνες στο προσωπικό του οργανισμού.
- Προσφέρει ευρύτερη γνώση σε όλους τους τομείς της ασφάλειας.
- Είναι ένας αξιόπιστος μηχανισμός για τη μέτρηση του βαθμού εφαρμογής και επιτυχίας των ελέγχων ασφαλείας.
- Παρέχει ισχυροποίηση στην εφαρμογή των πολιτικών και των διαδικασιών.

3.2.3 Απλή αναφορά controls ISO/IEC 27001:2005

Είναι αυτονόητο ότι για να ισχύει και να μπορεί να εφαρμοστεί το προτεινόμενο DR plan, υπάρχουν κάποια controls τα οποία είναι προαπαιτούμενα, προϋποθέσεις, για τα οποία έχουμε κάνει την παραδοχή ότι ισχύουν. Να αναφέρουμε ότι τα παρακάτω προαπαιτούμενα αφορούν την φάση PLAN του μοντέλου PCDA.

Αναλυτικότερα:

<u>Ασφάλεια Εξοπλισμού</u>

Αναφερόμαστε στη φυσική ασφάλεια του εξοπλισμού του τηλεπικοινωνιακού παρόχου, ο οποίος είναι υπεύθυνος ώστε να πληρούνται μια σειρά από μέτρα προστασίας.

1. Ο εξοπλισμός πρέπει να εδράζεται σε εγκαταστάσεις όπου θα ελέγχεται η φυσική πρόσβαση και θα επιτρέπεται η είσοδος μόνο σε εξουσιοδοτημένα άτομα. Ο έλεγχος πρόσβασης είναι ένα σύνολο από διαδικασίες και μηχανισμούς και αποσκοπεί στην επαλήθευση της ταυτότητας του προσώπου που αιτείται φυσικής πρόσβασης.

Αφορά αφενός διαδικασίες που εκτελούνται από φυσικά πρόσωπα (πχ εταιρία φύλαξης), αφετέρου αυτόματες διαδικασίες όπως για παράδειγμα είσοδος με μαγνητική κάρτα.

2. Θα είναι σε εγκαταστάσεις που θα διασφαλίζουν προστασία από περιβαντολλογικούς κινδύνους όπως σεισμούς, πλημμύρες, φωτιά, καθώς και αποφυγή κακόβουλων ενεργειών από τρίτους.
3. Για την αποφυγή ζημιάς του ενεργητικού της εταιρίας, θα πρέπει οι εγκαταστάσεις να είναι εφοδιασμένες με αδιάλειπτη παροχή ρεύματος (γεννήτριες, UPS) και ιδανικές συνθήκες κλιματισμού και ψύξης του χώρου του Datacenter.
4. Η καλωδίωση στο σύνολο της (υπόγεια και εναέρια), θα πρέπει να προστατεύεται από φυσικές ή ηθελημένες φθορές.
5. Οι εγκαταστάσεις πρέπει να ελέγχονται ανά τακτά χρονικά διαστήματα και ο οργανισμός να προβαίνει εγκαίρως σε οποιαδήποτε βελτιωτική ή διορθωτική ενέργεια.
6. Μηχανισμοί και διαδικασίες ενημέρωσης είναι υποχρεωτικό να υπάρχουν, έτσι ώστε η διοίκηση της εταιρίας να ενημερώνεται άμεσα για οποιοδήποτε πρόβλημα προκύπτει στις εγκαταστάσεις της.

Διαχείριση Δικτύου

Στόχος είναι η ασφάλεια του δικτύου της εταιρίας, και αυτό επιτυγχάνεται μέσω της αποτροπής πρόσβασης στις υπηρεσίες δικτύου σε μη εξουσιοδοτημένα άτομα. Σύμφωνα με τον ορισμό της Ασφάλειας Δικτύου από το Wikipedia [42], συμπεραίνουμε ότι η ασφάλεια δικτύου χαρακτηρίζει μια εταιρία όσον αφορά την ικανότητά της να διαφυλάσσει τα δεδομένα της από τυχόν αλλοιώσεις και καταστροφές. Η έννοια της ασφάλειας δικτύου είναι στενά συνυφασμένη με βασικές έννοιες που αναλύθηκαν παραπάνω, όπως εμπιστευτικότητα, ακεραιότητα, και διαθεσιμότητα. Η χρήση υπηρεσιών δικτύου πρέπει να παρέχεται μόνο σε πιστοποιημένα άτομα. Κάθε πρόσβαση θα πρέπει να ελέγχεται και να καταγράφεται από κατάλληλους ελέγχους και μεθόδους. Οι διαδικασίες ελέγχου και καταγραφής πρέπει να γίνονται μέσω αυτοματοποιημένου συστήματος, το οποίο θα είναι σε θέση να πιστοποιεί κάθε σύνδεση και να επιτρέπει πρόσβαση σε συγκεκριμένους τομείς υπηρεσιών. Η διαχείριση και ο έλεγχος των διαγνωστικών εργαλείων πρέπει να εκτελείται από συγκεκριμένα και όσο το δυνατόν λιγότερα άτομα.

Η τοπολογία του δικτύου θα πρέπει να είναι διαχωρισμένη. Λαμβάνοντας υπόψη τις υπηρεσίες της κάθε εταιρίας, τους χρήστες και τις ομάδες χρηστών τους, δεν θα πρέπει να υπάρχει ένα ενιαίο σύνολο από διευθύνσεις (IPs) δικτύου, το οποίο να εξυπηρετεί το σύνολο όλων των απαιτήσεων. Είναι αναγκαίο να υπάρχει κατακερματισμός σε μικρότερα υποδίκτυα (vlans), έτσι ώστε κάθε μια υπηρεσία ή ένα υποσύνολο χρηστών, να είναι αφενός προστατευμένη από κινδύνους παραβίασης των δικτυακών τους προσβάσεων, αφετέρου να μην έχει έτσι και αλλιώς προνόμια πρόσβασης σε άλλες υπηρεσίες δημιουργώντας τρύπες ασφάλειας.

Για κοινόχρηστα δίκτυα και ειδικότερα για όσα χρησιμοποιούνται και από εξωτερικούς συνεργάτες, και έχουν πρόσβαση στο core δίκτυο της εταιρίας, θα πρέπει να υπάρχει μέριμνα για πιο αυστηρή πολιτική πρόσβασης και μάλιστα οι προσβάσεις αυτές να έχουν περιορισμένη χρονική διάρκεια.

3.3 ISO/IEC 27031:2011

Το επόμενο ISO που θα χρησιμοποιηθεί είναι το ISO/IEC 27031:2011 [25]. Περιγράφει τις έννοιες και τις αρχές της ετοιμότητας για επιχειρησιακή συνέχεια των Πληροφοριακών Συστημάτων, και παρέχει ένα πλαίσιο μεθόδων και διαδικασιών για τον εντοπισμό και προσδιορισμό όλων των πτυχών, με στόχο την βελτίωση της ετοιμότητας ενός οργανισμού για τη διασφάλιση της επιχειρησιακής του συνέχειας. Μπορεί να εφαρμοστεί σε κάθε επιχείρηση (δημόσια ή ιδιωτική), ανεξαρτήτως μεγέθους και κλίμακας, αναπτύσσοντας και εξελίσσοντας την προετοιμασία και ετοιμότητα αυτών, μέσω του Προγράμματος Ετοιμότητας Επιχειρησιακής Συνέχειας (Information Readiness Business Continuity (IRBC) program). Απαιτεί από τις Πληροφοριακές υποδομές ετοιμότητα ώστε να μπορούν να υποστηρίξουν τις επιχειρηματικές δραστηριότητες στην περίπτωση ενδεχομένου συμβάντος ή συναφών διαταραχών που θα μπορούσαν να επηρεάσουν τη συνέχεια (συμπεριλαμβανομένης της ασφάλειας) των κρίσιμων επιχειρηματικών λειτουργιών. Δίνεται επίσης η δυνατότητα για μια εταιρία να μπορεί να μετράει την απόδοση των παραμέτρων που έχουν οριστεί για το πλάνο ετοιμότητας.

3.3.1 Οφέλη από το ISO/IEC 27031:2011

Ο σκοπός και το πεδίο εφαρμογής του προτύπου ISO/IEC 27031:2011 περιλαμβάνει όλα τα περιστατικά (συμπεριλαμβανομένων αυτών που αφορούν την ασφάλεια) που θα μπορούσαν να έχουν αντίκτυπο στις υποδομές των Πληροφοριακών Συστημάτων. Περιλαμβάνει και επεκτείνει τις πρακτικές διαχείρισης συμβάντων ασφάλειας των Πληροφοριακών Συστημάτων και επίσης περιλαμβάνει τη προετοιμασία και διαχείριση της ετοιμότητας των υποδομών. Η Ετοιμότητα Πληροφοριακών Συστημάτων για Επιχειρησιακή Συνέχεια (ICT Readiness for Business Continuity – IRBC), είναι προϋπόθεση και υποστηρικτικός κρίκος στην αλυσίδα της Διαχείρισης Επιχειρησιακής Συνέχειας (Business Continuity Management – BCM) διασφαλίζοντας ότι οι υπηρεσίες θα είναι τόσο «ανθεκτικές» σε καταστροφές έτσι ώστε να μπορούν να ανακτούνται εντός προκαθορισμένων χρονικών πλαίσιων, τα οποία θα έχουν προαποφασιστεί από την διοίκηση του εκάστοτε οργανισμού.

Η Ετοιμότητα Πληροφοριακών Συστημάτων (ICT Readiness) είναι σημαντικός παράγοντας για τους στόχους της Επιχειρησιακής Συνέχειας διότι:

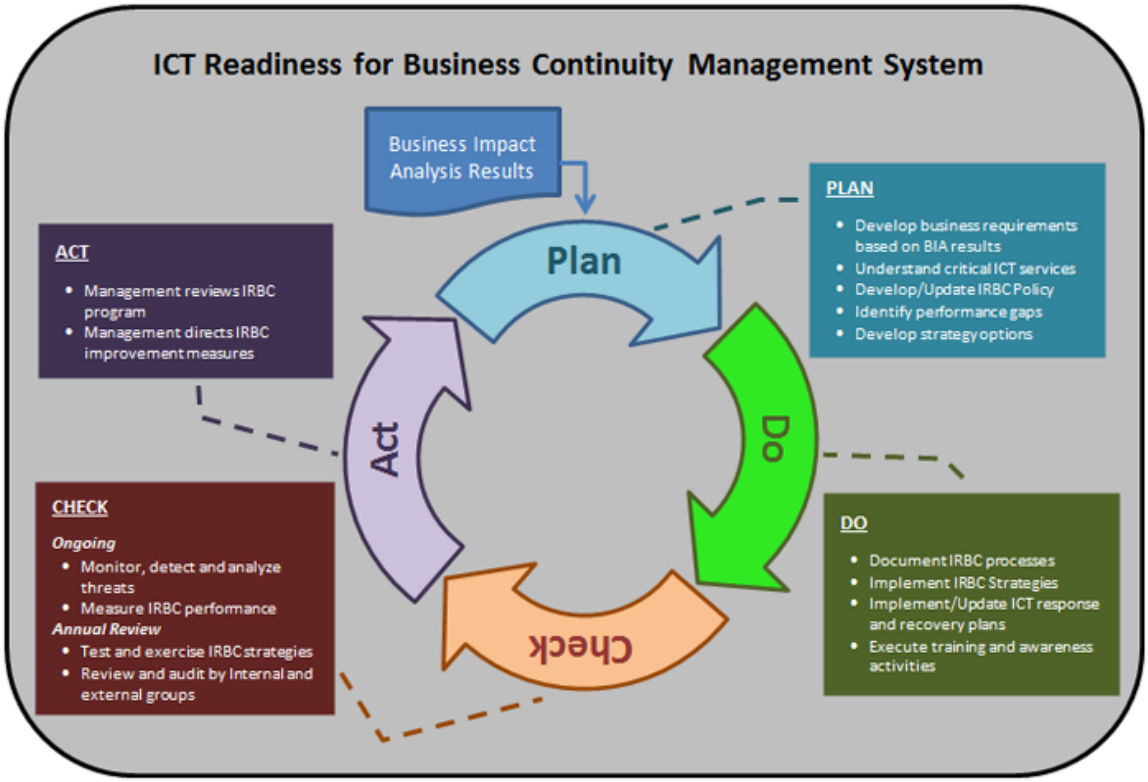
1. Τα Πληροφοριακά Συστήματα έχουν επικρατήσει σε όλες τις εταιρίες, σε όλους τους τομείς, και οι υπηρεσίες των εταιριών είναι άκρως εξαρτώμενες από τα Πληροφοριακά τους Συστήματα.
2. Το πλάνο επιχειρησιακής συνέχειας των οργανισμών είναι ημιτελές χωρίς επιπρόσθετα να υπολογίσουμε την διαθεσιμότητα των Πληροφοριακών Συστημάτων.

Η Ετοιμότητα Πληροφοριακών Συστημάτων (ICT Readiness) περικλείει:

1. Την προετοιμασία των υποδομών, των διεργασιών και των εφαρμογών του οργανισμού, συμπεριλαμβανομένου του προσωπικού, ενάντια σε οποιοδήποτε απρόβλεπτο συμβάν το οποίο θα μπορούσε να έχει επιπτώσεις στην ζωτικότητα του οργανισμού.
2. Την ενίσχυση των υπολογιστικών πόρων για επίτευξη επιχειρησιακής συνέχειας, ανάκαμψης από καταστροφή, ασφάλεια υπολογιστικών συστημάτων και άμεσης απόκρισης λόγω απρόοπτου συμβάντος.

Το πρότυπο ISO/IEC 27031:2011 ενσωματώνει και αυτό με τη σειρά του το μοντέλο

PCDA, επεκτείνοντας τις τυπικές διαδικασίες επιχειρησιακής συνέχειας, έτσι ώστε να ληφθεί υπόψη και ο τομέας των Πληροφοριακών Συστημάτων. Επίσης καθορίζει τις απαιτήσεις των Πληροφοριακών Συστημάτων για το πρόγραμμα Επιχειρησιακής Συνέχειας (IRBC program), και επιβάλλει την συνέχιση των διεργασιών των υποδομών ακόμα και όταν ένα συμβάν επηρεάζει τη συνέχεια των κρίσιμων επιχειρηματικών λειτουργιών. Αυτό περιλαμβάνει την «θωράκιση» των σημαντικότερων δεδομένων και των κρίσιμων διεργασιών. Έτσι, το εν λόγω πρότυπο ακολουθεί τον κύκλο των φάσεων του PCDA ως εξής (εικ. 3.2):



Εικόνα 3. 2: Κύκλοι φάσεων του πλάνου PCDA

1. PLAN. Καθιέρωση πολιτικών Ανάκαμψης από καταστροφή και Επιχειρησιακής Συνέχειας (Disaster Recovery Business Continuity), με στόχους, μετρήσεις, και διαδικασίες που θα σχετίζονται και θα αφορούν την διαχείριση κινδύνων, την βελτίωση των υποδομών και την ετοιμότητα της επιχείρησης, ώστε όλα να λειτουργούν σε πλαίσια καθορισμένα από το πρόγραμμα επιχειρησιακής συνέχειας.
2. DO. Εφαρμογή και λειτουργία των διαδικασιών που έχουν αποφασιστεί και διασαφηνιστεί μέσω των πολιτικών Επιχειρησιακής Συνέχειας και Ανάκαμψης από καταστροφή (BCDR policies).

3. CHECK. Αξιολόγηση και συνεχής παρακολούθηση των μετρήσεων απόδοσης, και κοινοποίηση των αποτελεσμάτων στην ανώτατη διοίκηση του οργανισμού. Αυτή η διαδικασία μπορεί να γίνει μέσω ενός ελέγχων, δοκιμών του πλάνου, ή μέσω πραγματικής εκτέλεσης κάποιου σεναρίου.
4. ACT. Τροποποίηση των πολιτικών του προγράμματος BCDR με βάση τα αποτελέσματα που εξήχθησαν στην προηγούμενη φάση του μοντέλου (έλεγχος, δοκιμή, ή η εκτέλεση του προγράμματος), προκειμένου να βελτιωθεί το πρόγραμμα Επιχειρησιακής Συνέχειας και Ανάκαμψης από καταστροφή (BCDR program).

3.3.2 Απλή αναφορά controls ISO/IEC 27031:2011

Είναι αυτονόητο ότι για να ισχύει και να μπορεί να εφαρμοστεί το προτεινόμενο DR plan, υπάρχουν κάποια controls τα οποία είναι προαπαιτούμενα, προϋποθέσεις, για τις οποίες έχουμε κάνει την παραδοχή ότι ισχύουν. Να αναφέρουμε ότι τα παρακάτω προαπαιτούμενα αφορούν την φάση PLAN (εκτός του τελευταίου το οποίο αφορά την φάση DO), του μοντέλου PCDA.

Αναλυτικότερα:

Επάρκεια Εξοπλισμού

Θα πρέπει να υπάρχει διαθέσιμο H/W για να μπορεί να υλοποιηθεί το BCDR program. Αναφερόμαστε σε racks, servers, storage arrays, tape devices, αλλά και σε δικτυακό εξοπλισμό όπως switches, routers και ότι άλλο χρειάζεται για να παρέχεται δικτυακή επικοινωνία (network connectivity) μεταξύ των εφαρμογών.

Ρόλοι και αρμοδιότητες BCDR

Θα πρέπει να έχουν οριστεί και να έχουν καταγραφεί ρόλοι, ευθύνες και αρμοδιότητες για όποιον εμπλέκεται με το BCDR [30]. Είναι απαραίτητο κάποιος να ηγείται του όλου εγχειρήματος, κάποιος ο οποίοες θα έχει οριστεί από τον οργανισμό και ο οποίος θα έχει τα ανάλογα προσόντα και ευθύνες.

Προμηθευτές

Ο οργανισμός θα πρέπει να έχει διακρίνει τυχόν εξαρτήσεις από προμηθευτές, οι οποίοι υποστηρίζουν το Πληροφοριακό Σύστημα, και να έχει εξασφαλίσει ότι οι υπηρεσίες

αυτές θα συνεχίσουν να παρέχονται αδιαλείπτως και εντός προσυμφωνημένων χρονικών πλαισίων. Τέτοιες εξαρτήσεις μπορεί να αφορούν hardware, λογισμικό, εφαρμογές τηλεπικοινωνιών, ή εξαρτήσεις που σχετίζονται με τις κτιριακές εγκαταστάσεις όπως κλιματιστικές μονάδες, μονάδες πυρασφάλειας κλπ. Προληπτικές ενέργειες που θα μπορούσαν να ελαττώσουν την πιθανότητα δυσάρεστων καταστάσεων θα μπορούσαν να είναι:

1. Η αγορά πρόσθετου εξοπλισμού και λογισμικού και η αποθήκευσή τους σε δευτερεύουσα τοποθεσία
2. Η ρητή δέσμευση των προμηθευτών για παράδοση εξοπλισμού σε πιο σύντομα χρονικά πλαίσια και για ταχύτατη αντικατάσταση προβληματικού εξαρτήματος.
3. Η κατάρτιση λίστας με εναλλακτικούς προμηθευτές σε περίπτωση αδυναμίας των πρώτων.

Ευαισθητοποίηση, δεξιότητες και γνώσεις

Όλα τα στοιχεία του BCDR όπως εργατικό δυναμικό, εγκαταστάσεις, δεδομένα, διαδικασίες, συμφωνίες με τους προμηθευτές, είναι πολύ σημαντικά για την εξασφάλιση της επιχειρησιακής συνέχειας του οργανισμού. Ως εκ τούτου, ο οργανισμός πρέπει να ενισχύει και να διατηρεί την ευαισθητοποίηση για το BCDR μέσω ενός συνεχιζόμενου προγράμματος εκπαίδευσης και πληροφόρησης του προσωπικού και να καθιερώσει διαδικασίες για την αξιολόγηση της αποτελεσματικότητας αυτών των εκπαιδεύσεων. Επίσης να διασφαλίζει ότι το προσωπικό γνωρίζει τον τρόπο που αυτές συμβάλλουν στην επίτευξη των στόχων της ετοιμότητας των Πληροφοριακών Συστημάτων (ICT Readiness). Θα πρέπει να διασφαλίζεται ότι το προσωπικό στο οποίο έχουν εκχωρηθεί αρμοδιότητες διαχείρισης του BCDR, είναι ικανό να εκτελέσει τις απαιτούμενες εργασίες.

Εγκαταστάσεις

Η φυσική τοποθεσία του πληροφοριακό συστήματος το οποίο θα έχει αναλάβει τον ρόλο ανάκτησης των κρίσιμων υπηρεσιών και δεδομένων θα πρέπει να διαχωρίζεται από την τοποθεσία του πρωτεύοντος πληροφοριακού συστήματος. Μόνο έτσι θα μείνει ανεπηρέαστο από το συμβάν που θα πλήξει το πρωτεύον σύστημα. Η επεκτασιμότητα, διαχειρισημότητα, οι επιδόσεις και το κόστος διαφόρων τεχνικών εφαρμογής BCDR θα πρέπει να εξεταστούν και να εντοπιστεί η πλέον κατάλληλη επιλογή για την επιθυμητή

στρατηγική του οργανισμού. Στρατηγική η οποία θα υποστηρίζει το σύνολο των σκοπών και των στόχων της επιχειρησιακής συνέχειας.

Αντιμετώπιση συμβάντων

Για κάθε περιστατικό που συμβαίνει, θα πρέπει να υπάρχει αποτελεσματική αντίδραση και απόκριση για να επιβεβαιώνεται γρήγορα η φύση και η έκταση του περιστατικού, έτσι ώστε οι κατάλληλοι άνθρωποι να αναλάβουν τον έλεγχο της κατάστασης. Θα πρέπει να διαπιστώσουν τι ακριβώς επηρεάζει το συμβάν και αν χρειάζεται να επικοινωνήσουν με τα ενδιαφερόμενα μέρη. Η απόκριση συμβάντος θα πρέπει να ενεργοποιεί την κατάλληλη ενέργεια του BCDR. Ο μηχανισμός απόκρισης θα πρέπει να είναι μέρος του συνολικού πλάνου επιχειρησιακής συνέχειας και οι διαδικασίες απόκρισης θα πρέπει να είναι ενσωματωμένες συνολικά στη Διαχείριση Επιχειρησιακής Συνέχειας (BCM).

Εφαρμογή Σχεδίου

Ο χρόνος που χάνεται στο δίλημμα αν πρέπει να τεθεί ή όχι σε εφαρμογή το πλάνο BCDR, δεν μπορεί να ανακτηθεί . Είναι προτιμότερο να τεθεί το πλάνο σε εφαρμογή, αρχίζοντας από τις διαδικασίες απόκρισης συμβάντος και ας ακυρωθεί στη συνέχεια, παρά να χαθεί η ευκαιρία να εντοπιστεί εγκαίρως ένα περιστατικό, με συνέπεια να υπάρξει κλιμάκωση των ζημιών. Συνεπώς, κάθε οργανισμός δεν πρέπει να διστάζει να θέσει σε εφαρμογή τις διαδικασίες του BCDR, ακολουθώντας όμως κάποια μεθοδολογία. Θα πρέπει να έχουν οριστεί διαδικασίες με τις οποίες θα γίνεται επίκληση του σχεδίου BCDR, σωστά τεκμηριωμένες και με σαφήνεια. Μόνο έτσι επιτυγχάνεται η εμπλοκή των ενδιαφερόμενων μερών στο συντομότερο δυνατό χρόνο, δρώντας είτε προλαμβάνοντας ένα συμβάν, είτε στη συνέχεια καταστέλλοντας το και μειώνοντας τις συνέπειες.

3.4 ISO/IEC 22301:2012

Το τελευταίο ISO που μελετάται, είναι το ISO/IEC 22301 [23], το πρώτο διεθνές πρότυπο του κόσμου για Διαχείριση Επιχειρησιακής Συνέχειας (Business Continuity Management – BCM). Έχει αναπτυχθεί για να βοηθήσει τους οργανισμούς να ελαχιστοποιήσουν τους κινδύνους τέτοιων καταστάσεων. Ο Διεθνής Οργανισμός

Τυποποίησης (International Organization for Standardization – ISO) έχει ξεκινήσει επίσημα το πρότυπο ISO 22301, "Κοινωνική ασφάλεια – Συστήματα Διαχείρισης Επιχειρησιακής Συνέχειας (BCMS) – Απαιτήσεις", αντικαθιστώντας το βρετανικό πρότυπο BS 25999.

3.4.1 Επισκόπηση ISO/IEC 22301:2012

Το ISO/IEC 22301:2012 καθορίζει τις απαιτήσεις για το σχεδιασμό, τη δημιουργία, την υλοποίηση, τη λειτουργία, την παρακολούθηση, αξιολόγηση και την συνεχή βελτίωση του συστήματος, έτσι ώστε να επιτυγχάνεται άμεση απόκριση και ανάκαμψη από διαταραχές, όταν αυτές προκύψουν.

Οι απαιτήσεις που καθορίζονται είναι γενικού χαρακτήρα και θα πρέπει να εφαρμόζονται σε όλους τους οργανισμούς (ή τμήματα αυτών), ανεξάρτητα από το είδος, το μέγεθος και τη φύση του οργανισμού. Η έκταση εφαρμογής των απαιτήσεων αυτών εξαρτάται από το λειτουργικό περιβάλλον και την πολυπλοκότητα του οργανισμού. Ισχύει για όλους τους τύπους και τα μεγέθη των οργανισμών που επιθυμούν να:

- Θεσπίσουν, εφαρμόσουν ή να βελτιώσουν ένα BCMS.
- Συμμορφωθούν με την πολιτική επιχειρησιακής συνέχειας του οργανισμού.
- Ζητήσουν πιστοποίηση του συστήματος BCM από έναν διαπιστευμένο φορέα πιστοποίησης.

Η τυποποίηση επιχειρησιακής συνέχειας, εξελίσσεται με το πρότυπο ISO 22301, προσθέτοντας:

- μεγαλύτερη έμφαση στον καθορισμό των στόχων, την παρακολούθηση της απόδοσης του συστήματος μέσω κατάλληλων μετρήσεων.
- Σαφέστερες προσδοκίες όσον αφορά την διαχείριση του BCMS.
- Πιο προσεκτικό σχεδιασμό για την προετοιμασία και τους πόρους που απαιτούνται για την εξασφάλιση της επιχειρησιακής συνέχειας.

Το ISO/IEC 22301:2012 είναι το πρώτο πρότυπο το οποίο είναι απολύτως συμβατό με τον οδηγό ISO 83 (ISO/Guide 83). Έχει αναπτυχθεί για να ευθυγραμμίζεται με τα

υπόλοιπα πρότυπα, γεγονός που διευκολύνει τους οργανισμούς στον εξορθολογισμό των συστημάτων τους, στη διασύνδεση και αναβάθμισή τους. Αυτό σημαίνει ότι είναι το πρώτο πρότυπο το οποίο ενσωματώνει πλήρως τις υποδομές Πληροφοριακών Συστημάτων σε άλλα συστήματα διαχείρισης, αρκεί αυτά να έχουν υιοθετήσει τις κατευθυντήριες γραμμές του ISO Guide 83.

3.4.2 Απλή αναφορά controls ISO/IEC 22301:2012

Είναι αυτονόητο ότι για να ισχύει και να μπορεί να εφαρμοστεί το προτεινόμενο DR plan, υπάρχουν κάποια controls τα οποία είναι προαπαιτούμενα, προϋποθέσεις, για τις οποίες έχουμε κάνει την παραδοχή ότι ισχύουν. Να αναφέρουμε ότι τα παρακάτω προαπαιτούμενα αφορούν την φάση PLAN του μοντέλου PCDA.

Αναλυτικότερα:

Ηγεσία

Η ανώτατη διοίκηση του οργανισμού πρέπει να καταδεικνύει τη διαρκή δέσμευση της στο BCMS. Μέσα από τις δράσεις της, μπορεί να δημιουργήσει ένα περιβάλλον στο οποίο όλοι οι εμπλεκόμενοι να λειτουργούν αποτελεσματικά και αρμονικά για τους στόχους του οργανισμού. Η διοίκηση είναι υπεύθυνη για να εξασφαλίσει ότι το BCMS είναι συμβατό με τη στρατηγική κατεύθυνση του οργανισμού, ότι ενσωματώνει τις επιχειρηματικές διαδικασίες του οργανισμού, και ότι παρέχονται στο BCMS οι απαιτούμενοι πόροι. Επίσης, σκοπός της διοίκησης είναι να επικοινωνήσει τη σπουδαιότητα της αποτελεσματικής διαχείρισης των διαδικασιών της επιχειρησιακής συνέχειας, διασφαλίζοντας ότι το BCMS επιτυγχάνει τις αναμενόμενες προσδοκίες και υποστηρίζοντας την συνεχή βελτίωσή του,

Έγκαιρη επικοινωνία

Ένα βασικό στοιχείο σε κάθε πλάνο επιχειρησιακής συνέχειας, είναι η έγκαιρη προειδοποίηση ή η ανίχνευση ενός περιστατικού. Με βάση αυτό ο κάθε οργανισμός πρέπει να ενσωματώνει ανάλογο σύστημα επικοινωνίας και να διευκολύνει την έγκαιρη και δομημένη επικοινωνία με το αρμόδιο προσωπικό εξασφαλίζοντας την λειτουργικότητα όλων των εμπλεκόμενων.

3.5 Επιλεγμένοι έλεγχοι (controls)

Παρακάτω ακολουθεί αναλυτική παρουσίαση και επεξήγηση κάθε ελέγχου που αναφέρεται στη λίστα των απαιτήσεων. Έχουν επιλεχθεί 101 έλεγχοι οι οποίοι περιλαμβάνουν 45 κύριους ελέγχους (main controls) και 56 υποελέγχους (sub-controls). Είναι δε χωρισμένοι με βάση τις φάσεις του μοντέλου Plan-Do-Check-Act και παρουσιάζονται κατά λογική σειρά υλοποίησης. Στη συνέχεια παρουσιάζονται συνοπτικά και σε λίστα κατά σειρά υλοποίησης του κάθε ελέγχου, όπως και ομαδοποιημένη λίστα ανά ISO και φάση υλοποίησης (ενότητα 3.5.5).

3.5.1 Φάση Καθορισμού (PLAN phase)

Η συγκεκριμένη φάση συμβολίζεται συντομογραφικά με το Αγγλικό γράμμα «P» και έτσι θα αρχίζει η ονομασία κάθε ελέγχου αυτής της φάσης. Στο τέλος κάθε ελέγχου αναφέρεται σε παρένθεση και το ISO στο οποίο ανήκει ο κάθε έλεγχος.

- **P1. Κατανόηση των αναγκών – understanding the needs (ISO 22301).** Όταν ένας οργανισμός υιοθετεί ένα σύστημα διαχείρισης επιχειρησιακής συνέχειας (BCMS), πρέπει να γνωρίζει τους άμεσα ενδιαφερόμενους οι οποίοι θα εμπλέκονται ενεργά με το σύστημα, καθώς και τις απαιτήσεις αυτών των εμπλεκομένων. Θα πρέπει να καταγραφούν οι ανάγκες και προσδοκίες τους από το νέο σύστημα, και αν υπάρχει κάποιο άλλο σύστημα που είναι τώρα σε εφαρμογή να καταγραφεί και αυτό. Είναι αναγκαίο να προσδιοριστούν τυχόν προβλήματα ή γεγονότα που έχουν συμβεί και που θα επηρεάσουν στο μέλλον την απόδοση του BCMS. Θα πρέπει να αναδειχθούν (και να καταγραφούν) μια σειρά από θέματα όπως:
  1. Οι δραστηριότητες του οργανισμού, οι υπηρεσίες που παρέχει και τα προϊόντα του, οι συνεργάτες του και οι πιθανές σχέσεις μεταξύ τους, και πιθανές επιπτώσεις από τυχόν διακοπή λόγω απρόοπτου συμβάντος.
  2. Αλληλοσυσχετισμοί μεταξύ των πολιτικών του υπό διαμόρφωση συστήματος και των στόχων και των πολιτικών διαχείρισης ρίσκου του οργανισμού.
  3. Ο βαθμός «ανοχής» του οργανισμού σε πιθανά ρίσκα.

  Μετά από αυτή την καταγραφή θα πρέπει να:

  1. Αποσαφηνιστούν οι στόχοι του οργανισμού όσον αφορά την

επιχειρησιακή συνέχεια.

2. Αποσαφηνιστούν οι εσωτερικοί και εξωτερικοί παράγοντες που αυξάνουν τα επίπεδα ρίσκου.
3. Οριστούν σαφή κριτήρια ρίσκου λαμβάνοντας υπόψη τις «ανοχές» του οργανισμού.
4. Καθοριστεί το πεδίο δράσης και οι στόχοι του BCMS.

- **P2 – P3 (ISO 27001).** Αυτοί οι έλεγχοι στην παρούσα διατριβή παρουσιάζονται ως απλή αναφορά. Επειδή ο σκοπός αυτής της μελέτης είναι οι εικονικές υποδομές, θεωρούμε αυτονόητο ότι ισχύουν οι εν λόγω έλεγχοι και δεν θα επεκταθούμε σε περαιτέρω ανάλυσή τους.
- **P4 – P8 (ISO 27031).** Ομοίως.

- **P9. Εξειδικευμένο προσωπικό - specialized people (ISO 27031/ISO 22301).** Είναι απαραίτητο να επιλεγεί προσωπικό με συγκεκριμένες ικανότητες και γνώσεις. Θα πρέπει να κατέχουν πάρα πολύ καλά έννοιες σχετικές με backup. Πέραν αυτού θα πρέπει και ο οργανισμός ο ίδιος να υιοθετήσει διαδικασίες για την συνεχή εκπαίδευση του προσωπικού και για την διατήρηση και εφαρμογή αυτών των γνώσεων πάνω στις διεργασίες του Πληροφοριακού Συστήματος. Μια μέθοδος είναι να μεταλαμπεδεύσουν τεχνογνωσία στο προσωπικό οι εξωτερικοί συνεργάτες. Άλλη μέθοδος είναι μέσω τεχνικών εγχειριδίων ή μέσω συνεχών εργαστηρίων (workshops) να εφαρμόζουν νέες τεχνικές γνώσεις.
- **P10 (ISO 27031).** Αυτοί οι έλεγχοι στην παρούσα διατριβή παρουσιάζονται ως απλή αναφορά. Επειδή ο σκοπός αυτής της μελέτης είναι οι εικονικές υποδομές, θεωρούμε αυτονόητο ότι ισχύουν οι εν λόγω έλεγχοι και δεν θα επεκταθούμε σε περαιτέρω ανάλυσή τους.
- **P11. Εγκαταστάσεις – facilities (ISO 27031).** Κατά την διαδικασία προσδιορισμού των κινδύνων, ο οργανισμός θα πρέπει να αναπτύξει στρατηγικές για τη μείωση των επιπτώσεων της μη διαθεσιμότητας των κύριων εγκαταστάσεων του Πληροφοριακού Συστήματος. Αυτό σημαίνει πρόσθετο H/W και μπορεί να περιλαμβάνει ένα ή περισσότερα από τα ακόλουθα:
    1. Εναλλακτικές (δευτερεύουσες) εγκαταστάσεις (alternative site) μέσα στην εταιρία που θα υποστηρίζουν ένα μερίδιο των υπηρεσιών.
    2. Εναλλακτικές εγκαταστάσεις οι οποίες θα εδρεύουν σε κάποιον άλλο συνεργάτη.
    3. Παρεχόμενες εναλλακτικές εγκαταστάσεις από εταιρίες που ειδικεύονται σε

αυτού του είδους τις υπηρεσίες.

Απαραίτητο όμως είναι η απόφαση για τον τύπο των εναλλακτικών εγκαταστάσεων. Θα πρέπει να υλοποιηθεί ένα alternative site το οποίο θα είναι «hot-standby» έτσι ώστε αν χρειαστεί να τεθεί σε παραγωγική λειτουργία να είναι άμεσα διαθέσιμο. Για να επιτευχθεί αυτό θα πρέπει όλη η υποδομή του Πληροφοριακού Συστήματος να γίνεται αντιγραφή (replicate) στο δευτερεύον site.

- **P12. Συντήρηση εξοπλισμού (ISO 27001).** Οι υποδομές πρέπει να συντηρούνται επαρκώς και να αναβαθμίζονται συνεχώς. Μόνο έτσι επιτυγχάνεται η διαθεσιμότητα του εξοπλισμού χωρίς διακοπές και απρόοπτα, διασφαλίζοντας την ακεραιότητα των δεδομένων (data integrity).
- **P13. Κατάλληλο λογισμικό ανάκαμψης υπηρεσιών – appropriate services recovery S/W (ISO 27031).** Πρέπει να έχουν εγκατασταθεί κατάλληλα προγράμματα λογισμικού τα οποία θα δίνουν την δυνατότητα για ανάκαμψη των υπηρεσιών έπειτα από καταστροφή. Η μεθοδολογία μπορεί να διαφέρει. Οι επιλογές έχουν να κάνουν μεταξύ της συνεχούς αντιγραφής δεδομένων σε εναλλακτική τοποθεσία (data replication), και της εκτέλεσης αντιγραφής ολόκληρης της εφαρμογής (image), ανά τακτά χρονικά διαστήματα.
- **P14. Υπογραφή πλάνου – sign off (ISO 27031).** Το πλάνο Επιχειρησιακής Συνέχειας και Ετοιμότητας (IRBC) θα πρέπει να υποβληθεί στην διοίκηση του οργανισμού, ενημερώνοντας την αν το επιλεγμένο πλάνο είναι σε θέσει να ανταποκριθεί στις απαιτήσεις του οργανισμού. Στη συνέχεια η διοίκηση θα πρέπει να επιλέξει ή όχι το προτεινόμενο πλάνο. Αν τελικά το εγκρίνει, θα πρέπει να υπογράψει τις τεκμηριωμένες προτάσεις που αναφέρονται σε αυτό, και να επιβεβαιώσει ότι υποστηρίζονται συνολικά οι απαιτήσεις περί επιχειρησιακής συνέχειας.
- **P15, P16 (ISO 22301).** Αυτοί οι έλεγχοι στην παρούσα διατριβή παρουσιάζονται ως απλή αναφορά. Επειδή ο σκοπός αυτής της μελέτης είναι οι εικονικές υποδομές, θεωρούμε αυτονόητο ότι ισχύουν οι εν λόγω έλεγχοι και δεν θα επεκταθούμε σε περαιτέρω ανάλυσή τους.
- **P17. Προϋπολογισμός – Budget (ISO 27031).** Η στρατηγική για Επιχειρησιακή Συνέχεια και Ετοιμότητα (IRBC), απαιτεί τον σχεδιασμό και υλοποίηση τεχνικών λύσεων οι οποίες να προσφέρουν ανθεκτικότητα υποδομών, πρόβλεψη και αποφυγή κινδύνων, γρήγορη ανάκαμψη. Οι λύσεις που θα προταθούν θα πρέπει να

υποστηρίζουν όλο το φάσμα των υπηρεσιών του οργανισμού. Όλα αυτά όμως μεταφράζονται σε σημαντικό κόστος για τον οργανισμό, κόστος που θα πρέπει να αποδεχτεί η διοίκηση.

- **P18. Πεδίο δράσης του BCMS – BCMS scope (ISO 22301).** Εδώ καθορίζονται τα όρια του συστήματος λαμβάνοντας υπόψη όσα καταγράφηκαν στον έλεγχο P1. Το πεδίο δράσης θα πρέπει να είναι διαθέσιμο ως καταγεγραμμένο έγγραφο και να:
    1. Περιέχει όλα τα τμήματα του οργανισμού τα οποία θα συμπεριλαμβάνονται στο σύστημα.
    2. Περιέχει τις απαιτήσεις του συστήματος λαμβάνοντας υπόψη τους στόχους, τις υποχρεώσεις και τις δεσμεύσεις του οργανισμού.
    3. Αναδεικνύει προϊόντα και υπηρεσίες του συστήματος.
    4. Λαμβάνει υπόψη τις απαιτήσεις και τις ανάγκες των εμπλεκομένων, είτε αυτοί είναι εσωτερικοί (υπάλληλοι, διοίκηση), είτε εξωτερικοί (πελάτες, προμηθευτές).
    5. Καθορίσει τα όρια δράσης του συστήματος λαμβάνοντας υπόψη το μέγεθος, την φύση και την πολυπλοκότητα του οργανισμού.
    6. Καταγράψει τυχόν εξαιρέσεις υπηρεσιών από το σύστημα. Εξαιρέσεις οι οποίες θα έχουν συμφωνηθεί από όλους τους εμπλεκόμενους, και θα γίνεται ρητώς σαφές ότι τυχόν διακοπή αυτών δεν θα επηρεάσει την λειτουργία του BCMS και την λειτουργία άλλων κρίσιμων υπηρεσιών, όπως αυτές θα έχουν καθοριστεί στο Business Impact Analysis και στο Risk Assessment.
- **P19 (ISO 27031).** Αυτοί οι έλεγχοι στην παρούσα διατριβή παρουσιάζονται ως απλή αναφορά. Επειδή ο σκοπός αυτής της μελέτης είναι οι εικονικές υποδομές, θεωρούμε αυτονόητο ότι ισχύουν οι εν λόγω έλεγχοι και δεν θα επεκταθούμε σε περαιτέρω ανάλυσή τους.
- **P20 Κατανόηση των αναγκών (ISO 22301).** Αναφέρθηκε και αναλύθηκε μαζί με τον έλεγχο P1.
- **P21. Inventory of assets (ISO 27001).** Με τον όρο «asset» (δηλ. περιουσιακό στοιχείο), αναφερόμαστε σε όλα όσα έχουν αξία για έναν οργανισμό. Αυτά είναι είτε δεδομένα, είτε πληροφορίες είτε ακόμα και υπολογιστικοί πόροι και h/w. Είναι απολύτως απαραίτητο κάθε εταιρία να έχει γνώση των στοιχείων που έχουν αξία για αυτήν και στη συγκεκριμένη περίπτωση να γνωρίζει τι έχει στην ιδιοκτησία της όσον αφορά το h/w. Επομένως θα πρέπει να καταγραφεί όλος ο εξοπλισμός που θα μετέχει στο DR plan, να διασαφηνίζεται πλήρως αν είναι στο σύνολο του σε

συμβόλαιο συντήρησης ή αν κάποιο κομμάτι του εξοπλισμού δεν είναι, και φυσικά αυτός ο κατάλογος εξοπλισμού να ανανεώνεται και να συντηρείται συνεχώς.

- **P22. Ανάλυση Επιχειρησιακού Αντίκτυπου – Business impact analysis - BIA (ISO 22301).** Η Ανάλυση Επιχειρησιακού Αντίκτυπου είναι μια μέθοδος προσδιορισμού των επιπτώσεων που ένας οργανισμός θα μπορούσε να υποστεί ως αποτέλεσμα ενός συμβάντος το οποίο θα έθετε σε κίνδυνο σημαντικές πληροφορίες του οργανισμού. Βοηθά στον προσδιορισμό των απαιτήσεων για ένα σύστημα επιχειρησιακής συνέχειας και ξεκαθαρίζει τα επόμενα βήματα που πρέπει να ακολουθήσει ο οργανισμός για την επαρκή προστασία των υπηρεσιών του. Είναι ένα σημαντικό στάδιο στη συνολική διαδικασία ανάλυσης κινδύνου και αποσκοπεί στον προσδιορισμό αποτελεσματικών μέτρων ασφαλείας με στόχο αφενός την ελαχιστοποίηση της συχνότητας εμφάνισης απρόοπτων συμβάντων, αφετέρου την ελαχιστοποίηση του επιχειρησιακού αντίκτυπου λόγω αυτών των πιθανών καταστροφικών γεγονότων.
- **P23. Μέγιστη ανεκτή περίοδος διακοπής – maximum tolerable period of disruption – MTPD (ISO 22301).** Θεωρείται η χρονική διάρκεια που επιτρέπεται μια υπηρεσία να είναι εκτός λειτουργίας. Είναι ο χρόνος κατά τον οποίο δεν υπάρχουν αρνητικές επιπτώσεις για τον οργανισμό. Επιπτώσεις που θα μπορούσαν να προκύψουν ως αποτέλεσμα της μη παροχής της υπηρεσίας.
- **P24. Ιεράρχηση – Prioritization (ISO 22301).** Λαμβάνοντας υπόψη την Ανάλυση Επιχειρησιακού Αντίκτυπου, θα πρέπει να γίνει μια λίστα με όλες τις υπηρεσίες κρίσιμες και μη, και ύστερα να ταξινομηθούν σε σειρά προτεραιότητας ανάλογα με την κρισιμότητα της καθεμίας. Με αυτό τον τρόπο θα γνωρίζουμε σε περίπτωση εφαρμογής του πλάνου επιχειρησιακής συνέχειας, ποιες υπηρεσίες πρέπει να ανακάμψουν άμεσα και ποιες θα έπονται.
- **P25 Καταγραφή και επιλογή – determination & selection (ISO 22301).** Με βάση την Ανάλυση Επιχειρησιακού Αντίκτυπου και την Ανάλυση Ρίσκου (που θα δούμε στη συνέχεια), θα πρέπει να καταγραφούν τυχόν εξαρτήσεις μεταξύ των υπηρεσιών και θα πρέπει να καταρτιστεί συγκεκριμένη στρατηγική ανάκαμψης η οποία:
    1. Θα προστατεύει πρωτίστως τις υπηρεσίες που είναι πρώτες στην λίστα ιεράρχησης.
    2. Θα προχωρά σε ανάκαμψη αυτών των υπηρεσιών καθώς και των εξαρτώμενων υπηρεσιών.

Σημαντικό είναι να αναφερθεί ότι τα παραπάνω θα πρέπει να γίνουν εντός των

χρονικών περιόδων που έχουν οριστεί από το MTPD.

- **P26. Επιδιωκόμενος χρόνος ανάκτησης – Recovery Time Objective (RTO) (ISO 22301).** Ορισμός και καταγραφή του επιδιωκόμενου χρόνου ανάκαμψης για κάθε υπηρεσία.
- **P27. Καθορισμός κρίσιμων υπηρεσιών (ISO 27031).** Μέσα στο πλήθος των υπηρεσιών μιας εταιρίας, υπάρχουν κρίσιμες και λιγότερο σημαντικές υπηρεσίες. Κάθε μια από τις κρίσιμες υπηρεσίες θα πρέπει να ανακτηθεί σε όσο το δυνατόν συντομότερο χρονικό διάστημα. Για κάθε υπηρεσία λοιπόν θα πρέπει να συνταχθεί ξεχωριστό έγγραφο Επιδιωκόμενου χρόνου ανάκτησης (Recovery Time Objective – RTO) και Επιδιωκόμενου σημείου ανάκτησης (Recovery Point Objective – RPO). Επιδιωκόμενος χρόνος ανάκτησης (RTO), είναι το χρονικό πλαίσιο μέσα στο οποίο η υπηρεσία πρέπει να ανακάμψει μετά από μια καταστροφή. Αφορά τον μέγιστο χρόνο κατά τον όποιο η υπηρεσία «επιτρέπεται» να παραμείνει μη διαθέσιμη. Χωρίς δηλαδή να προκαλούνται μη ανεκτές επιπτώσεις σε άλλους πόρους ή κρίσιμες επιχειρησιακές λειτουργίες. Εαν ο χρόνος ανάκαμψης είναι μεγαλύτερος από τη Μέγιστη Ανεκτή Περίοδος Διακοπής (MTPD), τότε θεωρείται ότι ο οργανισμός υφίσταται ανεπανόρθωτη ζημιά. Επιδιωκόμενο Σημείο Ανάκτησης (RPO) είναι το χρονικό διάστημα πριν από την βλάβη, για το οποίο θα χρειαστεί ανάκτηση δεδομένων. Για παράδειγμα εάν RPO=24 ώρες, σημαίνει ότι είναι υποχρεωτική η ανάκτηση δεδομένων των τελευταίων 24 ωρών. Άρα πρέπει να υπάρχει διαθέσιμο αντίγραφο ασφάλειας των τελευταίων 24 ωρών. Η παρακάτω εικόνα (εικ. 3.3), παρουσιάζει τους δύο κύριους παράγοντες της διαθεσιμότητας σε σχέση με ένα τυχαίο γεγονός διακοπής λειτουργίας των Πληροφοριακών Συστημάτων.

Εικόνα 3. 3: Παράγοντες διαθεσιμότητας

- **P28. Capacity Management (ISO 27001).** Για την δημιουργία του DR site θα πρέπει να υπολογιστούν οι απαιτούμενοι πόροι που χρειάζονται, έτσι ώστε να φιλοξενηθούν όσες υπηρεσίες κριθεί απαραίτητο ότι πρέπει να είναι στο DR site. Θα πρέπει λοιπόν να γίνει εκ των προτέρων μελέτη και υπολογισμός όσον αφορά h/w resources που θα χρειαστούν. Αναφερόμαστε σε racks, servers, απαιτήσεις σε cpu και memory και storage capacity. Ο στόχος είναι να λειτουργεί το DR ακόμα και με το μίνιμουμ των critical υπηρεσιών, αυτών δηλαδή που θα έχουν 1η προτεραιότητα για ανάκαμψη.
- **P29. Information back-up (ISO 27001/ISO 27031).** Ο οργανισμός θα πρέπει να εξετάσει μια σειρά από πολιτικές αντιγράφων ασφαλείας, για να είναι προετοιμασμένος για κάποιο πιθανό συμβάν στον τομέα των Πληροφοριακών Συστημάτων [31]. Οι επιλογές για προστασία και ανθεκτικότητα των υποδομών, καθώς και πρόβλεψη για άμεση ανάκτηση και αποκατάσταση των δεδομένων έπειτα από μια απρογραμμάτιστη διακοπή, είναι τελικά μονόδρομος αν θέλουμε να επιτευχθεί Επιχειρησιακή Συνέχεια και Ετοιμότητα (IRBC). Εδώ είναι αναγκαίο να κάνουμε έναν απαραίτητο διαχωρισμό. Άλλη ερμηνεία και χρησιμότητα έχει η έννοια «δεδομένα (data)» και άλλη ερμηνεία έχει η έννοια «πληροφορία (information)». Συμβουλευόμενοι τεχνικά εγχειρίδια ορίζουμε ως «δεδομένα» κάθε πληροφορία που έχει αποθηκευτεί σε κάποιο μέσω αποθήκευσης σε οποιαδήποτε μορφή (format) [16, 33]. Με τον όρο «πληροφορία» εννοούμε τα δεδομένα μαζί με την εννοιολογική τους σημασία. Για όλες οι κρίσιμες διεργασίες απαιτείται να υπάρχει συνεχής αναβάθμιση και να υπάρχουν αντίγραφα ασφαλείας των δεδομένων, τα οποία θα είναι όσο το δυνατόν πιο επίκαιρα, λαμβάνοντας πάντα υπόψη την πολιτική αντιγράφων ασφάλειας της εκάστοτε εταιρίας όσον αφορά την περιοδικότητα αυτών. Η περιοδικότητα των αντιγράφων ασφάλειας ορίζεται και εξαρτάται από το τι έχει συμφωνηθεί στα Recovery Point Objectives (RPO) για κάθε εφαρμογή. Θα πρέπει να έχουν ελεγχθεί ότι έχουν ολοκληρωθεί χωρίς λάθη και πρέπει να εκτελείται δοκιμαστική επαναφορά δεδομένων ανά τακτά χρονικά διαστήματα.
- **P30. Αποθήκευση αντιγράφων ασφάλειας (ISO 27031).** Οι κρίσιμες υπηρεσίες απαιτούν γρήγορη ανάκαμψη, άρα απαιτούν πρόσφατα και ενημερωμένα αντίγραφα ασφάλειας [34]. Η περιοδικότητα των αντιγράφων ασφάλειας θα πρέπει να έρχεται σε πλήρη συμφωνία με τα RTO, RPO της κάθε υπηρεσίας και να διασφαλίζουν την ακεραιότητα και διαθεσιμότητα των δεδομένων όπως ακριβώς απαιτεί και το ISO/IEC 27001:2005. Επομένως πρέπει να ληφθούν υπόψη μια σειρά

από παράγοντες όπως:

1. Με ποιο τρόπο αποθηκεύονται τα δεδομένα; Αποθηκεύονται σε δίσκους στο ίδιο το datacenter; Αποθηκεύονται σε οπτικούς δίσκους CD/DVD ROMs, ή αποθηκεύονται σε ταινίες; Για κάθε μια από τις προαναφερθείσες μεθόδους, θα πρέπει να υπάρχει και ο αντίστοιχος μηχανισμός ανάκτησης των δεδομένων αυτών.
2. Σε ποια τοποθεσία αποθηκεύονται τα δεδομένα; Αποθηκεύονται στην ίδια την εταιρία (onsite) ή εκτός εταιρίας (off site); Επίσης αν αποθηκεύονται off site, πόσα χιλιόμετρα είναι μακριά από το datacenter και πόση ώρα απαιτείται για να επιστρέψουν αν χρειαστεί;
3. Με ποιο τρόπο αποστέλλονται offsite; Μέσω δικτύου οπτικών ινών ή μέσω καθημερινής αποστολής οπτικών δίσκων;

- **P31. Information back-up (ISO 27001/ISO 27031).** Η διατήρηση των αντιγράφων ασφάλειας εξασφαλίζει επανάκτηση των δεδομένων σε περίπτωση βλάβης της υποδομής ή σε περίπτωση αποτυχημένης παραμετροποίησης κάποιου συστήματος, η οποία κατέληξε σε ολική ή μερική μη διαθεσιμότητα υπηρεσιών. Τα αντίγραφα ασφάλειας δεν έχουν καμία απολύτως αξία και χρησιμότητα, αν όταν χρειαστούν, διαπιστώσουμε ότι δεν μπορεί να γίνει επιτυχημένη επαναφορά δεδομένων λόγω προβληματικού backup. Όπως είπαμε και προηγουμένως λοιπόν, θα πρέπει να υπάρχουν οι κατάλληλοι μηχανισμοί ελέγχου backup και restore, έτσι ώστε να εξασφαλίζεται η εγκυρότητα και αρτιότητα του backup για να επιτυγχάνεται ακεραιότητα των αντιγράφων ασφάλειας (backup integrity). Ένας άλλος σημαντικός παράγοντας σε ότι αφορά την προστασία των δεδομένων, είναι η κρυπτογράφηση των αντιγράφων ασφάλειας. Υπάρχει η επιλογή της συμμετρικής και η επιλογή της ασύμμετρης κρυπτογράφησης. Κάθε μία έχει πλεονεκτήματα και αδυναμίες που η ανάλυσή τους ξεφεύγει από τα πλαίσια αυτής της διατριβής. Ένας γενικός κανόνας αναφέρει πως όσο πιο ισχυρή κρυπτογράφηση δεδομένων επιτυγχάνουμε, τόσο πιο δύσκολη γίνεται η χρήση των δεδομένων αυτών στο στάδιο της ανάκτησης.
- **P32. Information handling procedures – Privilege management (ISO 27001).** Θα πρέπει να έχουν οριστεί διαδικασίες διαχείρισης των αντιγράφων ασφαλείας έτσι ώστε να διασφαλίζεται η προστασία και η εμπιστευτικότητα των δεδομένων [34]. Η χρήση των αντιγράφων ασφαλείας θα πρέπει να επιτρέπεται μόνο σε εξουσιοδοτημένο προσωπικό το οποίο θα έχει πάρει άδεια μέσω καταγεγραμμένων

διαδικασιών και του οποίου η πρόσβαση θα πρέπει να καταγράφεται και να πιστοποιείται χρησιμοποιώντας προσωπικά διαπιστευτήρια (username/password).

- **P33. Management of removable media (ISO 27001).** Θα πρέπει να έχουν οριστεί διαδικασίες όσον αφορά την πρόσβαση στα εξωτερικά αντίγραφα ασφάλειας, έτσι ώστε να υπάρχει διαθεσιμότητα όταν και όποτε παραστεί ανάγκη χρησιμοποίησης αυτών. Θα πρέπει να είναι προσβάσιμα σε όλο το εξουσιοδοτημένο προσωπικό.
- **P34. Απαιτήσεις πόρων – resource requirements (ISO 22301).** Ο οργανισμός θα πρέπει να καθορίσει τους πόρους που απαιτούνται για να υλοποιηθούν οι στρατηγικές του πλάνου επιχειρησιακής συνέχειας. Σαν πόρους νοούνται:
    1. Το προσωπικό που θα αναλάβει να διεκπεραιώσει τις εν λόγω πολιτικές.
    2. Information and data.
    3. Κτιριακές εγκαταστάσεις.
    4. Υποδομές και εξοπλισμός πληροφοριακών συστημάτων.
    5. Διαθέσιμο budget.
    6. Συνεργάτες και προμηθευτές.
- **P35. Διαχείριση Επικινδυνότητας – Risk Assessment (ISO 22301).** Κατανόηση των κινδύνων και των απειλών. Κατανόηση των επιπτώσεων του σεναρίου μια απειλή να εξελιχθεί σε συμβάν. Για κάθε κρίσιμη υπηρεσία θα πρέπει να υπάρχει διαχείριση του αντίστοιχου ρίσκου ως εξής: είτε μειώνοντας την πιθανότητα διακοπής των υπηρεσιών, είτε μειώνοντας τη χρονική διάρκεια της διακοπής [44].

3.5.2 Φάση Εφαρμογής (DO phase)

Η συγκεκριμένη φάση συμβολίζεται συντομογραφικά με το Αγγλικό γράμμα «D» και έτσι θα αρχίζει η ονομασία κάθε ελέγχου αυτής της φάσης. Στο τέλος κάθε ελέγχου αναφέρεται σε παρένθεση και το ISO στο οποίο ανήκει ο καθένας.

- **D1. Στρατηγική Επιχειρησιακής Συνέχειας – BC strategy (ISO 22301).** Η στρατηγική και η δράσεις που θα αποφασιστούν, μελετώντας την Ανάλυση Επιχειρησιακού Αντίκτυπου (BIA) και το έγγραφο Διαχείρισης Κινδύνου (RA). Περιέχει μια δέσμη ενεργειών όπως η καταγραφή αλληλεξαρτήσεων, η εκ των προτέρων διασφάλιση των απαιτούμενων πόρων, και η απόφαση για ολική προστασία ή μερικό περιορισμό των επιπτώσεων.

- **D2. (D2.1 έως D2.3). Μέτρα προστασίας – Protection & mitigation measures (ISO 22301).** Για κάθε ρίσκο που έχει εντοπιστεί (και έχει αποφασιστεί η εξάλειψή του), πρέπει να οριστούν μέτρα προνοητικότητας (proactive measures), για:
    1. Να μειωθεί η πιθανότητα διακοπής των υπηρεσιών.
    2. Αν τελικά δεν αποφευχθεί η διακοπή, τουλάχιστον να μειωθει η χρονική διάρκεια αυτής.
    3. Να μειωθούν γενικότερα οι επιπτώσεις στον οργανισμό λόγω της διακοπής κάποιων υπηρεσιών.
- **D3. (D3.1 έως D3.6.4). Διαδικασίες πλάνου ανάκαμψης από καταστροφή – DRP procedures (ISO 22301).** Χρειάζονται διαδικασίες έτσι ώστε να διαχειριστεί σωστά μια αναπάντεχη διακοπή. Μια από αυτές τις διαδικασίες είναι και η εκπόνηση του Πλάνου Ανάκαμψης από Καταστροφή (Disaster Recovery Plan – DRP) το οποίο θα πρέπει να:
    1. Περιλαμβάνει συγκεκριμένα και άμεσα actions κατά την διάρκεια της διακοπής
    2. Είναι ευέλικτο σε απρόβλεπτα γεγονότα.
    3. Είναι εστιασμένο στις περιπτώσεις που είναι πιθανό να οδηγήσουν σε διακοπή υπηρεσιών.
    4. Έχει υιοθετηθεί βασισμένο σε σωστές προβλέψεις.
    5. Είναι αποτελεσματικό στη ελάττωση των συνεπειών. Αυτό επιτυγχάνεται μέσω εφαρμογής των προαποφασισμένων ενεργειών για τη μείωση του ρίσκου (risk mitigation).
    6. Υπάρχουν μηχανισμοί έγκαιρης ειδοποίησης, έτσι ώστε να εντοπίζεται έγκαιρα το τυχόν συμβάν και αφού εντοπιστεί, να υπάρχει ενδοεταιρική επικοινωνία για την ειδοποίηση των κατάλληλων ανθρώπων με σκοπό την διαχείριση του. Μετά το πέρας, θα πρέπει να συνεχίζεται η παρακολούθησή του.

- **D3.6.5. Απόκριση συμβάντος – incident response (ISO 27031).** Για κάθε πιθανό συμβάν που μπορεί να συμβεί, θα πρέπει να διασαφηνιστεί άμεσα η φύση του και το μέγεθος των πιθανών επιπτώσεων στην λειτουργία του οργανισμού. Άμεσα επίσης θα πρέπει να κοινοποιηθεί σε όλους τους εμπλεκόμενους (stakeholders), ενημερώνοντας τους σχετικά, και στη συνέχεια να τεθεί σε εφαρμογή το πλάνο των προσυμφωνηθέντων ενεργειών.

- **D4. (D4.1 – D4.6). Πλάνο Ανάκαμψης από Καταστροφή – Disaster Recovery Plan – DRP (ISO 22301).** Είναι συγκεντρωμένες και καταγεγραμμένες όλες οι διαδικασίες απόκρισης για κάθε πιθανό περιστατικό. Αποσκοπεί στο πως θα επιτευχθεί η επιχειρησιακή συνέχεια των υπηρεσιών (ή η ανάκαμψη αυτών), μέσα σε ένα προκαθορισμένο χρονικό πλαίσιο. Πρέπει να περιέχει:
    1. Καθορισμένους ρόλους και αρμοδιότητες σε συγκεκριμένα άτομα.
    2. Διαδικασία ενεργοποίησης απόκρισης.
    3. Λεπτομέρειες άμεσης διαχείρισης των επιπτώσεων όσον αφορά την υγεία των εμπλεκομένων, τις στρατηγικές ενέργειες αντιμετώπισης της διακοπής, την πρόληψη επέκτασης περαιτέρω διακοπής και σε άλλες κρίσιμες υπηρεσίες.
    4. Διαδικασίες για τον τρόπο που ο οργανισμός θα προβαίνει σε ανάκτηση των υπηρεσιών του, λαμβάνοντας υπόψη την σειρά προτεραιότητας.
    5. Διαδικασία τερματισμού του πλάνου επιχειρησιακής συνέχειας μετά το πέρας της διακοπής.
    6. Διαδικασίες ελέγχου του πλάνου για να σιγουρευτούμε ότι δεν έχουμε παραλείψει κάτι. Πρέπει να ορίσουμε:
        1. Περιγραφή σεναρίου.
        2. Περιγραφή προκαθορισμένου στόχου και σκοπού.
        3. Περιγραφή υποθέσεων και παραδοχών.
        4. Περιγραφή πιθανών ρίσκων.
        5. Περιγραφή κριτηρίων επιτυχής εκτέλεσης σεναρίου.
        6. Περιγραφή χρονικών περιθωρίων.
        7. Εγγύηση ότι όλα τα δεδομένα είναι σε αντίγραφα ασφαλείας.
        8. Ότι η διαδικασία των αντιγράφων ασφαλείας ολοκληρώθηκε εντός αποδεκτού χρονικά διαστήματος.
        9. Να εμπλέκονται σταδιακά όλοι όσοι έχουν οριστεί να συμμετέχουν.
        10. Να ελαχιστοποιείται το ρίσκο διακοπής των υπηρεσιών.
        11. Να παράγονται αναφορές (reports), με αποτελέσματα και προτάσεις βελτίωσης.
        12. Να διεξάγονται δοκιμαστικά σενάρια ανά τακτά χρονικά διαστήματα και ιδίως όταν συμβαίνουν σημαντικές αλλαγές στη δομή και στις διαδικασίες της εταιρίας.

- **D4.6.1 Περιγραφή σεναρίου (ISO 27031).** Ο οργανισμός θα πρέπει να δοκιμάσει την λειτουργία του πλάνου σε κάθε τομέα του Πληροφοριακού Συστήματος, δοκιμάζοντας όχι μόνο ανάκαμψη υπηρεσιών, αλλά και γενικότερα την διαθεσιμότητα, την επάρκεια και αξιοπιστία των υποδομών. Επίσης θα πρέπει να δοκιμαστούν οι διαδικασίες ελέγχου και ειδοποίησης συμβάντος.
- **D4.6.2 - D4.6.4. Δοκιμή πλάνου – test & exercise plan (ISO 27031).** Περιγραφή προκαθορισμένου στόχου και σκοπού. Περιγραφή υποθέσεων και παραδοχών. Περιγραφή πιθανών ρίσκων. Στις περισσότερες περιπτώσεις, το σύνολο των στοιχείων και διαδικασιών ενός IRBC δεν μπορεί να αποδειχθεί σε μία και μόνη δοκιμή και άσκηση. Ένα σωστό σενάριο άσκησης θα μπορούσε, επομένως, να είναι αυτό που θα προσομοίαζε πλήρως ένα πραγματικό περιστατικό. Ο δοκιμαστικός έλεγχος θα πρέπει να περιλαμβάνει διάφορα επίπεδα πρακτικής άσκησης, αρχίζοντας από μια δοκιμή της ανθεκτικότητας του Πληροφοριακού Συστήματος, μέχρι και την ολοκληρωτική ανάκαμψη υπηρεσιών. Οι στόχοι της δοκιμής θα πρέπει να ευθυγραμμίζονται πλήρως με το ευρύτερο πεδίο εφαρμογής της επιχειρησιακής συνέχειας του οργανισμού. Κάθε δοκιμή θα πρέπει να έχει καθορισμένους επιχειρηματικούς και τεχνικούς στόχους για την επικύρωση ή όχι ενός συγκεκριμένου στοιχείου της στρατηγικής IRBC. Η άσκηση σε επιμέρους στοιχεία του πλάνου (απομονωμένες ασκήσεις ελέγχου), είναι συμπληρωματική προς την πλήρη έλεγχο και λογίζεται ως μέρος ενός συνεχιζόμενου προγράμματος δοκιμών. Το πρόγραμμα δοκιμών θα πρέπει να καθορίζει τη συχνότητα, την έκταση και τη μορφή της κάθε άσκησης. Τα παρακάτω παραδείγματα αναφέρουν ανάλογα επιπέδα άσκησης:
    1. ανάκτηση δεδομένων: Ανάκτηση ενός μετά από καταστροφή.
    2. ανάκτηση συστήματος: Ανάκτηση ενός server μετά από καταστροφή.
    3. ανάκτηση εφαρμογής: Ανάκτηση μιας εφαρμογής. Είναι πιθανό να αποτελείται από διάφορους servers.
    4. Ανακατεύθυνση (failover) υπηρεσιών: Ανακατεύθυνση υπηρεσιών που φιλοξενούνται σε πλατφόρμα υψηλής διαθεσιμότητας (πχ virtualization, clustering).
    5. ανάκτηση δεδομένων από αντίγραφο ασφάλειας: Ανάκτηση δεδομένων από οπτικό δίσκο ή από ταινία.
    6. έλεγχος του δικτύου.

- **D4.6.5 - D4.6.8. Διαχείριση δοκιμαστικών ελέγχων – managing an exercise (ISO 27031).** Περιγραφή κριτηρίων επιτυχής εκτέλεσης σεναρίου. Περιγραφή χρονικών περιθωρίων. Εγγύηση ότι όλα τα δεδομένα είναι σε αντίγραφα ασφαλείας, και ότι η διαδικασία δημιουργίας αντιγράφων ασφαλείας ολοκληρώθηκε εντός χρονικά αποδεκτού διαστήματος. Μια σωστή δομή άσκησης θα πρέπει να εμπλέκει όλους τους όσους έχουν επιφορτιστεί με κάποιο ρόλο από το πλάνο. Επίσης να υπάρχει επάρκεια διαθέσιμο προσωπικού για να αναλάβει ενεργό ρόλο κατά την άσκηση. Να υπάρχουν ορόσημα (milestones) της άσκησης. Με το πέρας της άσκησης θα πρέπει να πληρούνται οι βασικοί στόχοι και τα ορόσημα αυτής, να παρακολουθούνται κάθε εν δυνάμει κίνδυνοι, να καταγράφεται κάθε επισκέπτης ή παρατηρητής και τέλος να ενημερώνονται όλοι οι συμμετέχοντες της άσκησης για τα αποτελέσματα αυτής.

- **D4.6.9 – D4.6.12. Reports και σενάρια δοκιμών (ISO 22301).** Αναφέρθηκε και αναλύθηκε στον έλεγχο D4 – D4.6.

3.5.3 Φάση Ελέγχου (CHECK phase)

Η συγκεκριμένη φάση εμφανίζεται συντομογραφικά με το Αγγλικό γράμμα «C» και έτσι θα αρχίζει η ονομασία κάθε ελέγχου αυτής της φάσης. Στο τέλος κάθε ελέγχου αναφέρεται σε παρένθεση και το ISO στο οποίο ανήκει ο καθένας.

- **C1 – C4. Παρακολούθηση, ανάλυση, αξιολόγηση – monitoring, analysis, evaluation (ISO 22301).** Ο οργανισμός θα πρέπει να καθορίσει ποιες ανάγκες του θα πρέπει να παρακολουθούνται και τι ακριβώς θα πρέπει να μετριέται. Πρέπει να καθοριστούν αποδεκτοί μέθοδοι παρακολούθησης και μέτρησης και να οριστούν κατάλληλα όρια (thresholds). Στη συνέχεια θα πρέπει να καταγραφεί η απόδοση των διαδικασιών του πλάνου, και να γίνονται εσωτερικοί έλεγχοι ανά τακτά χρονικά διαστήματα. Με αυτό τον τρόπο θα γίνεται γνωστό αν έχουν διαφοροποιηθεί οι απαιτήσεις και οι ανάγκες του οργανισμού, αν έχουν αλλάξει κάποιες από τις απαιτήσεις των διεθνών προτύπων ή αν υπάρχει αλλαγή στις επιθυμίες της ανώτατης διοίκησης. Προϋπόθεση για τους ελέγχους είναι, να έχουν επιλεγεί κατάλληλοι ελεγκτές (auditors) και να έχουν θεσπιστεί σωστά κριτήρια ελέγχου. Μετά την ολοκλήρωση του ελέγχου των αναγκών, σειρά έχει ο έλεγχος του πλάνου

ανά τακτά (και προγραμματισμένα) χρονικά διαστήματα. Πρέπει να διαπιστώνεται αν υπάρχουν νέες απαιτήσεις, ή αν υπάρχουν νέες τεχνολογίες και τεχνικές οι οποίες θα ήταν χρήσιμες. Να ελέγχεται αν έχουν ολοκληρωθεί όλες οι βελτιωτικές ενέργειες που αποφασίστηκαν σε προηγούμενους ελέγχους. Τέλος να αξιολογούνται τα ευρήματα του ελέγχου, να προτείνονται ενέργειες βελτίωσης του πλάνου, και να εκτιμώνται αν όντως θα συμβάλλουν ση βελτίωση του πλάνου. Τέλος να προγραμματίζονται οι επόμενοι έλεγχοι.

3.5.4 Φάση Βελτίωσης (ACT phase)

Η συγκεκριμένη φάση εμφανίζεται συντομογραφικά με το Αγγλικό γράμμα «Α» και έτσι θα αρχίζει η ονομασία κάθε ελέγχου αυτής της φάσης. Στο τέλος κάθε ελέγχου αναφέρεται σε παρένθεση και το ISO στο οποίο ανήκει ο καθένας.

- **Α1. Συνεχής επικαιροποίηση του BCP (improvement) (ISO 27031).** Ο οργανισμός θα πρέπει να βελτιώνει συνεχώς το πλάνο Επιχειρησιακής Συνέχειας και Ετοιμότητας (IRBC), μέσω προληπτικών και διορθωτικών ενεργειών έτσι ώστε να περιορίζονται στο μέγιστο βαθμό πιθανές επιπτώσεις που έχουν προσδιοριστεί μέσω του Business Impact Analysis και του Risk Assessment. Θα πρέπει να διορθώνονται τυχόν αποτυχίες των στοιχείων του πλάνου καθορίζοντας πιθανές αδυναμίες, προσδιορίζοντας αίτια αποτυχιών, καταγράφοντας τα αποτελέσματα από τις δοκιμές ελέγχου και επανεξετάζοντας τα διορθωμένα μέτρα.
- **Α2. Συνεχής βελτίωση πλάνου (Continual BCP improvement) (ISO 22301).** Ο οργανισμός θα πρέπει να βελτιώνει συνεχώς την προσαρμοστικότητα, την επάρκεια και την αποτελεσματικότητα του πλάνου.

3.5.5 Συνοπτικοί πίνακες ελέγχων

Στη συνέχεια παρουσιάζονται δύο πίνακες σχετικοί με τους ελέγχους που αναλύσαμε προηγουμένως. Ο πρώτος πίνακας (πιν. 3.1), περιέχει τους ελέγχους που αναλύσαμε πριν, με τη ίδια λογική σειρά υλοποίησης, αλλά αυτή τη φορά με πιο συνοπτική καταγραφή. Η πρώτη στήλη αναφέρει τον κωδικό του κάθε ελέγχου σε σχέση με την φάση στην οποία ανήκει, η δεύτερη στήλη περιέχει την περιγραφή του ελέγχου, ενώ στην τρίτη στήλη αναφέρεται το ISO που χρησιμοποιήθηκε. Η τέταρτη στήλη δηλώνει

αν ο συγκεκριμένος έλεγχος είναι προαπαιτούμενος και εκτός σκοπού της διατριβής, επομένως γίνεται μια απλή αναφορά σε αυτόν. Η πέμπτη στήλη αναφέρει ποιοι έλεγχοι τελικά εφαρμόστηκαν σε εικονικές υποδομές, και η τελευταία στήλη αναφέρει ποιοι έλεγχοι θα πρέπει να πληρούνται από τα εργαλεία αποκατάστασης εικονικών υποδομών που θα δούμε στο κεφάλαιο 4.

Code	Plan-Do-Check-Act phases	ISO used	Προαπαιτούμενος έλεγχος	Applied control	For recovery tools
PLAN phase					
P1	**Understanding the needs.** Κατανόηση και γνωριμία της εταιρίας, των συνεργατών και των δραστηριοτήτων. Ανάλυση του υπάρχοντος BCMS (εαν υπάρχει για virtual environments).	ISO 22301 clause 4		●	
P2	**Ασφάλεια εξοπλισμού:** Πρόληψη φθοράς των περιουσιακών στοιχείων της εταιρίας.	ISO 27001	●		
P2.1	Προστασία εξοπλισμού. Να προστατεύεται ο εξοπλισμός της εταιρίας από εξωτερικούς κινδύνους και καταστροφές.	ISO 27001	●		
P2.2	Υποστηρικτικές υπηρεσίες. Αδιάλειπτη παροχή ρεύματος	ISO 27001	●		
P2.3	Προστασία καλωδιώσεων από διακοπή υπηρεσιών λόγω φθοράς.	ISO 27001	●		
P3	**Διαχείριση δικτύου**	ISO 27001	●		
P3.1	Ασφάλεια δικτυακών υπηρεσιών	ISO 27001	●		
P3.2	Πολιτική χρήσης υπηρεσιών	ISO	●		

	δικτύου	27001			
P3.3	Πιστοποίηση χρηστών για συνδέσεις εκτός εσωτερικού δικτύου.	ISO 27001	●		
P3.4	Διαγνωστικά προγράμματα και προγράμματα προστασίας	ISO 27001	●		
P4	**Παροχή DR υποδομής** (racks, servers, storage arrays, tape devices).	ISO 27031 clause 7.2	●		
P5	Το DR θα πρέπει να είναι σε απομακρυσμένες εγκαταστάσεις σε σχέση με το Primary site.	ISO 27031 clause 7.2	●		
P6	**Παροχή δικτύου στο DR** (switches, routers, data connectivity)	ISO 27031 clause 5.3	●		
P7	Εξασφάλιση έγκαιρης παροχής ICT υπηρεσιών, s/w, h/w από τους προμηθευτές	ISO 27031 clause 6.4	●		
P8	Δημιουργία κατάλληλων ομάδων επιφορτισμένες με διακριτούς ρόλους η καθεμία. 'Ετσι η κάθε ομάδα θα έχει συγκεκριμένες ευθύνες και αρμοδιότητες κατά την εκτέλεση του DRP.	ISO 27031 clause 6.2, clause 7.4	●		
P9	**Specialized People.** Εύρεση κατάλληλων ανθρώπων με συγκεκριμένες ικανότητες και γνώσεις. Ιδιαιτέρως ικανοποιητικές γνώσεις σε backup.	ISO 27031 clause 5.3, 6.4.2.1 & ISO 22301 clause 7.2		●	
P10	Οι εμπλεκόμενες ομάδες να	ISO 27031	●		

	έχουν τα κατάλληλα προσόντα και γνώσεις, μέσω συνεχών εκπαιδεύσεων.	clause 7.2			
P11	**Facilities.** Διαθεσιμότητα πόρων. Πρόσθετες H/W υποδομές έτσι ώστε να φτιαχτεί ένα alternate site το οποίο θα είναι hot-standby mode, όπου όλο το ICT infrastructure θα γίνεται replicate και στο alternate site.	ISO 27031 clause 6.4.2.2, 7.2.3		●	
P12	**Συντήρηση εξοπλισμού.** Οι υποδομές πρέπει να συντηρούνται επαρκώς και να αναβαθμίζονται συνεχώς έτσι ώστε να διασφαλίζεται η διαθεσιμότητά της και να έχουμε data integrity.	ISO 27001 clause 9.2.4		●	
P13	**Services recovery S/W.** Κατάλληλο S/W για recovery.	ISO 27031 clause 5.3		●	●
P14	**Sign off.** Η πρόταση για BCMS να γίνει αποδεκτή από την ανώτατη διοίκηση.	ISO 27031 clause 6.5		●	
P15	Η διοίκηση να αποδέχεται και να παροτρύνει την ύπαρξη DRP.	ISO 22301 clause 5	●		
P16	Η διοίκηση να παροτρύνει την ενημέρωση όλων για την σπουδαιότητα και τη σημασία του DRP.	ISO 22301 clause 7.4	●		
P17	**Προϋπολογισμός.** Να έχει προβλεφθεί το ανάλογο	ISO 27031 clause		●	

	budget.	6.4			
P18	**Scope:** Γιατί χρειάζεται ένα BCMS. Business requirements.	ISO 22301 clause 4.3.2		●	
P19	Διαδικασία απόκρισης σε συμβάν. Περιέχει:	ISO 27031 clause 7.3	●		
P19.1	Επιβεβαίωση του συμβάντος και της φύσης αυτού.	ISO 27031 clause 7.3	●		
P19.2	Ανάληψη ελέγχου της διαμορφοθείσας κατάστασης	ISO 27031 clause 7.3	●		
P19.3	Ενημέρωση των stakeholders σχετικά με το συμβάν	ISO 27031 clause 7.3	●		
P19.4	Εκτέλεση DRP.	ISO 27031 clause 7.4	●		
P20	**Understanding the needs.** Αποδεκτά επίπεδα ρίσκου, καταγραφή όλων των εμπλεκόμενων και των ενδιαφερόμενων μερών (διοίκηση, εργαζόμενοι, προμηθευτές, πελάτες κλπ)	ISO 22301 clause 4		●	
P21	**Inventory of assets.** Καταγραφή όλων των υπηρεσιών του Οργανισμού	ISO 27001 clause 7.1.1		●	●
P22	**Business Impact Analysis.** Καθορισμός των επιπτώσεων από κάθε διακοπή υπηρεσιών. Καθορισμός των διεργασιών οι οποίες υποστηρίζουν προϊόντα και	ISO 22301 clause 4, 8		●	●

	υπηρεσίες. Καθορισμός επιπτώσεων από ενδεχόμενη καταστροφή, και διαβάθμιση αυτών.				
P23	**MTPD.** Ορισμός Maximum Tolerable Period of Disruption για κάθε ενέργεια.	ISO 22301 clause 4, 8		●	●
P24	**Prioritization.** Προτεραιοποίηση/ιεράρχηση των παραπάνω διεργασιών, σχετικά με την σειρά ανάκαμψης.	ISO 22301 clause 4, 8.3.1		●	●
P25	**Determination & selection.** Καταγραφή αλληλο-εξαρτήσεων για όλες τις διεργασίες.	ISO 22301 clause 4, 8.3.1		●	●
P26	**RTO.** Ορισμός και καταγραφή Recovery Time Objectives (RTO) για κάθε critical υπηρεσία.	ISO 22301 clause 4, 8		●	●
P27	**Καθορισμός κρίσιμων υπηρεσιών.** Ορισμός και καταγραφή Recovery Point Objectives (RPO) για κάθε critical υπηρεσία.	ISO 27031 clause 6.3.2		●	●
P28	**Capacity Management.** Capacity planning: Minimum Business Continuity Objectives (MBCO). Πόσο capacity θα χρειαστεί για να φιλοξενηθεί μια critical υπηρεσία στο alternate site.	ISO 27001 clause 10.3.1		●	●
P29	**Information back-up.** Κρίσιμες υπηρεσίες απαιτούν	ISO 27031 clause		●	●

	πρόσφατα (ή επικαιροποιημένα), αντίγραφα ασφάλειας.	6.4.2.4 & ISO 27001 clause 10.5.1			
P30	**Data.** Με ποιο τρόπο αποθηκεύονται τα data (disk, tapes, cd-roms).	ISO 27031 clause 6.4.2.4		●	●
P31	**Information back-up.** Integrity. Κατάλληλοι μηχανισμοί backup&restore θα πρέπει να ελεγχθούν για να σιγουρευτούμε για την εγκυρότητα και αρτιότητα του backup.	ISO 27031 & 27001 clause 10.5.1		●	●
P32	**Information handling procedures – Privilege management.** Confidentiality. Η χρήση των αντιγράφων ασφαλείας πρέπει να γίνεται μόνον από εξουσιοδοτημένο προσωπικό μέσω διαδικασιών επικύρωσης.	ISO 27001 clause 10.7.3, 11.2.2		●	●
P33	**Management of removable media.** Availability. Όλοι οι authorized personnel να έχουν πρόσβαση στα assets όταν απαιτηθεί.	ISO 27001 clause 10.7.1		●	●
P34	**Resource requirements.** Εκτίμηση πόρων που χρειάζονται για ανάκαμψη κάθε διεργασίας.	ISO 22301 clause 4, 8.3.2		●	
P35	**Risk Assessment.** Κατανόηση των κινδύνων και των	ISO 22301 clause		●	

	απειλών. Κατανόηση των επιπτώσεων του σεναρίου μια απειλή να εξελιχθεί σε συμβάν. Για κάθε critical activity θα πρέπει να υπάρχει διαχείριση του αντίστοιχου ρίσκου ως εξής: είτε μειώνοντας την πιθανότητα διακοπής των υπηρεσιών, είτε μειώνοντας τη χρονική διάρκεια της διακοπής.	4, 8.2.3			
DO					
D1	**BC strategy.** Η στρατηγική και η δράσεις που θα αποφασιστούν μελετώντας την Business Impact Analysis και το Risk Assessment.	ISO 22301 clause 6, 8		●	
D2	**Protection and mitigation measures.** Για κάθε ρίσκο που έχουμε βρει (και έχουμε αποφασίσει να το εξαλείψουμε), πρέπει να ορίσουμε proactive μέτρα για:	ISO 22301 clause 6, 8.3.3		●	●
D2.1	**Reduce likelihood.** Να μειώσουμε την πιθανότητα διακοπής υπηρεσιών	ISO 22301 clause 6, 8.3.3		●	●
D2.2	**Shorten period.** Να ελαττώσουμε την χρονική διάρκεια της διακοπής	ISO 22301 clause 6, 8.3.3		●	●
D2.3	**Limit impact.** Να ελαττώσουμε τις επιπτώσεις της διακοπής των υπηρεσιών.	ISO 22301 clause 6, 8.3.3		●	
D3	**BCP and procedures.**	ISO 22301		●	

	Διαδικασίες που να διαχειρίζονται σωστά μια αναπάντεχη διακοπή. Πρέπει να:	clause 6, 8			
D3.1	Περιλαμβάνει συγκεκριμένα και άμεσα actions (κατά την διάρκεια της διακοπής)	ISO 22301 clause 6, 8		●	
D3.2	Είναι ευέλικτο σε απρόβλεπτα γεγονότα.	ISO 22301 clause 6, 8		●	
D3.3	Είναι εστιασμένο στις περιπτώσεις που είναι πιθανό να οδηγήσουν σε διακοπή υπηρεσιών.	ISO 22301 clause 6, 8		●	
D3.4	Να υλοποιηθεί βασιζόμενο σε σωστές προβλέψεις.	ISO 22301 clause 6, 8		●	
D3.5	Να είναι αποτελεσματικό στο να μειώνει τις συνέπειες. Αυτό επιτυγχάνεται μέσω της εφαρμογής των αποφάσεων που έχουν παρθεί για mitigation.	ISO 22301 clause 6, 8		●	
D3.6	**Alerting.** Να υπάρχουν διαδικασίες προειδοποίησης.	ISO 22301 clause 6, 8.4.3		●	
D3.6.1	**Detection.** Εντοπισμός του συμβάντος	ISO 22301 clause 6, 8.4.3		●	
D3.6.2	**Surveillance.** Συχνή παρακολούθηση αυτού	ISO 22301 clause 6, 8.4.3		●	
D3.6.3	**Communication.** Ενδοεταιρική επικοινωνία για την διαχείριση αυτού	ISO 22301 clause 6, 8.4.3		●	

D3.6.4	**Notification.** Ειδοποίηση των κατάλληλων ανθρώπων	ISO 22301 clause 6, 8.4.3		●	
D3.6.5	**Incident response.** Το περιστατικό πρέπει να καθοριστεί και να κοινοποιηθεί σε όλους τους εσωτερικούς και εξωτερικούς ενδιαφερόμενους (stakeholders).	ISO 27031 clause 7.3		●	
D4	**BCP**: Καταγεγραμμένες διαδικασίες απόκρισης ενός γεγονότος. Πως θα επιτευχθεί η συνέχεια των υπηρεσιών (ή η ανάκαμψη αυτών), μέσα σε ένα προκαθορισμένο χρονικό πλαίσιο. Περιέχει:	ISO 22301 clause 6, 8.4.4		●	
D4.1	Καθορισμένους ρόλους και αρμοδιότητες σε συγκεκριμένα άτομα.	ISO 22301 clause 6, 8		●	
D4.2	Διαδικασία ενεργοποίησης απόκρισης	ISO 22301 clause 6, 8		●	
D4.3	Λεπτομέρειες σχετικά με την άμεση διαχείριση των συνεπειών στην υγεία των εμπλεκομένων, στις στρατηγικές ενέργειες αντιμετώπισης της διακοπής, στην πρόληψη περαιτέρω διακοπής και σε άλλες critical υπηρεσίες.	ISO 22301 clause 6, 8		●	
D4.4	Πως η εταιρία θα αποφασίσει να προβεί σε recovery τις υπηρεσίες της και μάλιστα κατά προτεραιότητα.	ISO 22301 clause 6, 8		●	
D4.5	Διαδικασία τερματισμού του BCP μετά το πέρας της διακοπής.	ISO 22301 clause 6, 8		●	

D4.6	Testing: Έλεγχος του BCP για να σιγουρευτούμε ότι είναι αυτό που θέλουμε και δεν έχουμε παραλείψει κάτι. Πρέπει:	ISO 22301 clause 6, 8		●	●
D4.6.1	**Elements of service recovery.** Περιγραφή σεναρίου.	ISO 27031 clause 8.1.3.3, 8.1.3.4		●	
D4.6.2	**Test & Exercise plan.** Περιγραφή προκαθορισμένου στόχου και σκοπού	ISO 27031 clause 8.1.3.2		●	
D4.6.3	**Test & Exercise plan.** Περιγραφή υποθέσεων και παραδοχών.	ISO 27031 clause 8.1.3.2		●	
D4.6.4	**Test & Exercise plan.** Περιγραφή πιθανών ρίσκων.	ISO 27031 clause 8.1.3.2		●	
D4.6.5	**Managing an exercise.** Περιγραφή κριτηρίων επιτυχής εκτέλεσης σεναρίου.	ISO 27031 clause 8.1.3.6		●	●
D4.6.6	**Managing an exercise.** Περιγραφή χρονικών περιθωρίων.	ISO 27031 clause 8.1.3.6		●	●
D4.6.7	**Managing an exercise.** Εγγύηση ότι τα δεδομένα είναι όλα σε αντίγραφα ασφαλείας.	ISO 27031 clause 8.1.3.6		●	●
D4.6.8	**Managing an exercise.** Ότι η διαδικασία των αντιγράφων ασφαλείας ολοκληρώθηκε εντός αποδεκτού χρονικά διαστήματος.	ISO 27031 clause 8.1.3.6		●	●
D4.6.9	Να εμπλέκονται σταδιακά όλοι όσοι έχουν οριστεί να συμμετέχουν.	ISO 22301 clause 6, 8		●	
D4.6.10	Να ελαχιστοποιείται το ρίσκο διακοπής των υπηρεσιών.	ISO 22301 clause 6, 8		●	
D4.6.11	Να παράγονται reports με αποτελέσματα και προτάσεις βελτίωσης.	ISO 22301 clause 6, 8		●	●

D4.6.12	Να διεξάγονται σενάρια ανά τακτά χρονικά διαστήματα και ιδίως όταν συμβαίνουν σημαντικές αλλαγές στη δομή και στις διαδικασίες της εταιρίας.	ISO 22301 clause 6, 8		●	●
CHECK					
C1	**Monitoring, measurement, analysis and implementation:**	ISO 22301 clause 9		●	
C1.1	Καθορισμός για το τι πρέπει να γίνεται monitored και το τι πρέπει να μετριέται.	ISO 22301 clause 9		●	
C1.2	Καθορισμός αποδεκτών μεθόδων monitoring και μέτρησης.	ISO 22301 clause 9		●	
C1.3	Καθορισμός performance metrics thresholds.	ISO 22301 clause 9		●	●
C1.4	Καταγραφή απόδοσης των διεργασιών και των διαδικασιών του BCP.	ISO 22301 clause 9		●	●
C2	Εσωτερικοί έλεγχοι ανά τακτά χρονικά διαστήματα:	ISO 22301 clause 9		●	
C2.1	Έλεγχος αν έχουν διαφοροποιηθεί οι απαιτήσεις και οι ανάγκες της εταιρίας.	ISO 22301 clause 9		●	
C2.2	Έλεγχος αν έχουν διαφοροποιηθεί οι απαιτήσεις των διεθνών standards.	ISO 22301 clause 9		●	
C2.3	Καθορισμός (από το top management), των κριτηρίων ελέγχου.	ISO 22301 clause 9		●	
C2.4	Επιλογή των κατάλληλων auditors.	ISO 22301 clause 9		●	
C3	Επανέλεγοχος του Disaster Recovery Plan σε προγραμματισμένα χρονικά διαστήματα	ISO 22301 clause 9		●	

C3.1	Καταγραφή των νέων αναγκών της εταιρίας	ISO 22301 clause 9		●	
C3.2	Έλεγχος αν ολοκληρώθηκαν actions από προηγούμενο review.	ISO 22301 clause 9		●	
C3.3	Ενημέρωση για τυχόν νέες τεχνολογίες και τεχνικές που θα ήταν χρήσιμες.	ISO 22301 clause 9		●	
C3.4	Αξιολόγηση αποτελεσμάτων από ελέγχους του πλάνου	ISO 22301 clause 9		●	
C3.5	Αξιολόγηση βελτιωτικών προτάσεων	ISO 22301 clause 9		●	
C4	Αξιολόγηση των διαδικασιών του BCP.	ISO 22301 clause 9		●	
ACT					
A1	**Improvement.** Συνεχής επικαιροποίηση του BCP.	ISO 27031 clause 9		●	
A2	**BCP improvement** Συνεχής βελτίωση του BCP	ISO 22301 clause 10		●	

Πίνακας 3. 1: Συνοπτική λίστα ελέγχων

Ο δεύτερος πίνακας (πιν. 3.2), αναφέρει πάλι όλους τους ελέγχους που χρησιμοποιήθηκαν, αλλά αυτή τη φορά ομαδοποιημένους κατά ISO και φάση υλοποίησης. Δηλαδή πρώτα αναφέρονται οι έλεγχοι του ISO 27001, στη συνέχεια οι έλεγχοι του ISO 27031 και τέλος αυτοί του ISO 22301.

ISO USED	PHASES	CONTROLS
ISO/IEC 27001	Phase: PLAN	P2, P2.1, P2.2, P2.3, P3, P3.1, P3.2, P3.3, P3.4, P12, P21, P28, P29, P31, P32, P33
ISO/IEC 27001	Phase: DO	Κανένας έλεγχος αυτού του ISO δεν χρησιμοποιήθηκε σε αυτή τη φάση.
ISO/IEC 27001	Phase: CHECK	Κανένας έλεγχος αυτού του ISO δεν χρησιμοποιήθηκε σε αυτή τη φάση.
ISO/IEC 27001	Phase: ACT	Κανένας έλεγχος αυτού του ISO δεν χρησιμοποιήθηκε σε αυτή τη φάση.
ISO/IEC 27031	Phase: PLAN	P4, P5, P6, P7, P8, P9, P10, P11, P13, P14, P17, P19, P19.1, P19.2, P19.3, P19.4, P27, P29, P30, P31
ISO/IEC 27031	Phase: DO	D3.6.5, D4.6.1, D4.6.2, D4.6.3, D4.6.4, D4.6.5, D4.6.6, D4.6.7, D4.6.8,
ISO/IEC 27031	Phase: CHECK	Κανένας έλεγχος αυτού του ISO δεν χρησιμοποιήθηκε σε αυτή τη φάση.
ISO/IEC 27031	Phase: ACT	A1
ISO/IEC 22301	Phase: PLAN	P1, P9, P15, P16, P18, P20, P22, P23, P24, P25, P26, P34, P35
ISO/IEC 22301	Phase: DO	D1, D2, D2.1, D2.2, D2.3, D3, D3.1, D3.2, D3.3, D3.4, D3.5, D3.6, D3.6.1, D3.6.2, D3.6.3, D3.6.4, D4, D4.1, D4.2, D4.3, D4.4, D4.5, D4.6, D4.6.9, D4.6.10, D4.6.11, D4.6.12
ISO/IEC 22301	Phase: CHECK	C1, C1.1, C1.2, C1.3, C1.4, C2, C2.1, C2.2, C2.3, C2.4, C3, C3.1, C3.2, C3.3, C3.4, C3.5, C4
ISO/IEC 22301	Phase: ACT	A2

Πίνακας 3.2: Ομαδοποιημένοι έλεγχοι ανά ISO

Κεφάλαιο 4

Προτεινόμενο DR plan – Παρουσίαση εργαλείων

Στο κεφάλαιο αυτό παρουσιάζεται ένα προτεινόμενο Πλάνο Ανάκαμψης από Καταστροφή προσαρμοσμένο κυρίως σε τηλεπικοινωνιακούς παρόχους, υλοποιώντας με πραγματικές πληροφορίες σχεδόν όλους τους ελέγχους. Ενδεικτικά να αναφέρουμε ότι καταγράφονται οι εικονικές μηχανές και οι κρισιμότερες υπηρεσίες που συνήθως έχουν οι τηλεπικοινωνιακοί πάροχοι και καθορίζεται ο μέγιστος ανεκτός χρόνος διακοπής για κάθε υπηρεσία καθώς και οι χρόνοι RTO και RPO. Για όλες τις υπηρεσίες γίνεται μια πρώτη Ανάλυση Επιχειρησιακού Αντίκτυπου και διεξάγεται ενδεικτικά για μία από αυτές εκτενέστερη μελέτη. Ακολουθεί μελέτη διαχείρισης ρίσκου και στη συνέχεια παρουσιάζονται συγκεκριμένες διαδικασίες του πλάνου ανάκαμψης όσον αφορά την απόκριση και διαχείριση συμβάντος, τη στρατηγική των αντιγράφων ασφάλειας και ενέργειες δοκιμών και αξιολόγησης του πλάνου. Στο 2ο μισό του κεφαλαίου παρουσιάζονται τέσσερα εργαλεία ανάκαμψης από καταστροφή, για

εικονικές υποδομές, με αναλυτικές πληροφορίες εγκατάστασης και διαχείρισης αυτών, καθώς και εκτενή κατάλογο προσφερόμενων και μη προσφερόμενων χαρακτηριστικών, σύμφωνα και με τουε ελέγχους του κεφαλαίου 3. Θα πρέπει να σημειωθεί ότι η εφαρμογή του πλάνου έγινε μόνον όσον αφορά τη διαδικασία λήψης αντιγράφων ασφάλειας και της επαναφοράς.. Θεωρείται δεδομένο πως για να εφαρμοστούν οι κανόνες του πλάνου που αφορούν τις προαναφερθείσες διαδικασίες, έχουν υλοποιηθεί εκ των προτέρων οι προγενέστεροι έλεγχοι του πλάνου, όπως εύρεση κατάλληλων ανθρώπων, δημιουργία αντίστοιχων ομάδων, εύρεση πόρων, επιλογή auditors κλπ (Πιν. 3.1, Στήλη «Applied control»). Τέλος να τονίσουμε ότι το παρόν DRP δεν έχει δοκιμαστεί ακόμη σε πραγματικές συνθήκες, για τον τηλεπικοινωνιακό πάροχο που υλοποιήθηκε, λόγω επιχειρησιακών περιορισμών (πχ διάθεση στην κυκλοφορία νέων προϊόντων με αυξημένη ζήτηση).

4.1 Προτεινόμενο Disaster Recovery Plan

Το προτεινόμενο Πλάνο Ανάκαμψης από Καταστροφή αποτελείται από τους ελέγχους που αναφέρθηκαν στο προηγούμενο κεφάλαιο και συμπληρώνεται σταδιακά υλοποιώντας κάθε έναν από αυτούς τους ελέγχους. Λόγω του ότι οι έλεγχοι είναι αρκετοί, περισσότεροι από εκατό, για την όσο το δυνατόν καλύτερη απεικόνισή τους επιλέχθηκε να διατηρηθεί η ονομασία που είχαν στο κεφάλαιο 3.

- **P1, P20. Κατανόηση των αναγκών (understanding the needs).** Οι υπηρεσίες ενός τηλεπικοινωνιακού παρόχου είναι η παροχή σταθερής και κινητής τηλεφωνίας, η παροχή συνδέσεων internet και ενδεχομένως παροχή τηλεόρασης μέσω internet. Βεβαίως υπάρχουν και εσωτερικές υπηρεσίες της εταιρίας όπως είναι η μισθοδοσία των υπαλλήλων, η τιμολόγηση των προϊόντων, η λογιστική διαχείριση των πελατών. Όλες οι παραπάνω υπηρεσίες είναι αλληλοσυσχετιζόμενες και πιθανή διακοπή μιας εξ' αυτών ενδέχεται να προκαλέσει πρόβλημα και σε κάποια άλλη. Οι επιπτώσεις από τυχόν διακοπή των παραπάνω υπηρεσιών είναι τεράστιες τόσο σε κόστος όσο και στη φήμη της εταιρίας, ειδικά αν αναφερόμαστε σε υπηρεσίες προσφερόμενες στο καταναλωτικό κοινό. Όσον αφορά τις ενδοεταιρικές υπηρεσίες οι επιπτώσεις δεν είναι ιδιαίτερα σημαντικές λόγω του ότι τυχόν διακοπή τους δεν θα γίνει γνωστή στο ευρύ κοινό. Επομένως μπορούμε να πούμε ότι ο οργανισμός έχει

μηδενική ανοχή σε πιθανή διακοπή υπηρεσιών που σχετίζονται με τους πελάτες, ενώ σε ενδοεταιρικές υπηρεσίες υπάρχει κάποιο μικρό ποσοστό ανοχής.

Μετά από αυτά καταλήγουμε ότι το πεδίο δράσης και οι στόχοι του BCMS είναι η εκπλήρωση των αναγκών της εταιρίας όσον αφορά την αδιάλειπτη παροχή των προαναφερθεισών υπηρεσιών ή στην χειρότερη περίπτωση τον ελάχιστο χρόνο ανάκαμψης αυτών σε περίπτωση κάποιου απρόοπτου συμβάντος. Σαν εσωτερικοί παράγοντες ορίζουμε τις εμπλεκόμενες διευθύνσεις (πχ εμπορικό, τεχνικό, οικονομικό, ανθρώπινο δυναμικό), και σαν εξωτερικούς παράγοντες ορίζουμε τις εταιρίες HP, DELL οι οποίες προμηθεύουν το H/W.

- **P9. Εξειδικευμένο προσωπικό (specialized people).** Είναι όλοι οι μηχανικοί οι οποίοι έχουν σαν job description "Backup Administrator" καθώς και οι μηχανικοί με job description "Systems Administrator".
- **P11. Εγκαταστάσεις (facilities).** Για την υλοποίηση του προτεινόμενου Disaster Recovery Plan χρειάζονται εναλλακτικές εγκαταστάσεις (DR site), σε διαφορετική τοποθεσία από τις κύριες εγκαταστάσεις, και σε απόσταση 100χλμ τουλάχιστον από αυτές. Το DR site θα εκτελεί χρέη «hot-standby site». Αυτό σημαίνει ότι οι υποδομές του θα είναι αντίγραφα (replicas) των πρωτευόντων υπηρεσιών με συνεχή ανανέωση δεδομένων. Το πόσο συνεχής θα είναι η ενημέρωση των δεδομένων, ορίζεται από το RPO, και αυτό στην περίπτωσή μας είναι αποφασισμένο στα 5 λεπτά.
- **P12. Συντήρηση εξοπλισμού εξοπλισμού:** Η συντήρηση των υποδομών είναι στην αρμοδιότητα των system administrators και θα πρέπει να ακολουθείται πλάνο αναβάθμισης υποδομών εκτελούμενο κάθε 4 μήνες.
- **P13. Κατάλληλο λογισμικό ανάκαμψης υπηρεσιών (appropriate services recovery S/W).** Στην παρούσα διατριβή δοκιμάστηκαν και αξιολογήθηκαν σε πραγματικές συνθήκες εργασίας τα δωρεάν εργαλεία ghettoVCB, Veeam Backup free edition, VMware vSphere Replication, XSI backup. Τα αποτελέσματα των δοκιμών μπορείτε να τα δείτε στο επόμενο (5ο) κεφάλαιο.
- **P14. Υπογραφή πλάνου (sign off).** Είναι η υπογραφή του προτεινόμενου πλάνου από τον Διευθύνων Σύμβουλο της εταιρίας (CEO), και όλους τους εμπλεκόμενους Διευθυντές Διευθύνσεων.
- **P17. Προϋπολογισμός (Budget).** Το κόστος για την αγορά, εγκατάσταση και συντήρηση του H/W δεν θα πρέπει να υπολείπεται του ποσού των 500.000€
- **P18. Πεδίο δράσης του BCMS (BCMS scope).**

Εδώ καθορίζεται το πεδίο εφαρμογής του συστήματος διαχείρισης Επιχειρησιακής Συνέχειας (BCMS) [08]. Δραστηριότητες που σχετίζονται με τη διαχείριση και την παροχή των προαναφερθέντων προϊόντων και υπηρεσιών στο πλαίσιο της συμφωνίας μεταξύ της ομάδας υλοποίησης του BCMS και του οργανισμού. Το περιεχόμενο του πεδίου εφαρμογής έχει σχεδιαστεί για να φιλοξενήσει είτε την επέκταση είτε την προσθήκη είτε ακόμα και την απόσυρση οποιουδήποτε προϊόντος ή εφαρμογής. Στο εν λόγω έγγραφο περιλαμβάνονται τα: Ανάλυση Επιχειρηματικού Αντίκτυπου (BIA), Επιδιωκόμενος χρόνος ανάκτησης (RTO), Μέγιστη ανεκτή περίοδος διακοπής (MTPD), Διαχείριση Επικινδυνότητας (RA), πλάνο ασκήσεων του συστήματος, εκπαίδευση του προσωπικού και αξιολόγηση του συστήματος.

- **P21. Inventory of assets:** Θα υπάρχει ένα inventory το οποίο θα περιέχει μια καταγραφή των συστημάτων και ένα δεύτερο inventory το οποίο θα περιέχει μια καταγραφή των υπηρεσιών. Ακολουθεί η καταγραφή μερικών ενδεικτικών συστημάτων (πιν 4.1) και υπηρεσιών (πιν. 4.2).

Virtual Machine	CPUs	Memory	Storage Capacity	Operating System
3par	4	4 MB	61 GB	Red Hat Enterprise Linux 5 (64-bit)
ASlinux	2	3 MB	40 GB	Red Hat Enterprise Linux 6 (64-bit)
ASlinux2	2	3 MB	43 GB	Red Hat Enterprise Linux 6 (64-bit)
BIS	8	16 MB	81 GB	Red Hat Enterprise Linux 5 (64-bit)
BISrv5	4	8 MB	40 GB	Red Hat Enterprise Linux 5 (64-bit)
boserv	8	16 MB	40 GB	Novell SUSE Linux Enterprise 10 (64-bit)
Bosrv01	12	26 MB	43 GB	Novell SUSE Linux Enterprise 11 (64-bit)
BuildSrv	2	4 MB	40 GB	Red Hat Enterprise Linux 6 (64-bit)
CiscoIse02	4	16 MB	30 GB	Red Hat Enterprise Linux 5 (64-bit)

clone	4	20 MB	20 GB	Red Hat Enterprise Linux 5 (64-bit)
CloudControl	8	16 MB	143 GB	Microsoft Windows Server 2008 R2 (64-bit)
xvas	2	8 MB	143 GB	Red Hat Enterprise Linux 6 (64-bit)
cvantage3	4	3 MB	143 GB	Novell SUSE Linux Enterprise 10 (64-bit)
Das1	8	8 MB	30 GB	Novell SUSE Linux Enterprise 10 (64-bit)
Das2	8	8 MB	31 GB	Microsoft Windows XP Professional (32-bit)
Dasbuilder	8	30 MB	81 GB	Red Hat Enterprise Linux 6 (64-bit)
Dasquery1	8	49 MB	53 GB	Red Hat Enterprise Linux 6 (64-bit)
Dasquery2	8	49 MB	62 GB	Red Hat Enterprise Linux 6 (64-bit)
DasRep4	4	6 MB	25 GB	Red Hat Enterprise Linux 6 (64-bit)
Datacl2	2	3 MB	81 GB	Red Hat Enterprise Linux 6 (64-bit)
demodem	1	4 MB	11 GB	Red Hat Enterprise Linux 6 (64-bit)

Πίνακας 4. 1: Πίνακας συστημάτων και καταγραφή βασικών υπηρεσιών (πιν 4.2)

Υπηρεσία	**Περιγραφή**
Σταθερή τηλεφωνία	Παροχή υπηρεσιών σταθερής τηλεφωνίας σε συνδρομητές
Κινητή τηλεφωνία	Παροχή υπηρεσιών κινητής τηλεφωνίας σε συνδρομητές
ADSL	Παρχή υπηρεσιών internet (συνδέσεις ADSL)
VDSL	Παρχή υπηρεσιών internet (συνδέσεις VDSL)
TV over Ethernet	Παροχή υπηρεσιών τηλεόρασης μέσω internet

Human Resources	Παροχή ενδοεταιρικών υπηρεσιών σχετιζόμενες με εργασίες του Ανθρώπινου Δυναμικού της εταιρίας
ERP	Παροχή ενδοεταιρικών υπηρεσιών σχετικά με την συνολική διαχείριση των διαδικασιών της εταιρίας
Customer Help	Παροχή ενδοεταιρικών υπηρεσιών σχετικά με την εξυπηρέτηση πελατών της εταιρίας
Finance	Παροχή ενδοεταιρικών υπηρεσιών σχετικά με την λογιστική κα οικονομική διαχείριση της εταιρίας
Billing	Παροχή ενδοεταιρικών υπηρεσιών σχετικά με την λογιστική χρέωση των υπηρεσιών και των προϊόντων που προσφέρει η εταιρία στους πελάτες
Employee Payroll	Παροχή ενδοεταιρικών υπηρεσιών σχετικά με την μισθοδοσία των εργαζομένων στην εταιρία
Intranet	Παροχή ενδοεταιρικών υπηρεσιών σχετικά με την αντιμετώπιση βλαβών των προσωπικών υπολογιστών του υπαλληλικού προσωπικού.

Πίνακας 4.2: Πίνακας υπηρεσιών

- **P22. Ανάλυση Επιχειρησιακού Αντίκτυπου (Business impact analysis - BIA).** Πρόκειται για τη μέθοδο που αξιολογεί ποσοτικά και ποιοτικά την επίδραση που έχει σε έναν οργανισμό η μη διαθεσιμότητα κάποιας υπηρεσίας ή η μη λειτουργία κάποιου συστήματος [15, 38]. Στόχος της ανάλυσης των επιπτώσεων είναι:
  1. Να καταγραφούν και να κατανοηθούν οι επιπτώσεις που μπορεί να έχουν στην εταιρία οι (ολικές ή μερικές) διακοπές των υπηρεσιών που παρέχονται από τα Πληροφοριακά Συστήματα (μετρήσιμες και μη).
  2. Να βρεθούν οι σχέσεις και αλληλεξαρτήσεις των Πληροφοριακών Συστημάτων (Εφαρμογών) και των διαδικασιών που παρέχουν τις υπηρεσίες.
  3. Να προσδιοριστούν τα απαιτούμενα ελάχιστα χρονικά διαστήματα για την ανάκτηση αυτών των Εφαρμογών (Recovery Time Objective - RTO και Recovery Point Objective - RPO).
  4. Να προσδιοριστούν οι προτεραιότητες ανάκτησης των Εφαρμογών.

Ακολουθεί πίνακας με τις κρίσιμες υπηρεσίες, την επίδραση που θα έχουν στον οργανισμό και τις συνέπειες τυχόν διακοπής αυτών και το προτεινόμενο RTO. Στη συνέχεια ακολουθεί λεπτομερέστερη ανάλυση ενδεικτικά για μια από αυτές τις υπηρεσίες.

Κρίσιμες υπηρεσίες	Περιγραφή	Επίδραση	Συνέπειες διακοπής	RTO
Σταθερή τηλεφωνία	Παροχή υπηρεσιών σταθερής τηλεφωνίας σε συνδρομητές	High	Θα διακοπεί το δίκτυο σταθερής τηλεφωνίας σε όλους τους συνδρομητές και δεν θα μπορούν να πραγματοποιήσουν ή να λάβουν τηλεφωνική κλήση. Συνέπεια αυτών είναι ο καταποντισμός της φήμης της εταιρίας με πιθανότητα πολλοί συνδρομητές να αλλάξουν τηλεπικοινωνιακό πάροχο.	30 λεπτά
Κινητή τηλεφωνία	Παροχή υπηρεσιών κινητής τηλεφωνίας σε συνδρομητές	High	Θα διακοπεί το δίκτυο κινητής τηλεφωνίας σε όλους τους συνδρομητές και δεν θα μπορούν να πραγματοποιήσουν ή να λάβουν τηλεφωνική κλήση. Συνέπεια αυτών είναι ο καταποντισμός της φήμης της εταιρίας με πιθανότητα πολλοί συνδρομητές να αλλάξουν τηλεπικοινωνιακό πάροχο.	30 λεπτά
ADSL	Παρχή υπηρεσιών internet (συνδέσεις ADSL)	High	Θα διακοπεί το δίκτυο παροχής internet σε όλους τους συνδρομητές. Συνέπεια αυτών είναι ο καταποντισμός της φήμης της εταιρίας και είναι πιθανό πολλοί συνδρομητές να αλλάξουν πάροχο.	30 λεπτά

VDSL	Παρχή υπηρεσιών internet (συνδέσεις VDSL)	High	Θα διακοπεί το δίκτυο παροχής VDSL πλοήγησης στο internet σε όλους τους συνδρομητές. Συνέπεια αυτών είναι ο καταποντισμός της φήμης της εταιρίας με πιθανότητα αλλαγή παρόχου πολλών συνδρομητών.	30 λεπτά
TV over Ethernet	Παροχή υπηρεσιών τηλεόρασης μέσω internet	High	Θα διακοπεί η προβολή τηλεόρασης σε όλους τους συνδρομητές και δεν θα μπορούν να πραγματοποιήσουν ή να λάβουν τηλεφωνική κλήση. Συνέπεια αυτών είναι ο καταποντισμός της φήμης της εταιρίας με πιθανότητα πολλοί συνδρομητές να αλλάξουν πάροχο.	30 λεπτά
Human Resources	Παροχή ενδο-εταιρικών υπηρεσιών σχετιζόμενες με εργασίες του Ανθρώπινου Δυναμικού της εταιρίας	Low	Θα διακοπεί η δυνατότητα διαχείρισης υπηρεσιών που έχουν να κάνουν με το Ανθρ. Δυν. της εταιρίας. Θα επηρεαστούν μόνο οι υπάλληλοι της συγκεκριμένης Διεύθυνσης. Οι επιπτώσεις είναι αμελητέες διότι η διακοπή δεν θα γίνει ευρέως αντιληπτή.	120 λεπτά
CRM	Διαχείριση εταιρικών πελατών. Εφαρμογή εισαγωγής αιτήματος πελάτη για κάθε	High	Δεν θα είναι δυνατή η καταγραφή και η εξυπηρέτηση των αιτημάτων των πελατών.	30 λεπτά

	παρεχόμενη υπηρεσία			
ERP	Παροχή ενδο-εταιρικών υπηρεσιών σχετικά με την συνολική διαχείριση των εταιρικών διαδικασιών.	Medium	Δεν θα είναι δυνατή η διαχείριση και η παρακολούθηση ενδοεταιρικών διαδικασιών. Αφορά μόνο τους υπάλληλους της εταιρίας και όχι το καταναλωτικό κοινό. Οι συνέπειες είναι περιορισμένης εμβέλειας.	60 λεπτά
Customer Help	Παροχή ενδο-εταιρικών υπηρεσιών σχετικά με την εξυπηρέτηση πελατών της εταιρίας	High	Δεν θα είναι δυνατή η διαχείριση και η τεχνική εξυπηρέτηση των πελατών της εταιρίας. Οι συνέπειες είναι σοβαρότατες και είναι πιθανό πολλοί συνδρομητές να αλλάξουν πάροχο.	30 λεπτά
CDR	Λήψη, επεξεργασία και αποστολή των αρχείων τηλεφωνικών κλήσεων των συνδρομητών	Medium	Δεν θα είναι δυνατή η αποστολή των CDRs στα συστήματα τιμολόγησης για την έκδοση των λογαριασμών των πελατών. Οι συνέπειες είναι περιορισμένης εμβέλειας.	60 λεπτά
Finance	Παροχή ενδο-εταιρικών υπηρεσιών σχετικά με την λογιστική κα οικονομική διαχείριση της εταιρίας	Medium	Δεν θα είναι δυνατή η διαχείριση λογιστικών και οικονομικών θεμάτων της εταιρίας. Αφορά μόνο τους υπάλληλους των συγκεκριμένων διευθύνσεων της εταιρίας και όχι το καταναλωτικό κοινό. Οι	60 λεπτά

			συνέπειες είναι περιορισμένης εμβέλειας.	
Billing	Παροχή ενδο-εταιρικών υπηρεσιών σχετικά με την λογιστική χρέωση των υπηρεσιών και των προϊόντων που προσφέρει η εταιρία στους πελάτες	High	Δεν θα είναι δυνατή η τιμολόγηση και η χρέωση των παρεχόμενων υπηρεσιών. Συνέπεια αυτού είναι η «δωρεάν» παροχή υπηρεσιών στο καταναλωτικό κοινό για όσο διάστημα διαρκεί η διακοπή. Οι συνέπειες είναι τεράστιες όχι μόνο λόγω διαφυγόντων κερδών αλλά και λόγω δυσφήμισης του κύρους της εταιρίας.	30 λεπτά
Employee Payroll	Παροχή ενδο-εταιρικών υπηρεσιών σχετικά με την μισθοδοσία των εργαζομένων στην εταιρία	Medium	Δεν θα είναι δυνατή η επεξεργασία της μισθοδοσίας των υπαλλήλων. Αφορά μόνο τους υπάλληλους της εταιρίας και όχι το καταναλωτικό κοινό. Οι συνέπειες είναι σοβαρές αλλά περιορισμένης εμβέλειας.	60 λεπτά
Intranet services	Παροχή ενδο-εταιρικών υπηρεσιών για επίλυση βλαβών των προσωπικών υπολογιστών του προσωπικού.	Low	Δεν θα είναι δυνατή η παροχή βοηθητικών και υποστηρικτών υπηρεσιών όσον αφορά βλάβες υπολογιστών του προσωπικού. Αφορά μόνο τους υπάλληλους της εταιρίας και όχι το καταναλωτικό κοινό. Οι συνέπειες είναι περιορισμένης εμβέλειας.	120 λεπτά

Πίνακας 4. 3: Υπηρεσίες κρίσιμων συστημάτων

Μία από τις υπηρεσίες για την οποία θα προχωρήσουμε σε περαιτέρω ανάλυση επιχειρησιακού αντίκτυπου είναι η υπηρεσία «Customer Relationship Manager» (CRM).

Γενικά χαρακτηριστικά

Η βασική λειτουργία της υπηρεσίας είναι η εξυπηρέτηση των εταιρικών πελατών του οργανισμού. Σε αυτήν υπάρχει το ιστορικό του πελάτη, όπου καταγράφονται τα αιτήματά του για παροχή υπηρεσιών. Οι αιτήσεις του στη συνέχεια μεταβιβάζονται στις αντίστοιχες εφαρμογές, είτε για να υλοποιηθούν από τις τεχνικές υπηρεσίες είτε για να τιμολογηθούν. Πρόκειται για αρχιτεκτονική Client-Server.

Απαιτήσεις Ανάκτησης (Recovery Time Objective – Recovery Point Objective)

RTO: Η μέγιστη αποδεκτή χρονική διάρκεια στην οποία η υπηρεσία επιτρέπεται να μην είναι διαθέσιμη, προτού οι επιπτώσεις γίνουν μη αποδεκτές για τον οργανισμό, θα είναι: 30 λεπτά.

RPO: Η χρονική στιγμή πριν την καταστροφή, της οποίας τα δεδομένα θα πρέπει να είναι διαθέσιμα όταν η υπηρεσία τεθεί ξανά σε λειτουργία, θα είναι: 5 λεπτά.

Οικονομικές Επιπτώσεις

Σε περίπτωση μη διαθεσιμότητας της υπηρεσίας καθίσταται αδύνατη η καταγραφή και στη συνέχεια η εξυπηρέτηση των αιτημάτων των εταιρικών πελατών. Αυτό έχει σαν συνέπεια να καθυστερείται η είσπραξη των χρηματικών ποσών που αντιστοιχούν στη διεκπεραίωσή τους και τη μετέπειτα κίνηση των πελατών. Στο κόστος των μη διεκπεραιωμένων αιτημάτων πρέπει να συνυπολογιστεί και η απώλεια εσόδων από ήδη υπάρχοντες πελάτες, οι οποίοι λόγω βλάβης στο τηλέφωνό τους για παρατεταμένη διάρκεια δε θα πληρώσουν το βασικό μηνιαίο τέλος και δε θα έχουν καμία κίνηση στο λογαριασμό τους. Επίσης, υπάρχει πιθανότητα απώλειας πελατών προς ανταγωνιστικές εταιρίες, λόγω χαμηλού επιπέδου εξυπηρέτησης και διεκπεραίωσης των αιτημάτων τους.

Λειτουργικές Επιπτώσεις

Εξυπηρέτηση Πελατών**:** Τα αιτήματα των πελατών καθυστερούν να εξυπηρετηθούν.

Αύξηση Ευθυνών / Υποχρεώσεων: Δημιουργείται συσσωρευμένη εργασία για καταχώρηση των αιτημάτων μετά την επαναφορά της εφαρμογής.

Δημόσια Εικόνα: Οι αντιδράσεις του κοινού και το χαμηλό επίπεδο εξυπηρέτησης επηρεάζουν την εικόνα του οργανισμού.

Χρηματικές Ροές: Η αδυναμία είσπραξης των διαφόρων χρηματικών ποσών, όπως προαναφέρθηκε, είναι δυνατό να επιβαρύνει τις οικονομικές (χρηματικές) ροές.

Κρίσιμες Χρονικά Περίοδοι (Time Sensitivity): Δεν υπάρχει κάποια περίοδος μέσα στο έτος που να διαφοροποιείται σε κρισιμότητα ή φόρτο εργασίας από τις άλλες.

Υφιστάμενος Εξοπλισμός (Principal Systems/Resources)

System Name: CRMCC (DB & Application Server)

Model of Hypervisor: HP BL 460c Gen 6

O.S. Version: RedHat Enterprise Linux 5.5

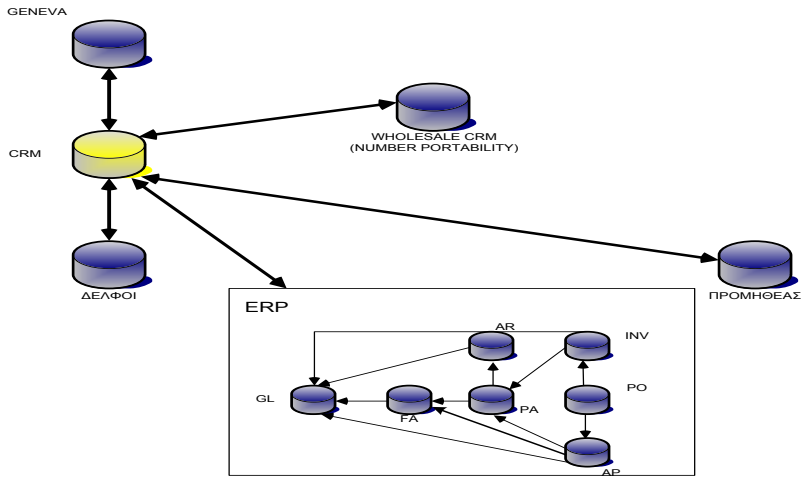
CPU: 2x4=8 cores

Memory: 16 GB

Αντίγραφα Ασφαλείας (Backups)

Συνεχές replication των δεδομένων του συστήματος με μέγιστη καθυστέρηση 5 λεπτών.

Αλληλεξαρτήσεις με Εφαρμογές (Interfaces)



Εικόνα 4. 1: Αλληλοεξαρτήσεις εφαρμογής CRM

- **P23. Μέγιστη ανεκτή περίοδος διακοπής (maximum tolerable period of disruption – MTPD).** Ορίζουμε σαν μέγιστη περίοδο διακοπής υπηρεσιών τη μισή ώρα (30 λεπτά) για τις κρίσιμες υπηρεσίες και τις 2 ώρες (120 λεπτά) για τις δευτερεύουσες (υποστηρικτικές) υπηρεσίες.

Κρισιμότητα	**Υπηρεσίες**	**MTPD**
Υψηλή	Σταθερή τηλεφωνία	30 λεπτά
Υψηλή	Κινητή τηλεφωνία	30 λεπτά
Υψηλή	ADSL	30 λεπτά
Υψηλή	VDSL	30 λεπτά
Υψηλή	TV over Ethernet	30 λεπτά
Υψηλή	Customer Help	30 λεπτά
Υψηλή	Billing	30 λεπτά
Υψηλή	CRM	30 λεπτά
Μεσαία	Employee Payroll	120 λεπτά
Μεσαία	ERP	120 λεπτά
Μεσαία	CDRs	120 λεπτά
Μεσαία	Finance	120 λεπτά
Χαμηλή	Human Resources	120 λεπτά
Χαμηλή	Intranet services	120 λεπτά

Πίνακας 4. 4: Μέγιστο ανεκτό διάστημα διακοπής υπηρεσιών

- **P24. Ιεράρχηση (Prioritization).** Λαμβάνοντας υπόψη της Ανάλυση Επιχειρησιακού Αντίκτυπου, καταρτίζεται μια λίστα υπηρεσιών κατά σειρά κρισιμότητας και σημαντικότητας έτσι ώστε να υπάρχει μια σειρά προτεραιοποίησης κατά την ανάκαμψη καθεμιάς από αυτές. Κατά σειρά λοιπόν εστιάζουμε πρώτα στην ανάκαμψη των υπηρεσιών «Υψηλής προτεραιότητας», ύστερα της «Μεσαίας» και τελευταία την «Χαμηλής προτεραιότητας».

Προτεραιότητα	**Κρίσιμες υπηρεσίες**
Υψηλή	Σταθερή τηλεφωνία
Υψηλή	Κινητή τηλεφωνία

Υψηλή	ADSL
Υψηλή	VDSL
Υψηλή	TV over Ethernet
Υψηλή	Customer Help
Υψηλή	Billing
Υψηλή	CRM
Μεσαία	Employee Payroll
Μεσαία	ERP
Μεσαία	CDRs
Μεσαία	Finance
Χαμηλή	Human Resources
Χαμηλή	Intranet services

Πίνακας 4. 5: Ιεράρχηση υπηρεσιών

- **P25. Καταγραφή και επιλογή (determination & selection).** Με βάση την ανάλυση επιχειρησιακού αντίκτυπου, την διαχείριση επικινδυνότητας και πάντα στα πλαίσια του ανεκτού χρόνου ανάκαμψης, πρέπει να καταγράψουμε τυχόν εξαρτήσεις των υπηρεσιών από άλλες υπηρεσίες ή ακόμα και μεταξύ τους. Όσον αφορά την προτεραιότητα ανάκαμψης, έχει δηλωθεί προηγουμένως (ως «Ιεράρχηση»).

Υπηρεσία	**Εξάρτηση**
Σταθερή τηλεφωνία	Καμία εξάρτηση
Κινητή τηλεφωνία	Καμία εξάρτηση
ADSL	Εξάρτηση από την Σταθερή Τηλεφωνία
VDSL	Εξάρτηση από την Σταθερή Τηλεφωνία
TV over Ethernet	Εξάρτηση από ADSL ή VDSL
Customer Help	Καμία εξάρτηση
Billing	Εξάρτηση από το CRM
CRM	Εξάρτηση από το Billing
Employee Payroll	Καμία εξάρτηση
ERP	Καμία εξάρτηση
CDRs	Καμία εξάρτηση

Finance	Εξάρτηση από το Billing
Human Resources	Καμία εξάρτηση
Intranet services	Καμία εξάρτηση

Πίνακας 4. 6: Εξαρτήσεις υπηρεσιών

- **P26. Επιδιωκόμενος χρόνος ανάκτησης (Recovery Time Objective – RTO).** Θέτουμε λοιπόν για κρίσιμες υπηρεσίες RTO=30min και για υποστηρικτικές υπηρεσίες RTO=120min.
- **P27. Καθορισμός κρίσιμων υπηρεσιών.** Προτείνεται οι εφαρμογές να κατηγοριοποιηθούν ως προς την προτεραιότητα ανάκτηση τους σύμφωνα με την παρακάτω κλίμακα [15]:

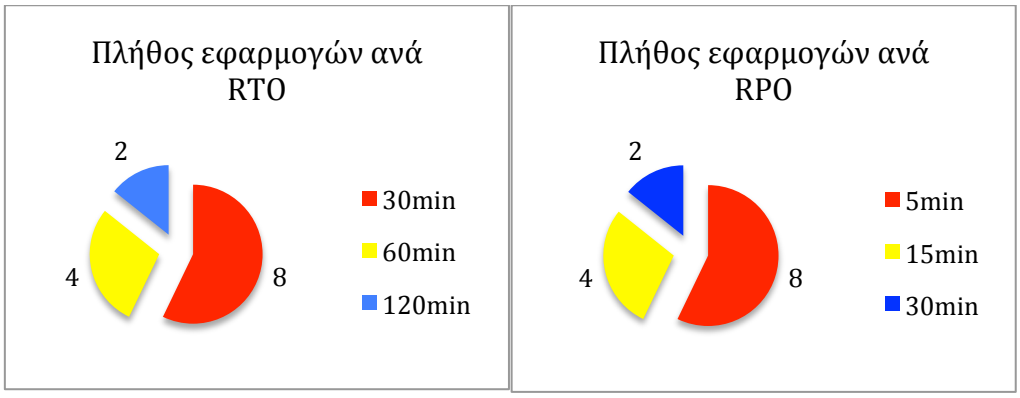
Προτεραιότητα 0 (υψηλή)	RTO=30 λεπτά RPO=5 λεπτά	Η εφαρμογή είναι κρίσιμη για την ομαλή και άμεση εξυπηρέτηση όλων των πελατών της εταιρίας και για την διασφάλιση της δημόσιας εικόνας της.
Προτεραιότητα 1 (μεσαία)	RTO=60 λεπτά RPO=15 λεπτά	Η εφαρμογή είναι αρκετά σημαντική για την ομαλή εξυπηρέτηση των πελατών της εταιρίας και για την διεκπεραίωση των καθημερινών εργασιών.
Προτεραιότητα 2 (χαμηλή)	RTO=120 λεπτά RPO=30 λεπτά	Η εφαρμογή είναι σημαντική για την ομαλή εξυπηρέτηση των πελατών της εταιρίας και γενικότερα για την διεκπεραίωση των εργασιών της.

Πίνακας 4. 7: Προτεραιότητες ανάκτησης

Ακολουθεί πίνακας με τις υπηρεσίες και τα RTO, RPO για κάθε μια από αυτές καθώς και μια γραφική αναπαράσταση με την αναλογία του πλήθους των εφαρμογών ανά RTO και RPO.

Προτεραιότητα	Κρίσιμες υπηρεσίες	RTO	RPO
Υψηλή	Σταθερή τηλεφωνία	30 λεπτά	5 λεπτά
Υψηλή	Κινητή τηλεφωνία	30 λεπτά	5 λεπτά
Υψηλή	ADSL	30 λεπτά	5 λεπτά
Υψηλή	VDSL	30 λεπτά	5 λεπτά
Υψηλή	TV over Ethernet	30 λεπτά	5 λεπτά
Υψηλή	Customer Help	30 λεπτά	5 λεπτά
Υψηλή	Billing	30 λεπτά	5 λεπτά
Υψηλή	CRM	30 λεπτά	5 λεπτά
Μεσαία	Employee Payroll	60 λεπτά	15 λεπτά
Μεσαία	ERP	60 λεπτά	15 λεπτά
Μεσαία	CDRs	60 λεπτά	15 λεπτά
Μεσαία	Finance	60 λεπτά	15 λεπτά
Χαμηλή	Human Resources	120 λεπτά	30 λεπτά
Χαμηλή	Intranet services	120 λεπτά	30 λεπτά

Πίνακας 4. 8: Ορισμοί RTO, RPO



Εικόνα 4.2: Αναλογία εφαρμογών ανά RTO και RPO

- **P28. Capacity Management:** Θα πρέπει να αποφασιστεί αν οι πόροι του DR site θα είναι στην ίδια κλίμακα (1 προς 1) με το Primary SITE, ή θα είναι σε μικρότερη κλίμακα (πχ 30% του primary site). Θα πρέπει επίσης να συνυπολογιστεί και το διαθέσιμο budget για το DR. Μια συνηθισμένη λογική είναι το DR site να μην έχει την ίδια κλίμακα με το πρωτεύον αλλά μειωμένους πόρους τουλάχιστον κατά 50%, δεδομένου ότι η λειτουργία του θα είναι πάντοτε προσωρινή έως ότου ανακάμψει το

πρωτεύον site. Επομένως θα πρέπει να υπολογιστούν στο 50% τα racks, οι servers, οι υπολογιστική ισχύ σε cpu και μνήμη των servers, καθώς και το storage capacity για αυτούς.

- **P29,P31. Information back-up.** Η πολιτική backup-restore εφόσον αναφερόμαστε σε εικονικές μηχανές, θα πρέπει να είναι ως εξής: Να υπάρχει ένα αρχικό full backup κατά την 1η εκκίνηση της μηχανής και στη συνέχεια να υπάρχουν αντίγραφα ασφάλειας με τις αλλαγές των δεδομένων (incremental backup). Η περιοδικότητα των αντιγράφων ασφάλειας θα οριστεί σύμφωνα με τι θα αποφασίσουμε για τις τιμές των RTO και RPO των υπηρεσιών. Θέτουμε λοιπόν (για κρίσιμες υπηρεσίες), RTO=30 λεπτά και RPO=5 λεπτά. Καλό θα ήταν τα αντίγραφα να έχουν κρυπτογράφηση, αλλά αν αυτό καθυστερεί σημαντικά την διαδικασία λήψης backup τότε μπορεί να αγνοηθεί. Κάθε ολοκληρωμένο αντίγραφο ασφάλειας θα πρέπει να ελέγχεται ότι ολοκληρώθηκε σωστά.
- **P30. Αποθήκευση αντιγράφων ασφάλειας.** Τα αντίγραφα ασφάλειας είναι επί της ουσίας τα αντίγραφα των παραγωγικών εικονικών μηχανών. Δημιουργούνται στο DR site και θα πρέπει να έχουν περιοδικότητα ανανέωσης δεδομένων 5 λεπτά. Δεν αποθηκεύονται ούτε σε CD-ROMS, ούτε σε εξωτερικές μονάδες αποθήκευσης. Αποθηκεύονται σε ξεχωριστά συστήματα αποθήκευσης και διαχείρισης δεδομένων (storage arrays), τα οποία βρίσκονται και αυτά στο DR site. Η διασύνδεσή τους με το παραγωγικό storage γίνεται μέσω οπτικών ινών για την όσο το δυνατόν ταχύτερη μεταφορά των δεδομένων.
- **P32. Information handling procedures – Privilege management.** Δικαιοδοσία χρήσης των αντιγράφων ασφάλειας δίνεται μόνο στα άτομα τα οποία είναι επιφορτισμένα με το job description “Backup Administrator”.
- **P33. Management of removable media.** Τα άτομα της παραπάνω ομάδας “Backup Administrator”, θα πρέπει να έχουν πρόσβαση και στα απομακρυσμένα αντίγραφα ασφάλειας (off-site backups).
- **P34. Απαιτήσεις πόρων (resource requirements).** Σαν πόρους πρέπει να διασφαλίσουμε τα κάτωθι:
  1. Μηχανικοί συστημάτων (Systems administrators), οι οποίοι θα είναι υπεύθυνοι για τη σωστή λειτουργία των συστημάτων στο DR.
  2. Απαιτούμενο H/W
  3. Κτιριακές εγκαταστάσεις
  4. Υποδομές και εξοπλισμός πληροφοριακών συστημάτων

5. Budget (πάνω από 500.000 ευρώ)
6. Προμηθευτές (DELL, HP)

- **P35. Διαχείριση Επικινδυνότητας (Risk Assessment).** Η Διαχείριση Επικινδυνότητας (ΔΕ), λαμβάνει υπόψη την ευαισθησία και την κρισιμότητα των δεδομένων, και ορίζει τα περιουσιακά στοιχεία (assets), εκείνα τα οποία μπορούν να θεωρηθούν ως «σημεία υψηλού κινδύνου» [15, 38, 44]. Η ΔΕ επομένως, πρέπει να ελέγχεται και να αναθεωρείται όποτε χρειάζεται. Οι έλεγχοι που έχουν θεσπιστεί για τα εν λόγω σημεία είναι ιδιαιτέρως σημαντικοί και πρέπει να εξετάζονται πρώτα από την Διεύθυνση Ασφάλειας της εταιρίας. Υπάρχουν πολλές πιθανές απειλές που μπορεί να συμβούν ανά πάσα στιγμή και να επηρεάσουν την ομαλή λειτουργία της εταιρίας. Έχει εξεταστεί ένα ευρύ φάσμα πιθανών απειλών με τα αποτελέσματα των ερευνών να περιλαμβάνονται σε αυτή την ενότητα. Εστιάσαμε σε επίπεδο επιχειρηματικότητας η οποία θα μπορούσε να διαταραχθεί από κάθε τύπο καταστροφής.

  Ακολουθούν οι πίνακες με τις διαβαθμίσεις πιθανότητας εμφάνισης κινδύνου και των συνεπειών αυτών όπως ορίζονται από το ινστιτούτο AIRMIC 2002 [13].

Πιθανότητα	**Περιγραφή**
Υψηλή (πιθανό)	Πιθανό να προκύπτει κάθε χρόνο. Πιθανότητα εμφάνισης μεγαλύτερη του 25%.
Μέση (δυνατό)	Πιθανό να προκύπτει μία φορά κάθε 10 χρόνια. Πιθανότητα εμφάνισης μικρότερη του 25%.
Χαμηλή (ασυνήθιστο)	Όχι πιθανό να προκύψει στα επόμενα 10 χρόνια. Πιθανότητα εμφάνισης μικρότερη του 2%.

Πίνακας 4. 9: Πιθανότητα εμφάνισης κινδύνου

Συνέπεια	Περιγραφή
Υψηλή	Οικονομικός αντίκτυπος μεγαλύτερος των 10.000€. Ισχυρός αντίκτυπος στη δημόσια εικόνα της εταιρίας.
Μέση	Οικονομικός αντίκτυπος μεταξύ των 2.000€ και των 10.000€. Μέτριος αντίκτυπος στη δημόσια εικόνα της εταιρίας.
Χαμηλή	Οικονομικός αντίκτυπος μικρότερος των 2.000 €. Μικρός αντίκτυπος στη δημόσια εικόνα της εταιρίας.

Πίνακας 4. 10: Συνέπειες κινδύνου

Οι πιθανές καταστροφές έχουν αξιολογηθεί ως ακολούθως:

Πιθανός κίνδυνος	Πιθανότητα	Συνέπεια
Πλημμύρα	Χαμηλή	Υψηλή
Φωτιά	Μέση	Υψηλή
Διακοπή ρεύματος	Υψηλή	Υψηλή
Δολιοφθορά	Μέση	Υψηλή
Σεισμός	Υψηλή	Υψηλή

Πίνακας 4. 11: Αξιολόγηση κινδύνου

D1. Στρατηγική Επιχειρησιακής Συνέχειας (BC strategy). Η στρατηγική που αποφασίζεται είναι η πλήρης και άμεση μεταγωγή των υπηρεσιών σε εναλλακτικό Μηχανογραφικό Κέντρο (DR site). Το νέο μηχανογραφικό κέντρο θα έχει ρόλο «Hot Stand-by Site» και οι υπηρεσίες θα ανακτώνται από αυτό. Το εναλλακτικό Μηχανογραφικό Κέντρο θα είναι σε θέση να διασφαλίσει ρυθμίσεις και συναφείς απαιτήσεις των συστημάτων των υπηρεσιών έτσι ώστε να είναι διαθέσιμο ανά πάσα στιγμή. Ως εκ τούτου, η ανάγκη ετήσιας δοκιμής θα είναι ένα μέρος αυτής της στρατηγικής.

- **D2. (D2.1 – D2.3). Μέτρα προστασίας (Protection & mitigation measures).** Για κάθε ρίσκο που έχει εντοπιστεί, αποφασίζουμε να το εξαλείψουμε μεταφέροντας αντίγραφα των επηρεαζόμενων υπηρεσιών στο DR site και φροντίζοντας για τη συνεχή επικαιροποίηση των δεδομένων τους. Όλα αυτά τίθενται σε εφαρμογή μέσω του Πλάνου Ανάκτησης από Καταστροφή (DR plan).

- **D3. (D3.1 – D3.6.4). Διαδικασίες πλάνου ανάκαμψης από καταστροφή (DRP procedures).** Αποφασίζονται οι διαδικασίες και οι πολιτικές για ανάκαμψη από καταστροφή του Πληροφοριακού Συστήματος μιας εταιρίας και μάλιστα με προτεραιότητα των πιο κρίσιμων υπηρεσιών. Καθορίζεται έπειτα από συναντήσεις με τους αρμόδιους επιχειρησιακά και τεχνικά υπεύθυνους των εφαρμογών. Σκοπός των συναντήσεων αυτών είναι η συγκέντρωση πληροφοριών σχετικά με την κρισιμότητα των εφαρμογών, τον μέγιστο αποδεκτό χρόνο μη διαθεσιμότητας τους, το κόστος της μη διαθεσιμότητας τους - σε συνάρτηση με το χρόνο σε ώρες ανά ημέρας μη διαθεσιμότητας, τις συμβατικές και κανονιστικές υποχρεώσεις της εταιρίας ως προς αυτές. τις υπηρεσίες. Σε αυτό το σημείο συγκεντρώνουμε όλες τις προτεινόμενες διαδικασίες ανάκαμψης, με σκοπό να διασφαλιστεί το Πληροφοριακό Σύστημα και η ακεραιότητα και διαθεσιμότητα των δεδομένων, ώστε να μην διασαλευτεί ούτε στο ελάχιστο η Επιχειρησιακή Συνέχεια της εταιρίας.
- **D3.6.5. Απόκριση συμβάντος (incident response).** Η παρακάτω ενδεικτική λίστα περιγράφει μια προτεινόμενη δέσμη ενεργειών διαχείρισης νέου συμβάντος:

Παρουσιάζεται το συμβάν	☐
Το πρώτο άτομο που παρατηρεί το περιστατικό ακολουθεί τις συμφωνημένες διαδικασίες έκτακτης ανάγκης και ενημερώνει την Ομάδα Αξιολόγησης (ΟΑ).	☐
Η ΟΑ αναλύει και διερευνά το περιστατικό, χρησιμοποιώντας μια λίστα ελέγχου, και καθορίζει αν η Ομάδα Διαχείρισης Συμβάντων (ΟΔΣ) πρέπει να ενεργοποιηθεί.	☐
Εάν χρειαστεί, η ΟΑ ενημερώνει και ενεργοποιεί την ΟΔΣ. Η ΟΔΣ ορίζει έναν Σύνδεσμο Επικοινωνίας (ΣΕ) για το περιστατικό. Ο ΣΕ ξεκινά διαδικασία ενημέρωσης των εμπλεκομένων.	☐
Όσο πιο σύντομα είναι δυνατό ο ΣΕ της ΟΔΣ ενημερώνει τον Γενικό Διευθυντή Συμβάντων (ΓΔΣ) (αριθμός τηλεφώνου) και το Κέντρο Διαχείρισης Απειλών (ΚΔΑ) (αριθμός τηλεφώνου) σχετικά με το συμβάν.	☐
Το ΚΔΑ ορίζει τον συντονισμό του συμβάντος με σημείο επαφής την ΟΔΣ, αναλύοντας το συμβάν και ενημερώνοντας σχετικά τα ανώτερα διοικητικά στελέχη του οργανισμού.	☐
Ο ΓΔΣ ειδοποιεί την τοπική ΟΔΣ σχετικά με το συμβάν.	☐
Το ΚΔΑ αποφασίζει αν χρειάζεται κλιμάκωση της προτεραιοποίησης του	☐

συμβάντος σύμφωνα με την ενημέρωση που παρέχεται από την Ομάδα Αξιολόγησης Ζημιών (ΟΑΖ) και την ΟΔΣ.	
Υποθέτοντας ότι απαιτείται κλιμάκωση των ενεργειών, ο ΟΔΣ επαναξιολογεί την κατάσταση, ενημερώνει την το ΚΔΑ και τον ΓΔΣ και κινεί την διαδικασία αντιμετώπισης καταστροφής.	☐
Αν μια καταστροφή δεν έχει δηλωθεί η ΟΔΣ συμβουλεύει το ΚΔΑ και τον ΓΔΣ.	☐
Αν μια καταστροφή έχει δηλωθεί, η ΟΔΣ 1. Ειδοποιεί το ΚΔΑ και τον ΓΔΣ 2. Ενεργοποιεί το Κέντρο Επιχειρήσεων Έκτακτης Ανάγκης (ΚΕΕΑ) 3. Ενεργοποιεί το πλάνο της Επιχειρησιακής Συνέχειας – Διαχείρισης Συμβάντος (Business Continuity – Incident Management plan) 4. Εκκινεί τις διαδικασίες αντιμετώπισης καταστάσεων έκτακτης ανάγκης.	☐
Ο ΓΔΣ διαβουλεύεται με το ΚΔΑ για το συμβάν. Η πληροφορία που δίνει το ΚΔΑ μεταφέρεται στο σημείο επικοινωνίας διαχείρισης συμβάντος.	☐
Το προσωπικό του οργανισμού ενημερώνεται για το συμβάν και την πορεία διαχείρισής του.	☐
Το πλάνο διαχείρισης συμβάντος και επιχειρησιακής συνέχειας συνεχίζεται να εκτελείται μέχρι την επίλυση του προβλήματος.	☐

Πίνακας 4. 12: Ροή απόκρισης συμβάντος

- **D4. (D4.1 – D4.6.12). Πλάνο Ανάκαμψης από Καταστροφή (Disaster Recovery Plan – DRP).** Πολλά από τα συστατικά του πλάνου αναφέρονται και μεμονωμένα. Τέτοια είναι η στρατηγική επιχειρησιακής συνέχειας, η Διαχείριση Επικινδυνότητας, η απόκριση συμβάντος, ο έλεγχος του πλάνου βασισμένος στην εκτέλεση συγκεκριμένων σεναρίων και η αξιολόγηση των αποτελεσμάτων και λήψη κατάλληλων αποφάσεων.

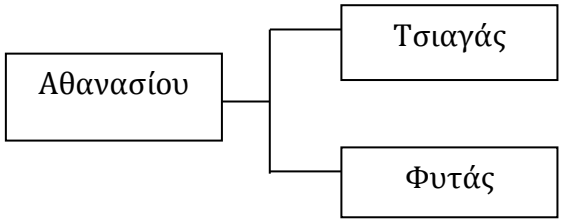
  Αυτά που απομένουν για να συμπληρωθεί το πλάνο είναι:

  1. Κατάλογος στοιχείων του προσωπικού. Ενδεικτικά τα ονόματα μερικών μηχανικών οι οποίοι εμπλέκονται στο DR plan.

Όνομα, Αρμοδιότητα	Στοιχεία	Αριθμός
Θάνος Αθανασίου, Section Manager	Εργασία	210 3456789
	Κινητό	697 2486999
	Σπιτιού	211 9988756
	Email Address	aathan@you.gr
Κώστας Τσιαγάς, System engineer	Εργασία	210 3456784
	Κινητό	697 7236545
	Σπιτιού	210 9544541
	Email Address	ktsiagas@you.gr
Νίκος Φυτάς, System engineer	Εργασία	210 3456782
	Κινητό	694 6789743
	Σπιτιού	210 5632958
	Email Address	nikosf@you.gr

Πίνακας 4. 13: Στοιχεία προσωπικού

2. Η ροή των καλούμενων εμπλεκομένων του προσωπικού.



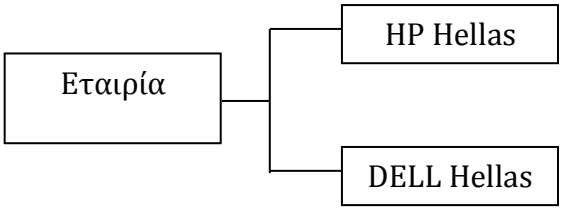
Εικόνα 4. 3: Ροή επικοινωνίας προσωπικού

3. Κατάλογος στοιχείων των εξωτερικών συνεργατών της εταιρίας

Όνομα, Αρμοδιότητα	**Στοιχεία**	**Αριθμός**
HP Hellas	Εργασία	211 2343444
	Email Address	info@hp.com.gr
DELL Hellas	Εργασία	801 11 234567
	Email Address	support@dell.gr

Πίνακας 4. 14: Στοιχεία συνεργατών

4. Η ροή των καλούμενων εμπλεκομένων των συνεργατών



Εικόνα 4. 4: Ροή επικοινωνίας συνεργατών

5. Η στρατηγική των αντιγράφων ασφάλειας [31]. Οι βασικές επιχειρηματικές διεργασίες και η συμφωνηθείσα στρατηγική των αντιγράφων ασφάλειας αναφέρονται παρακάτω. Η στρατηγική που επιλέχθηκε είναι αυτή του πλήρους αντίγραφου του συστήματος (fully mirrored virtual machine). Αυτό συνεπάγεται τη διατήρηση ενός ειδώλου (image) της μηχανής η οποία επιτρέπει την στιγμιαία εναλλαγή μεταξύ του πρωτεύοντος συστήματος και του ειδώλου.

Βασικές επιχειρηματικές διεργασίες	**Στρατηγική backup**
Σταθερή τηλεφωνία	Fully mirrored
Κινητή τηλεφωνία	Fully mirrored
ADSL	Fully mirrored
VDSL	Fully mirrored
TV over Ethernet	Fully mirrored

Customer Help	Fully mirrored
Billing	Fully mirrored
CRM	Fully mirrored
Employee Payroll	Fully mirrored
ERP	Fully mirrored
CDRs	Fully mirrored
Finance	Fully mirrored
Human Resources	Fully mirrored
Intranet services	Fully mirrored

Πίνακας 4. 15: Στρατηγική αντιγράφων ασφάλειας

6. Η ροή ενεργοποίησης του πλάνου. Το πλάνο τίθεται σε εφαρμογή μόλις συμβεί κάποιο συμβάν σχετικό με τη λίστα των καταστροφών. Στη συνέχεια ακολουθείται η ροή που περιγράφεται παρακάτω ως «απόκριση συμβάντος».

- **D4.6.1 Περιγραφή σεναρίου.** Ο οργανισμός βιώνει μία απρογραμμάτιστη διακοπή ρεύματος η οποία έχει θέσει εκτός το σύστημα τιμολόγησης των πελατών (Billing System), το οποίο φιλοξενείται στο πρωτεύον datacenter.
- **D4.6.2 - D4.6.8. Δοκιμή πλάνου και έλεγχος (test & exercise plan).** Περιγραφή του σεναρίου που θα δοκιμαστεί, του τύπου των δοκιμών που θα γίνουν, των στόχων που αναμένουμε. Επίσης συμπεριλαμβάνονται τα βήματα εκτέλεσης των δοκιμών και οι απαιτούμενες αλλαγές στο πλάνο, αν προκύψουν τέτοιες [09].

Ακολουθεί περιγραφή σεναρίου διακοπής των υπηρεσιών Billing:

Δοκιμή σεναρίου	Μια απρογραμμάτιστη διακοπή ρεύματος έχει θέσει εκτός λειτουργίας το σύστημα τιμολόγησης των πελατών το οποίο φιλοξενείται στο πρωτεύον datacenter.
Απαιτούμενες διορθωτικές κινήσεις	1. Κατόπιν ελέγχου της υπηρεσίας υποδεικνύεται ότι πρέπει να ξεκινήσει διαδικασία ανάκαμψης από το DR. 2. 2. Το αντίγραφο ασφαλείας της υπηρεσίας είναι διαθέσιμο στο DR. 3. Ανάκαμψη από το DR. 4. Επαναφορά της υπηρεσίας
Στόχοι σεναρίου	Ο κύριος στόχος αυτού του σεναρίου δοκιμής είναι να ανακάμψει η υπηρεσία στα προβλεπόμενα χρονικά πλαίσια, διασφαλίζοντας την σωστή και απρόσκοπτη λειτουργία της.
Ημερομηνία δοκιμής	27 Μαρτίου 2015
Τύπος δοκιμής	Δοκιμή πλήρους διακοπής υπηρεσίας
Συμμετέχοντα άτομα ή ομάδα	Datacenter Team, DRP Team
Προβλεπόμενο downtime	30 λεπτά

Πίνακας 4. 16: Ροή διακοπής υπηρεσίας

Χρονοδιάγραμα δοκιμαστικού ελέγχου του σεναρίου

	Ενέργειες	**Ομάδα**	**Χρόνος ολοκλήρωσης**
1	Εντοπισμός συμβάντος	Datacenter team	16:00
2	Ειδοποίηση του DRP manager	DRP team	16:05
3	Ειδοποίηση της DRP ομάδας	DRP team	16:07
4	Εκκίνηση πλάνου ανάκαμψης	DRP team	16:10
5	Ανάκαμψη υπηρεσίας	DRP team	16:20
6	Έλεγχος λειτουργίας	DRP team	16:25
7	Τερματισμός πλάνου	DRP team	16:30

Πίνακας 4. 17: Ροή ελέγχου σεναρίου

Λίστα ελέγχων του σεναρίου:

	Λίστα ελέγχου	Αποτελέσματα
1	Η ομάδα ανάκαμψης είχε επαρκή πληροφόρηση για την αποκατάσταση της υπηρεσίας;	ΝΑΙ
2	Υπήρχε τεκμηρίωση άμεσα διαθέσιμη για να βοηθήσει την ομάδα;	ΝΑΙ
3	Ήταν διαθέσιμοι όλοι οι πόροι και τα απαραίτητα εργαλεία για την εφαρμογή του πλάνου;	ΝΑΙ
4	Συμμετείχαν οι κατάλληλοι άνθρωποι;	ΝΑΙ
5	Πόσος χρόνος χρειάστηκε για να αποκατασταθεί η υπηρεσία;	30 λεπτά

Πίνακας 4. 18: Έλεγχοι σεναρίου

Απαιτούμενες διορθωτικές ενέργειες:

Απαιτούμενες διορθωτικές ενέργειες	Πρόσωπο / Ομάδα που ανατέθηκε	Αναμενόμενη Ημερομηνία Ολοκλήρωσης
Παροχή ασύρματων τηλεφώνων για ταχύτερη ενημέρωση του DRP manager	Datacenter Team	6 Απριλίου 2015

Πίνακας 4. 19: Διορθωτικές ενέργειες

Επανέλεχος σεναρίου:

Ημερομηνία επανέλεγχου	Αιτιολογία	Αλλαγές που έγιναν
13 Απριλίου	Datacenter Team	Αγορά ασύρματων τηλεφώνων (Dect)

Πίνακας 4. 20: Προγραμματισμός επανέλεγχου σεναρίου

- **C1 – C4. Παρακολούθηση, ανάλυση, αξιολόγηση (monitoring, analysis, evaluation).** Καταγραφή νέων κρίσιμων υπηρεσιών, επανεξέταση όλων των ήδη κρίσιμων υπηρεσιών για εντοπισμό κάποιας κατηργημένης υπηρεσίας. Ορίζουμε ως εργαλείο καταγραφής απόδοσης του πλάνου και των αποκρίσεων των ομάδων το επίσημο monitoring tool της εταιρίας (πχ HP Openview).
- **A1. Συνεχής επικαιροποίηση του BCP (improvement).** Θεσπίζεται περιοδική εξέταση το πλάνου Επιχειρησιακής Συνέχειας και Ετοιμότητας μία (1) φορά τον χρόνο και συγκεκριμένα την 1η βδομάδα του Ιουνίου.
- **A2. Συνεχής βελτίωση πλάνου (Continual BCP improvement).** Ο οργανισμός θα πρέπει να σημειώνει τυχόν παραλείψεις και νέες ιδέες βελτίωσης του πλάνου για να συζητηθούν κατά την περίοδο επικαιροποίησης αυτού.

4.2 Εργαλεία αποκατάστασης εικονικών υποδομών

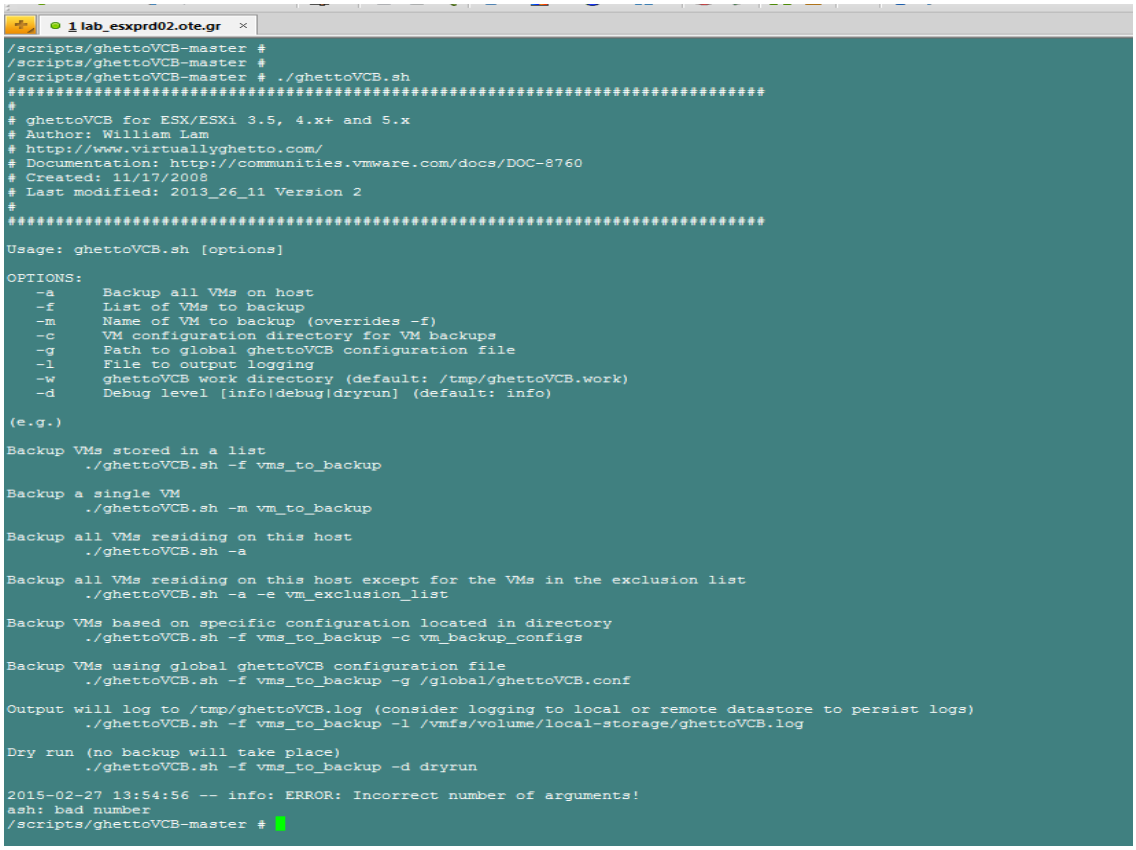
Για να έχει νόημα το πλάνο που μόλις παρουσιάσαμε, θα πρέπει να βρίσκει εφαρμογή μέσω κατάλληλων εργαλείων τα οποία να προσφέρουν υπηρεσίες ανάκαμψης από καταστροφή των εικονικών υποδομών. Υπάρχουν πολλά προϊόντα λογισμικού στο εμπόριο. Κύριο κριτήριο επιλογής ήταν να βρεθούν δωρεάν εργαλεία, έτσι ώστε να επιτύχουμε αυτό που αναφέρεται στον τίτλο της διατριβής ως «αποκατάσταση μηδενικού κόστους». Υπό αυτό το πρίσμα λοιπόν τα πρϊόντα λογισμικού που επιλέχθησαν να δοκιμαστούν και να συγκριθούν οι επιδόσεις τους είναι (κατά σειρά παρουσίασης) τα:

- ghettoVCB
- Veeam Backup free Edition
- VMware vSphere Replication
- XSI Backup

Θα πρέπει να επισημανθεί ότι τα πειράματα έγιναν σε περιβάλλον VMware virtualization. Οι hypervisors είναι δύο PowerEdge R710 rack-mounted servers της DELL, οι οποίοι έχουν 12 cores hypertheaded και 98GB RAM ο καθένας. Έχουν λειτουργικό vmware ESXi 5.5, και το storage που χρησιμοποιούν είναι το 3PAR της HP.

4.2.1 ghettoVCB.sh

Το συγκεκριμένο script προσφέρεται από τον ιστότοπο επικοινωνίας της Vmware [12] και δημιουργεί αντίγραφα ασφαλείας των εικονικών μηχανών που φιλοξενούνται σε εξυπηρετητές ESXi 3.5/4.x/5.x, χρησιμοποιώντας μεθοδολογία παρόμοια με το εργαλείο "Vmware Consolidated Backup" της VMware [06]. Διαθέτει αρκετές παραμέτρους στις εντολές του και παρέχει την δυνατότητα λήψης αντιγράφων ασφαλείας μεμονωμένων virtual machines ή όλων όσων είναι δηλωμένα σε προκαθορισμένη λίστα. Η λίστα αυτή είναι ένα απλό αρχείο κειμένου το οποίο περιέχει το όνομα της κάθε εικονικής μηχανής για τις οποίες θέλουμε να πάρουμε αντίγραφα ασφαλείας (εικ. 4.5).

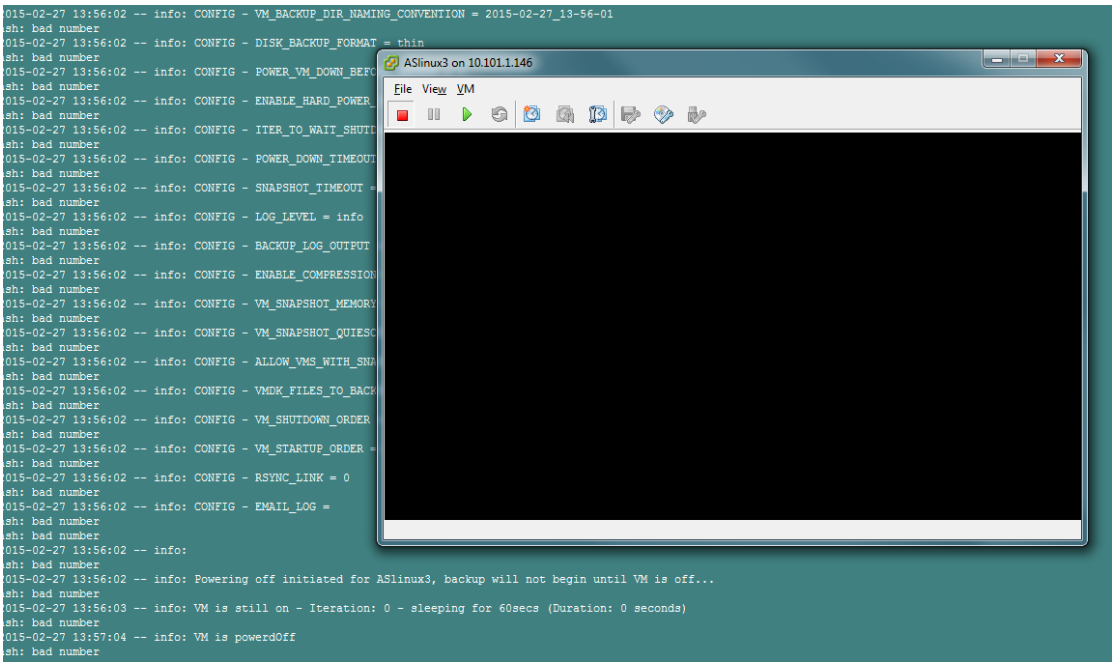


Εικόνα 4.5: Λίστα εντολών λήψης αντιγράφων

Επίσης, ορίζεται η σειρά προτεραιότητας των αντιγράφων ασφάλειας, καθώς και η τοποθεσία αποθήκευσης του backup, είτε τοπικά στον εξυπηρετητή, είτε σε NFS storage. Το script παίρνει ένα αντίγραφο στιγμιότυπου (snapshot) της εικονικής μηχανής ενόσω αυτή είναι σε πλήρη λειτουργία. Στη συνέχεια, κάνει shutdown το μηχάνημα και αφού αυτό κλείσει, δημιουργεί ένα αντίγραφο ασφαλείας του εικονικού filesystem (VMDK) (εικ. 4.6, 4.7).

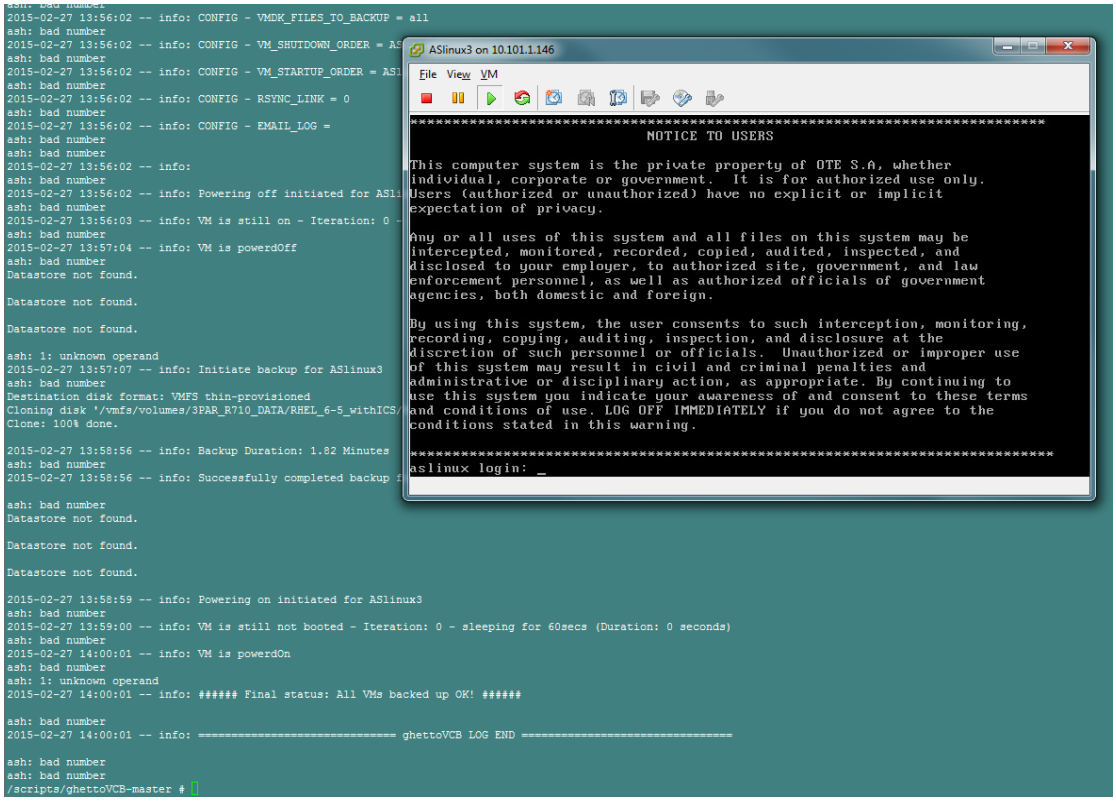
```
/scripts/ghettoVCB-master #
/scripts/ghettoVCB-master # ./ghettoVCB.sh -m ASlinux3
Logging output to "/tmp/ghettoVCB-2015-02-27_13-56-01-84857164.log" ...
ash: bad number
2015-02-27 13:56:02 -- info: ============================ ghettoVCB LOG START ============================

ash: bad number
ash: 1: unknown operand
2015-02-27 13:56:02 -- info: CONFIG - VERSION = 2013_26_11_2
ash: bad number
2015-02-27 13:56:02 -- info: CONFIG - GHETTOVCB_PID = 84857164
ash: bad number
2015-02-27 13:56:02 -- info: CONFIG - VM_BACKUP_VOLUME = /vmfs/volumes/530c8165-66f605c1-f73e-b8ac6f8f80ad/backups
ash: bad number
ash: bad number
2015-02-27 13:56:02 -- info: CONFIG - VM_BACKUP_ROTATION_COUNT = 3
ash: bad number
2015-02-27 13:56:02 -- info: CONFIG - VM_BACKUP_DIR_NAMING_CONVENTION = 2015-02-27_13-56-01
ash: bad number
2015-02-27 13:56:02 -- info: CONFIG - DISK_BACKUP_FORMAT = thin
ash: bad number
2015-02-27 13:56:02 -- info: CONFIG - POWER_VM_DOWN_BEFORE_BACKUP = 0
ash: bad number
2015-02-27 13:56:02 -- info: CONFIG - ENABLE_HARD_POWER_OFF = 0
ash: bad number
2015-02-27 13:56:02 -- info: CONFIG - ITER_TO_WAIT_SHUTDOWN = 3
ash: bad number
2015-02-27 13:56:02 -- info: CONFIG - POWER_DOWN_TIMEOUT = 5
ash: bad number
2015-02-27 13:56:02 -- info: CONFIG - SNAPSHOT_TIMEOUT = 15
ash: bad number
2015-02-27 13:56:02 -- info: CONFIG - LOG_LEVEL = info
ash: bad number
2015-02-27 13:56:02 -- info: CONFIG - BACKUP_LOG_OUTPUT = /tmp/ghettoVCB-2015-02-27_13-56-01-84857164.log
ash: bad number
2015-02-27 13:56:02 -- info: CONFIG - ENABLE_COMPRESSION = 0
ash: bad number
2015-02-27 13:56:02 -- info: CONFIG - VM_SNAPSHOT_MEMORY = 0
ash: bad number
2015-02-27 13:56:02 -- info: CONFIG - VM_SNAPSHOT_QUIESCE = 0
ash: bad number
2015-02-27 13:56:02 -- info: CONFIG - ALLOW_VMS_WITH_SNAPSHOTS_TO_BE_BACKEDUP = 0
ash: bad number
2015-02-27 13:56:02 -- info: CONFIG - VMDK_FILES_TO_BACKUP = all
ash: bad number
2015-02-27 13:56:02 -- info: CONFIG - VM_SHUTDOWN_ORDER = ASlinux3
ash: bad number
2015-02-27 13:56:02 -- info: CONFIG - VM_STARTUP_ORDER = ASlinux3
ash: bad number
2015-02-27 13:56:02 -- info: CONFIG - RSYNC_LINK = 0
ash: bad number
2015-02-27 13:56:02 -- info: CONFIG - EMAIL_LOG =
```

Εικόνα 4.6: Έναρξη λήψης αντιγράφου



Εικόνα 4.7: Πρόοδος λήψης αντιγράφου

Μετά την ολοκλήρωση του αντιγράφου ασφάλειας, διαγράφει το στιγμιότυπο και προχωρά σε εκκίνηση της μηχανής (εικ. 4.8).



Εικόνα 4.8: Τέλος λήψης αντιγράφου

Όλες οι ενέργειες, καθώς και οι χρόνοι των διεργασιών λήψης αντιγράφων ασφαλείας καταγράφονται σε αρχείο (log file) τοπικά στον εξυπηρετητή (εικ. 4.9).

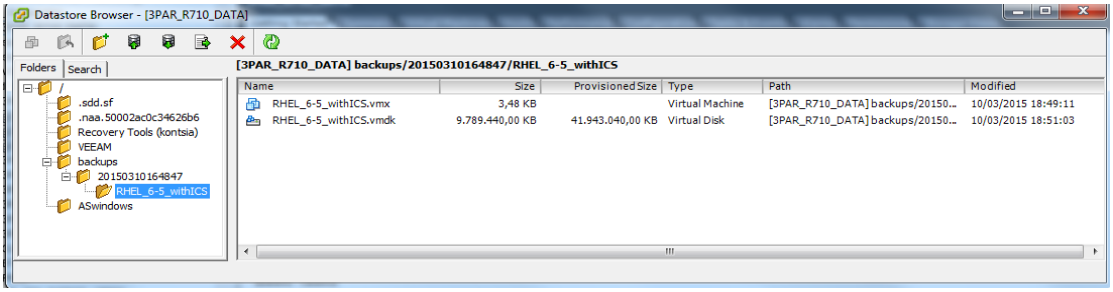
```
/scripts/ghettoVCB-master #
/scripts/ghettoVCB-master #
/scripts/ghettoVCB-master # ls -ltr /tmp/ghettoVCB*
-rw-r--r--    1 root     root          4192 Feb 24 17:27 /tmp/ghettoVCB-2015-02-24_17-20-42-84198647.log
-rw-r--r--    1 root     root          4192 Feb 27 14:00 /tmp/ghettoVCB-2015-02-27_13-56-01-84857164.log
/scripts/ghettoVCB-master #
```

Εικόνα 4.9: logfile

Όσον αφορά την διαδικασία ανάκαμψης της εικονικής μηχανής, δεν υπάρχει αυτόματη διαδικασία recovery. Διαδικασία δηλαδή η οποία θα αντιλαμβάνεται ότι η εικονική μηχανή έχει σταματήσει να ανταποκρίνεται και θα προχωρά σε αυτόματη διαδικασία ανάκαμψης. Αυτό γίνεται εύκολα μεν, με χειροκίνητο τρόπο δε. Θα πρέπει να αντιγραφεί το αντίγραφο ασφάλειας από τον αποθηκευτικό χώρο όπου τοποθετήθηκε αρχικά, στο δίσκο (datastore) του πρωτεύοντος site. Αν έχει καταστραφεί ολόκληρο το

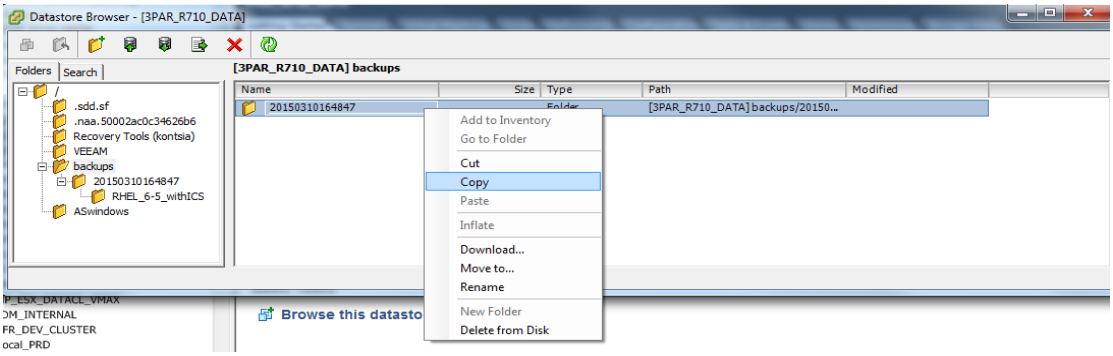
προτεύον site, θα πρέπει να σηκωθεί η μηχανή από το υπάρχον αποθηκευτικό χώρο στο DR site.

Επομένως βρίσκουμε τον φάκελο του αντιγράφου ασφάλειας στο storage (εικ. 4.10)

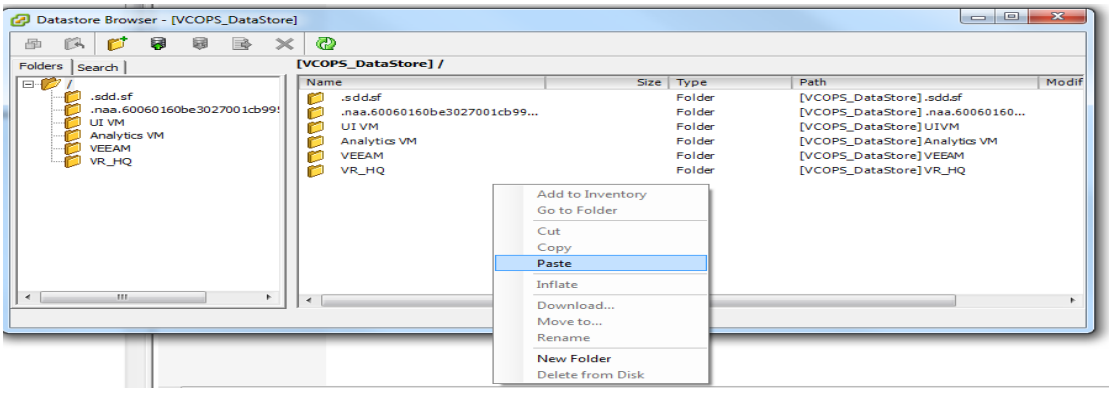


Εικόνα 4.10: Τοποθεσία αντίγραφου ασφάλειας

και στη συνέχεια κάνουμε αντιγραφή του backup στο χώρο του πρωτεύοντος datacenter (εικ. 4.11, 4.12)

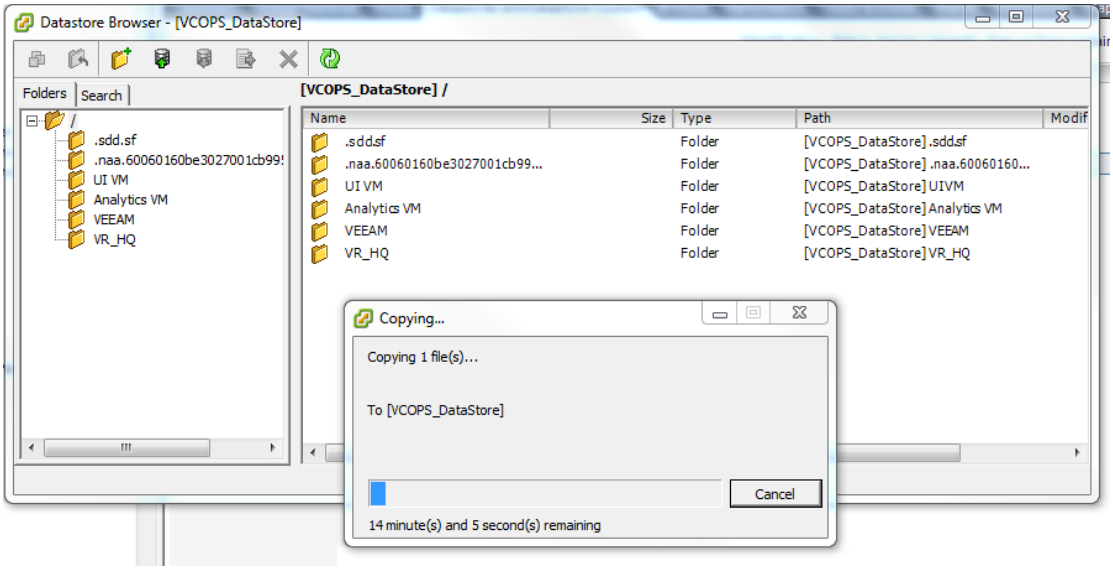


Εικόνα 4.11: Αντιγραφή αντίγραφου ασφάλειας

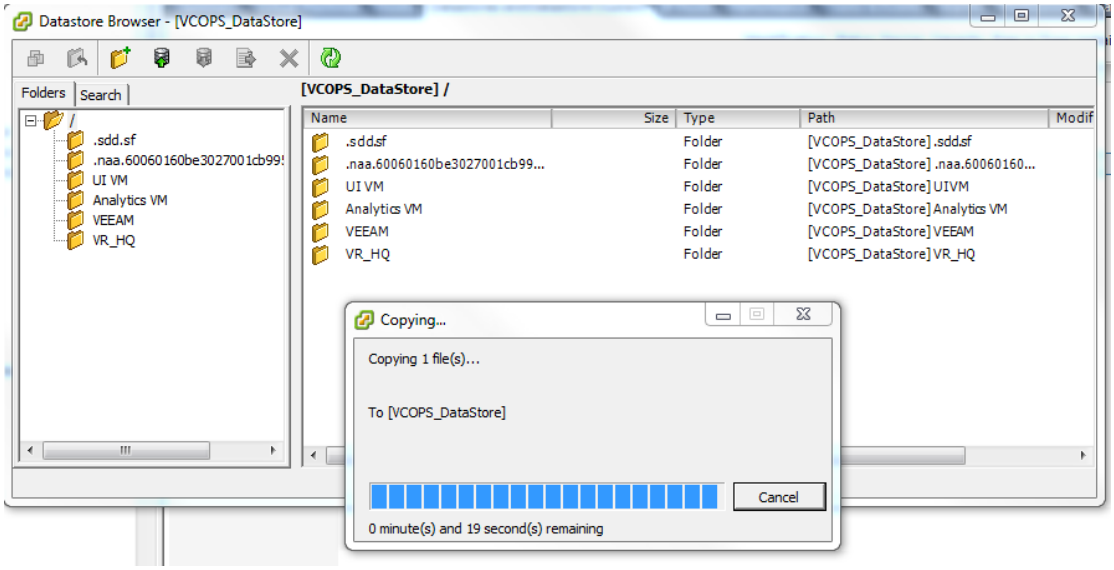


Εικόνα 4.12: Επικόλληση αντίγραφου ασφάλειας

Ο χρόνος αντιγραφής είναι άμεσα εξαρτώμενος από το εύρος της δικτυακής διασύνδεσης των δύο αποθηκευτικών μέσων και ποικίλει ανάλογα με τον όγκο των δεδομένων που θα μεταφερθούν (εικ. 4.13, 4.14).

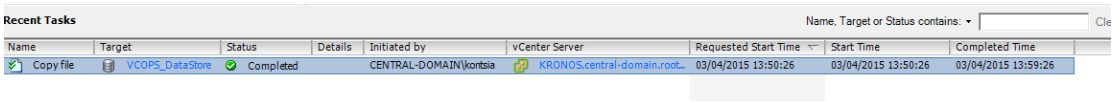


Εικόνα 4.13: Αρχική εκτίμηση χρόνου αντιγραφής



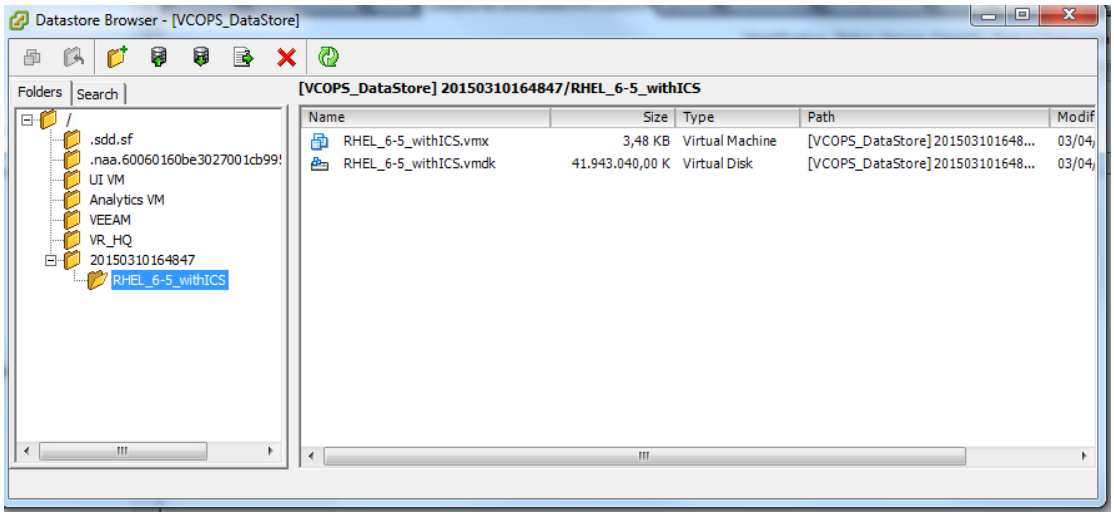
Εικόνα 4.14: Τέλος αντιγραφής

αλλά στο τέλος μπορούμε να διαπιστώσουμε τον πραγματικό χρόνο διάρκειας της αντιγραφής (εικ. 4.15)



Εικόνα 4.15: Πραγματικός χρόνος αντιγραφής

Αφού τελειώσει η αντιγραφή μπορούμε να σηκώσουμε την εικονική μηχανή (εικ. 4.16).



Εικόνα 4.16: Νέα τοποθεσία εικονικής μηχανής

Οι περιορισμοί του εν λόγω script έγκειται στο γεγονός ότι χρησιμοποιεί διαθέσιμους πόρους του εξυπηρετητή ESXi, αλλά το σημαντικότερο είναι ότι απαιτείται downtime των υπηρεσιών της εικονικής μηχανής λόγω του cold backup. Επίσης προϋποθέτει εγκατεστημένα VMware tools σε κάθε εικονική μηχανή. Έχει δοκιμαστεί στις εκδόσεις 3.5, 4.x, 5.x σε ESX και ESXi και υποστηρίζει αντίγραφα ασφάλειας σε τοπικό αποθηκευτικό χώρο (local storage), Storage Area Network (SAN) και Network File System (NFS). Μπορεί επίσης να ρυθμιστεί ώστε να εκτελείται σε προγραμματισμένες ώρες μέσω του μηχανισμού cron του ESXi. Επιπλέον, για ESXi περιβάλλοντα που δεν έχουν NFS datastores προορισμένα για απόθεση των αντιγράφων ασφαλείας, το script προσφέρει τη δυνατότητα αυτόματης σύνδεσης του ESXi διακομιστή σε εξωτερικό NFS storage με αυτόματη αποσύνδεση μετά την ολοκλήρωση δημιουργίας αντιγράφων ασφαλείας. Στη σημερινή του μορφή, το πρόγραμμα επιτρέπει έως και τρία (3)

μοναδικά αντίγραφα ασφαλείας της εικονικής μηχανής. Κάθε επόμενο αντίγραφο αντικαθιστά το παλαιότερο.

Τελειώνοντας να αναφέρουμε ότι δεν απαιτείται εγκατάσταση. Αρκεί ένας ftp client για να μεταφέρει το script σε κάποια τοποθεσία στο file system του λειτουργικού του ESXi εξυπηρετητή και η πρόσβαση σε αυτό είναι μέσω ssh επικοινωνίας με τον ESXi. Είναι συμβατό με κάθε linux-based hypervisor. Συγκεκριμένα για περιβάλλον VMware, είναι συμβατό με τις εκδόσεις των hosts ESX(i) 3.5 / 4.x και 5.x.

4.2.1.1 Υποστηριζόμενα χαρακτηριστικά

- Υποστηρίζει αντίγραφα ασφάλειας πολλαπλών δίσκων VMDK ανά VM.
- Υποστηρίζει προτεραιοποίηση του backup (οι πιο σημαντικές εικονικές μηχανές δηλώνονται πρώτες στην λίστα).
- Δυνατότητα προγραμματισμένων backup μέσω του crontab μηχανισμού του λειτουργικού.
- Δεν υπάρχει περιορισμός στον αριθμό των προγραμματισμένων εργασιών αντιγράφων ασφάλειας (scheduled backup jobs).
- Παρέχεται report με το πέρας του αντιγράφου ασφάλειας σε μορφή logfile.
- Παρέχεται δυνατότητα ενημέρωσης μέσω email μετά την ολοκλήρωση του backup.
- Δυνατότητα καταγραφής χρονικής διάρκειας του backup (μέσω του logfile).
- Παρέχεται εξαγωγή των αντιγράφων ασφάλειας σε NFS share.
- Δεν επιβαρύνει σημαντικά τους ESXis κατά την διάρκεια της λειτουργίας του, ούτε σε cpu αλλά ούτε και σε memory.
- Παρέχεται η δυνατότητα για memory snapshot.
- Εξασφαλισμένο σβήσιμο των στιγμιότυπων (snapshots) πριν την εκτέλεση επόμενης εντολής για αντίγραφο ασφάλειας.
- Τα αντίγραφα ασφάλειας μπορεί να είναι είτε thin, είτε thick (eager-zero or zero).
- Είναι συμβατό με κάθε πλατφόρμα hypervisor η οποία όμως πρέπει να φιλοξενεί linux-based environment.
- Υποστηρίζει είτε SCSI είτε IDE δίσκους.

4.2.1.2 Μη υποστηριζόμενα χαρακτηριστικά

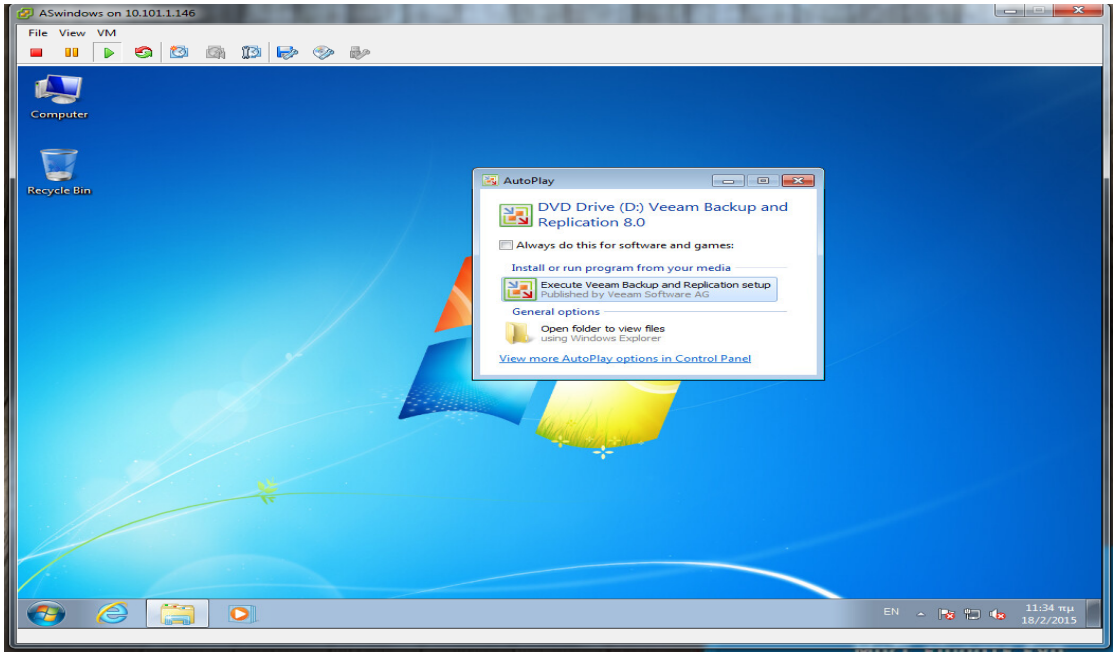
- Δεν υποστηρίζει έλεγχο και επιβεβαίωση του backup (backup verification), παρά μόνον αν γίνει δοκιμαστικό restore.
- Δεν παρέχεται η δυνατότητα online backup (hot backup). Η εικονική μηχανή πρέπει να κλείσει για να ξεκινήσει η διαδικασία του backup.
- Δεν παρέχεται η δυνατότητα για differential ή incremental backup ή δυνατότητα για διαγραφή διπλότυπων δεδομένων (data deduplication). Παρέχεται μόνον full backup.
- Δεν παρέχεται η δυνατότητα συνεχούς ενημέρωσης των δεδομένων των αντιγράφων ασφάλειας (rsync backup files).
- Δεν παρέχεται η δυνατότητα κρυπτογράφησης των αντιγράφων ασφάλειας (backup encryption).
- Δεν παρέχεται δυνατότητα εξαγωγής των αντιγράφων ασφάλειας στο σύννεφο ή σε άλλα μέσα αποθήκευσης (CD-ROM, tapes, NAS, DVD, Blu-Ray, USB drives, FTP servers).
- Δεν παρέχεται δυνατότητα επανάκτησης σε καθορισμένο χρονικό σημείο (point-in-time recovery). Μόνο στο χρονικό σημείο που πάρθηκε το backup.
- Δεν παρέχεται η δυνατότητα για επανάκτηση σε επίπεδο αρχείου filesystem, αλλά μόνο ολοκληρωτικής ανάκτησης της εικονικής μηχανής.
- Δεν προσφέρει αυτοματοποιημένη διαδικασία recovery, αλλά από το αντίγραφο της εικονικής μηχανής, μπορούμε να επανακτήσουμε το μηχάνημα με σχετική ευκολία. Η εικονική μηχανή πρέπει να κλείσει και στη συνέχεια να προβούμε σε διαδικασία restore με ενέργειες σε επίπεδο ESXi. Δηλαδή να αντιγραφεί το αντίγραφο ασφάλειας στο path που βρίσκεται το αρχικό, και να εκιννήσει η μηχανή.
- Δεν υποστηρίζει αντίγραφα ασφάλειας παρά μόνο για δίσκους που περιέχουν VMDK files.
- Δεν παίρνει backup εικονικές μηχανές που έχουν snapshots. Θα πρέπει προηγουμένως να αφαιρούνται τα snapshots.
- Δεν έχει εύκολη διαχείριση καθότι είναι script και δεν προσφέρει graphical user interface (GUI) αλλά μόνο command-line interface (CLI).
- Δεν υποστηρίζει συμπίεση αντιγράφων ασφάλειας (backup compression).
- Δεν υποστηρίζει Raw Device Disk (RDM).

4.2.2 Veeam Backup free Edition

Είναι μια λύση που επίσης παρέχει προστασία των δεδομένων και ανάκτηση υπηρεσιών από καταστροφή [28]. Είναι συμβατό με εικονικές πλατφόρμες VMware vSphere και Hyper-V οποιουδήποτε μεγέθους και πολυπλοκότητας. Συνδυάζοντας όλες τις απαραίτητες λειτουργίες σε ένα φιλικό interface, βοηθά στην επίλυση κρίσιμων προβλημάτων των virtualized υποδομών παρέχοντας προστασία στις εικονικές μηχανές από αστοχίες υλικού και λογισμικού. Το προϊόν προσφέρεται είτε σε πλήρη έκδοση (με αγορά αντίστοιχης άδειας), είτε σε δωρεάν έκδοση. Εδώ εξετάζεται η δωρεάν λειτουργία. Η δωρεάν έκδοση προσφέρει όπως είναι αναμενόμενο περιορισμένες δυνατότητες. Παρόλα αυτά, ππορούμε να δημιουργήσουμε αντίγραφα ασφάλειας των εικονικών μηχανών, να προχωρήσουμε σε ανάκτηση (recover), να δημιουργήσουμε αντίγραφα ασφάλειας μέσω στιγμιότυπων του αποθηκευτικού χώρου (backup snapshot storage), να κάνουμε αντιγραφή σε επίπεδο αρχείων, μεταγωγή (migration) εικονικών μηχανών και τέλος να δημιουργήσουμε αντίγραφα ασφάλειας σε κασέτες. Προσφέρει κρυπτογράφηση των αντιγράφων ασφάλειας (backup encryption), με χρήση κωδικού ασφάλειας, έτσι ώστε να προστατεύονται τα δεδομένα από μη εξουσιοδοτημένη πρόσβαση. Προσφέρει ιστορικότητα των αντιγράφων ασφάλειας (backup retention), με δυνατότητα να σβήνονται αυτόματα μετά από 1, 3 η 7 ημέρες. Προσφέρει συμπίεση των αντιγράφων ασφάλειας (backup compression), με διάφορες διαβαθμίσεις συμπίεσης (default, high, extreme compression), έτσι ώστε να επιτυγχάνεται εξοικονόμηση αποθηκευτικού χώρου. Η λύση της Veeam χρησιμοποιεί την τεχνολογία «VMware Tools quiescence» για τις εικονικές μηχανές της VMware, και τεχνολογία «Hyper-V quiescing» για τις εικονικές μηχανές που υλοποιούνται σε περιβάλλον Microsoft. Το εργαλείο «παγώνει» στιγμιαία την εικονική μηχανή έτσι ώστε να είναι δυνατή η λήψη αντίγραφου ασφάλειας του λειτουργικού και των εφαρμογών του. Είναι χρήσιμο για μηχανές οι οποίες εκτελούν πολλές συναλλαγές/επικοινωνίες (transactions) με πολλά άλλα συστήματα, και θέλουμε να είμαστε σίγουροι ότι η διαδικασία επανάκτησης θα είναι επιτυχής χωρίς απώλεια δεδομένων.

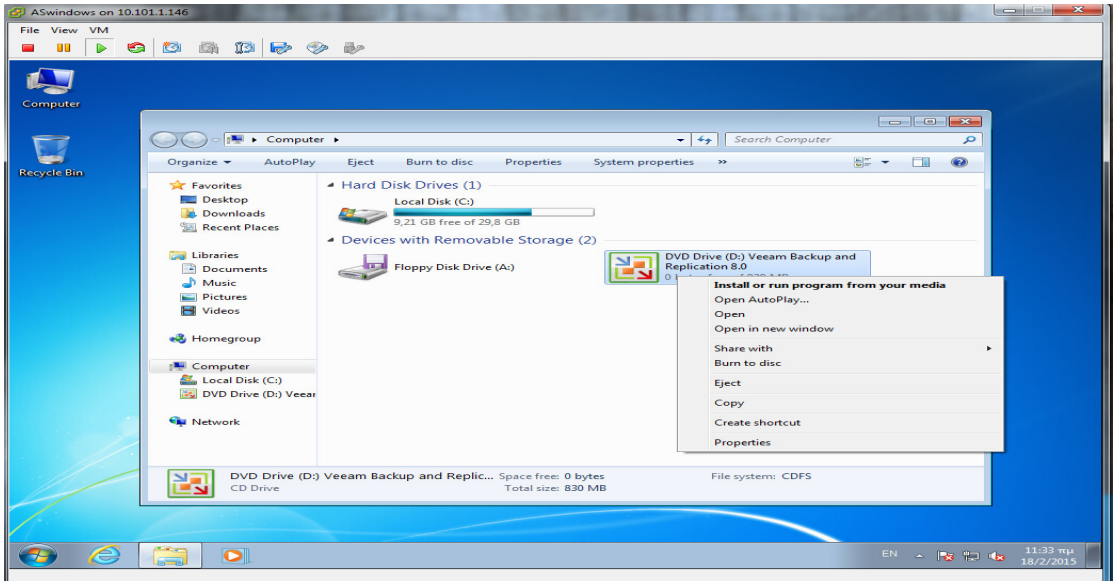
Η εγκατάσταση του εργαλείου έχει αρκετά προαπαιτούμενα. Χρειάζεται ένα μηχάνημα με λειτουργικό WINDOWS 64-bit Win, και απαιτεί και εγκατάσταση Microsoft SQL Server database. Προαπαιτούμενα επίσης είναι η ύπαρξη Microsoft Visual C++ 2010, Microsoft PowerShell v2.0 και χρήση τεχνολογίας .Net. Η λύση για όλα τα παραπάνω είναι ήταν ένα virtual machine με λειτουργικό win7 64-bit και όλα τα τελευταία updates από την Microsoft. Η εγκατάσταση εκτελείται μέσω ενός οδηγού (wizard), ο οποίος

καθοδηγεί τον χρήστη χωρίς να του δημιουργεί αμφιβολίες και δύσκολες αποφάσεις. Όπως θα δείτε και παρακάτω από τις εικόνες εγκατάστασης, το πρόγραμμα είναι auto play από το CD-ROM (εικ. 4.17),



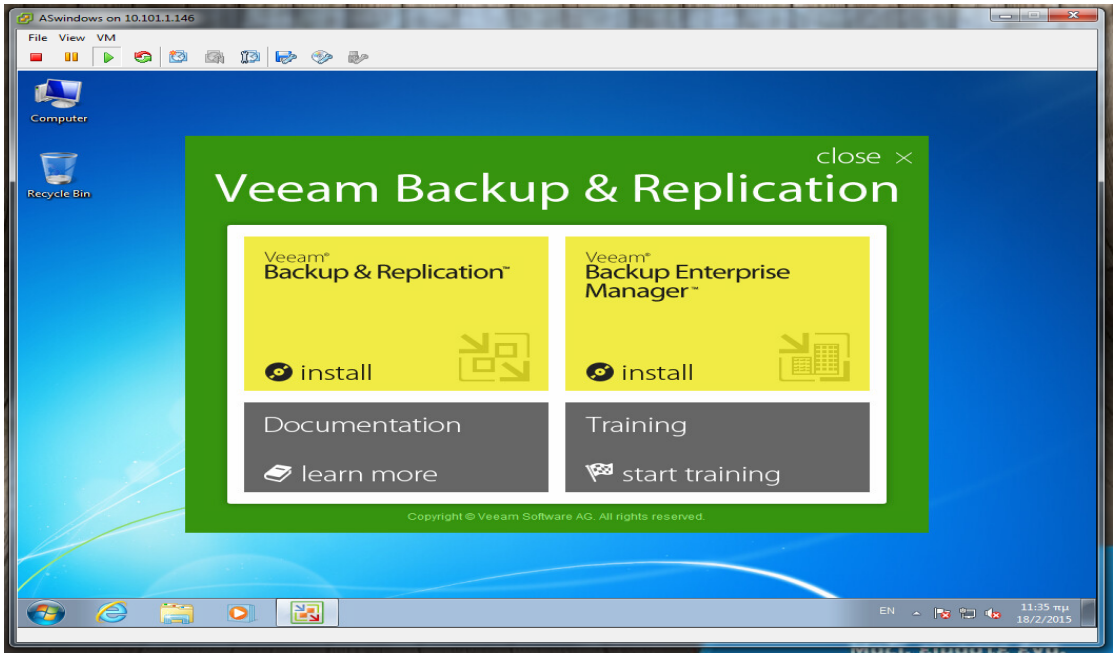
Εικόνα 4.17: Αυτόματη εκκίνηση εγκατάστασης

ή μπορεί να το εκκινήσει ο χρήστης (εικ. 4.18).



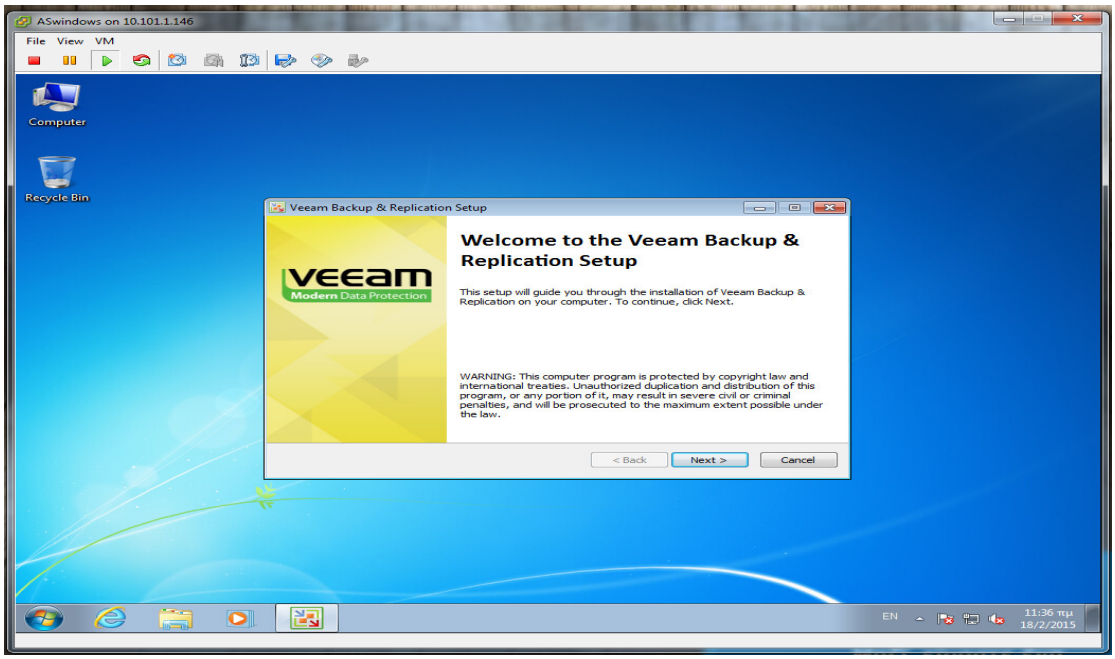
Εικόνα 4.18: Χειροκίνητη εκκίνηση εγκατάστασης

Αφού επιλέξει να εγκαταστήσει την εφαρμογή “Backup & Replication” πατώντας το αντίστοιχο “install” (εικ. 4.19),



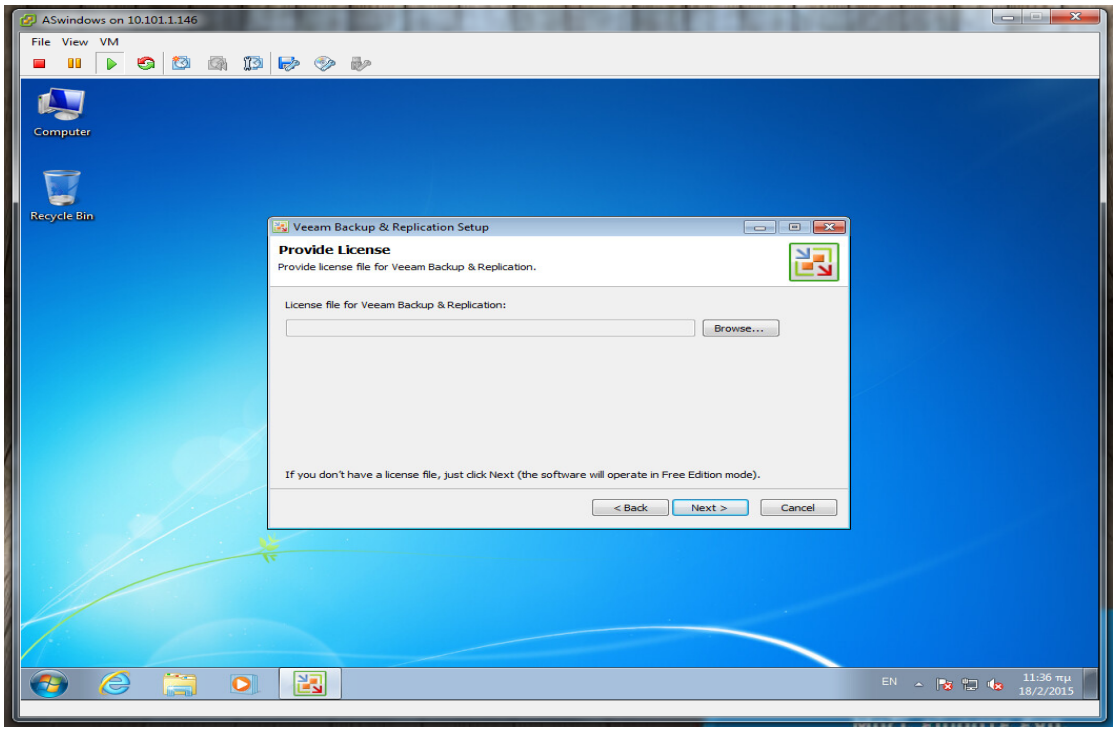
Εικόνα 4.19: Επιλογή λογισμικού

αρχίζει ο οδηγός εγκατάστασης να επικοινωνεί με τον χρήστη (εικ. 4.20).



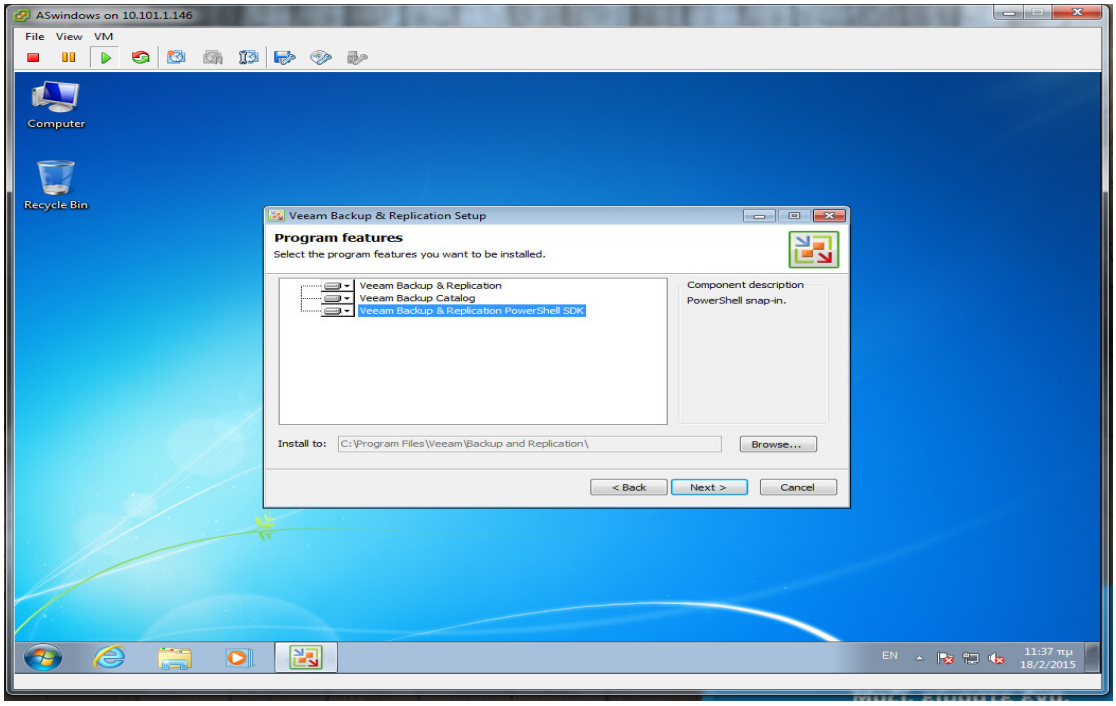
Εικόνα 4.20: Οθόνη καλωσορίσματος

Επιλέγουμε να βάλουμε την δωρεάν έκδοση του λογισμικού (εικ. 4.21),



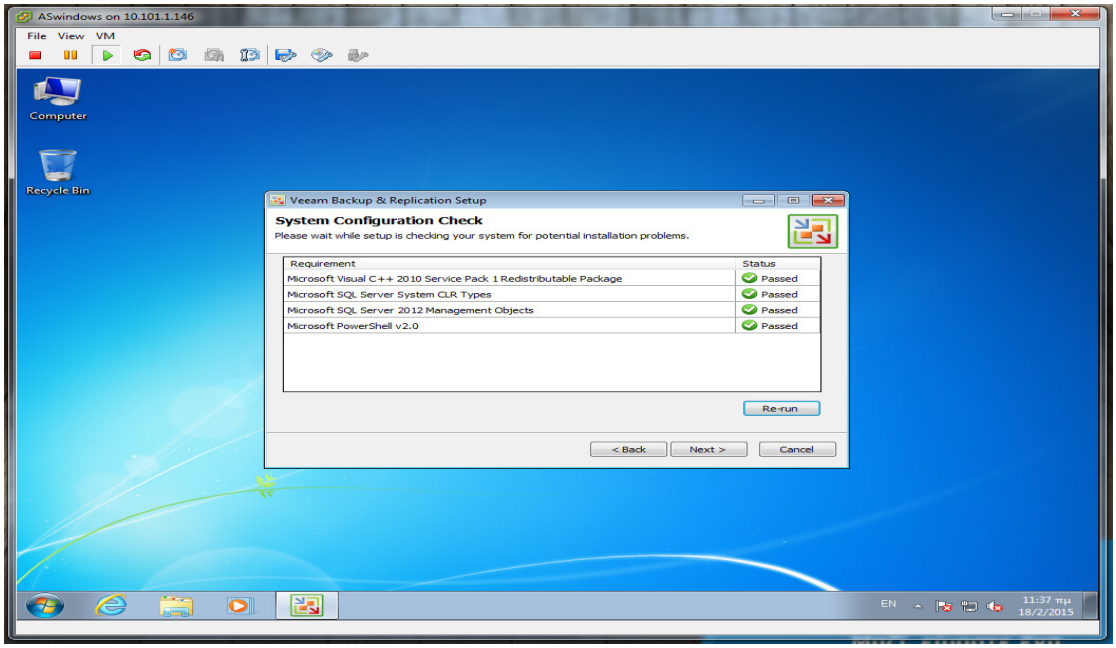
Εικόνα 4.21: Επιλογή έκδοσης λογισμικού

και όλα τα εργαλεία που προσφέρονται (εικ. 4.22).



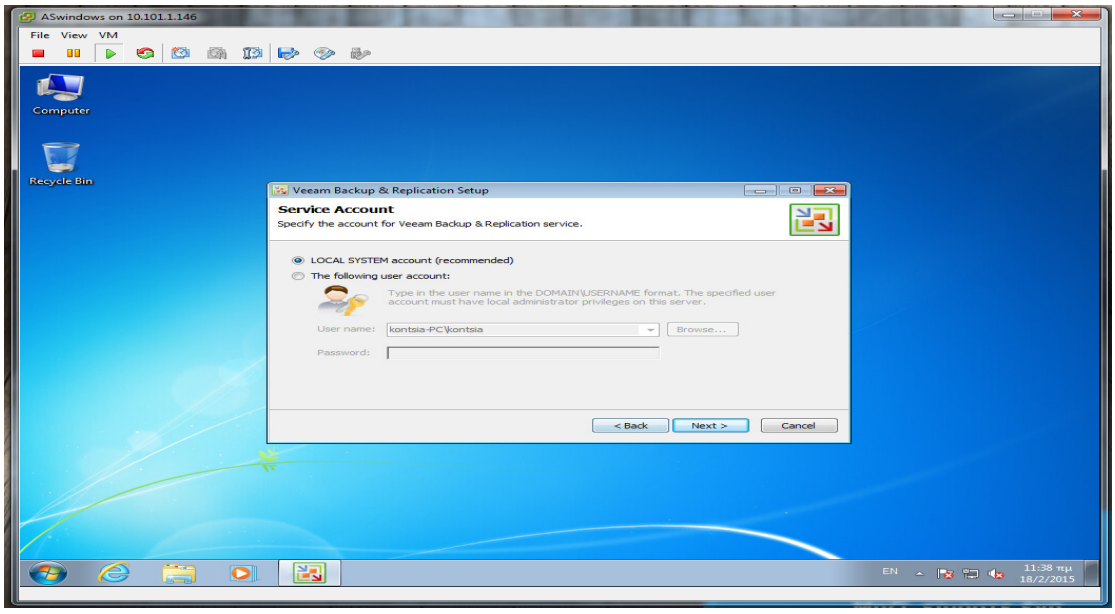
Εικόνα 4.22: Πακέτα εγκατάστασης

Στη συνέχεια ο οδηγός κάνει έναν έλεγχο του συστήματος για πιθανές ελλείψεις σε βιβλιοθήκες και πακέτα των C++, MS SQL srv, MS PowerShell και ότι δεν βρει, αναλαμβάνει να το εγκαταστήσει αυτόματα (εικ. 4.23).



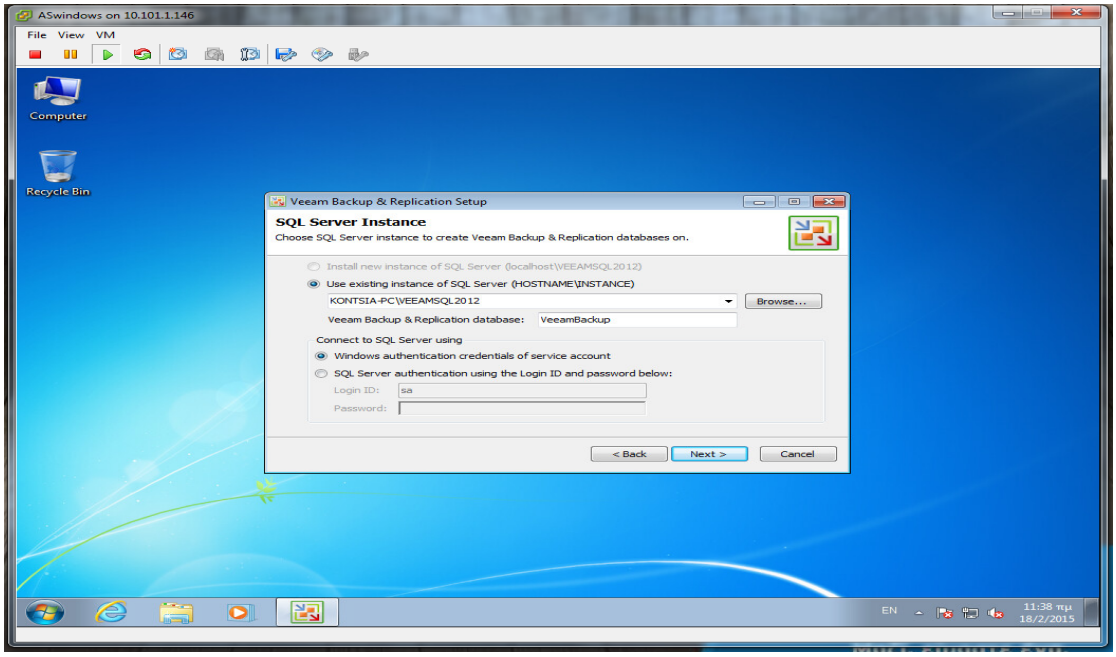
Εικόνα 4.23: Έλεγχος προαπαιτούμενων

Η εγκατάσταση δίνει την δυνατότητα να χρησιμοποιηθεί κάποιος χρήστης του λειτουργικού που υπάρχει ήδη ή αν αυτό δεν είναι επιθυμητό, τότε δημιουργεί νέο χρήστη. Εμείς επιλέξαμε να χρησιμοποιεί τον τοπικό χρήστη του συστήματος (εικ. 4.24),



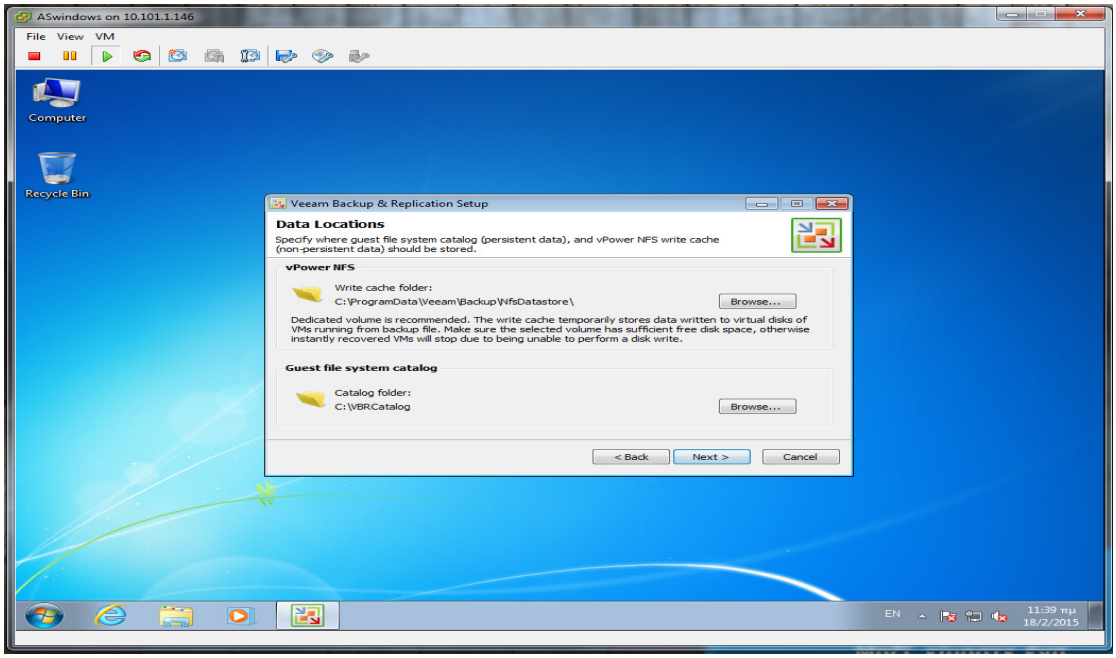
Εικόνα 4.24: Δημιουργία χρήστη εφαρμογής

και με αυτόν το χρήστη θα συνδέεται στο σχήμα της βάσης που θα δημιουργήσει τοπικά στο μηχάνημα (εικ. 4.25).



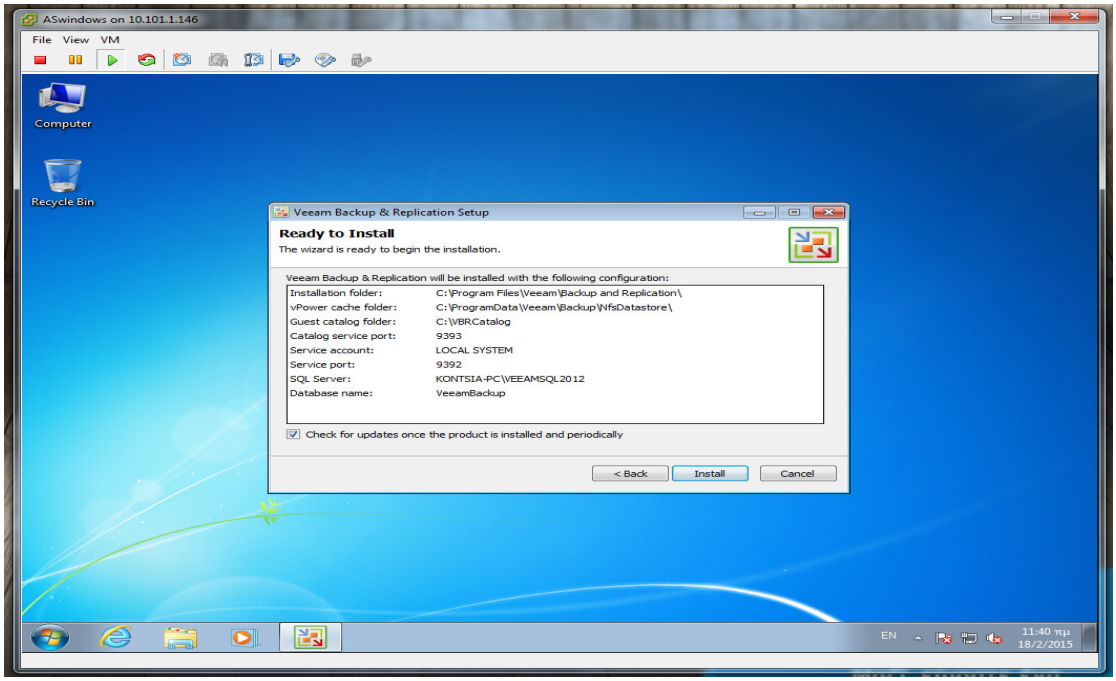
Εικόνα 4.25: Σύνδεση με τη βάση της εφαρμογής

Στη συνέχεια προτείνει που θα ήταν σωστό να αποθηκεύονται προσωρινές πληροφορίες του εργαλείου, καθώς και οι παράμετροι καταλογοποίησης των αντιγράφων ασφάλειας. Εμείς επιλέξαμε τις προκαθορισμένες ρυθμίσεις (εικ. 4.26).



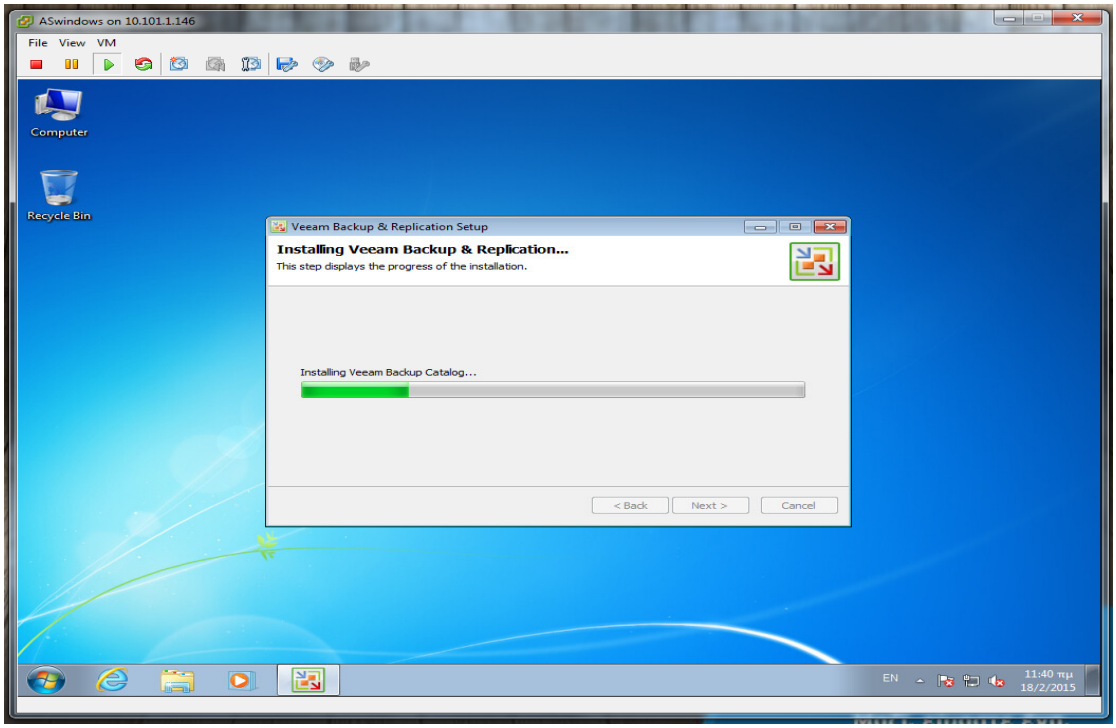
Εικόνα 4.26: Διαδρομή αποθήκευσης βοηθητικών αρχείων

Αφού εμφανίζεται μια συγκεντρωτική περίληψη των ρυθμίσεων που έχουμε αποφασίσει (εικ. 4.27),



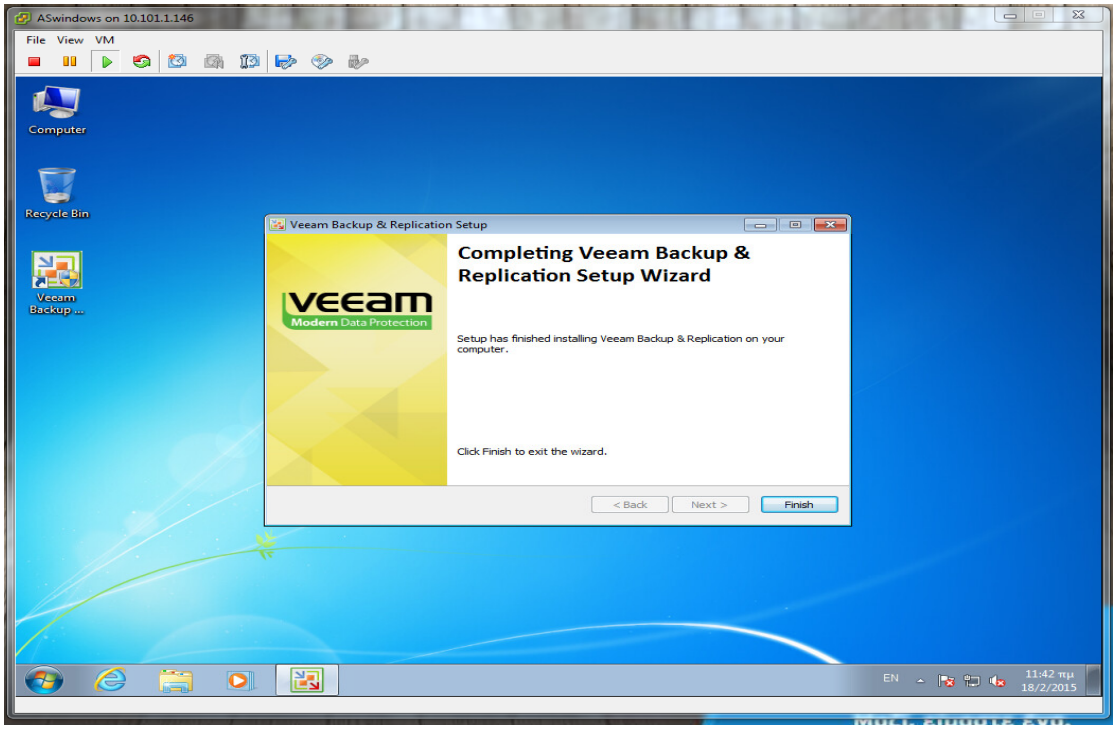
Εικόνα 4.27: Περίληψη εγκατάστασης

αρχίζει η εγκατάσταση του εργαλείου (εικ. 4.28),



Εικόνα 4.28: Πρόοδος εγκατάστασης

η οποία διαρκεί λίγα λεπτά και τερματίζει χωρίς απρόοπτα ή ανάγκη επανεκκίνησης του μηχανήματος (εικ. 4.29).



Εικόνα 4.29: Ολοκλήρωση εγκατάστασης

4.2.2.1 Λειτουργίες «Veeam backup» και «Veeam recovery»

Η λειτουργία «Veeam backup» δημιουργεί μια κόπια των δεδομένων, την συμπιέζει και την αποθηκεύει ορίζοντάς την πλέον ως ανεξάρτητο σημείο ανάκτησης (restore point). Στην δωρεάν έκδοση επιτρέπεται να μπει μόνο μια εικονική μηχανή ανά εντολή backup, αλλά είναι επιτρεπτό να εκτελούνται ταυτόχρονα όσες εντολές backup θέλουμε. Επίσης η δωρεάν έκδοση δεν προσφέρει προγραμματισμένες εντολές (scheduled tasks), αλλά θα πρέπει κάθε εντολή να εκτελείται χειροκίνητα. Επίσης κάθε backup job τρέχει στο παρασκήνιο, οπότε ακόμα και αν κλείσει το γραφικό του προγράμματος, δεν διακόπτονται οι τρέχουσες διεργασίες.

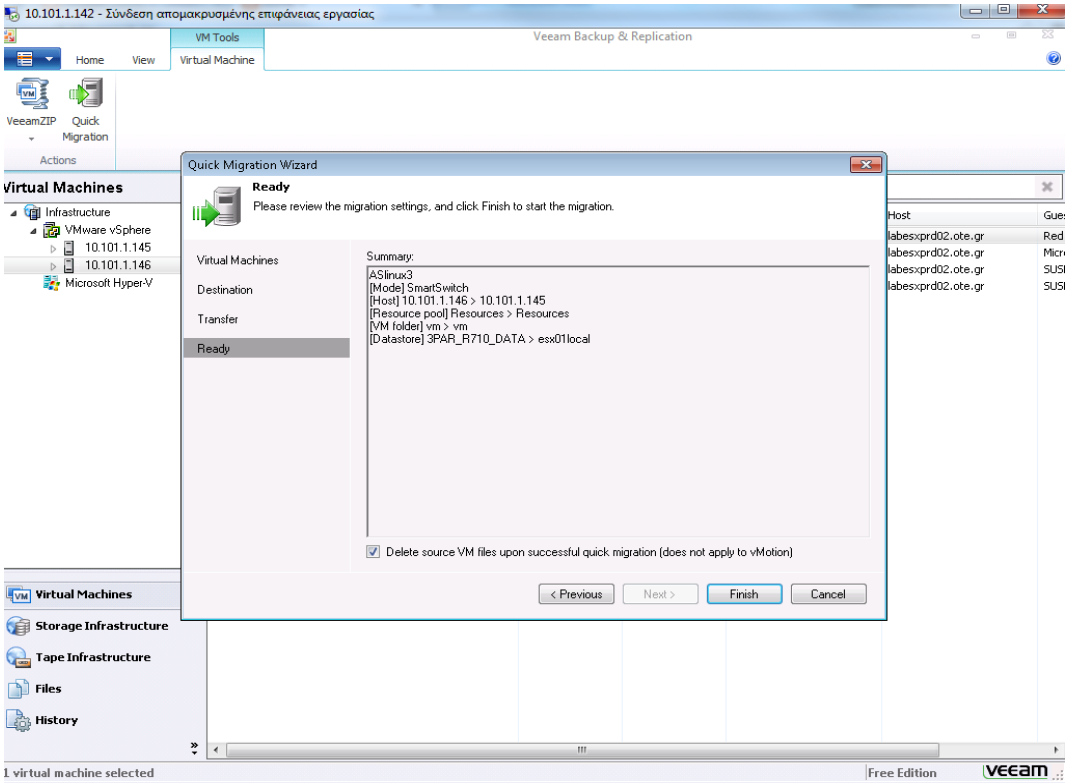
Όσον αφορά τη λειτουργία «Veeam recovery», η δωρεάν έκδοση του εργαλείου προσφέρει πληθώρα επιλογών ανάκτησης δεδομένων.

1. Από το veeamZIP αρχείο που δημιουργήθηκε τοπικά στον δίσκο του μηχανήματος, μπορεί να γίνει ανάκτηση ολόκληρου του μηχανήματος. Το ίδιο ισχύει αν αντί για πλατφόρμα VMware έχουμε Hyper-V. Δεν υποστηρίζει μαζική και

προγραμματισμένη ανάκτηση πολλών μηχανών. Θα πρέπει να ορίζεται από τον χρήστη ένα μηχάνημα την φορά.

2. Δίνεται η δυνατότητα ανάκτησης σε επίπεδο αρχείων συστήματος. Είναι χρήσιμο σε περιπτώσεις όπου έχουμε file corruption μόνο σε μερικά τμήματα του δίσκου και δεν θα ήταν χρήσιμη μια ανάκτηση – επαναφορά ολόκληρου του virtual machine.

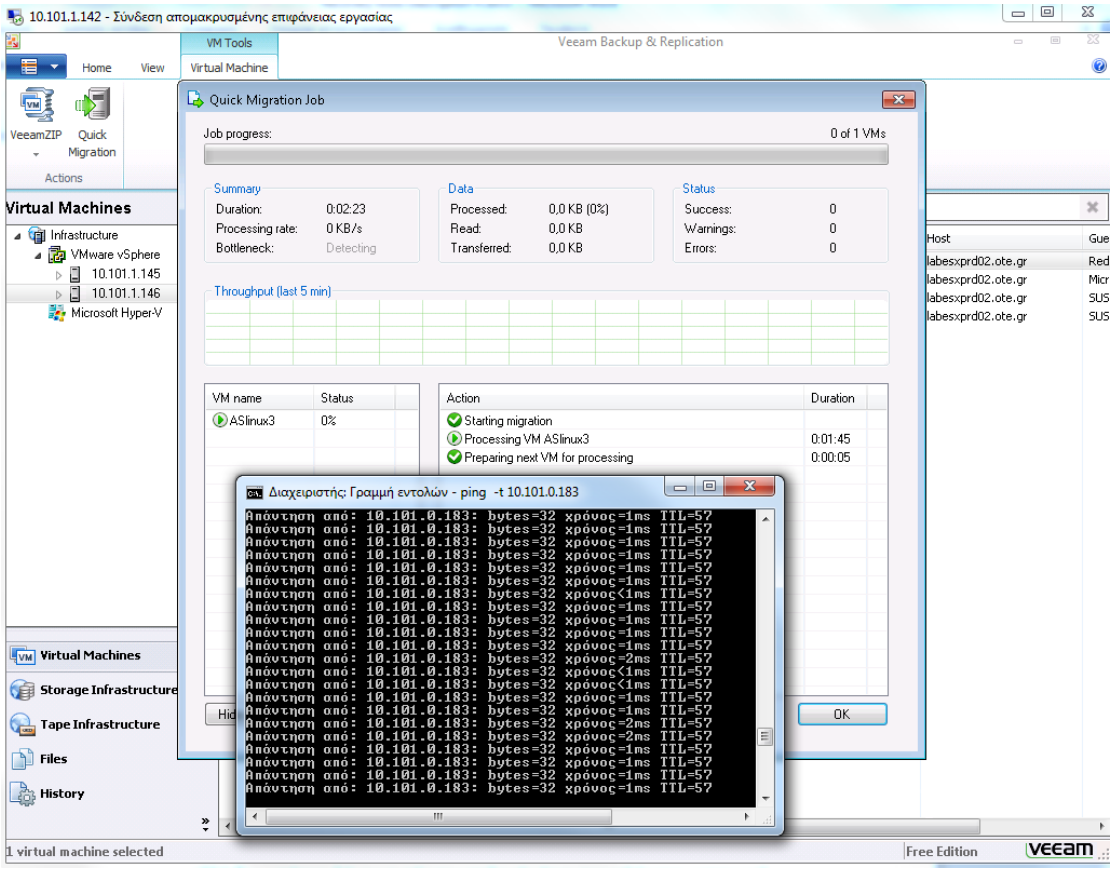
3. Μια άλλη επιλογή που και αυτή εξυπηρετεί σκοπούς ανάκτησης μηχανήματος και υπηρεσίας, είναι η μεταγωγή (migration) του virtual machine σε άλλον ESXi εξυπηρετητή (host) ή σε άλλη τοποθεσία αποθηκευτικού μέσου (datastore). Ιδιαίτερα χρήσιμη δυνατότητα αν έχουμε δυσλειτουργία σε κάποιον ESXi εξυπηρετητή ή κάποιο datastore παρουσιάζει αργή απόκριση και αντιμετωπίζουμε πιθανή διακοπή υπηρεσιών. Το λεγόμενο vm migration υποστηρίζεται μόνο για μηχανές οι οποίες φιλοξενούνται σε πλατφόρμα της VMware και όχι για αυτές οι οποίες είναι σε Hyper-V. Η διαδικασία της μεταγωγής σε άλλο host γίνεται με το μηχάνημα σε λειτουργία με πολύ σύντομη καθυστέρηση των υπηρεσιών που εκτελεί εκείνη τη στιγμή (hot migration) και η μόνη διακοπή είναι όταν ολοκληρωθεί η μεταγωγή όπου θα πρέπει να κλείσει το παλιό μηχάνημα και να εκκινήσει το migrated machine. Βέβαια υπάρχει και η επιλογή να κλείσει το μηχάνημα εξ' αρχής και να γίνει ύστερα η μεταγωγή του (cold migration), (εικ. 4.30).



Εικόνα 4.30: Hot migration

Δεν υπάρχει όμως λόγος αυτής της επιλογής, όταν προσφέρεται μεταγωγή χωρίς μεγάλη διακοπή υπηρεσιών (minimum downtime migration). Η μεταγωγή αναλύεται σε πολλά στάδια, και παρόλο που η ανάλυσή τους ίσως ξεφεύγει από τον σκοπό αυτής της μελέτης, εντούτοις μπορούμε να αναφέρουμε επιγραμματικά τι συμβαίνει στο παρασκήνιο (εικ. 4.31).

- Γίνεται αντιγραφή των ρυθμίσεων του virtual machine (vm configuration file – vmx file) στο host (ή datastore) που θα μεταφερθεί.
- Γίνεται αντιγραφή όλων των δεδομένων του vm στο νέο προορισμό (snapshot).



Εικόνα 4.31: Πρόοδος μεταγωγής

4. Υπάρχει επίσης η δυνατότητα αποθήκευσης των δεδομένων σε ταινίες. Απαραίτητη βεβαίως καθίσταται η ύπαρξη ενός backup server ο οποίος θα είναι συνδεδεμένος με το εργαλείο είτε μέσω οπτικής ίνας (FC), είτε μέσω καλωδίου SCSI για να μπορεί να εκτελείται η λήψη ή η ανάκτηση των αντιγράφων ασφάλειας.

5. Μια ακόμη χρήσιμη επιλογή είναι η ανάκτηση από αντίγραφο στιγμιότυπου του μηχανήματος σε επίπεδο storage (storage snapshot). Οι περισσότερες εταιρίες

αποθηκευτικών μέσων προσφέρουν και αυτές με την σειρά τους μεθόδους backup οι οποίες γίνονται σε επίπεδο δίσκων. Μια γνωστή λοιπόν δυνατότητα είναι και το storage snapshot το οποίο λαμβάνει αντίγραφο όλου του volume του storage ανά περιοδικά διαστήματα. Στη συνέχεια, και όποτε παραστεί ανάγκη, το πιο πρόσφατο στιγμιότυπο μπορεί να χρησιμοποιηθεί για την ανάκτηση του μηχανήματος. Η διαδικασία βέβαια είναι ιδιαίτερα πολύπλοκη και χρονοβόρα, διότι απαιτεί μια σειρά από ενέργειες στην εικονική υποδομή για να μπορέσει αυτή με την σειρά της να αναγνωρίσει το νέο δίσκο και να τον προσαρτήσει στο μηχάνημα. Επιγραμματικά, θα πρέπει να γίνει δηλωθεί το νέο κομμάτι δίσκου στη φάρμα, να αναγνωριστεί από όλους τους εξυπηρετητές ESXis, να προσαρτηθεί ο δίσκος στο μηχάνημα, και ύστερα από επανεκκίνηση της μηχανής, αυτή να δει τελικά τον δίσκο. Η εναλλακτική που μας προσφέρει το VEEAM backup & replication ονομάζεται "Veeam Explorer for Storage Snapshots" και υπόσχεται γρήγορη και εύκολη ανάκτηση της μηχανής από τα αντίγραφα στιγμιότυπων. Είναι μια νέα τεχνολογία η οποία επιτρέπει την επαναφορά των δεδομένων στην VMware υποδομή απευθείας από αντίγραφα στιγμιότυπα. Έχει σχεδιαστεί και αναπτυχθεί σε συνεργασία με την HP και την NetApp και και μέχρι στιγμής υποστηρίζει το storage μόνον αυτών των δύο εταιριών.

6. Τελευταία επιλογή η οποία τείνει να γίνει και η πιο "σύγχρονη", είναι η λήψη αντιγράφων στο σύννεφο (backup cloud). Μέχρι τώρα δεν υπήρχε η δυνατότητα για αντίγραφα ασφάλειας απευθείας στο περιβάλλον του υπολογιστικού σύννεφου (vCloud Director), αλλά σε ένα επίπεδο πιο κάτω, στο περιβάλλον της εικονικής πλατφόρμας (μέσω του VMware vCenter). Η κοινή πρακτική λοιπόν ήταν η λήψη αντιγράφων ασφάλειας σε επίπεδο VMware vCenter και αν χρειαζόταν επαναφορά κάποιου συστήματος έπρεπε πρώτα να γίνει επαναφορά σε επίπεδο vCenter και στη συνέχεια να γίνει import το σύστημα στο σύννεφο (μέσω του vCloud Director). Πλέον αυτό αλλάζει καθώς το Veeam backup & replication tool παρέχει τη δυνατότητα απευθείας επικοινωνίας με τον vCloud Director για άμεση λήψη αντιγράφων ασφαλείας και επαναφορά συστήματος.

4.2.2.2 Υποστηριζόμενα χαρακτηριστικά

- Υποστηρίζει αντίγραφα ασφάλειας πολλαπλών δίσκων VMDK ανά VM.
- Υποστηρίζει προτεραιοποίηση του backup (ποιο vm θα πάρει 1ο backup και ποιο θα ακολουθήσει).

- Δεν υπάρχει περιορισμός στον αριθμό των προγραμματισμένων εργασιών αντιγράφων ασφάλειας (scheduled backup jobs).
- Παρέχεται report με το πέρας του αντιγράφου ασφάλειας σε μορφή history file.
- Δυνατότητα καταγραφής χρονικής διάρκειας του backup.
- Παρέχεται η δυνατότητα online backup (hot backup). Το vm δεν χρειάζεται να κλείσει για να ξεκινήσει η διαδικασία του backup.
- Παρέχεται η δυνατότητα κρυπτογράφησης των αντιγράφων ασφάλειας (backup encryption).
- Παρέχεται δυνατότητα εξαγωγής των αντιγράφων ασφάλειας στο σύννεφο ή σε tapes.
- Παρέχεται εξαγωγή των αντιγράφων ασφάλειας σε NFS share.
- Παρέχεται η δυνατότητα για επανάκτηση σε επίπεδο αρχείου filesystem.
- Δεν επιβαρύνει τους ESXis με Processor utilization (CPU load).
- Παρέχεται η δυνατότητα για memory snapshot.
- Εξασφαλισμένο σβήσιμο των στιγμιότυπων (snapshots) πριν να προχωρήσει στο επόμενο virtual machine.
- Τα αντίγραφα ασφάλειας μπορεί να είναι είτε thin, είτε thick (eager-zero or zero).
- Είναι supported για κάθε πλατφόρμα η οποία προσφέρει virtualized υπηρεσίες.
- Έχει εύκολη διαχείριση καθότι προσφέρει graphical user interface (GUI).
- Υποστηρίζει είτε SCSI είτε IDE δίσκους.
- Υποστηρίζει συμπίεση αντιγράφων ασφάλειας (backup compression).

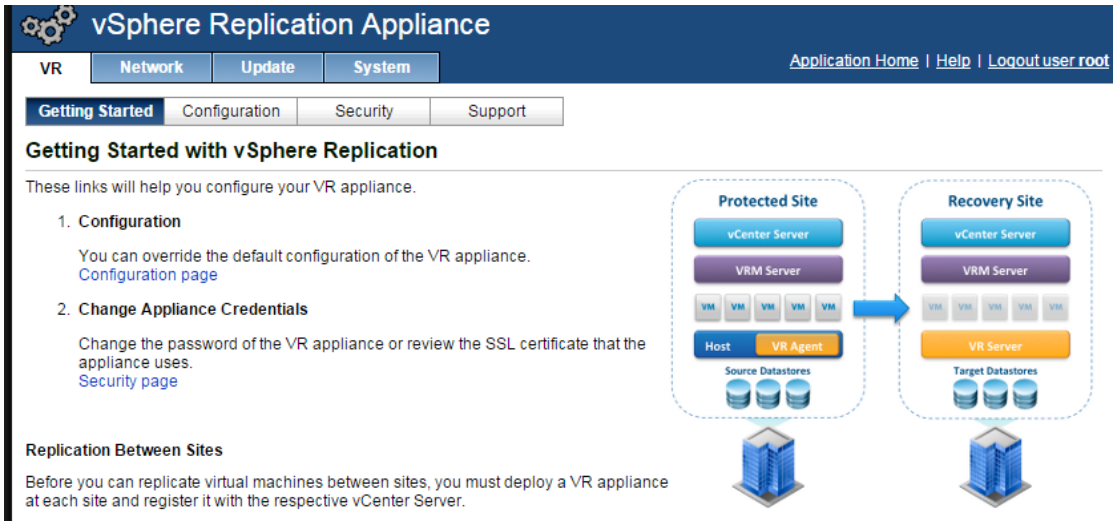
4.2.2.3 Μη υποστηριζόμενα χαρακτηριστικά

- Δεν υποστηρίζει δυνατότητα για scheduled backup.
- Δεν υποστηρίζει επιβεβαίωση και έλεγχο του backup (backup verification), παρά μόνον αν γίνει δοκιμαστικό restore.
- Δεν παρέχεται δυνατότητα ενημέρωσης μέσω email μετά την ολοκλήρωση του backup.
- Δεν παρέχεται η δυνατότητα για differential, incremental backup ή δυνατότητα για data deduplication. Παρέχεται μόνον full backup.
- Δεν παρέχεται η δυνατότητα για συνεχής ενημέρωση δεδομένων των αντιγράφων ασφάλειας (rsync backup files).
- Δεν παρέχεται η δυνατότητα εξαγωγής των αντιγράφων ασφάλειας σε άλλα μέσα αποθήκευσης (CD-ROM, NAS, DVD, Blu-Ray, USB drives, FTP servers).

- Δεν παρέχεται δυνατότητα επανάκτησης σε καθορισμένο χρονικό σημείο (point-in-time recovery).
- Δεν προσφέρει αυτοματοποιημένη διαδικασία recovery&replication, αλλά από το αντίγραφο της εικονικής μηχανής, μπορούμε να επανακτήσουμε το μηχάνημα με σχετική ευκολία.
- Υποστηρίζει αντίγραφα ασφάλειας μόνο για δίσκους που περιέχουν VMDKs.
- Δεν παίρνει backup vms που έχουν ήδη snapshots.
- Δεν υποστηρίζει αντίγραφα ασφάλειας σε εικονικές μηχανές οι οποίες έχουν Raw Device Disks (RDMs).

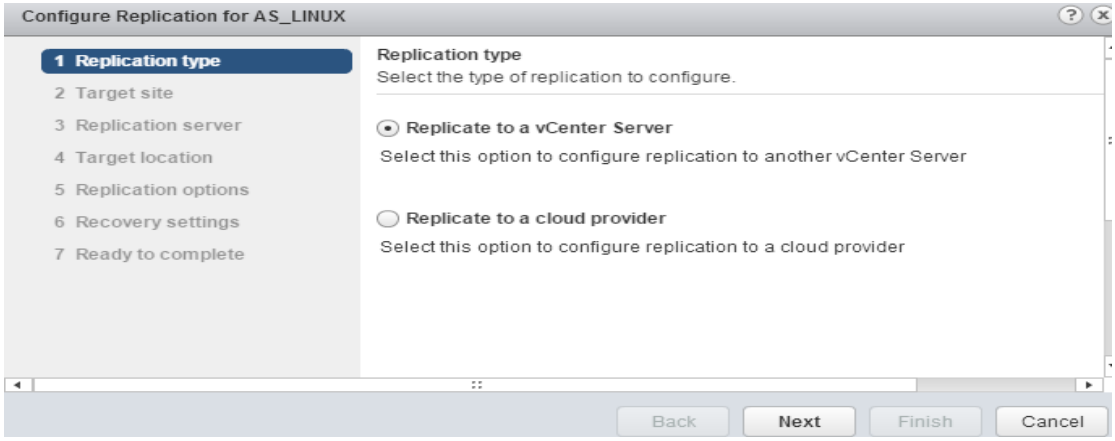
4.2.3 VMware vSphere Replication

Είναι μια λύση για προστασία δεδομένων και για ανάκαμψη από καταστροφή [04, 07]. Είναι πλήρως συμβατό σε περιβάλλον vmware και προσφέρει ασύγχρονη αντιγραφή δεδομένων (asynchronous data replication) των εικονικών μηχανών. Είναι δωρεάν εφόσον υπάρχει προεγκατεστημένο virtualization περιβάλλον της vmware. Οι λύσεις που προσφέρει ποικίλουν ανάλογα με τις εκάστοτε ανάγκες (εικ. 4.32).

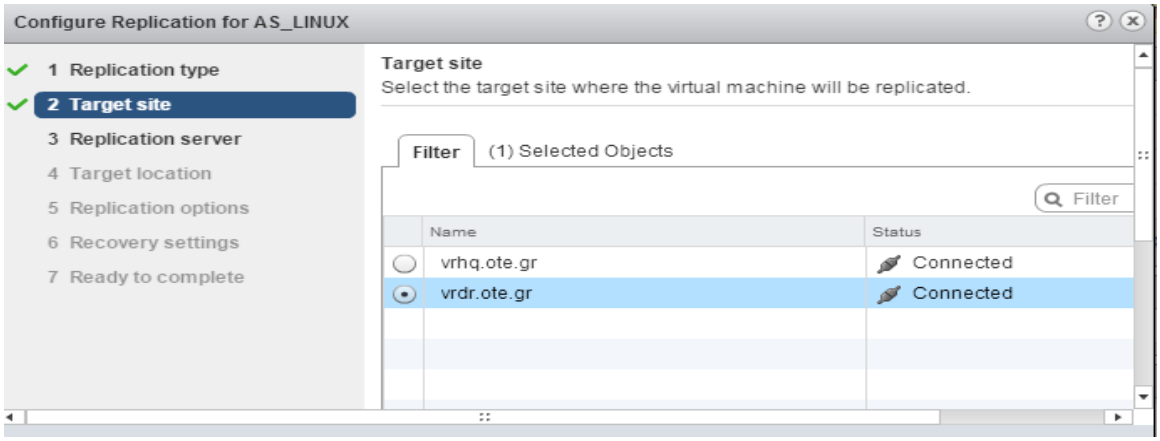


Εικόνα 4.32: Αρχικές παραμετροποιήσεις replication

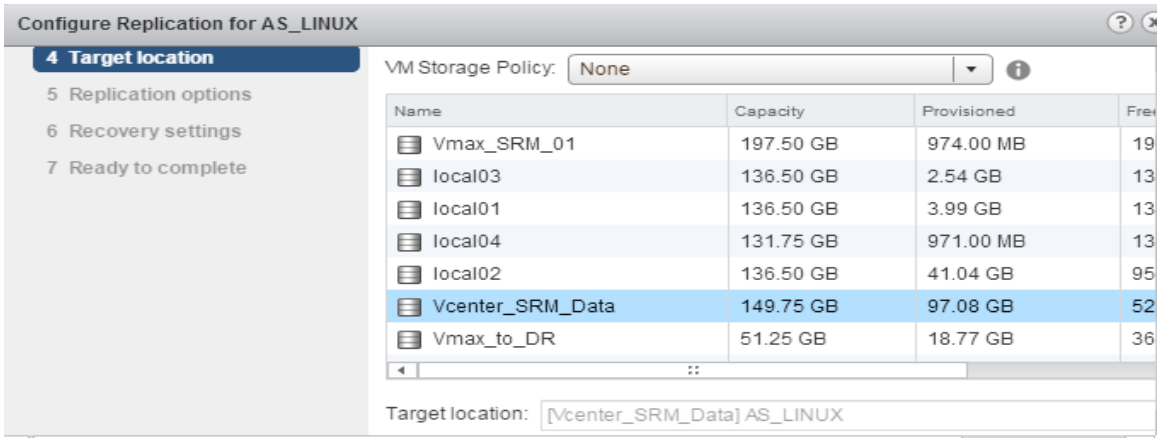
Δίνει την δυνατότητα για υλοποίηση αντιγραφής δεδομένων από ένα πρωτεύων site στο disaster site, επιλογή αντιγραφής ολόκληρου του virtual datacenter, επιλογή για αντιγραφή δεδομένων απευθείας στο σύννεφο (cloud) (εικ. 4.33, 4.34, 4.35).



Εικόνα 4.33: Επιλογή προορισμού αντιγραφέντων δεδομένων

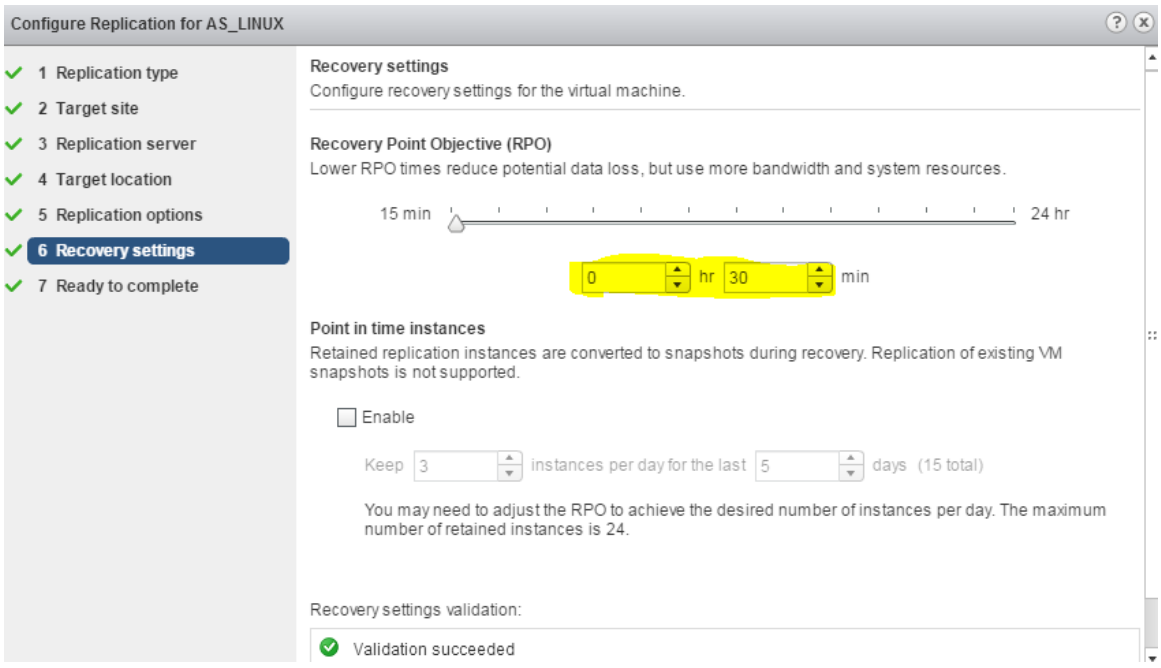


Εικόνα 4.34: Επιλογή του DR site



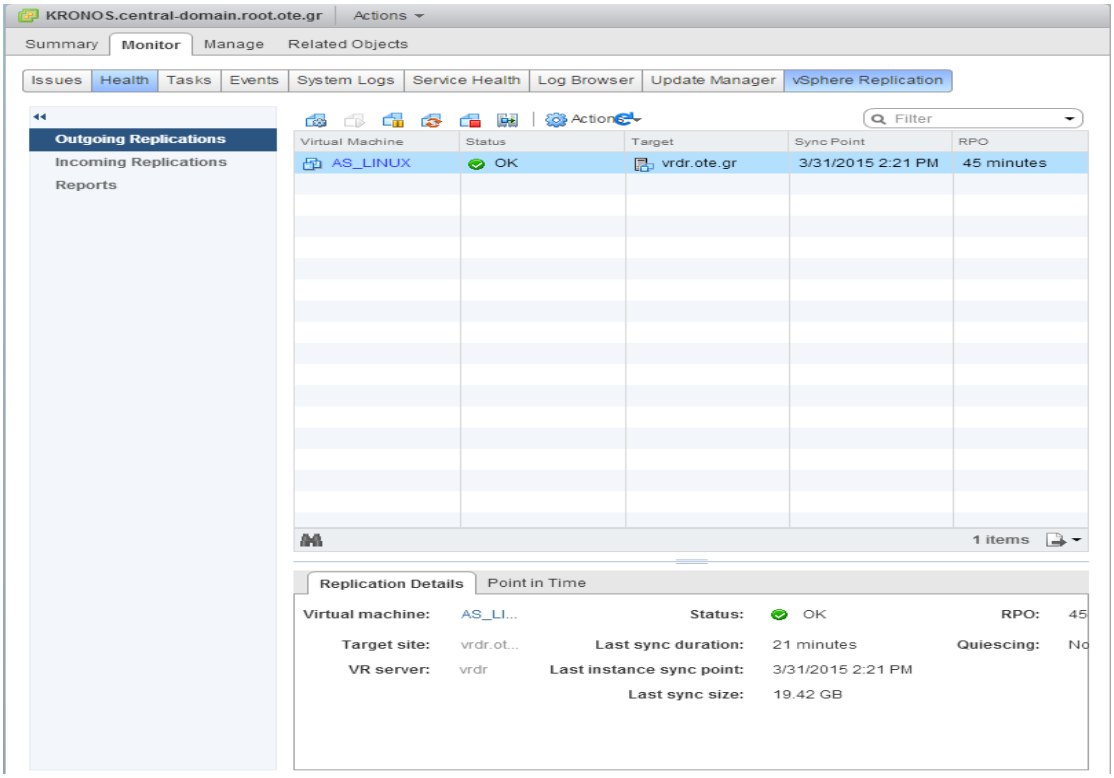
Εικόνα 4.35: Επιλογή storage

Κατά την δημιουργία ενός backup/replication job ορίζεται και η πολιτική που θα εκτελεστεί κατά την αντιγραφή (εικ. 4.36). Ορίζονται τα Recovery Point Objectives (RPO) των εικονικών μηχανών, τον χρόνο δηλαδή που θα μεσολαβεί , μεταξύ των ενημερώσεων της αντιγραφήσας εικονικής μηχανής (πχ κάθε 30min), αν θα είναι ενεργή η δυνατότητα για memory quiescing, αν θα υπάρχει συμπίεση των αντιγραφόμενων δεδομένων, αν θα υπάρχει data encryption κλπ.



Εικόνα 4.36: Επιλογή Recovery Point Objective

Μετά τις αρχικές ρυθμίσεις του replication job, το εργαλείο εκτελεί μια αρχική αντιγραφή ολόκληρης της εικονικής μηχανής, έναν συγχρονισμό όλων των δεδομένων του virtual machine. Ο χρόνος ολοκλήρωσης ποικίλλει, και εξαρτάται από τον όγκο των δεδομένων και το εύρος της δικτυακής διασύνδεσης. Πάντως αυτό δεν θα είναι ο χρόνος του backup γενικότερα, καθώς στις επόμενες εκτελέσεις δεν θα γίνεται αντιγραφή όλων των δεδομένων εκ νέου αλλά μόνο των αλλαγών αυτών. Ακολουθεί ένα αρχικό full replication μιας εικονικής μηχανής (εικ. 4.37).



Εικόνα 4.37: Πρόοδος replication

Μετά την ολοκλήρωση του 1ης «εν συνόλω» αντιγραφής, στη συνέχεια θα εντοπίζονται οι αλλαγές στα δεδομένα και θα αντιγράφονται μόνον αυτές, με συχνότητα η οποία έχουμε οριστεί μέσω της τιμής του που δώσαμε εξ' αρχής στο RPO. Κατά την διάρκεια της αντιγραφής, τα προς αντιγραφή δεδομένα αποθηκεύονται σε κάποια αρχεία ονόματι "redo logs" τα οποία είναι σε ξεχωριστό αποθηκευτικό μέσο από το δίσκο προορισμού. Όταν ολοκληρωθούν όλες οι διεργασίες αντιγραφής των δεδομένων στο redo log file, δηλαδή όταν έχουν αντιγραφεί όλες οι αλλαγές στα δεδομένα, τότε μόνον τα περιεχόμενα του redo log περνάνε στο αποθηκευτικό δίσκο προορισμού. Αυτό είναι ιδιαίτερα σημαντικό διότι διασφαλίζει την ακεραιότητα των δεδομένων σε πιθανό απρόοπτο τερματισμό του εργαλείου κατά την διάρκεια αντιγραφής δεδομένων (πχ λόγω δικτυακού προβλήματος). Με αυτό τον τρόπο τα δεδομένα της εικονικής μηχανής είναι αποθηκευμένα «προσωρινά» σε ένα redo log file και έτσι επιτυγχάνεται ταχεία ανάκαμψη ακόμα μετά και από απρόοπτη διακοπή του replication.

Μία ακόμα χρήσιμη δυνατότητα είναι η ενεργοποίηση multiple recovery points κατά την διάρκεια του κύκλου των αντιγραφών. Είπαμε προηγουμένως ότι υπάρχει η δυνατότητα να οριστούν on-demand RPOs για το replication. Δηλαδή να ορίσουμε πχ για μια εικονική μηχανή RPO=4. Αυτό σημαίνει ότι κάθε 4 ώρες θα εκτελείται

αντιγραφή (replication). Άρα έχουμε έξι (6) κύκλους αντιγραφής ανά ημέρα. Αυτή η δυνατότητα είναι ιδιαιτέρως χρήσιμη όταν έχουμε κάποιο συμβάν και το ανακαλύπτουμε μερικές ώρες (ή και μέρες), μετά την εμφάνισή του. Για παράδειγμα ας υποθέσουμε ότι μια εικονική μηχανή στην οποία έχουμε ορίσει 4-h RPO, έχει μολυνθεί από ιό (virus) και αυτό έγινε αντιληπτό μετά από 6 ώρες. Το αποτέλεσμα είναι ο ιός να αντιγράφηκε και στην backup εικονική μηχανή αφού εκτελέστηκε replication στις 4 ώρες. Με τα multiple recovery points μπορούμε να επανακτήσουμε την μηχανή χρησιμοποιώντας την πιο πρόσφατη αντιγραφή και στην συνέχεια να χρησιμοποιήσουμε το κατάλληλο recovery point για να επαναφέρουμε την μηχανή σε κάποια χρονική στιγμή πριν της μόλυνσης. Το πλήθος των multiple recovery points είναι σε άμεση συνάρτηση με τους κύκλους των αντιγραφών κα απαιτείται μεγαλύτερος αποθηκευτικός χώρος. Αν και υπάρχει η δυνατότητα του retention, δηλαδή να διατηρούνται πχ. τα τελευταία 6 recovery points, εν τούτοις θα πρέπει να προγραμματίζεται ανάλογα με τον διαθέσιμο χώρο του storage.

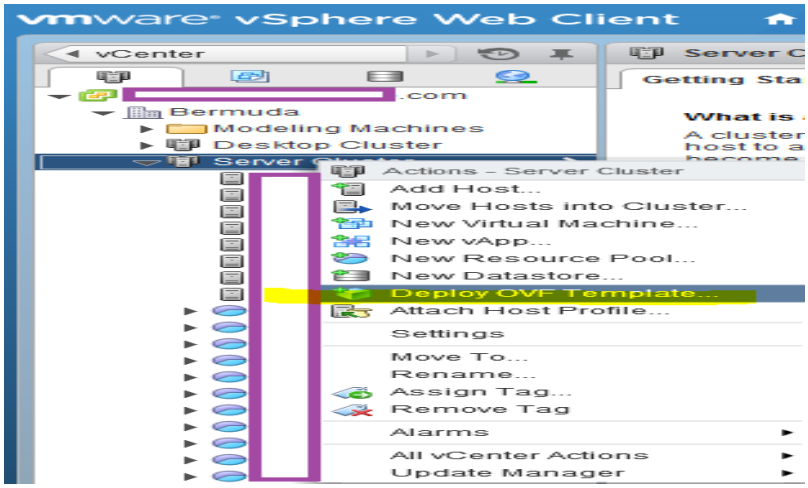
Ας δούμε λίγο τώρα την διαδικασία ανάκαμψης (recovery process). Αν χρειαστεί επαναφορά (recovery) κάποιας πρωτεύουσας (primary) εικονικής μηχανής, υπάρχουν δύο επιλογές ανάκαμψης ανάλογα με το μέγεθος καταστροφής της εικονικής μηχανής.

- Συγχρονισμός των τελευταίων αλλαγών. Αυτή η επιλογή χρησιμοποιείται όταν η εικονική μηχανή είναι προσβάσιμη αλλά είναι κλειστή. Όλες οι τελευταίες αλλαγές της primary virtual machine αντιγράφονται στην backup μηχανή πριν γίνει αυτή primary. Παρόλο που αυτό αυξάνει τους χρόνους ανάκαμψης, είμαστε εξασφαλισμένοι ότι δεν θα έχουμε απώλεια δεδομένων.
- Χρήση των πιο πρόσφατων διαθέσιμων δεδομένων. Χρησιμοποιείται όταν η κύρια εικονική μηχανή δεν είναι πλέον διαθέσιμη για οποιοδήποτε λόγο. Είτε λόγω διαγραφής της, είτε λόγω γενικότερης καταστροφής. Σε αυτή την περίπτωση δεν υπάρχει συγχρονισμός δεδομένων πριν την επαναφορά και όπως είναι κατανοητό υπάρχει ενδεχόμενο απώλειας δεδομένων. Το μέγεθος της απώλειας αυτής εξαρτάται από τον ρυθμό των αντιγραφών που είχε οριστεί στο RPO και στο πλήθος των recovery points.

Μέσω του περιβάλλοντος διαχείρισης του εργαλείου παρέχονται και γραφήματα με πληροφορίες για το πλήθος των εικονικών μηχανών που αντιγράφονται, για τον όγκο των δεδομένων που μεταφέρονται, για τα RPOs των μηχανών και αν αυτά μερικές φορές καταστρατηγούνται (πχ σε ad-hoc replication). Όλα αυτά τα γραφήματα

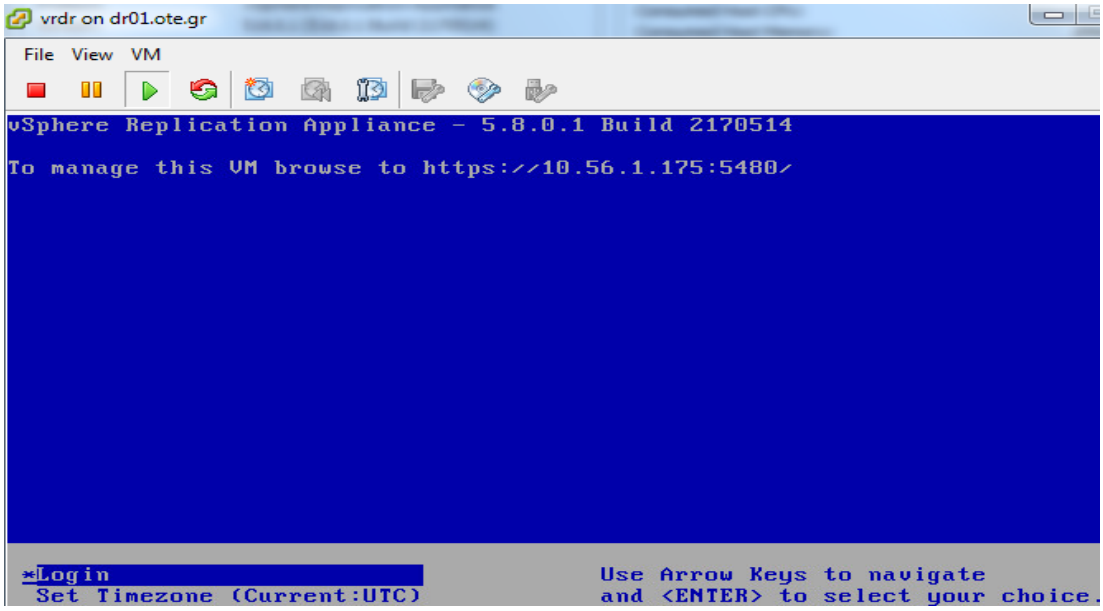
μπορούν να εμφανίσουν πιο συγκεκριμένες και αναλυτικές πληροφορίες μιας και είναι πλήρως παραμετροποιήσιμα.

Όσον αφορά την εγκατάσταση, δεν έχει κάποια ιδιαίτερη δυσκολία, καθώς προσφέρεται υπό μορφής εικονικής μηχανής με όλες τις αρχικές ρυθμίσεις προκαθορισμένες (εικ. 4.38).



Εικόνα 4.38: Εγκατάσταση εργαλείου vSphere Replication

Από την στιγμή που θα εισαχθεί στο virtual datacenter και τεθεί σε λειτουργία, ένα γραφικό περιβάλλον είναι διαθέσιμο μέσω οποιουδήποτε internet browser για την ολοκλήρωση της εγκατάστασης (εικ. 4.39).



Εικόνα 4.39: Αρχική διαχείριση εργαλείου

4.2.3.1 Υποστηριζόμενα χαρακτηριστικά

- Υποστηρίζει αντίγραφα ασφάλειας πολλαπλών δίσκων VMDK ανά VM.
- Υποστηρίζει προτεραιοποίηση του backup (ποιο vm θα πάρει 1ο backup και ποιο θα ακολουθήσει).
- Υποστηρίζεται η δυνατότητα scheduled replication.
- Δεν υπάρχει περιορισμός στον αριθμό των προγραμματισμένων εργασιών αντιγράφων ασφάλειας (scheduled backup jobs).
- Υποστηρίζει επιβεβαίωση και έλεγχο του replication.
- Παρέχεται reporting αναφέροντας όλες τις αντιγραφές που έχουν εκτελεστεί.
- Παρέχεται δυνατότητα ενημέρωσης μέσω email μετά την ολοκλήρωση του replication.
- Δυνατότητα καταγραφής χρονικής διάρκειας του backup.
- Παρέχεται η δυνατότητα online replication. Το vm δεν χρειάζεται να διακόψει τις υπηρεσίες του.
- Παρέχεται η δυνατότητα για incremental replication εκτός από full replication.
- Παρέχεται η δυνατότητα για συνεχής ενημέρωση δεδομένων των αντιγράφων ασφάλειας.
- Παρέχεται δυνατότητα εξαγωγής των αντιγράφων ασφάλειας στο σύννεφο.
- Παρέχεται εξαγωγή των αντιγράφων ασφάλειας σε NFS share.
- Παρέχεται η δυνατότητα επανάκτησης σε καθορισμένο χρονικό σημείο (point-in-time recovery).
- Δεν επιβαρύνει τους ESXis με Processor utilization (CPU load).
- Παρέχεται η δυνατότητα για memory snapshot.
- Υποστηρίζεται αντιγραφή εικονικών μηχανών που έχουν ήδη snapshots.
- Τα αντίγραφα ασφάλειας μπορεί να είναι είτε thin, είτε thick (eager-zero or zero).
- Έχει εύκολη διαχείριση καθότι προσφέρει graphical user interface (GUI).
- Υποστηρίζει είτε SCSI είτε IDE δίσκους.

4.2.3.2 Μη υποστηριζόμενα χαρακτηριστικά

- Δεν παρέχεται η δυνατότητα κρυπτογράφησης των αντιγράφων ασφάλειας (backup encryption).
- Δεν παρέχεται η δυνατότητα εξαγωγής των αντιγράφων ασφάλειας σε άλλα μέσα αποθήκευσης (CD-ROM, NAS, DVD, Blu-Ray, USB drives, FTP servers).
- Δεν παρέχεται η δυνατότητα για επανάκτηση σε επίπεδο αρχείου filesystem.

- Δεν προσφέρει αυτοματοποιημένη διαδικασία recovery&replication, αλλά από το αντίγραφο της εικονικής μηχανής, μπορούμε να επανακτήσουμε το μηχάνημα με σχετική ευκολία.
- Είναι supported μόνο για πλατφόρμα VMware virtualization.
- Δεν υποστηρίζει συμπίεση αντιγράφων ασφάλειας (backup compression).
- Δεν υποστηρίζει αντίγραφα ασφάλειας σε εικονικές μηχανές οι οποίες έχουν Raw Device Disks (RDMs).

4.2.4 XSI Backup

Είναι και αυτή μια δωρεάν λύση δημιουργίας αντιγράφων ασφαλείας σχεδιασμένη για περιβάλλον VMware ESXi 5.1, 5.5 και 6.0 η οποία επιτρέπει με ευφυή τρόπο τον καθορισμό backup πολιτικών των εικονικών μηχανών [01, 02, 03, 41]. Διαθέτει αρκετές παραμέτρους στις εντολές του και δίνει την δυνατότητα λήψη αντιγράφων ασφαλείας μεμονωμένων virtual machines ή πολλών μαζί ορίζοντας προτεραιότητα στα περισσότερο σημαντικά με βάση το όνομα εμφάνισης της κάθε εικονικής μηχανής για τις οποίες θέλουμε να πάρουμε αντίγραφα ασφαλείας (εικ. 4.40).

```
/scripts/XSIbackup # ./xsibackup
© 33HOPS, Sistemas de Informacion y Redes, S.L. - 33hops.com - © xsibackup 4.1.4
Backup Utility for the © VMware ESXi 5.X Hypervisor Series

RULES:
Arguments are a list of variable/value pairs separated by an equal sign.
You can use any character to define values with the exception of double quotes (") and the equal sign (=).
You must double quote variables if you use spaces or any scapable character.

USAGE:
Example 1 (backup all running VMs):
xsibackup --backup-point=/vmfs/volumes/backup --backup-type=running --mail-from=email.sender@yourdomain.com
--mail-to=email.recipient@anotherdomain.com --smtp-srv=smtp.yourdomain.com --smtp-port=25 --smtp-usr=username
--smtp-pwd=password

Example 2 (backup 3 VMs even if they are swiched off):
xsibackup --backup-point=/vmfs/volumes/backup --backup-type=custom --backup-vms="WINDOWSVM1,LINUXVM2,New VM"
--mail-from=email.sender@yourdomain.com --mail-to=email.recipient@anotherdomain.com --smtp-srv=smtp.yourdomain.com
--smtp-port=25 --smtp-usr=username --smtp-pwd=password

OPTIONS:

--install-cron          This will install the cron system and file xsibackup-cron to the current dir.
                        You can add as many XSIBackup commands as you want into this file, one per line.
                        The only thing you have to do is add the parameter --time, i.e. --time="Mon 23:30".

--backup-point          1) Full path to the backup mount point within the local server, it will tipically be under
                        /vmfs/volumes, i.e. /vmfs/volumes/backup, /vmfs/volumes/datastore2.
                        2) Full path in a remote ESXi host by using the following syntax:
                        --backup-point="IP.OF.REMOTE.SERVER:PORT:/full/path/todatastore:METHOD(F,D)"
                        Example: --backup-point="192.168.1.200:22:/vmfs/volumes/datastore2:F
                        METHOD (F,D): (F)ull or (D)elta. If F is chosen all bits will be copied, if D is
                        chosen only differential bits will be copied but can take longer. D is default.
                        You need to previously link the remote server to this host by using --link-srv option.

--backup-how            hot | cold
                        Hot (default): selected virtual machines are backed up without being switched off,
                        this is usefull for e-mail, http servers and VMs that cannot be switched off. If
                        you do not specify a value for --backup-how a hot backup will be carried out.
                        Cold: selected VMs will be switched off before backup and turned on right afterwards.
                        Good if you need a reboot cicle from time to time to refresh resources and don't
                        mind having a little downtime.

--backup-type           custom | all | running
                        Custom: if this methos is chosen then a list of the VMs to backup must be passed to
                        the --backup-vms option.
                        All: backup -all- VMS.
                        Running: backup only running virtual machines.

--backup-vms            List of virtual machines to backup as a colon separated list,
                        i.e: --backup-vms=VM1,VM2,VM3, only needed if custom is selected as the --backup-type

--test-mode=true        Allows testing backup procedure and e-mail submission without having to wait for a
                        full backup process. In this mode VMs are not copied to the backup disk.

--mail-from             E-mail address as from where the HTML e-mail report will be sent.

--mail-to               E-mail address to which the HTML e-mail report will be sent.
```

Εικόνα 4.40: Εντολές λήψης αντιγράφου ασφάλειας

Δημιουργεί αυτόνομα αντίγραφα ασφαλείας των εικονικών μηχανών που φιλοξενεί ένας ESXi εξυπηρετητής, τα οποία αποθηκεύονται είτε στο ίδιο datastore της εικονικής μηχανής, είτε σε άλλη απομακρυσμένη τοποθεσία αποθήκευσης δεδομένων μέσω δικτυακής διασύνδεσης. Δεν χρειάζεται εγκατάσταση κάποιου agent διότι τρέχει απευθείας στον hypervisor. Με το εργαλείο XSIBackup έχουμε την δυνατότητα να επιλέξουμε τη δημιουργία online (hot) backup εκτός από offline (cold backup). Μάλιστα, δεν χρειάζεται κάποια παράμετρο διότι είναι η προκαθορισμένη (default) επιλογή. Αν ζητηθεί αντίγραφο ασφάλειας με την εικονική μηχανή ανοιχτή, τότε το πρόγραμμα δίνει εντολή μέσω των εγκατεστημένων vmware tools της μηχανής, για normal shutdown του λειτουργικού. Αφού περιμένει για 30 δευτερόλεπτα, ελέγχει αν όντως έκλεισε η μηχανή. Αν δεν έχει κλείσει, κάνει ακόμα τρεις ελέγχους με διαφορά 10 δευτερολέπτων, και αν ακόμα συνεχίζει να είναι επάνω, εκτελεί force shutdown. Είναι λοιπόν αυτονόητο ότι κάθε εικονική μηχανή πρέπει να έχει εγκατεστημένα τα tools της vmware.

Στην αρχή της δημιουργίας κάθε αντιγράφου ασφάλειας, είτε είναι online (hot) backup είτε offline (cold backup), ελέγχει αν υπάρχει ελεύθερος χώρος στο δίσκο αποθήκευσης του αντίγραφου ασφάλειας και αν δεν υπάρχει διαγράφει τα παλιότερα backups (εικ. 4.41, 4.42).

```
/scripts/XSIbackup #
/scripts/XSIbackup # ./xsibackup --backup-point=/vmfs/volumes/530c8165-66f605c1-f73e-b8ac6f8f80ad/backups --backup-type=custom --backup-vms=ASlinux3
Tue, 10 Mar 2015 16:10:48 +0000
Found --backup-point at /vmfs/volumes/530c8165-66f605c1-f73e-b8ac6f8f80ad/backups
The e-mail report will not be sent becouse of the followig reasons:
The --mail-from string has not been set.
The --mail-to string has not been set.
The --smtp-srv string has not been set.
The --smtp-usr string has not been set, you need --smtp-usr if --smtp-auth is other than -none-.
The --smtp-pwd string has not been set, you need --smtp-pwd if --smtp-auth is other than -none-.


Getting list of all VMs...
1708   UI VM       [VCOPS_DataStore] UI VM/UI VM.vmx                      sles11_64Guest     vmx-07    VMware vCenter Operations Manager 5.8
1710   ASlinux3    [3PAR_R710_DATA] RHEL_6-5_withICS/RHEL_6-5_withICS.vmx rhel6_64Guest      vmx-08
1711   ASwindows   [3PAR_R710_DATA] ASwindows/ASwindows.vmx                windows7_64Guest   vmx-08
1713   VR_HQ       [VCOPS_DataStore] VR_HQ/VR_HQ.vmx                      sles11_64Guest     vmx-07    vSphere Replication Appliance
VMs to backup:
1710   ASlinux3    [3PAR_R710_DATA] RHEL_6-5_withICS/RHEL_6-5_withICS.vmx rhel6_64Guest      vmx-08
Needed room: 44 Gb.
Available room: 79 Gb.
Hot backup selected for VM: ASlinux3 will not be switched off
All snapshots removed for ASlinux3
Destination disk format: VMFS thin-provisioned
Cloning disk '/vmfs/volumes/530c8165-66f605c1-f73e-b8ac6f8f80ad/RHEL_6-5_withICS/RHEL_6-5_withICS.vmdk'...
Clone: 100% done.
/scripts/XSIbackup # ls
```

Εικόνα 4.41: Λήψη αντιγράφου ασφάλειας linux μηχανής

```
/scripts/XSIbackup #
/scripts/XSIbackup # ./xsibackup --backup-point=/vmfs/volumes/530c8165-66f605c1-f73e-b8ac6f8f80ad/backups --backup-type=custom --backup-vms=ASwindows
Tue, 10 Mar 2015 16:31:02 +0000
Found --backup-point at /vmfs/volumes/530c8165-66f605c1-f73e-b8ac6f8f80ad/backups
The e-mail report will not be sent becouse of the followig reasons:
The --mail-from string has not been set.
The --mail-to string has not been set.
The --smtp-srv string has not been set.
The --smtp-usr string has not been set, you need --smtp-usr if --smtp-auth is other than -none-.
The --smtp-pwd string has not been set, you need --smtp-pwd if --smtp-auth is other than -none-.


Getting list of all VMs...
1708   UI VM       [VCOPS_DataStore] UI VM/UI VM.vmx                      sles11_64Guest     vmx-07    VMware vCenter Operations Manager 5.8
1710   ASlinux3    [3PAR_R710_DATA] RHEL_6-5_withICS/RHEL_6-5_withICS.vmx rhel6_64Guest      vmx-08
1711   ASwindows   [3PAR_R710_DATA] ASwindows/ASwindows.vmx               windows7_64Guest   vmx-08
1713   VR_HQ       [VCOPS_DataStore] VR_HQ/VR_HQ.vmx                      sles11_64Guest     vmx-07    vSphere Replication Appliance
VMs to backup:
1711   ASwindows   [3PAR_R710_DATA] ASwindows/ASwindows.vmx               windows7_64Guest   vmx-08
Needed room: 34 Gb.
Available room: 69 Gb.
Hot backup selected for VM: ASwindows will not be switched off
All snapshots removed for ASwindows
Destination disk format: VMFS thin-provisioned
Cloning disk '/vmfs/volumes/530c8165-66f605c1-f73e-b8ac6f8f80ad/ASwindows/ASwindows.vmdk'...
Clone: 100% done.
/scripts/XSIbackup #
```

Εικόνα 4.42: Λήψη αντίγραφου ασφάλειας windows μηχανής

Επίσης έχει τη δυνατότητα αποστολής λεπτομερών reports ενημέρωσης μέσω e-mail αναφέροντας κάθε διεργασία του backup (ταχύτητα, κλείσιμο ή όχι του vm, έλεγχος διαθέσιμου χώρου, χρόνοι ολοκλήρωσης διεργασιών κλπ). Επιπρόσθετα, μπορούν να προγραμματιστούν εργασίες backup μέσω εισαγωγής κατάλληλων εντολών στο crontab του λειτουργικού του ESXi μέσω της παραμέτρου *--install-cron*. Αυτό θα εγκαταστήσει το σύστημα cron και θα δημιουργήσει ένα αρχείο crontab (πχ στο /vmfs/volumes/datastore1/xsibackup-cron). Στη συνέχεια μπορούμε να προγραμματίσουμε όσες εντολές αντιγράφων ασφάλειας θέλουμε. Το μόνο που πρέπει να κάνουμε είναι να προσθέσουμε την παράμετρο *--time*, δηλαδή *--time ="Fri 04:22"*, και ένα αρχείο καταγραφής θα κρατήσει το αποτέλεσμα στο /vmfs/volumes/datastore1/xsibackup-cron.log.

Δηλαδή: */vmfs/volumes/datastore1/xsibackup --time="Fri 04:22" --backup-point=/vmfs/volumes/backups --backup-type=custom -- backup-vms=ASlinux3*

Έτσι, αν θέλουμε ένα αντίγραφο ασφαλείας να προγραμματιστεί για κάθε μέρα, πρέπει να προστεθούν 7 γραμμές στο crontab αρχείο (xsibackup-cron), ένα για κάθε ημέρα. Τέλος, μπορούμε να απεγκαταστήσουμε την λειτουργία crontab πολύ εύκολα, εκτελώντας πάλι *--install-cron*.

Μια άλλη σημαντική δυνατότητα του συγκεκριμένου εργαλείου είναι η λειτουργία XSIBackup-Rsync. Με τη χρήση Rsync σε συνδυασμό με το XSIBackup επιτυγχάνεται συνεχής συγχρονισμός δεδομένων μεταξύ της εικονικής μηχανής και της κόπιας της. Φαινομενικά ακούγεται ιδεατό, μιας που θα μας έδινε την δυνατότητα επανάκτησης δεδομένων σε καθορισμένο χρονικό σημείο του παρελθόντος (point-in-time recovery), εν' τούτοις έχει μερικά πολύ σημαντικά μειονεκτήματα. Δεδομένου ότι συγκρίνει block by block το storage της πρωτεύουσας εικονικής μηχανής σε σχέση με το storage της

κόπιας, αυξάνονται κατακόρυφα οι απαιτήσεις σε υπολογιστική ισχύ του ESXi εξυπηρετητή. Όσο μεγαλύτερο είναι το vmdk αρχείο που θα συγκριθεί με το αντίγραφό του, τόσο περισσότερη υπολογιστική ισχύ απαιτείται. Τελικά καταλήγουμε στο συμπέρασμα ότι καλύτερα να μεταφέρεται όλο το vmdk αρχείο παρά να μεταφέρονται μόνο οι αλλαγές αυτού, αφού στην 2η περίπτωση το cpu overhead είναι σε αποδεκτά επίπεδα ανεξάρτητα από το πόσο μεγάλη είναι μια εικονική μηχανή από θέμα πόρων ή από το λειτουργικό της (windows ή linux). Άλλωστε τέτοιες υποδομές έχουν πρόσβαση στο storage μέσω ικανοποιητικών ταχυτήτων δικτυακών καναλιών.

Όσον αφορά την εγκατάσταση, είναι συμβατό με ESXi 5.x και 6.x και δεν χρειάζεται κάτι λόγω του ότι είναι script. Αρκεί ένας ftp client για να μεταφέρει το script σε κάποιο path του λειτουργικού του ESXi host και στη συνέχεια πρόσβαση μέσω SSH επικοινωνίας στον εξυπηρετητή (εικ. 4.43).

```
/scripts/XSIbackup # ls -la
total 1024
drwxr-xr-x    1 root     root           512 Mar 10 16:13 .
drwxr-xr-x    1 root     root           512 Mar 10 10:24 ..
-rw-r--r--    1 root     root         35147 Mar 10 10:25 LICENSE.txt
-rw-r--r--    1 root     root         13435 Mar 10 10:25 README.txt
-rwx------    1 root     root         44194 Mar 10 10:25 xsibackup
-rwx------    1 root     root        939248 Mar 10 10:25 xsibackup-rsync
/scripts/XSIbackup #
```

Εικόνα 4.43: Εγκατάσταση εργαλείου XSI backup

4.2.4.1 Υποστηριζόμενα χαρακτηριστικά

- Χρησιμοποιεί γραμμή εντολών (CLI) με απόκριση πραγματικού χρόνου.
- Παρέχει προγραμματιζόμενες εργασίες μέσω crontab.
- Δημιουργία αντιγράφων ασφάλειας χωρίς διακοπή υπηρεσιών (hot backups).
- Προληπτικός έλεγχος διεργασίας backup παρακολουθώντας τον ελεύθερο χώρο αποθήκευσης των αντιγράφων ασφαλείας, σβήνοντας τα παλιότερα αντίγραφα.
- Αποστολή λεπτομερών εκθέσεων ανά εικονική μηχανή (ταχύτητα, χώρος προβλέψεων, οι χρόνοι που λαμβάνονται, κλπ ...)
- Υποστηρίζει αντίγραφα ασφάλειας πολλαπλών δίσκων VMDK ανά VM.
- Υποστηρίζει προτεραιοποίηση του backup (οι πιο σημαντικές εικονικές μηχανές δηλώνονται πρώτες στην λίστα).
- Δυνατότητα για scheduled backup μέσω του crontab μηχανισμού του λειτουργικού.

- Δεν υπάρχει περιορισμός στον αριθμό των προγραμματισμένων εργασιών αντιγράφων ασφάλειας (scheduled backup jobs).
- Παρέχεται report με το πέρας του αντιγράφου ασφάλειας σε μορφή email.
- Παρέχεται δυνατότητα ενημέρωσης μέσω email μετά την επιτυχή (ή όχι) ολοκλήρωση του backup.
- Δυνατότητα καταγραφής χρονικής διάρκειας του backup (μέσω του email ενημέρωσης).
- Παρέχεται η δυνατότητα online backup (hot backup).
- Παρέχεται εξαγωγή των αντιγράφων ασφάλειας σε NFS share.
- Δεν επιβαρύνει σημαντικά τους ESXis κατά την διάρκεια της λειτουργίας του, ούτε σε cpu αλλά ούτε και σε memory.
- Υποστηρίζει αντίγραφα ασφάλειας για δίσκους που περιέχουν και raw devices.
- Τα αντίγραφα ασφάλειας μπορεί να είναι είτε thin, είτε thick (eager-zero or zero).
- Είναι supported σε κάθε πλατφόρμα hypervisor η οποία θα τρέχει κάποιο Linux-based environment.
- Υποστήριξη για SCSI και IDE δίσκους
- Υποστηρίζει είτε SCSI είτε IDE δίσκους.
- Υποστηρίζει Raw Device Disk (RDM).

4.2.4.2 Μη υποστηριζόμενα χαρακτηριστικά

- Δεν έχει εύκολη διαχείριση καθότι είναι script και δεν προσφέρει graphical user interface (GUI) αλλά μόνο command-line interface (CLI).
- Δεν υποστηρίζει έλεγχο και επιβεβαίωση του backup (backup verification), παρά μόνον αν γίνει δοκιμαστικό restore.
- Δεν παρέχεται η δυνατότητα για differential, incremental backup ή δυνατότητα data deduplication. Παρέχεται μόνον full backup.
- Δεν παρέχεται η δυνατότητα συνεχούς ενημέρωσης των δεδομένων των αντιγράφων ασφάλειας, (παρά μόνο μέσω της συνεργασίας XSIBackup και Rsync εργαλείου).
- Δεν παρέχεται η δυνατότητα κρυπτογράφησης των αντιγράφων ασφάλειας (backup encryption).

- Δεν παρέχεται δυνατότητα εξαγωγής των αντιγράφων ασφάλειας στο σύννεφο ή σε άλλα μέσα αποθήκευσης (CD-ROM, tapes, NAS, DVD, Blu-Ray, USB drives, FTP servers).
- Δεν παρέχεται δυνατότητα επανάκτησης σε καθορισμένο χρονικό σημείο (point-in-time recovery).
- Δεν παρέχεται η δυνατότητα για επανάκτηση σε επίπεδο αρχείου filesystem, αλλά μόνο ολοκληρωτικής ανάκτησης της εικονικής μηχανής, (εφόσον δεν χρησιμοποιείται το XSIBackup-Rsync).
- Δεν προσφέρει αυτοματοποιημένη διαδικασία recovery, αλλά από το αντίγραφο της εικονικής μηχανής, μπορούμε να επανακτήσουμε το μηχάνημα με σχετική ευκολία. Η εικονική μηχανή πρέπει να κλείσει και στη συνέχεια να προβούμε σε διαδικασία restore με ενέργειες σε επίπεδο ESXi. Δηλαδή θα κάνουμε copy το αντίγραφο ασφάλειας στο path που βρίσκεται το αρχικό, και θα εκιννήσουμε τη μηχανή.
- Δεν παίρνει backup vms που έχουν ήδη snapshots. Υποχρεωτικά πρέπει να σβηστούν τα στιγμιότυπα (snapshots) πριν την εκτέλεση επόμενης εντολής για αντίγραφο ασφάλειας.
- Δεν έχει εύκολη διαχείριση καθότι είναι script και δεν προσφέρει graphical user interface (GUI) αλλά μόνο command-line interface (CLI).
- Δεν υποστηρίζει συμπιεσμένα αντίγραφα ασφάλειας (backup compression).

Κεφάλαιο 5

Αποτελέσματα

Σε αυτό το κεφάλαιο παρουσιάζονται τα χαρακτηριστικά των τεσσάρων εργαλείων και με μια γρήγορη ματιά μπορούμε να διαπιστώσουμε τα πλεονεκτήματα και μειονεκτήματα του καθένα. Στη συνέχεια παρέχονται αναλυτικοί πίνακες με τις μετρήσεις των εργαλείων, των χρόνων που απαιτήθηκαν για την περαίωση των διαδικασιών δημιουργίας αντιγράφου ασφάλειας και επαναφοράς. Τα γραφήματα που έπονται των πινάκων, προσφέρουν μια φιλικότερη οπτική απεικόνιση αυτών των μετρήσεων. Το κεφάλαιο τελειώνει με τα αποτελέσματα που εξάγονται από τις μετρήσεις των εργαλείων και την αναφορά στην εκπλήρωση των στόχων που είχαν τεθεί στο 1ο κεφάλαιο.

5.1 Συγκεντρωτικό γράφημα των χαρακτηριστικών των εργαλείων

Εδώ παρουσιάζεται ένας συγκεντρωτικός πίνακας όλων των χαρακτηριστικών που θα θέλαμε να προσφέρουν τα εργαλεία ανάκαμψης από καταστροφή. Παρουσιάζεται λοιπόν για κάθε χαρακτηριστικό – ευκολία αν προσφέρεται ή όχι από το καθένα από τα τέσσερα εργαλεία.

Requirement	**Recovery Tools**			
	GhettoVCB	VEEAM free ed.	VMware vSp. Repl.	XSI
Δυνατότητα προτεραιοποίησης του backup (ποιο vm θα πάρει 1ο backup και ποιο θα ακολουθήσει).	✓	✓	✓	✓
Δυνατότητα scheduled backup.	✓	✗	✓	✓
Multiple backup jobs can be supported	✓	✓	✓	✓
Δυνατότητα backup verification.	✗	✗	✓	✗
Δυνατότητα παραγωγής report μετά το πέρας του backup.	✓	✓	✓	✓
Δυνατότητα mail notification στη λήψη του backup job, αναφέροντας αν είναι succeeded ή όχι.	✓	✗	✓	✓
Δυνατότητα καταγραφής χρονικής διάρκειας του backup	✓	✓	✓	✓
Δυνατότητα hot backup (χωρίς να πρέπει να κλείσει το vm για να παρθεί backup)	✗	✓	✓	✓
Δυνατότητα differential, incremental backup (εκτός από full backup). —> data deduplication	✗	✗	✓	✗
Δυνατότητα backup εικονικών μηχανών με snapshots	✗	✗	✓	✗

Δυνατότητα backup εικονικών μηχανών τα οποία έχουν RDMs	✗	✗	✗	✓
Δυνατότητα συνεχούς rsync δεδομένων	✗	✗	✓	✓
Δυνατότητα backup encryption	✗	✓	✗	✗
Δυνατότητα backup export to cloud	✗	✓	✓	✗
Δυνατότητα backup export to media tapes	✗	✓	✗	✗
Δυνατότητα backup export to other devices (CD-ROM, NAS, DVD, Blu-Ray, RDX, USB drives, FTP servers)	✗	✗	✗	✗
Backup to nfs share	✓	✓	✓	✓
Δυνατότητα point-in-time recovery	✗	✗	✓	✗
Near-continuous data protection and streamlined disaster recovery	✗	✗	✓	✗
Δυνατότητα file recovery (εκτός από full recovery option)	✗	✓	✗	✗
Low Processor utilization (CPU load)	✓	✓	✓	✓
Δυνατότητα memory quiesce	✓	✓	✓	✓
Easy Recovery and Replication	✗	✓	✓	✗
Support for other systems	✓	✓	✗	✓
User friendly interface	✗	✓	✓	✗

Πίνακας 5.1: Χαρακτηριστικά εργαλείων

5.2 Συγκεντρωτικός πίνακας επιδόσεων

Οι παρακάτω πίνακες προσφέρουν ολοκληρωμένη και σφαιρική άποψη περί των μετρήσεων που έγιναν σε κάθε εργαλείο. Επιλέχθηκαν δύο εικονικές μηχανές. Η μία με λειτουργικό linux (RedHat Enterprise Linux 6 64-bit) και μία με λειτουργικό windows (Window 7 64-bit). Το σκεπτικό επιλογής δύο μηχανών με διαφορετικό λειτουργικό σύστημα έγινε για να υπάρχει σφαιρικότερη εικόνα περί της συμπεριφοράς των εργαλείων, δεδομένου ότι τα δύο λειτουργικά είναι εντελώς διαφορετικά μεταξύ τους. Έχουν διαφορετικό filesystem, διαχειρίζονται εντελώς διαφορετικά τη cpu και τη μνήμη, και ως εκ τούτου θέλαμε να δούμε αν θα διαφέρουν οι τιμές από το ένα σύστημα στο άλλο. Επίσης οι δύο εικονικές μηχανές έχουν πανομοιότυπα τεχνικά χαρακτηριστικά όσον αφορά την επεξεργαστική ισχύ τους (cpu), τη διαθέσιμη μνήμη τους και το μέγεθος του δίσκου τους.

Παρουσιάζεται συγκριτική μελέτη των τεσσάρων εργαλείων σε μετρήσεις που αφορούσαν τη διάρκεια του backup, τη διάρκεια του restore, τον ρυθμό επεξεργασίας δεδομένων και στις δύο φάσεις μετρημένο σαν MB/sec. Σχετικά με τους Hypervisors πάρθηκαν μετρήσεις όσον αφορά την ενδεχόμενη επιβάρυνσή τους είτε σε cpu, είτε σε μνήμη. Με το ίδιο σκεπτικό μετρήθηκαν και οι εικονικές μηχανές για τυχόν επιβάρυνση σε μνήμη και cpu έτσι ώστε να καταγραφεί ενδεχόμενη επιβράδυνση της μηχανής και κατ' επέκταση των υπηρεσιών που φιλοξενεί. Τέλος παρουσιάζονται μετρήσεις για καθυστερήσεις σε επίπεδο storage και επίπεδο δικτύου, κατά τη διάρκεια του backup και του restore.

Οι μετρήσεις παρουσιάζονται ομαδοποιημένες σε τέσσερις πίνακες. Ο πρώτος (πιν. 5.2), αφορά το backup της εικονικής μηχανής η οποία τρέχει linux και ο δεύτερος (πιν. 5.3), αφορά το restore της ίδιας μηχανής. Οι υπόλοιποι δύο πίνακες (πιν 5.4 και 5.5), ακολουθούν την ίδια λογική για τη μηχανή που φιλοξενεί λειτουργικό σύστημα windows.

BACKUP PROCESS (of LINUX MACHINE)				
	GhettoVCB	**VEEAM**	**Vmware vSph. Repl.**	**XSI backup**
Operating System	Linux RedHat	Linux RedHat	Linux RedHat	Linux RedHat
Virtual machine hard disk size	40GB	40GB	40GB	40GB
Backup duration	6:33 minutes	12:06 minutes	21 minutes	2:30 minutes
M.O. processing rate	104,2 MB/s	61 MB/s	32,5 MB/s	273 MB/s
Type of backup	offline	online	online	online
ESXi CPU load overhead (%)	20%	25%	0%	10%
ESXi MEMORY load overhead (%)	0%	0%	0%	0%
ESXi network usage (trasmit/receive rate)	73000 KBps/2000 KBps	70000 KBps/ 70000 KBps	125000 KBps / 10000 KBps	70000 KBps/ 6000 KBps
Datastore latency overhead (read/write)	15 milliseconds/ 20 milliseconds	20millisecond/ 20milliseconds	22milliseconds/ 20milliseconds	2 milliseconds /0,5milliseconds
Virtual machine CPU overhead (%)	0%	0%	0%	0%
Virtual machine MEMORY overhead (%)	0%	0%	39%	0%

Πίνακας 5.2: Επιδόσεις διαδικασίας backup linux μηχανής

RESTORE PROCESS (of LINUX MACHINE)				
	GhettoVCB	**VEEAM**	**Vmware vSph. Repl.**	**XSI backup**
Operating System	Linux RedHat	Linux RedHat	Linux RedHat	Linux RedHat
Virtual machine hard disk size	40GB	40GB	40GB	40GB
Restore duration	9 minutes	5:14 minutes	4 minutes	10 minutes
M.O. processing rate	75,85 MB/s	49 MB/s	170,6 MB/s	68,2 MB/s
Type of restore	offline	offline	offline	offline
ESXi CPU load overhead (%)	6%	65%	47%	6%
ESXi MEMORY load overhead (%)	0%	0%	0%	0%
ESXi network usage (trasmit/receive rate)	1700 KBps/ 1700 KBps	60000 KBps/60000 KBps	125000 KBps / 100000 KBps	1700 KBps/1700 KBps
Datastore latency overhead (read/write)	8 milliseconds/ 12 milliseconds	10millisecond/ 17milliseconds	22milliseconds/ 22milliseconds	8milliseconds/ 12milliseconds
Virtual machine CPU overhead (%)	0%	0%	0%	0%
Virtual machine MEMORY overhead (%)	0%	0%	0%	0%

Πίνακας 5.3: Επιδόσεις διαδικασίας restore linux μηχανής

BACKUP PROCESS (of WINDOWS MACHINE)				
	GhettoVCB	**VEEAM**	**Vmware vSph. Repl.**	**XSI backup**
Operating System	Win7 64-bit	Win7 64-bit	Win7 64-bit	Win7 64-bit
Virtual machine hard disk size	30GB	30GB	30GB	30GB
Backup duration	8:03 minutes	11:55 minutes	19 minutes	6:08 minutes
M.O. processing rate	63,6 MB/s	42,9 MB/s	26,9 MB/s	83,47 MB/s
Type of backup	offline	online	online	online
ESXi CPU load overhead (%)	20%	15%	0%	4%
ESXi MEMORY load overhead (%)	0%	0%	0%	0%
ESXi network usage (trasmit/receive rate)	5000 KBps/ 2000 KBps	47000 KBps/ 2000 KBps	110000 KBps / 7000 KBps	120000 KBps/ 4000 KBps
Datastore latency overhead (read/write)	12milliseconds/ 20milliseconds	20millisecond/ 20milliseconds	22milliseconds/ 20milliseconds	1,5milliseconds /0,5 milliseconds
Virtual machine CPU overhead (%)	0%	0%	0%	0%
Virtual machine MEMORY overhead (%)	0%	20%	25%	0%

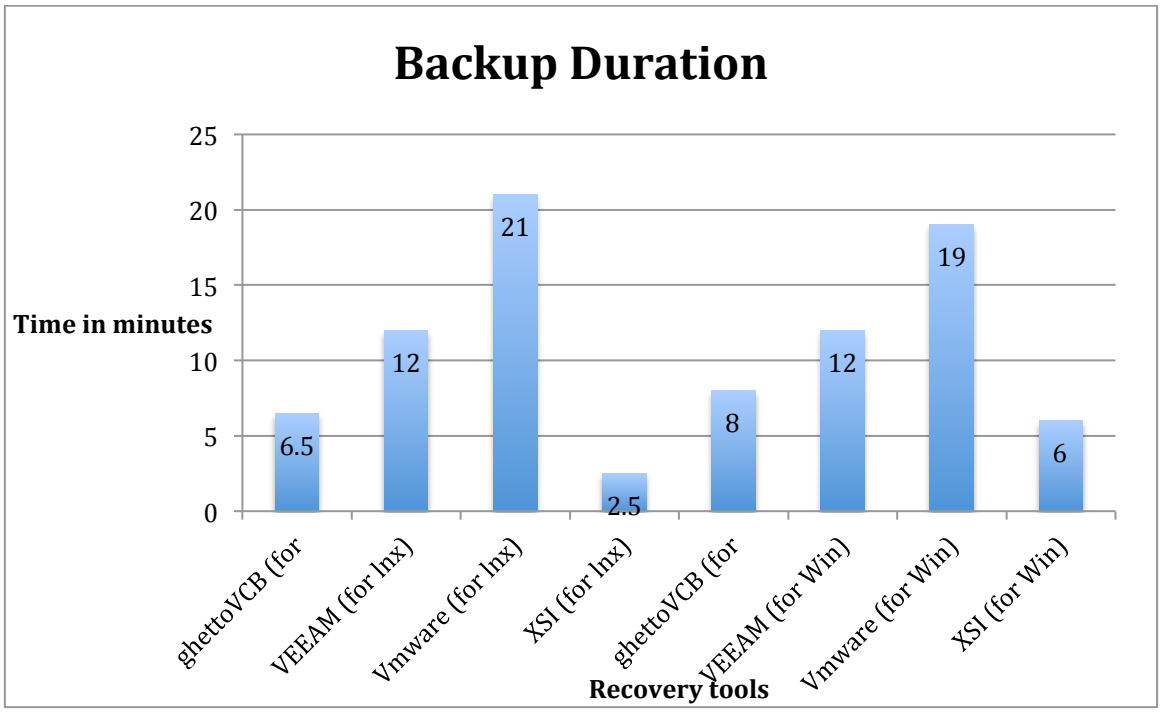
Πίνακας 5.4: Επιδόσεις διαδικασίας backup windows μηχανής

RESTORE PROCESS (of WINDOWS MACHINE)				
	GhettoVCB	**VEEAM**	**Vmware vSph. Repl.**	**XSI backup**
Operating System type	Win7 64-bit	Win7 64-bit	Win7 64-bit	Win7 64-bit
Virtual machine hard disk size	30GB	30GB	30GB	30GB
Restore duration	7 minutes	24:40 minutes	3,5 minutes	8 minutes
M.O. processing rate	73,1 MB/s	22 MB/s	146,2 MB/s	64 MB/s
Type of restore	offline	offline	offline	offline
ESXi CPU load overhead (%)	5%	30%	40%	6%
ESXi MEMORY load overhead (%)	0%	none	0%	0%
ESXi network usage (trasmit/receive rate)	1500 KBps/ 1500 KBps	28000KBps/ 27000KBps	100000 KBps / 100000 KBps	1500 KBps / 1500 KBps
Datastore latency overhead (read/write)	8milliseconds/ 12milliseconds	27milliseconds/ 12milliseconds	21milliseconds/ 22milliseconds	8milliseconds/12 milliseconds
Virtual machine CPU overhead (%)	0%	0%	0%	0%
Virtual machine MEMORY overhead (%)	0%	0%	0%	0%

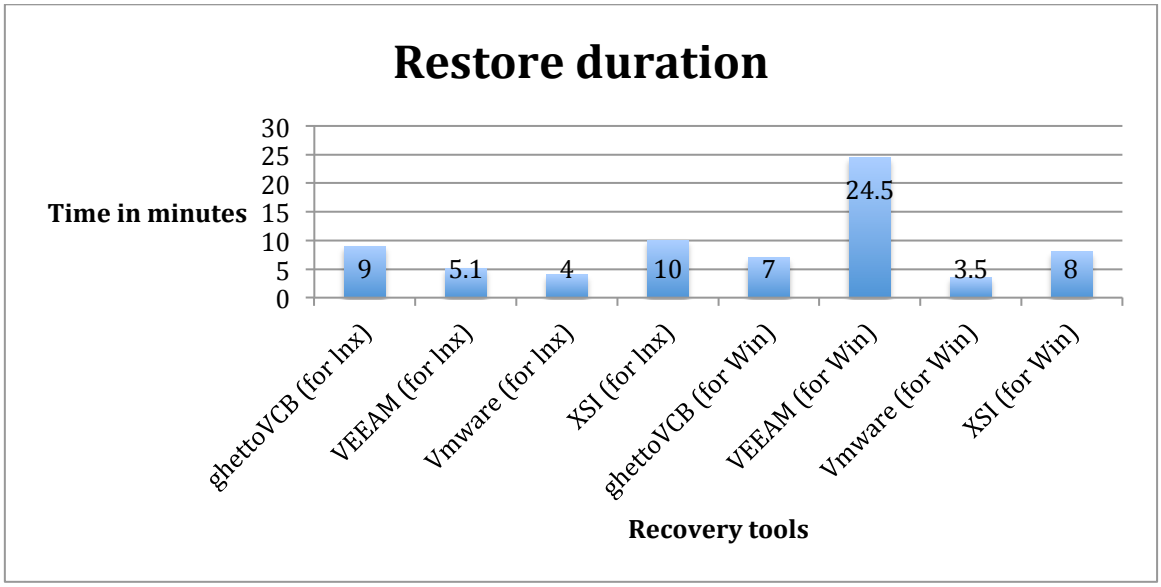
Πίνακας 5.5: Επιδόσεις διαδικασίας restore windows μηχανής

5.3 Συγκεντρωτικά γραφήματα επιδόσεων

Παρακάτω παρουσιάζονται σε γραφικές απεικονίσεις όσα είδαμε στην προηγούμενη ενότητα. Στις εικόνες 5.1 και 5.2 βλέπουμε τον συνολικό χρόνο που απαιτήθηκε για τις διαδικασίες backup και restore και των δύο μηχανών (linux και windows) με κάθε εργαλείο.

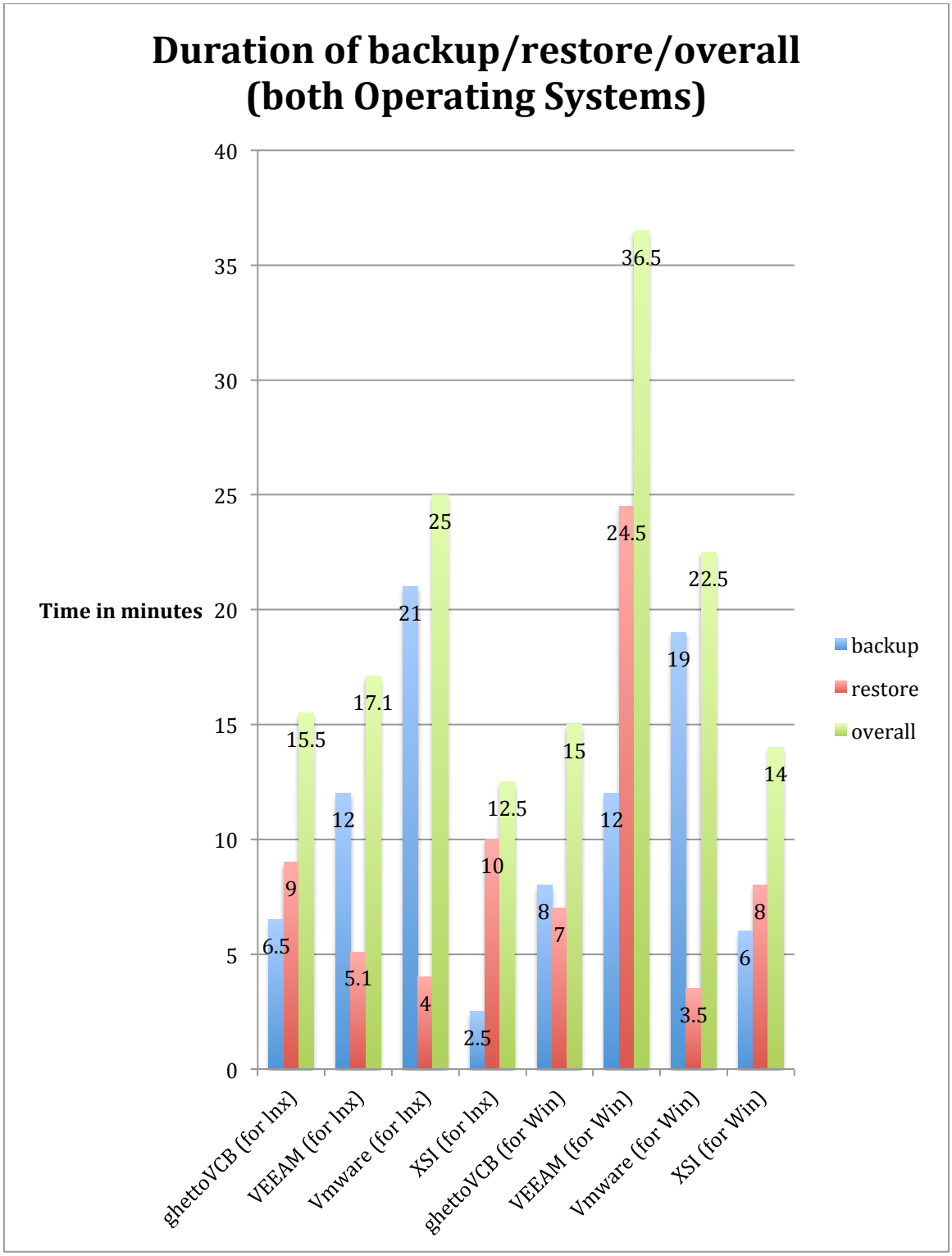


Εικόνα 5.1: Διάρκεια backup κάθε εργαλείου για linux & win OS



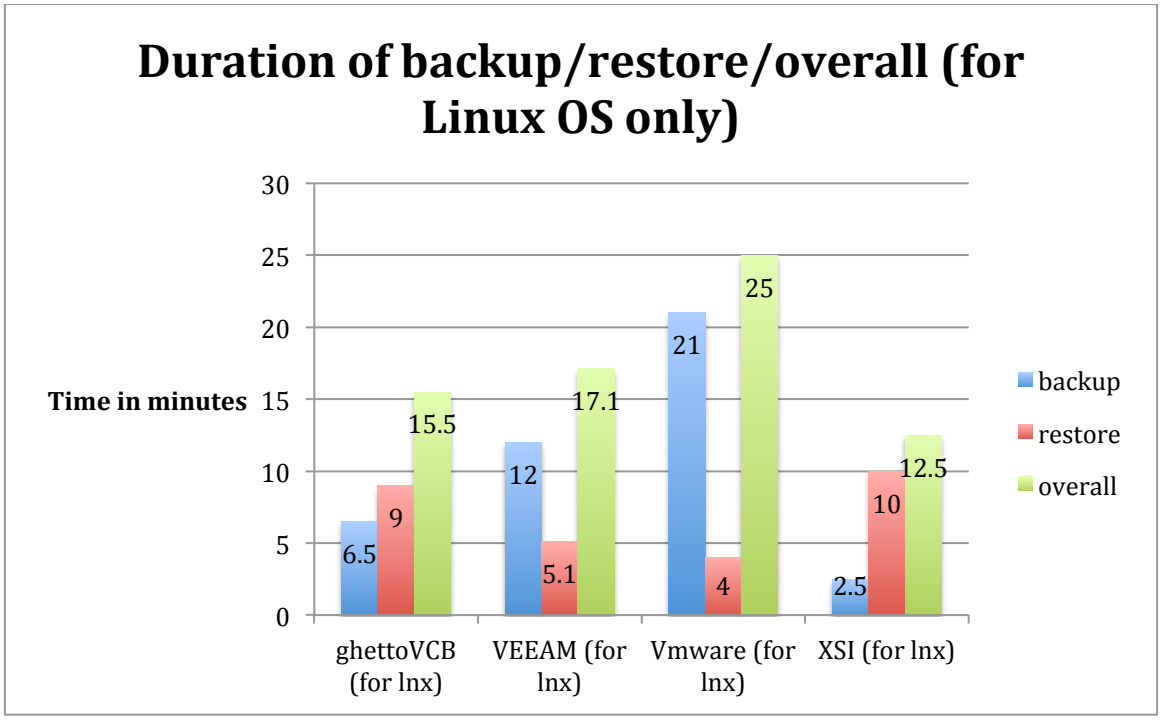
Εικόνα 5.2: Διάρκεια restore κάθε εργαλείου για linux & win OS

Εδώ παρουσιάζεται οι χρόνοι backup, restore, καθώς και το άθροισμα αυτών των χρόνων (εικ. 5.3).

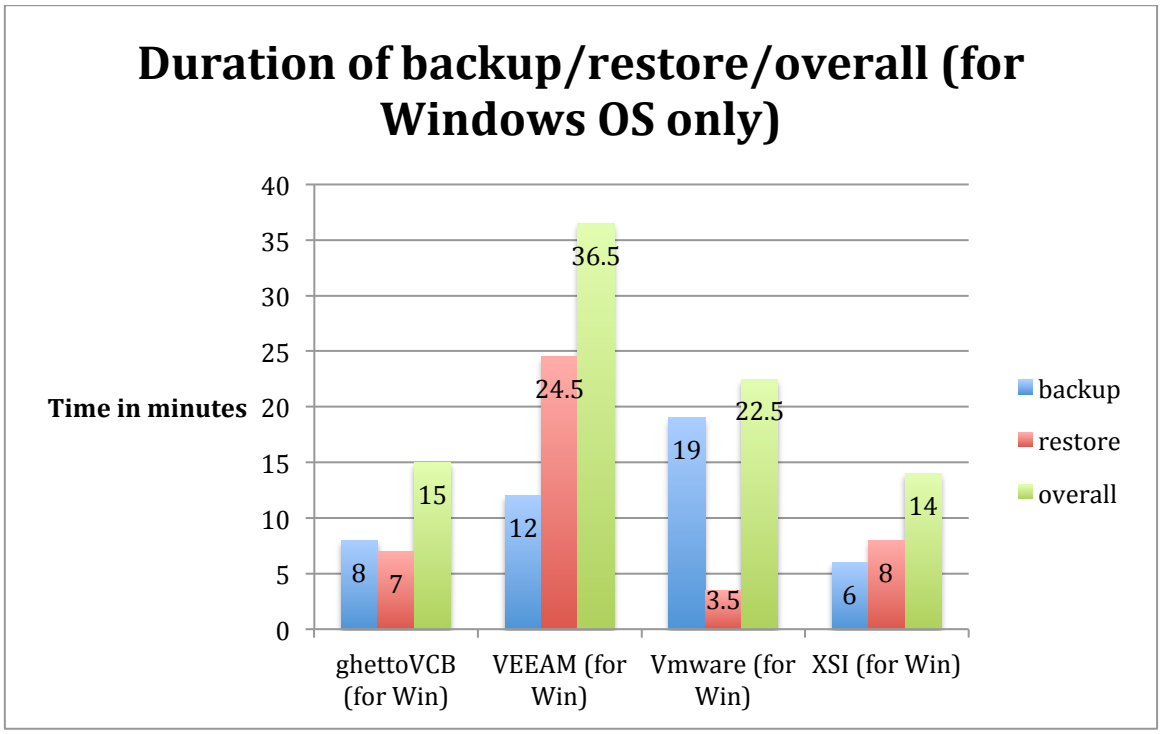


Εικόνα 5.3: Συνολικοί χρόνοι ολοκλήρωσης backup/restore όλων των μηχανών

Οι χρόνοι backup, restore, καθώς και ο συνολικός χρόνος ξεχωριστά για τις linux και τις windows μηχανές αναπαριστάται στις εικόνες 5.4 και 5.5

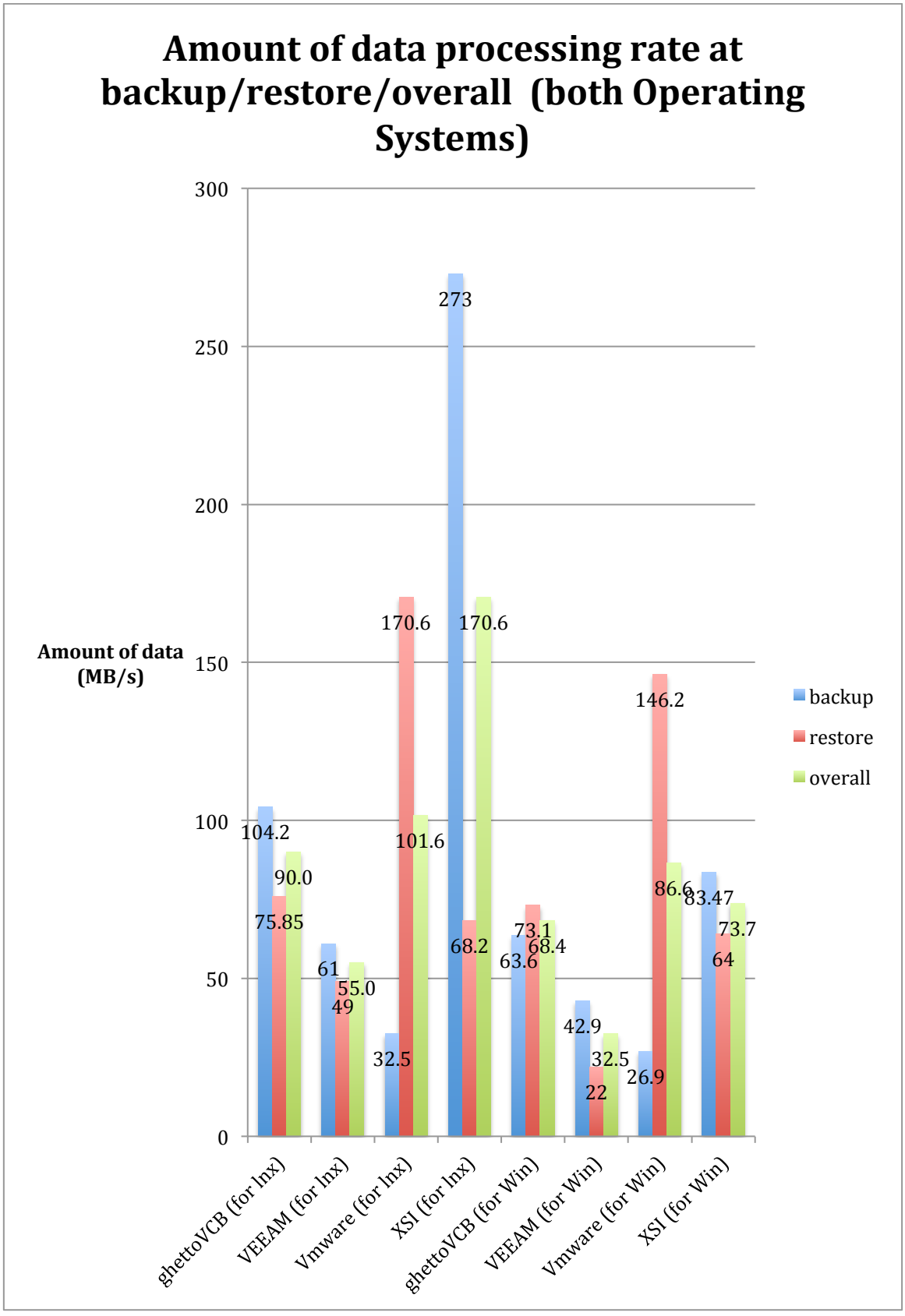


Εικόνα 5.4: Συνολικοί χρόνοι ολοκλήρωσης backup/restore των linux μηχανών



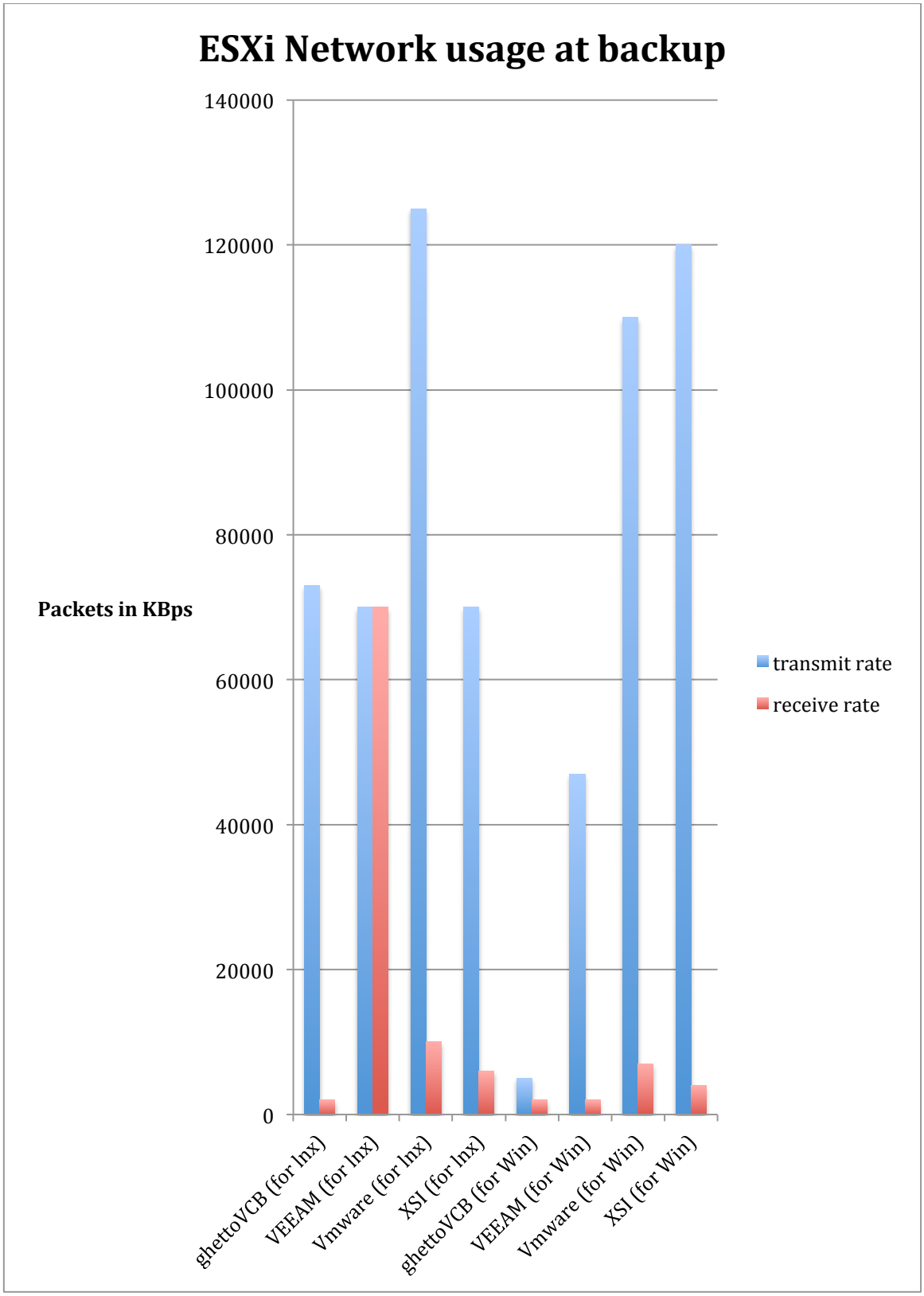
Εικόνα 5.5: Συνολικοί χρόνοι ολοκλήρωσης backup/restore των Windows μηχανών

Η παρακάτω εικόνα (εικ 5.6) δείχνει την ικανότητα του κάθε εργαλείου στο μέγεθος των δεδομένων που μπορούν να επεξεργαστούν σε κάθε φάση (backup ή restore), αλλά και συνολικά.



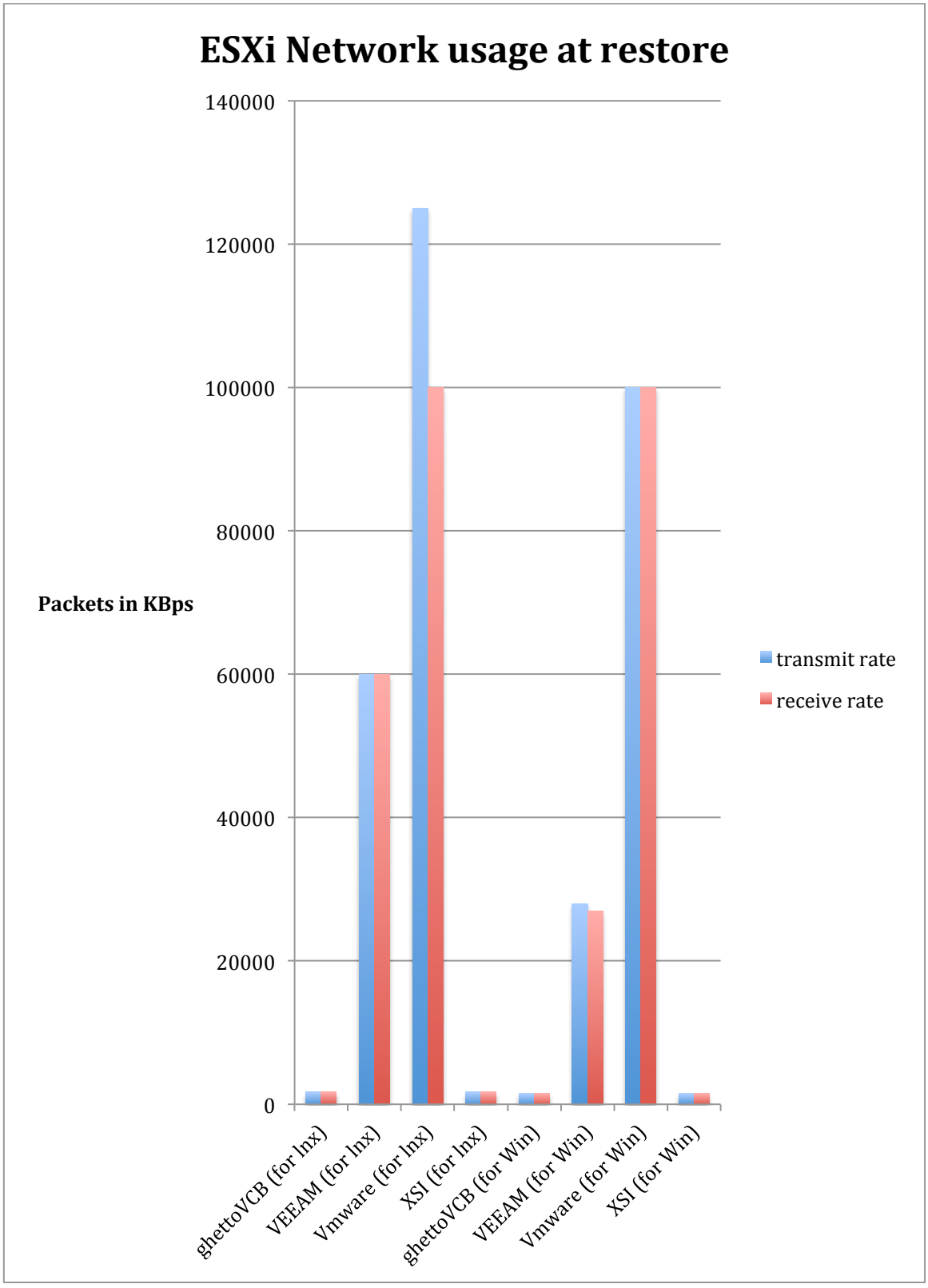
Εικόνα 5.6: Όγκος επεξεργασίας δεδομένων

Ακολουθεί η επιβάρυνση του δικτυακού εξοπλισμού της υποδομής κατά τη διάρκεια του backup (εικ. 5.7).



Εικόνα 5.7: Επιβάρυνση δικτύου για κάθε εργαλείο κατά την διάρκεια του backup

Και η συνολική επιβάρυνση του δικτύου κατά τη διαδικασία του restore (εικ 5.8).



Εικόνα 5.8: Επιβάρυνση δικτύου για κάθε εργαλείο κατά την διάρκεια του restore

5.4 Αποτελέσματα μετρήσεων

Από την μελέτη του πίνακα επιδόσεων των εργαλείων καθώς και από τις γραφικές αναπαραστάσεις των μετρήσεων, εξάγονται μερικά χρήσιμα συμπεράσματα.

1. Όσον αφορά τη διάρκεια που χρειάζεται για να δημιουργηθεί αντίγραφο ασφάλειας παρατηρείται ότι το εργαλείο της VMware χρειάζεται τον περισσότερο χρόνο και από τα τέσσερα εργαλεία, περίπου 20 λεπτά, είτε δημιουργεί αντίγραφο ασφάλειας για linux , είτε για windows εικονική μηχανή. Το πιο γρήγορο εργαλείο σε αυτή την κατηγορία είναι το XSI, με μόλις 4 ¼ λεπτά, γεγονός απόλυτα λογικό και εξηγήσιμο αν αναλογιστούμε ότι το XSI εκτελεί απλή αντιγραφή δεδομένων (file-copy).
2. Κατά τη διάρκεια του restore βλέπουμε ότι το εργαλείο της VMware εκτελεί ταχύτατη αποκατάσταση και στις δύο τύπου μηχανές, με αποτέλεσμα η διαδικασία της ανάκαμψης να κυμαίνεται περίπου στα 4 λεπτά κατά μέσο όρο. Το εργαλείο με τον περισσότερο απαιτούμενο χρόνο ανάκαμψης είναι αυτό της Veeam, κοντά στη μισή ώρα (24 λεπτά). Είναι κατανοητό ότι η διάρκεια της φάσης ανάκαμψης είναι πολύ σημαντικό να είναι όσο το δυνατόν πιο σύντομη, διότι σε εκείνο το σημείο η εταιρία δεν δύναται να λειτουργήσει ομαλά. Μπορεί να μας είναι σχετικά αδιάφορο πόσο χρόνο θα διαρκέσει η δημιουργία ενός αντιγράφου ασφάλειας, αλλά στη διάρκεια της ανάκαμψης στηρίζεται η επιβίωση ενός οργανισμού. Με αυτό το κριτήριο λοιπόν το εργαλείο της VMware αν και χρειάζεται 4πλάσιο χρόνο για να πάρει backup, παρέχει πολύ γρήγορη διαδικασία επαναφοράς.
3. Σχετικά με τον ρυθμό επεξεργασίας δεδομένων κατά τη διαδικασία του backup, το XSI προσφέρει τον μεγαλύτερο ρυθμό, περίπου 270MB ανά δευτερόλεπτο. Σε αυτό το γεγονός οφείλεται αυτό που είπαμε προηγουμένως, ότι δηλαδή δημιουργεί αντίγραφα ασφάλειας σε λιγότερο από 5 λεπτά. Αντίθετα όμως παρουσιάζει μεγάλη κάμψη στο ρυθμό επεξεργασίας δεδομένων κατά τη φάση της ανάκαμψης. Εκεί υπερέχει σαφώς η VMware με 170MB/s στη linux μηχανή και 146MB/s στη μηχανή με windows, και για αυτό έχει ταχύτατο χρόνο ανάκαμψης.
4. Ο γρήγορος χρόνος ανάκαμψης που καταφέρνει το εργαλείο της VMware, φαίνεται και από τις μετρήσεις που αφορούν τη επιβάρυνση του δικτύου κατά της φάση ανάκαμψης. Εκεί η χρήση του δικτύου ξεπερνάει τα 120.000 πακέτα (μετρημένα σε KB/sec), για linux μηχανές, και 100.000 πακέτα για windows μηχανές.
5. Σχετικά με το ποσοστό επιβάρυνσης των hypervisors κατά τη διάρκεια και του backup και του restore δεν παρατηρήθηκε κάποια επιβάρυνση όσον αφορά τη μνήμη. Κανένα εργαλείο δεν έκανε χρήση μνήμης, σε αντίθεση με το cpu όπου τα

τρία από τα τέσσερα εργαλεία κατά τη διάρκεια του backup χρειάστηκαν από 10 έως 25% της επεξεργαστικής ισχύος του hypervisor. Εξαίρεση το εργαλείο Vmware το οποίο δεν έκανε καθόλου χρήση της cpu. Κατά το restore όλα τα εργαλεία χρειάστηκαν υπολογιστική ισχύ, με τα Veeam και VMware να επιβαρύνουν κατά μέσο όρο 50% τους hypervisors ενώ τα Ghetto, XSI αρκέστηκαν στο 10% περίπου.

6. Όσον αφορά το ποσοστό επιβάρυνσης των εικονικών μηχανών κατά τη δημιουργία αντιγράφων ασφάλειας, δεν υπήρξε καμία επιβάρυνση στο cpu, ούτε στις linux, ούτε στις windows μηχανές.
7. Όσον αφορά τα επίπεδα χρήσης μνήμης των εικονικών μηχανών κατά τη διάρκεια και του backup, το VMware επιβαρύνει σημαντικά τη μνήμη της μηχανής, κατά 40% για linux μηχανές και κατά 25% για windows. Οπότε σε τυχόν επιλογή αυτού του εργαλείου θα πρέπει να προβλεφθεί και αντίστοιχη αύξηση της μνήμης των μηχανών που θα διαχειρίζεται. Τα υπόλοιπα εργαλεία δεν έκαναν καθόλου χρήση της μνήμης. Κατα το restore δεν παρατηρήθηκε κάποια επιβάρυνση όσον αφορά τη μνήμη.
8. Εννοείται βεβαίως ότι στη φάση ανάκαμψης δεν εμφανίζονται οι παραπάνω επιβαρύνσεις στις εικονικές μηχανές, λόγου του ότι δεν είναι λειτουργικές μέχρις ότου να ολοκληρωθεί η επαναφορά του αντίγραφου ασφαλείας και να αποκατασταθεί η λειτουργία τους.

Κεφάλαιο 6

Επίλογος

Στο πρώτο κεφάλαιο έγινε μια ιστορική αναδρομή στις πολιτικές επιχειρησιακής συνέχειας και στις διαδικασίες ανάκαμψης από καταστροφή. Επίσης υπήρξε μια σύντομη αναφορά – επεξήγηση στην τεχνολογία των εικονικών υποδομών, και τέθηκαν οι στόχοι της παρούσας διατριβής αναφέροντας και τα σημεία εκείνα τα οποία θεωρούνται καινοτόμα. Στη συνέχεια ακολούθησε στο 2ο κεφάλαιο εμπεριστατωμένη ανάλυση της επιχειρησιακής συνέχειας (Business Continuity), καθώς και τι σημαίνει επί της ουσίας πλάνο ανάκαμψης από καταστροφή (Disaster Recovery Plan). Αναφέρθηκαν πρότυπα οργανισμών σχετικά με disaster recovery, και σχολιάστηκαν εκτενώς DR plans άλλων οργανισμών με αιτιολόγηση των συνηθέστερεων λόγων αποτυχίας ενός πλάνου.
Στο τρίτο κεφάλαιο παρουσιάστηκαν με λεπτομέρεια τα ISO που εφαρμόστηκαν στη διατριβή και επιλέχθηκαν τα σημεία ελέγχου (controls) των ISO τα οποία πληρούν τις ανάγκες του προτεινόμενου disaster recovery plan για τηλεπικοινωνιακούς παρόχους.
Στο τέταρτο κεφάλαιο υλοποιήθηκαν τα σημεία ελέγχου του προτεινόμενου DR plan, παρουσιάστηκαν και δοκιμάστηκαν τέσσερα δωρεάν εργαλεία ανάκαμψης από καταστροφή. Στο πέμπτο κεφάλαιο παρουσιάστηκαν τα χαρακτηριστικά των εργαλείων που δοκιμάστηκαν, ποιες απαιτήσεις ικανοποιούν και ποιες όχι. Επίσης εκπονήθηκε συγκριτική μελέτη των επιδόσεων των εργαλείων και τα αποτελέσματα παρουσιάστηκαν σε πίνακες και γραφικές αναπαραστάσεις.

6.1 Ολοκληρωμένοι στόχοι

Ολοκληρώνοντας τη διατριβή συνοψίζουμε τους στόχους που είχαν τεθεί στο 1ο κεφάλαιο, δηλαδή:

1. Αποδείχθηκε ότι υπάρχει αδήριτη ανάγκη υλοποίησης και εφαρμογής Πλάνου Ανάκαμψης από Καταστροφή.
2. Καθορίστηκαν οι κατάλληλοι έλεγχοι για εικονικά περιβάλλοντα μέσα από μελέτη όχι ενός πλαισίου (framework), αλλά μετά από συνδυασμό τριών διεθνών προτύπων.
3. Με βάση τους προαναφερθέντες ελέγχους, συντάχθηκε Disaster Recovery Plan πλήρως προσαρμοσμένο στις ανάγκες εικονικών υποδομών τηλεπικοινωνιακών παρόχων, με δυνατότητα ανάκτησης δεδομένων σε καθορισμένο χρονικό σημείο του παρελθόντος.
4. Βρέθηκαν και δοκιμάστηκαν δωρεάν εργαλεία τα οποία προσφέρουν αποκατάσταση υπηρεσιών και παρουσιάστηκαν λεπτομερώς πλεονεκτήματα και μειονεκτήματα του καθενός από αυτά.
5. Μέσω των μετρήσεων αυτών των εργαλείων και των αποτελεσμάτων που εξήχθησαν, διαπιστώθηκε ότι η χρήση δωρεάν προϊόντων λογισμικού μπορεί να μειώσει αισθητά τους χρόνους ανάκαμψης των εικονικών συστημάτων.

6.2 Συμπεράσματα – Μελλοντικές επεκτάσεις

Οι προαναφερθέντες παράγοντες είναι μεγάλης σημασίας και στέκονται ως ακλόνητα επιχειρήματα σε όλους όσους όσοι πιστεύουν ότι μπορούν να διαχειριστούν μια καταστροφή χωρίς εκ των προτέρων προετοιμασία. Είναι πλέον αδιαμφισβήτητο το γεγονός ότι η συστηματική προετοιμασία και πρόληψη είναι φθηνότερη και αποτελεσματικότερη από την προσπάθεια ανάκαμψης χωρίς σχέδιο.

Με τη χρήση ενός DRP η εταιρία επιτυγχάνει γρήγορη και όσο το δυνατόν χωρίς περαιτέρω συνέπειες, ανάκτηση των δεδομένων τους μετά από μια καταστροφή. Ένα καλά οργανωμένο πλάνο ανάκαμψης από καταστροφή συμβάλλει έτσι ώστε:

- Να μειωθεί ο κίνδυνος λήψης λανθασμένων αποφάσεων υπό το βάρος του πανικού.
- Όλο το προσωπικό θα είναι ενήμερο εκ των προτέρων για τις ενέργειες που θα πρέπει να εκτελέσει.
- Η εταιρία θα είναι πλήρως προστατευμένη σε κάθε πιθανό κίνδυνο.

Η εταιρία θα παραμείνει λειτουργική και μετά την καταστροφή, ίσως όχι 100% λειτουργική αλλά στο μεγαλύτερο δυνατό βαθμό.

Η παρούσα διατριβή παρουσίασε ένα πλάνο ανάκαμψης από καταστροφή για εικονικές υποδομές βασισμένο στους ελέγχους των ISO 27001, 27301 καιι 22301. Επίσης δοκιμάστηκαν τέσσερα εργαλεία ανάκαμψης με σκοπό να διαπιστωθεί σε ποιους τομείς υπερτερεί το καθένα. Κάθε ενδιαφερόμενος που θα ήθελε να συνεχίσει την έρευνα έχει να διαλέξει από ένα ευρύ φάσμα επιλογών. Θα μπορούσε το προτεινόμενο DR plan να εμπλουτιστεί και με ελέγχους άλλων προτύπων όπως το πρότυπο COBIT. Επίσης συνεχώς εμφανίζονται νέα εργαλεία που προσφέρουν υπηρεσίες ανάκαμψης τα οποία θα πρέπει και αυτά με τη σειρά τους να δοκιμαστούν συγκριτικά με τα προϋπάρχοντα. Μια ακόμα εναλλακτική επιλογή είναι η εφαρμογή του πλάνου στο cloud διότι όπως γίνεται αντιληπτό κερδίζει έδαφος ολοένα και περισσότερο.

6.3 Επίλογος

Η εικονικοποίηση κάνει χρήση ενός φυσικού εξυπηρετητή και φιλοξενεί πολλές εικονικές μηχανές έτσι ώστε πολλοί χρήστες να μπορούν να εκμεταλλεύονται τους ίδιους φυσικούς πόρους χρησιμοποιώντας διαφορετικές και ετερόκλητες εφαρμογές [14]. Αυτό έχει σαν συνέπεια να αυξάνεται η αποδοτικότητα, να μειώνονται τα κόστη των υλικών και να αυξάνεται η επεκτασιμότητα και διαθεσιμότητα των υπηρεσιών. Η τεχνολογίες ανάκαμψης εικονικών υποδομών επιτρέπουν στους οργανισμούς γρήγορη και αποτελεσματική αποκατάσταση των κρίσιμων υπηρεσιών τους, μειώνοντας τους χρόνους διακοπής σε σχέση με παραδοσιακές τοπολογίες Πληροφοριακών Συστημάτων. Επίσης γίνεται πιο εύκολη και η διαδικασία δοκιμών των στρατηγικών και των μεθοδολογιών. Οι συμβατικές λύσεις ανάκαμψης προϋποθέτουν ακριβό και περίπλοκο hardware, οπότε καθίσταται πολύ δύσκολο να ενταχθούν σε ένα πλάνο συστηματικών και επαναλαμβανόμενων δοκιμών. Οι υλοποιήσεις ανάκαμψης χρησιμοποιώντας εικονικές μηχανές προσφέρουν τη δυνατότητα δοκιμών όποτε αυτό είναι επιθυμητό, χωρίς να απαιτείται διακοπή υπηρεσιών.

Βιβλιογραφία

[01] 33hops.com, (2015). *33HOPS ::: Usage of xsibackup-rsync in an ESXi environment.*. [online] Available at: http://33hops.com/blog_xsibackup-rsync-considerations.html [Accessed 7 Apr. 2015].

[02] 33hops.com, (2015). *33HOPS ::: XSIBackup Man Page*. [online] Available at: http://33hops.com/xsibackup-help-man-page.html [Accessed 7 Apr. 2015].

[03] 33hops.com, (2015). *33HOPS ::: XSIbackup, Open Source free backup software for Vmware ESXi 5.1 and above.*. [online] Available at: http://33hops.com/xsibackup-vmware-esxi-backup.html [Accessed 7 Apr. 2015].

[04] Abhilash, G. (2014). Disaster recovery using VMware vSphere replication and vCenter site recovery manager. Birmingham, U.K.: Packt Pub.

[05] Andress, J. (2011). *The basics of information security*. Waltham, MA: Syngress.

[06] Anon, (2015). [online] Available at: http://www.vmware.com/files/pdf/vcb_best_practices.pdf [Accessed 7 Apr. 2015].

[07] Anon, (2015). [online] Available at: http://www.vmware.com/files/pdf/vsphere/VMware-vSphere-Replication-Overview.pdf [Accessed 7 Apr. 2015].

[08] Anon, (2015). 1st ed. [ebook] Available at: http://www.bsigroup.com/Documents/iso-22301/resources/BSI-ISO-22301-Self-Assesment-checklist.pdf [Accessed 29 Apr. 2015].

[09] Anon, (2015). 1st ed. [ebook] Available at: https://www.google.gr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&sqi=2&ved=0CDEQFjAB&url=https%3A%2F%2Fcommunity.spiceworks.com%2Fattachments%2Fpost%2F0008%2F1834%2FDRP-Test-Worksheet.docx&ei=4fNAVZH1B6u07gaVtoGwBg&usg=AFQjCNG5p5-sFv96F7sOnELHhkMNwq-tEw&sig2=d96emX0msy-58OODdWAq6w&bvm=bv.91665533,d.bGg&cad=rja [Accessed 29 Apr. 2015].

[10] Bahan, C. (2003). *The Disaster Recovery Plan*. 1st ed. [ebook] SANS Institute. Available at: http://www.sans.org/reading-room/whitepapers/recovery/disaster-recovery-plan-1164 [Accessed 30 May 2015].

[11] Bright, A. (2010). *Disaster Recovery & Business Continuity Plan for ICT Services*. 1st ed. [ebook] Dartmoor: Dartmoor National Park Authority. Available at: http://www.dartmoor.gov.uk/__data/assets/pdf_file/0006/59127/ICT-Disaster-Recovery-Plan-Rev-0810.pdf [Accessed 26 May 2015].

[12] Communities.vmware.com, (2015). *ghettoVCB.sh - Free alternative for backing up ... | VMware Communities*. [online] Available at: https://communities.vmware.com/docs/DOC-8760 [Accessed 7 Apr. 2015].

[13] Crouhy, M., Galai, D. and Mark, R. (2006). *The essentials of risk management*. New York: McGraw-Hill.

[14] EC-Council, (2011). *Disaster Recovery by EC-Council.pdf*. 1st ed. [ebook] NY, USA: Sengage Learning. Available at: http://www.ourebook.org/technical-list/disaster-recovery-by-ec-council_1t72e.html [Accessed 21 May 2015].

[15] Gibson, D. (2011). *Managing risk in information systems*. Sudbury, Mass.: Jones & Bartlett Learning.

[16] Goh, M. (2013). Dictionary of Business Continuity and Disaster Recovery. 4th ed. BCM Institute.

[17] Goldberg, R. (1974). Survey of virtual machine research. *Computer*, 7(6), pp.34-45.

[18] Golden, C. and Oblinger, D. (2007). The Myth about Business Continuity and Disaster Recovery. *EDUCAUSE*, [online] vol. 42(no. 3). Available at: http://www.educause.edu/ero/article/myth-about-business-continuity-and-disaster-recovery [Accessed 10 Oct. 2014].

[19] Harkins, M. (2013). *Managing risk and information security*. [New York]: Apress.

[20] International Data Corporation (IDC), (2002). *Worldwide Information Security Services Forecast 2001-2006*. IDC report no. 26899. IDC.

[21] Isaca.org, (2014). *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*. [online] Available at: http://www.isaca.org/cobit/pages/default.aspx [Accessed 7 Jun. 2015].

[22] Iso.org, (2000). *ISO/IEC 17799:2000 - Information technology -- Code of practice for information security management*. [online] Available at: http://www.iso.org/iso/catalogue_detail.htm?csnumber=33441 [Accessed 7 Jun. 2015].

[23] ISO/IEC 22301:2012 "Societal security — Business continuity management systems — Requirements". (2012). 1st ed. [ebook] Geneva: International Organization for Standardization. Available at: http://www.iso.org/iso/catalogue_detail?csnumber=50038 [Accessed 29 Oct. 2014].

[24] ISO/IEC 27001:2005 "Information technology – Security techniques – Information security management systems – Requirements". (2005). 1st ed. [ebook] Geneva: International Organization for Standardization. Available at: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=42103 [Accessed 22 Oct. 2014].

[25] ISO/IEC 27031:2011 "Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity". (2011). 1st ed. [ebook] Geneva: International Organization for Standardization. Available at: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44374 [Accessed 11 Nov. 2014].

[26] Jaquith, A. (2007). *Security metrics*. Upper Saddle River, NJ: Addison-Wesley.

[27] Lam, W. (2002). Ensuring business continuity. *IT Prof.*, 4(3), pp.19-25.

[28] Mohn, C. (2014). Learning Veeam backup & replication for VMware vShpere. Birmingham, U.K.: Packt Pub.

[29] Morgan Doyle, (2014). *ICT Business Continuity & Disaster Recovery for Local Authorities White Paper*. [online] Available at: http://www.morgandoyle.co.uk/white-papers/drbc.pdf [Accessed 26 May 2015].

[30] Nine principles of a Risk Intelligent Framework for Risk Management. (2015). .

[31] Quarterman, J. (2006). Risk management solutions for Sarbanes-Oxley section 404 IT compliance. Indianapolis, Ind.: Wiley Pub.

[32] Radicke, J., Rodén, B. and Yunke, L. (2009). *Exploring Views on Data Centre Power Consumption and Server Virtualization*. Postgraduate. Lund University.

[33] Rao, U. and Nayak, U. (2014). *The InfoSec handbook*. New York, U.S.A.: Appress Media.

[34] Raval, V. and Fichadia, A. (2007). *Risks, controls, and security*. Hoboken, NJ: Wiley.

[35] Riley, A., Pomales Palmer, J. and Samuel, J. (2014). *ITIL - ITIL*. [online] Itlibrary.org. Available at: http://www.itlibrary.org/index.php?page=ITIL [Accessed 7 Jun. 2015].

[36] Sites.utoronto.ca, (2011). *CSA - Disaster Recovery Planning*. [online] Available at: http://sites.utoronto.ca/security/documentation/business_continuity/dis_rec_plan.htm [Accessed 26 May 2015].

[37] Smith, J. and Ravi Nair, (2005). The architecture of virtual machines. *Computer*, 38(5), pp.32-38.

[38] Stoneburner, G., Goguen, A. and Feringa, A. (2002). *Risk management guide for information technology systems*. Gaithersburg, Md.: U.S. Dept. of Commerce, National Institute of Standards and Technology.

[39] Sugerman, S., Venkitachalam, G. and Lim, B. (2001). Virtualizing I/O Devices on VMware Workstation's Hosted Virtual Machine Monitor.

[40] U.S Department of Commerce, National Institute of Standards and Technology, (2006). *Guide for Developing Security Plans for Federal Information Systems, Special Publication 800-18*. National Institute of Standards and Technology.

[41] VMs, (2015). *Free Backup Software for VMware ESXi VMs*. [online] SourceForge. Available at: http://sourceforge.net/projects/xsibackup/ [Accessed 7 Apr. 2015].

[42] Wikipedia, (2005). *Information system*. [online] Available at: http://en.wikipedia.org/wiki/Information_system [Accessed 8 Nov. 2014].

[43] Woodruffe, D. (2014). *ICT Disaster Recovery and Business Continuity Plan*. [online] East London NHS Foundation Trust. Available at: http://www.eastlondon.nhs.uk/About-Us/Freedom-of-Information/Trust-Policies-and-Procedure/Risk-Management-Policies/ICT-Disaster-Recovery-Plan.pdf [Accessed 26 May 2015].

[44] Workman, M., Phelps, D. and Gathegi, J. (2013). *Information security for managers*. Burlington, MA: Jones & Bartlett Learning.

[45] Wright, J. and Katan, A. (2004). High Availability: A Perspective. *Gartner Research*, ID Number: DPRO-90193.

Παράρτημα Α
Γλωσσάριο και συντομογραφίες

acceptance (αποδοχή)

Επίσημη συμφωνία ότι μια υπηρεσία, μια διεργασία, ένα σχέδιο ή κάποιο άλλο παραδοτέο πληροφορικής και τηλεπικοινωνιών είναι πλήρες, ακριβές, αξιόπιστο και πληροί τις προδιαγραφές. Η αποδοχή συνήθως έπεται της αξιολόγησης ή δοκιμής των αλλαγών και συχνά αποτελεί προϋπόθεση για τη μετάβαση στο επόμενο στάδιο ενός έργου ή μιας διεργασίας. *Βλέπε επίσης* κριτήρια αποδοχής υπηρεσίας.

Alert (προειδοποίηση)

Ειδοποίηση ότι προσεγγίστηκε ένα όριο, ότι υπήρξε μια αλλαγή ή ότι σημειώθηκε αστοχία. Η δημιουργία και διαχείριση των προειδοποιήσεων γίνεται συχνά από εργαλεία διαχείρισης συστήματος. Η διαχείρισή τους γίνεται στο πλαίσιο της διεργασίας διαχείρισης γεγονότων.

Application Εφαρμογή

Λογισμικό που παρέχει λειτουργίες που απαιτούνται για μια υπηρεσία πληροφορικής και τηλεπικοινωνιών. Κάθε εφαρμογή μπορεί να είναι τμήμα περισσότερων από μίας υπηρεσιών πληροφορικής και τηλεπικοινωνιών. Μια εφαρμογή εκτελείται σε έναν ή

περισσότερους διακομιστές ή πελάτες. *Βλέπε επίσης* διαχείριση εφαρμογών, χαρτοφυλάκιο εφαρμογών.

assessment (αξιολόγηση)

Επιθεώρηση και ανάλυση για να διαπιστωθεί εάν ένα πρότυπο ή μια δέσμη κατευθυντήριων γραμμών τηρείται, εάν τα τηρούμενα αρχεία είναι ακριβή ή εάν οι στόχοι αποδοτικότητας και αποτελεσματικότητας επιτυγχάνονται. *Βλέπε επίσης* έλεγχος.

asset (περιουσιακό στοιχείο)

Κάθε διαθέσιμος πόρος ή/και δυνατότητα. Τα περιουσιακά στοιχεία ενός παρόχου υπηρεσιών περιλαμβάνουν οτιδήποτε μπορεί να συμβάλλει στην παροχή μιας υπηρεσίας. Τα περιουσιακά στοιχεία μπορεί να έχουν κάποια από τις ακόλουθες μορφές: διαχείριση, οργάνωση, διεργασία, γνώση, ανθρώπινοι πόροι, πληροφορίες, εφαρμογές, υποδομές ή χρηματοοικονομικό κεφάλαιο. *Βλέπε επίσης* περιουσιακό στοιχείο πελάτη, περιουσιακό στοιχείο υπηρεσίας, στρατηγικό περιουσιακό στοιχείο.

asset management (διαχείριση περιουσιακών στοιχείων)

Γενική δραστηριότητα ή διεργασία που είναι υπεύθυνη για την παρακολούθηση και την παροχή πληροφόρησης σχετικά με την αξία και την κυριότητα των περιουσιακών στοιχείων κατά τη διάρκεια ολόκληρου του κύκλου ζωής τους. *Βλέπε επίσης* διαχείριση και διαμόρφωση περιουσιακών στοιχείων υπηρεσιών, διαχείριση πάγιων περιουσιακών στοιχείων, διαχείριση λογισμικού.

audit (έλεγχος)

Επίσημη επιθεώρηση και επαλήθευση για να διαπιστωθεί εάν ένα πρότυπο ή μια δέσμη κατευθυντήριων γραμμών τηρείται, εάν τα τηρούμενα αρχεία είναι ακριβή ή εάν οι στόχοι αποδοτικότητας και αποτελεσματικότητας επιτυγχάνονται. Έλεγχοι διενεργούνται από εσωτερικές ή εξωτερικές ομάδες. *Βλέπε επίσης* αξιολόγηση, πιστοποίηση.

availability (διαθεσιμότητα)

Η δυνατότητα μιας υπηρεσίας πληροφορικής και τηλεπικοινωνιών ή άλλου στοιχείου διαμόρφωσης να επιτελέσει τη συμφωνημένη λειτουργία της/του όταν ζητείται. Η

διαθεσιμότητα καθορίζεται με βάση την αξιοπιστία, τη συντηρησιμότητα, τη δυνατότητα τεχνικής υποστήριξης, την απόδοση και την ασφάλεια. Η διαθεσιμότητα υπολογίζεται συνήθως ως ποσοστό. Ο υπολογισμός αυτός γίνεται συχνά βάσει του συμφωνημένου χρόνου παροχής υπηρεσίας και του χρόνου διακοπής λειτουργίας. Η βέλτιστη πρακτική είναι να υπολογίζεται η διαθεσιμότητα μιας υπηρεσίας πληροφορικής και τηλεπικοινωνιών χρησιμοποιώντας μετρήσεις των παραγόμενων αποτελεσμάτων της επιχειρηματικής δραστηριότητας.

backup (δημιουργία αντιγράφων ασφαλείας)
Αντιγραφή δεδομένων για προστασία από ενδεχόμενη απώλεια της ακεραιότητας ή της διαθεσιμότητας των αρχικών δεδομένων.

Billing (χρέωση)
Μέρος της διεργασίας χρέωσης. Πρόκειται για τη δραστηριότητα που είναι υπεύθυνη για την έκδοση ενός τιμολογίου ή ενός λογαριασμού και την είσπραξη των χρημάτων από τους πελάτες. *Βλέπε επίσης* τιμολόγηση.

budget (προϋπολογισμός)
Κατάλογος όλων των χρηματικών ποσών που ένας οργανισμός ή μια επιχειρησιακή μονάδα προγραμματίζει ότι θα εισρεύσουν και θα εκρεύσουν σε μια δεδομένη χρονική περίοδο. *Βλέπε επίσης* σύνταξη και παρακολούθηση προϋπολογισμών, σχεδιασμός.

business (Επιχειρηματικός (-ή)(-ό) / Επιχείρηση)

Εταιρική οντότητα ή οργανισμός που αποτελείται από ένα σύνολο επιχειρησιακών μονάδων. Στο πλαίσιο της διαχείρισης υπηρεσιών πληροφορικής και τηλεπικοινωνιών, ο όρος περιλαμβάνει τόσο τους οργανισμούς του δημόσιου τομέα και τους μη κερδοσκοπικούς οργανισμούς όσο και τις ιδιωτικές εταιρείες. Ένας πάροχος υπηρεσιών πληροφορικής και τηλεπικοινωνιών παρέχει υπηρεσίες πληροφορικής και τηλεπικοινωνιών σε έναν πελάτη που ανήκει σε μια επιχείρηση. Ο πάροχος υπηρεσιών πληροφορικής και τηλεπικοινωνιών μπορεί να ανήκει στην ίδια επιχείρηση με τον πελάτη του (εσωτερικός πάροχος υπηρεσιών) ή να ανήκει σε άλλη επιχείρηση (εξωτερικός πάροχος υπηρεσιών).

business continuity management (BCM) (διαχείριση επιχειρησιακής συνέχειας

(BCM))

Η επιχειρησιακή διεργασία που είναι υπεύθυνη για τη διασφάλιση της επιχειρηματικής συνέχειας μέσω της διαχείρισης των κινδύνων που μπορούν να επηρεάσουν σημαντικά την επιχείρηση. Η διαχείριση επιχειρησιακής συνέχειας προασπίζει τα συμφέροντα των βασικών ενδιαφερομένων, τη φήμη και το όνομα της επιχείρησης και τις δραστηριότητες που παράγουν αξία. Η διεργασία περιλαμβάνει τον περιορισμό των κινδύνων σε αποδεκτά επίπεδα και τον κατάλληλο σχεδιασμό για την ανάκαμψη των επιχειρησιακών διεργασιών σε περίπτωση διατάραξης της ομαλής λειτουργίας της επιχείρησης. Στο πλαίσιο της διαχείρισης επιχειρησιακής συνέχειας τίθενται οι στόχοι, το πεδίο εφαρμογής και οι απαιτήσεις για τη διαχείριση της συνέχειας των υπηρεσιών πληροφορικής και τηλεπικοινωνιών.

business continuity plan (BCP) (σχέδιο επιχειρησιακής συνέχειας (BCP))

Σχέδιο που καθορίζει τις ενέργειες που απαιτούνται για την αποκατάσταση των επιχειρησιακών διεργασιών μετά τη διατάραξη της ομαλής λειτουργίας τους. Στο σχέδιο προσδιορίζονται επίσης οι μηχανισμοί ενεργοποίησης, τα πρόσωπα που θα κινητοποιηθούν, οι επικοινωνίες κ.λπ. Τα σχέδια συνέχειας υπηρεσιών πληροφορικής και τηλεπικοινωνιών αποτελούν σημαντικές συνιστώσες ευρύτερων σχεδίων επιχειρησιακής συνέχειας.

business impact analysis (BIA) (ανάλυση επιχειρηματικού αντίκτυπου (BIA))

Ανάλυση επιχειρηματικού αντίκτυπου είναι η δραστηριότητα στο πλαίσιο της διαχείρισης επιχειρησιακής συνέχειας μέσω της οποίας προσδιορίζονται οι ζωτικές επιχειρηματικές λειτουργίες και οι εξαρτήσεις τους. Σε αυτές τις εξαρτήσεις συγκαταλέγονται προμηθευτές, ανθρώπινοι πόροι, άλλες επιχειρησιακές διεργασίες, υπηρεσίες πληροφορικής και τηλεπικοινωνιών κ.λπ. Η ανάλυση επιχειρηματικού αντίκτυπου προσδιορίζει τις απαιτήσεις ανάκαμψης σε σχέση με τις υπηρεσίες πληροφορικής και τηλεπικοινωνιών. Οι απαιτήσεις αυτές συμπεριλαμβάνουν στόχους χρόνου ανάκαμψης, στόχους σημείου ανάκαμψης και στόχους ελάχιστου επιπέδου υπηρεσιών για κάθε υπηρεσία πληροφορικής και τηλεπικοινωνιών.

capacity (δυναμικότητα)

Η μέγιστη διεκπεραιωτική ικανότητα ενός στοιχείου διαμόρφωσης ή μιας υπηρεσίας

πληροφορικής και τηλεπικοινωνιών. Για ορισμένους τύπους στοιχείων διαμόρφωσης, π.χ. για μια μονάδα δίσκου, η δυναμικότητα μπορεί να αφορά μέγεθος ή χωρητικότητα.

capacity management (διαχείριση δυναμικότητας)
Διεργασία που αναλαμβάνει να διασφαλίζει ότι η δυναμικότητα των υπηρεσιών πληροφορικής και τηλεπικοινωνιών και των υποδομών πληροφορικής και τηλεπικοινωνιών είναι σε θέση να ανταποκρίνεται στις συμφωνημένες απαιτήσεις δυναμικότητας και απόδοσης κατά οικονομικά αποτελεσματικό και έγκαιρο τρόπο. Στο πλαίσιο της διαχείρισης δυναμικότητας εξετάζονται όλοι οι πόροι που απαιτούνται για την παροχή μιας υπηρεσίας πληροφορικής και τηλεπικοινωνιών και λαμβάνεται μέριμνα για την κάλυψη τόσο των υφιστάμενων όσο και των μελλοντικών αναγκών της επιχείρησης σε επίπεδο δυναμικότητας και απόδοσης. Η διαχείριση δυναμικότητας περιλαμβάνει τρεις επιμέρους διεργασίες: τη διαχείριση επιχειρηματικής δυναμικότητας, τη διαχείριση δυναμικότητας υπηρεσιών και τη διαχείριση δυναμικότητας συστατικών στοιχείων. *Βλέπε επίσης* πληροφοριακό σύστημα διαχείρισης δυναμικότητας.

compliance (συμμόρφωση)
Η διασφάλιση ότι τηρείται ένα πρότυπο ή ένα σύνολο κατευθυντήριων γραμμών, ή ότι εφαρμόζονται συνεπείς λογιστικές ή άλλες πρακτικές.

component (συστατικό στοιχείο)
Περιληπτικός όρος που αναφέρεται σε μία συνιστώσα ενός πιο σύνθετου πράγματος. Για παράδειγμα, ένα σύστημα Η/Υ μπορεί να αποτελεί συστατικό στοιχείο μιας υπηρεσίας πληροφορικής και τηλεπικοινωνιών και μια εφαρμογή μπορεί να αποτελεί συστατικό στοιχείο μιας μονάδας ενημερωμένης έκδοσης. Τα συστατικά στοιχεία που χρήζουν διαχείρισης πρέπει να λογίζονται ως στοιχεία διαμόρφωσης.

confidentiality (εμπιστευτικότητα)
Αρχή της ασφάλειας που ορίζει ότι πρόσβαση σε δεδομένα πρέπει να έχουν μόνο τα εξουσιοδοτημένα άτομα.

dependency (εξάρτηση)
Όταν μια διεργασία ή δραστηριότητα βασίζεται άμεσα ή έμμεσα σε κάποια άλλη.

document (έγγραφο)

Πληροφορίες σε αναγνώσιμη μορφή. Ένα έγγραφο μπορεί να έχει έντυπη ή ηλεκτρονική μορφή – για παράδειγμα, ένα έγγραφο πολιτικής, μια συμφωνία επιπέδου υπηρεσιών, ένα αρχείο συμβάντος ή ένα διάγραμμα με τη διαρρύθμιση ενός computer room.

downtime (χρόνος εκτός λειτουργίας)

Ο χρόνος κατά τον οποίο μια υπηρεσία πληροφορικής και τηλεπικοινωνιών ή κάποιο άλλο στοιχείο διαμόρφωσης δεν είναι διαθέσιμο κατά τη διάρκεια του συμφωνημένου χρόνου παροχής υπηρεσίας. Η διαθεσιμότητα μιας υπηρεσίας πληροφορικής και τηλεπικοινωνιών υπολογίζεται συχνά βάσει του συμφωνημένου χρόνου παροχής υπηρεσίας και του χρόνου εκτος λειτουργίας.

efficiency (αποδοτικότητα)

Μέτρο του κατά πόσο έχει γίνει χρήση της βέλτιστης ποσότητας των πόρων για την παροχή μιας διεργασίας, υπηρεσίας ή δραστηριότητας. Μια αποδοτική διεργασία επιτυγχάνει τους στόχους της με την ελάχιστη ανάλωση χρόνου, χρήματος, ανθρώπινων ή άλλων πόρων. *Βλέπε επίσης* βασικός δείκτης απόδοσης.

estimation (εκτίμηση)

Πρόχειρος υπολογισμός μιας κατά προσέγγιση τιμής για ένα δείκτη μέτρησης ή ένα κόστος βάσει πείρας. Χρησιμοποιείται επίσης στο πλαίσιο της διαχείρισης δυναμικότητας και διαθεσιμότητας ως η φθηνότερη και λιγότερο ακριβής μέθοδος μοντελοποίησης.

event (γεγονός)

Αλλαγή κατάστασης που έχει σημασία για τη διαχείριση μιας υπηρεσίας πληροφορικής και τηλεπικοινωνιών ή κάποιου άλλου στοιχείου διαμόρφωσης. Ο όρος αναφέρεται επίσης στην προειδοποίηση ή την ειδοποίηση που δημιουργείται από μια υπηρεσία πληροφορικής και τηλεπικοινωνιών, ένα στοιχείο διαμόρφωσης ή ένα εργαλείο παρακολούθησης. Η επέλευση ενός γεγονότος συνήθως απαιτεί την πραγματοποίηση κάποιας ενέργειας από το προσωπικό λειτουργιών πληροφορικής και τηλεπικοινωνιών και συχνά έχει ως αποτέλεσμα την καταγραφή του σχετικού συμβάντος.

facilities management (διαχείριση εγκαταστάσεων)

Η λειτουργία που είναι υπεύθυνη για τη διαχείριση του φυσικού περιβάλλοντος όπου βρίσκονται οι υποδομές πληροφορικής και τηλεπικοινωνιών. Η διαχείριση εγκαταστάσεων περιλαμβάνει όλες τις πτυχές της διαχείρισης του φυσικού περιβάλλοντος, όπως για παράδειγμα την ηλεκτροδότηση και τον κλιματισμό, τη διαχείριση της πρόσβασης στις κτιριακές εγκαταστάσεις και την παρακολούθηση των περιβαλλοντικών συνθηκών.

failure (αστοχία)

Απώλεια της ικανότητας λειτουργίας σύμφωνα με τις προδιαγραφές ή επίτευξης των προβλεπόμενων αποτελεσμάτων. Ο όρος χρησιμοποιείται σε σχέση με υπηρεσίες πληροφορικής και τηλεπικοινωνιών, διεργασίες, δραστηριότητες, στοιχεία διαμόρφωσης κ.λπ. Οι αστοχίες συχνά προκαλούν συμβάντα.

high availability (υψηλή διαθεσιμότητα)

Προσέγγιση ή σχεδιασμός που ελαχιστοποιεί ή αποκρύπτει τις επιπτώσεις της αστοχίας ενός στοιχείου διαμόρφωσης για τους χρήστες μιας υπηρεσίας πληροφορικής και τηλεπικοινωνιών. Οι λύσεις υψηλής διαθεσιμότητας είναι σχεδιασμένες να εξασφαλίζουν το συμφωνημένο επίπεδο διαθεσιμότητας και να κάνουν χρήση τεχνικών όπως η ανοχή σε σφάλματα / βλάβες, η ανθεκτικότητα και η ταχεία ανάκαμψη για τη μείωση του αριθμού και του αντίκτυπου των συμβάντων.

hot standby (υψηλή ετοιμότητα)

Βλέπε immediate recovery (άμεση ανάκαμψη)

immediate recovery (άμεση ανάκαμψη)

Εναλλακτική επιλογή ανάκαμψης που είναι γνωστή και ως υψηλή ετοιμότητα (hot standby). Στο πλαίσιο αυτής λαμβάνονται τα κατάλληλα μέτρα για την ανάκαμψη της υπηρεσίας πληροφορικής και τηλεπικοινωνιών, χωρίς σημαντική απώλεια υπηρεσίας για τον πελάτη. Για την άμεση ανάκαμψη κατά κανόνα γίνεται χρήση τεχνολογιών κατοπτρισμού (mirroring), ίσου καταμερισμού φορτίου (load balancing) και διαχωρισμού σε διαφορετικές φυσικές τοποθεσίες (split-site).

impact (αντίκτυπος / επίπτωση)

Μέτρο της επίδρασης ενός συμβάντος, ενός προβλήματος ή μιας αλλαγής στις επιχειρησιακές και επιχειρηματικές διεργασίες. Συχνά βασίζεται στο πώς θα

επηρεαστεί το επίπεδο υπηρεσιών. Η επίπτωση και η επιτακτικότητα χρησιμοποιούνται για την ιεράρχηση προτεραιοτήτων.

incident (συμβάν)

Μη προγραμματισμένη διακοπή λειτουργίας μιας υπηρεσίας πληροφορικής και τηλεπικοινωνιών ή υποβάθμιση της ποιότητας μιας υπηρεσίας πληροφορικής και τηλεπικοινωνιών. Συμβάν θεωρείται και η αστοχία ενός στοιχείου διαμόρφωσης που δεν έχει επηρεάσει ακόμη την υπηρεσία, όπως για παράδειγμα η αστοχία ενός από τους δίσκους ενός συνόλου ειδώλων (mirror set).

information security management (ISM) (διαχείριση ασφάλειας πληροφοριών (ISM))

Διεργασία που είναι υπεύθυνη να διασφαλίζει ότι η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των περιουσιακών στοιχείων, των πληροφοριών, των δεδομένων και των υπηρεσιών πληροφορικής και τηλεπικοινωνιών ενός οργανισμού ανταποκρίνονται στις συμφωνημένες ανάγκες της επιχείρησης. Η διαχείριση ασφάλειας πληροφοριών υποστηρίζει την επιχειρηματική ασφάλεια, έχει ευρύτερο πεδίο εφαρμογής από εκείνη του παρόχου υπηρεσιών πληροφορικής και τηλεπικοινωνιών και καλύπτει τη διαχείριση των εντύπων, την πρόσβαση στις κτιριακές εγκαταστάσεις, τις τηλεφωνικές συνδιαλέξεις κ.λπ. για το σύνολο του οργανισμού. *Βλέπε επίσης* πληροφοριακό σύστημα διαχείρισης ασφάλειας

information security management system (ISMS) (σύστημα διαχείρισης ασφάλειας πληροφοριών (ISMS))

Το πλαίσιο της πολιτικής, των διεργασιών, των λειτουργιών, των προτύπων, των κατευθυντήριων γραμμών και των εργαλείων που διασφαλίζει ότι ένας οργανισμός μπορεί να επιτύχει τους στόχους του σε επίπεδο διαχείρισης ασφάλειας πληροφοριών. *Βλέπε επίσης* πληροφοριακό σύστημα διαχείρισης ασφάλειας.

information security policy (πολιτική ασφάλειας πληροφοριών)

Πολιτική που διέπει το πώς προσεγγίζει ένας οργανισμός τη διαχείριση ασφάλειας πληροφοριών.

information system (πληροφοριακό σύστημα)
Βλέπε management information system (πληροφοριακό σύστημα διαχείρισης).

information technology (IT) (πληροφορική και τηλεπικοινωνίες (IT))

Η χρήση τεχνολογίας για την αποθήκευση, μετάδοση ή επεξεργασία πληροφοριών. Η εν λόγω τεχνολογία περιλαμβάνει συνήθως ηλεκτρονικούς υπολογιστές, τηλεπικοινωνίες, εφαρμογές και άλλο λογισμικό. Στις πληροφορίες υπό διαχείριση συγκαταλέγονται επιχειρησιακά δεδομένα, φωνή, εικόνες, βίντεο κ.λπ. Η πληροφορική χρησιμοποιείται συχνά για την υποστήριξη επιχειρησιακών διεργασιών μέσω υπηρεσιών πληροφορικής και τηλεπικοινωνιών.

integrity (ακεραιότητα)
Αρχή της ασφάλειας που διασφαλίζει ότι τα δεδομένα και τα στοιχεία διαμόρφωσης τροποποιούνται μόνο από προσωπικό και δραστηριότητες που φέρουν σχετική εξουσιοδότηση. Στο πλαίσιο της ακεραιότητας εξετάζονται όλα τα πιθανά αίτια μιας τροποποίησης, συμπεριλαμβανομένης της αστοχίας λογισμικού και υλικού, της επίδρασης περιβαλλοντικών παραγόντων και της ανθρώπινης παρέμβασης.

International Organization for Standardization (ISO) (Διεθνής Οργανισμός Τυποποίησης (ISO))
Ο Διεθνής Οργανισμός Τυποποίησης (ISO) είναι ο μεγαλύτερος φορέας ανάπτυξης προτύπων στον κόσμο. Ο ISO είναι ένας μη κυβερνητικός οργανισμός-δίκτυο που αποτελείται από τους εθνικούς οργανισμούς τυποποίησης 156 χωρών. Βλέπε www.iso.org για περισσότερες πληροφορίες σχετικά με τον ISO.

internet service provider (ISP) (πάροχος υπηρεσιών διαδικτύου (ISP))

Εξωτερικός πάροχος υπηρεσιών που παρέχει πρόσβαση στο διαδίκτυο. Οι περισσότεροι ISP παρέχουν και άλλες υπηρεσίες πληροφορικής και τηλεπικοινωνιών, όπως φιλοξενία ιστοσελίδων (web hosting).

invocation (ενεργοποίηση)
Έναρξη εφαρμογής των ενεργειών που προβλέπονται σε ένα σχέδιο. Για παράδειγμα, θέση σε εφαρμογή του σχεδίου συνέχειας υπηρεσιών πληροφορικής και τηλεπικοινωνιών για μία ή περισσότερες υπηρεσίες πληροφορικής και τηλεπικοινωνιών.

ISO/IEC 27001

Διεθνής προδιαγραφή για τη διαχείριση της ασφάλειας των πληροφοριών. *Βλέπε επίσης* πρότυπο.

IT infrastructure (υποδομές πληροφορικής και τηλεπικοινωνιών)

Δραστηριότητες που εκτελούνται από τη λειτουργία Έλεγχος λειτουργιών πληροφορικής και τηλεπικοινωνιών, συμπεριλαμβανομένης της διαχείρισης κονσόλας/επιχειρησιακού κέντρου λειτουργίας (console management/operations bridge), του προγραμματισμού εργασιών (job scheduling), της αποθήκευσης και ανάκτησης δεδομένων (backup and restore) και της διαχείρισης εκτυπώσεων και αντιγραφών (print and output management). Ο όρος αυτός χρησιμοποιείται επίσης ως συνώνυμο της λειτουργίας υπηρεσιών.

IT operations (λειτουργίες πληροφορικής και τηλεπικοινωνιών)

Δραστηριότητες που εκτελούνται από τη λειτουργία Έλεγχος λειτουργιών πληροφορικής και τηλεπικοινωνιών, συμπεριλαμβανομένης της διαχείρισης κονσόλας/επιχειρησιακού κέντρου λειτουργίας (console management/operations bridge), του προγραμματισμού εργασιών (job scheduling), της αποθήκευσης και ανάκτησης δεδομένων (backup and restore) και της διαχείρισης εκτυπώσεων και αντιγραφών (print and output management). Ο όρος αυτός χρησιμοποιείται επίσης ως συνώνυμο της λειτουργίας υπηρεσιών.

IT service (υπηρεσία πληροφορικής και τηλεπικοινωνιών)

Υπηρεσία που παρέχει ένας πάροχος υπηρεσιών πληροφορικής και τηλεπικοινωνιών. Μια υπηρεσία πληροφορικής και τηλεπικοινωνιών αποτελείται από ένα συνδυασμό τεχνολογιών της πληροφορίας και των τηλεπικοινωνιών, ανθρώπινων πόρων και διεργασιών. Μια υπηρεσία πληροφορικής και τηλεπικοινωνιών πρώτης γραμμής υποστηρίζει τις επιχειρησιακές διεργασίες ενός ή περισσότερων πελατών και οι στόχοι για το επίπεδο της παροχής της πρέπει να καθορίζονται στο πλαίσιο μιας συμφωνίας επιπέδου υπηρεσιών. Άλλες υπηρεσίες πληροφορικής και τηλεπικοινωνιών, οι οποίες ονομάζονται υποστηρικτικές υπηρεσίες, δε χρησιμοποιούνται απευθείας από την επιχείρηση, αλλά τις χρειάζεται ο πάροχος υπηρεσιών για την παροχή των υπηρεσιών πρώτης γραμμής. *Βλέπε επίσης*

κεντρική υπηρεσία, βοηθητική υπηρεσία, βελτιωτική υπηρεσία, υπηρεσία, πακέτο υπηρεσιών.

key performance indicator (KPI) (βασικός δείκτης απόδοσης (KPI))

Δείκτης μέτρησης που χρησιμοποιείται στο πλαίσιο της διαχείρισης μιας υπηρεσίας πληροφορικής και τηλεπικοινωνιών, μιας διεργασίας, ενός σχεδίου, ενός έργου ή κάποιας άλλης δραστηριότητας. Οι βασικοί δείκτες απόδοσης χρησιμοποιούνται για τη μέτρηση του βαθμού επίτευξης κρίσιμων παραγόντων επιτυχίας. Πολλοί δείκτες μέτρησης μπορεί να μετρούνται, αλλά μόνο οι πλέον σημαντικοί από αυτούς ορίζονται ως βασικοί δείκτες μέτρησης και χρησιμοποιούνται για την ενεργή διαχείριση της διεργασίας, της υπηρεσίας πληροφορικής και τηλεπικοινωνιών ή της δραστηριότητας και για την παροχή σχετικής πληροφόρησης. Πρέπει να επιλέγονται κατά τρόπο ώστε να διασφαλίζεται η διαχείριση της αποδοτικότητας, της αποτελεσματικότητας και της οικονομικής αποτελεσματικότητας.

live environment (επιχειρησιακό περιβάλλον)

Ελεγχόμενο περιβάλλον το οποίο περιέχει στοιχεία διαμόρφωσης σε επιχειρησιακή λειτουργία που χρησιμοποιούνται για την παροχή υπηρεσιών πληροφορικής και τηλεπικοινωνιών σε πελάτες.

management information system (MIS) (πληροφοριακό σύστημα διαχείρισης (MIS))

Σύνολο εργαλείων, δεδομένων και πληροφοριών που χρησιμοποιούνται για την υποστήριξη μιας διεργασίας ή μιας λειτουργίας. Σχετικά παραδείγματα είναι το πληροφοριακό σύστημα διαχείρισης διαθεσιμότητας και το πληροφοριακό σύστημα διαχείρισης προμηθευτών και συμβάσεων. *Βλέπε επίσης* σύστημα διαχείρισης γνώσης για παρεχόμενες υπηρεσίες.

metric (δείκτης μέτρησης)

Κάτι που μετράται και γνωστοποιείται προς διευκόλυνση της διαχείρισης μιας διεργασίας, υπηρεσίας πληροφορικής και τηλεπικοινωνιών ή δραστηριότητας. *Βλέπε επίσης* βασικός δείκτης απόδοσης.

monitoring (παρακολούθηση)

Επαναλαμβανόμενη παρακολούθηση ενός στοιχείου διαμόρφωσης, μιας υπηρεσίας πληροφορικής και τηλεπικοινωνιών ή μιας διεργασίας με σκοπό τον εντοπισμό συμβάντων και τη διάγνωση της τρέχουσας κατάστασης.

objective (αντικειμενικός στόχος)

Τα αποτελέσματα που αποτελούν το ζητούμενο μιας διεργασίας, μιας δραστηριότητας ή ενός οργανισμού, ώστε να εξασφαλιστεί η εκπλήρωση του σκοπού τους. Οι αντικειμενικοί στόχοι εκφράζονται συνήθως ως μετρήσιμοι στόχοι. Στην καθομιλουμένη ο όρος έχει και την έννοια της απαίτησης.

operation (λειτουργία)

Καθημερινή διαχείριση μιας υπηρεσίας πληροφορικής και τηλεπικοινωνιών, ενός συστήματος ή κάποιου άλλου στοιχείου διαμόρφωσης. Ο όρος αναφέρεται επίσης σε κάθε προκαθορισμένη δραστηριότητα ή συναλλαγή, όπως για παράδειγμα η φόρτωση μιας μαγνητοταινίας, η αποδοχή χρημάτων σε ένα σημείο πώλησης ή η ανάγνωση δεδομένων από μια μονάδα δίσκου.

organization (οργανισμός)

Εταιρεία, νομικό πρόσωπο ή άλλη οντότητα. Ο όρος αναφέρεται ενίοτε και σε οτιδήποτε διαθέτει ανθρώπινους ή άλλους πόρους και προϋπολογισμό, όπως για παράδειγμα ένα έργο ή μια επιχειρηματική μονάδα.

performance (απόδοση)

Μέτρο του τι επιτυγχάνεται ή παρέχεται από ένα σύστημα, πρόσωπο, ομάδα, διεργασία ή υπηρεσία πληροφορικής και τηλεπικοινωνιών.

plan (σχέδιο)

Αναλυτική πρόταση που περιγράφει τις δραστηριότητες και τους πόρους που απαιτούνται για την επίτευξη ενός στόχου – για παράδειγμα, ένα σχέδιο για την εφαρμογή μιας νέας υπηρεσίας πληροφορικής και τηλεπικοινωνιών ή διεργασίας. Το ISO/IEC 20000 προβλέπει την ύπαρξη σχεδίου για τη διαχείριση κάθε διεργασίας διαχείρισης υπηρεσίας πληροφορικής και τηλεπικοινωνιών.

Plan-Do-Check-Act (PDCA) (Σχεδιάζω-Εκτελώ- Ελέγχω-Ενεργώ (PDCA))

Κύκλος τεσσάρων σταδίων για τη διαχείριση διεργασιών, που αποδίδεται στον Edward Deming. Η μεθοδολογία «Σχεδιάζω-Εκτελώ-Ελέγχω- Βελτιώνω» είναι

γνωστή και ως Κύκλος του Deming. **Σχεδιάζω** – σχεδιασμός ή αναθεώρηση διεργασιών που υποστηρίζουν τις διεργασίες πληροφορικής και τηλεπικοινωνιών / **Εκτελώ** – εφαρμογή του σχεδίου και διαχείριση των διεργασιών / **Ελέγχω** – μέτρηση των διεργασιών και των υπηρεσιών πληροφορικής και τηλεπικοινωνιών, σύγκριση με στόχους και εκπόνηση εκθέσεων / **Ενεργώ** – σχεδίαση και υλοποίηση αλλαγών για τη βελτίωση των διεργασιών.

planning (σχεδιασμός)

Δραστηριότητα που είναι υπεύθυνη για τη δημιουργία ενός ή περισσότερων σχεδίων – για παράδειγμα, σχεδιασμός δυναμικότητας.

policy (πολιτική)

Επίσημα καταγεγραμμένες προσδοκίες και προθέσεις της διοίκησης. Οι πολιτικές χρησιμοποιούνται ως οδηγός για τη λήψη αποφάσεων, όπως και για τη συνεπή και πρόσφορη ανάπτυξη και υλοποίηση διεργασιών, προτύπων, ρόλων, δραστηριοτήτων, υποδομών πληροφορικής και τηλεπικοινωνιών κ.λπ.

priority (προτεραιότητα)

Κατηγορία που χρησιμοποιείται για τον προσδιορισμό της σχετικής σπουδαιότητας ενός συμβάντος, ενός προβλήματος ή μιας αλλαγής. Η προτεραιότητα εξαρτάται από τον αντίκτυπο και την επιτακτικότητα και χρησιμοποιείται για τον προσδιορισμό των προβλεπόμενων προθεσμιών για την πραγματοποίηση ενεργειών. Για παράδειγμα, στη συμφωνία επιπέδου υπηρεσιών μπορεί να ορίζεται ότι τα συμβάντα Προτεραιότητας 2 πρέπει να επιλύονται εντός 12 ωρών.

procedure (διαδικασία)

Έγγραφο που περιέχει βήματα που καθορίζουν πώς πρέπει να πραγματοποιείται μια δραστηριότητα. Οι διαδικασίες διαμορφώνονται ως τμήματα διεργασιών. *Βλέπε επίσης* οδηγίες εργασίας.

process (διεργασία)

Δομημένο σύνολο δραστηριοτήτων που έχουν σχεδιαστεί για την επίτευξη ενός συγκεκριμένου αντικειμενικού στόχου. Μια διεργασία παίρνει μία ή περισσότερες καθορισμένες εισροές (input) και τις μετατρέπει σε καθορισμένες εκροές (output). Μπορεί να περιλαμβάνει όλους τους ρόλους, τις αρμοδιότητες, τα εργαλεία και τους μηχανισμούς ελέγχου διαχείρισης που απαιτούνται για την αξιόπιστη εξασφάλιση των

εκρούν. Μια διεργασία μπορεί, εάν απαιτείται κάτι τέτοιο, να διαμορφώνει πολιτικές, πρότυπα, κατευθυντήριες γραμμές, δραστηριότητες και οδηγίες εργασίας.

process owner (κύριος διεργασίας)

Το πρόσωπο που είναι υπεύθυνο να διασφαλίζει ότι μια διεργασία είναι κατάλληλη για τον προβλεπόμενο σκοπό. Οι αρμοδιότητες του κυρίου διεργασίας περιλαμβάνουν το συντονισμό, το σχεδιασμό, τη διαχείριση αλλαγών και τη συνεχή βελτίωση της διεργασίας και των δεικτών μέτρησής της. Με τα καθήκοντα αυτά επιφορτίζεται συχνά το ίδιο πρόσωπο που ασκεί καθήκοντα υπεύθυνου διεργασίας (process manager), όμως στους μεγάλους οργανισμούς οι δύο ρόλοι ενδέχεται να είναι διακριτοί.

production environment (παραγωγικό περιβάλλον)

Βλέπε live environment (επιχειρησιακό περιβάλλον)

recovery (ανάκαμψη)

Επαναφορά στοιχείου διαμόρφωσης ή υπηρεσίας πληροφορικής και τηλεπικοινωνιών σε λειτουργική κατάσταση. Η ανάκαμψη μιας υπηρεσίας πληροφορικής και τηλεπικοινωνιών συχνά περιλαμβάνει την επαναφορά δεδομένων σε γνωστή, συνεκτική κατάσταση. Μετά την ανάκαμψη ενδέχεται να απαιτηθούν περαιτέρω βήματα προτού η υπηρεσία πληροφορικής και τηλεπικοινωνιών μπορέσει να καταστεί διαθέσιμη στους χρήστες (αποκατάσταση).

recovery point objective (RPO) (στόχος σημείου ανάκαμψης (RPO))

Η μέγιστη ποσότητα δεδομένων που μπορεί να απολεσθεί όταν αποκαθίσταται η υπηρεσία μετά από μια διακοπή λειτουργίας. Ο στόχος σημείου ανάκαμψης εκφράζεται ως χρονικό διάστημα πριν από την αστοχία. Για παράδειγμα, όταν ως στόχος σημείου ανάκαμψης ορίζεται η μία ημέρα, ο στόχος αυτός μπορεί να υποστηρίζεται από ημερήσια δημιουργία αντιγράφων ασφαλείας και στην περίπτωση αυτή μπορεί να χαθούν δεδομένα έως 24 ωρών. Οι στόχοι σημείου ανάκαμψης για κάθε υπηρεσία πληροφορικής και τηλεπικοινωνιών πρέπει να αποτελούν αντικείμενο διαπραγμάτευσης, συμφωνίας και καταγραφής, και να χρησιμοποιούνται ως απαιτήσεις στο πλαίσιο του σχεδιασμού υπηρεσιών και της εκπόνησης των σχεδίων

συνέχειας υπηρεσιών πληροφορικής και τηλεπικοινωνιών.

recovery time objective (RTO) (στόχος χρόνου ανάκαμψης (RTO))

Ο μέγιστος χρόνος που επιτρέπεται για την ανάκαμψη μιας υπηρεσίας πληροφορικής και τηλεπικοινωνιών μετά από μια διακοπή λειτουργίας. Το προς παροχή επίπεδο υπηρεσίας μπορεί να είναι χαμηλότερο από τους συνήθεις στόχους επιπέδου υπηρεσιών. Οι στόχοι χρόνου ανάκαμψης για κάθε υπηρεσία πληροφορικής και τηλεπικοινωνιών πρέπει να αποτελούν αντικείμενο διαπραγμάτευσης, συμφωνίας και καταγραφής. *Βλέπε επίσης* ανάλυση επιχειρησιακού αντίκτυπου.

redundancy (εφεδρεία)

Χρήση ενός ή περισσότερων πρόσθετων στοιχείων διαμόρφωσης για την εξασφάλιση ανοχής σε σφάλματα / βλάβες. Ο όρος έχει επίσης και τη γενικότερη έννοια του πράγματος που απαξιώνεται ή καθίσταται περιττό.

reliability (αξιοπιστία)

Μέτρο του χρονικού διαστήματος κατά το οποίο μια υπηρεσία πληροφορικής και τηλεπικοινωνιών ή κάποιο άλλο στοιχείο διαμόρφωσης μπορεί να επιτελεί απρόσκοπτα τη συμφωνημένη λειτουργία του. Συνήθως μετράται ως μέσος χρόνος μεταξύ αστοχιών (MTBF) ή ως μέσος χρόνος μεταξύ συμβάντων υπηρεσίας (MTBSI). Ο όρος χρησιμοποιείται επίσης για να δηλωθεί το πόσο πιθανό είναι μια διεργασία, λειτουργία κ.λπ. να αποφέρει τα απαιτούμενα αποτελέσματα. *Βλέπε επίσης* διαθεσιμότητα.

requirement (απαίτηση)

Επίσημη διατύπωση ενός ζητούμενου, όπως για παράδειγμα μια απαίτηση για το επίπεδο των παρεχόμενων υπηρεσιών, μια απαίτηση σχετικά με ένα έργο ή τα ζητούμενα παραδοτέα μιας διεργασίας. *Βλέπε επίσης* έκθεση απαιτήσεων.

resource (πόρος)

Περιληπτικός όρος που περιλαμβάνει τις υποδομές πληροφορικής και τηλεπικοινωνιών, το ανθρώπινο δυναμικό, τη χρηματοδότηση και καθετί άλλο που μπορεί να συμβάλλει στην υλοποίηση μιας υπηρεσίας πληροφορικής και τηλεπικοινωνιών. Οι πόροι θεωρούνται περιουσιακά στοιχεία ενός οργανισμού.

response time (χρόνος απόκρισης)

Μέτρο του χρόνου που απαιτείται για την ολοκλήρωση μιας λειτουργίας ή συναλλαγής. Χρησιμοποιείται στη διαχείριση δυναμικότητας ως μέτρο της απόδοσης υποδομών πληροφορικής και τηλεπικοινωνιών, καθώς και στη διαχείριση συμβάντων ως μέτρο του χρόνου που μεσολαβεί μέχρι να απαντηθεί μια κλήση ή μέχρι να ξεκινήσει η διάγνωση.

restore (αποκαθιστώ)

Προβαίνω στις απαιτούμενες ενέργειες για να τεθεί μια υπηρεσία πληροφορικής και τηλεπικοινωνιών και πάλι στη διάθεση των χρηστών μετά την επιδιόρθωση / επισκευή και την ανάκαμψη από ένα συμβάν. Πρόκειται για τον πρωταρχικό στόχο της διαχείρισης συμβάντων.

risk (Κίνδυνος / ρίσκο)

Δυνητικό γεγονός που μπορεί να προκαλέσει ζημία ή απώλεια ή να επηρεάσει την ικανότητα επίτευξης στόχων. Η αποτίμηση ενός κινδύνου γίνεται βάσει της πιθανότητας μιας απειλής, της ευπάθειας ενός περιουσιακού στοιχείου σε αυτήν την απειλή και του αντίκτυπου που θα επέφερε τυχόν πραγμάτωσή της. Ο κίνδυνος ορίζεται και ως η αβεβαιότητα ενός αποτελέσματος και μπορεί να χρησιμοποιείται στο πλαίσιο της αποτίμησης της πιθανότητας να επισυμβεί το αποτέλεσμα αυτό, είτε είναι θετικό είτε αρνητικό.

risk assessment (αξιολόγηση κινδύνων)

Τα πρώτα στάδια της διαχείρισης κινδύνων: ανάλυση της αξίας των περιουσιακών στοιχείων για την επιχείρηση, προσδιορισμός των σε βάρος τους απειλών και αξιολόγηση της ευπάθειας κάθε περιουσιακού στοιχείου σε αυτές τις απειλές. Η αξιολόγηση κινδύνων μπορεί να είναι είτε ποσοτική (να βασίζεται δηλαδή σε αριθμητικά δεδομένα), είτε ποιοτική.

risk management (διαχείριση κινδύνων)

Διεργασία που είναι υπεύθυνη για τον προσδιορισμό, την αξιολόγηση και τον έλεγχο των κινδύνων. Ο όρος «διαχείριση κινδύνων» αναφέρεται και στο δεύτερο σκέλος της συνολικής διεργασίας αξιολόγησης και διαχείρισης κινδύνων, αυτό δηλαδή που έπεται του προσδιορισμού και της αξιολόγησης των κινδύνων. Η συγκεκριμένη διεργασία δεν περιγράφεται αναλυτικά στους βασικούς τόμους του ITIL. *Βλέπε επίσης* risk assessment (αξιολόγηση κινδύνων).

role (ρόλος)

Σύνολο αρμοδιοτήτων, δραστηριοτήτων και εξουσιών που ανατίθενται σε ένα πρόσωπο ή μια ομάδα. Οι ρόλοι καθορίζονται στο πλαίσιο μιας διεργασίας ή μιας λειτουργίας. Ένα πρόσωπο ή μια ομάδα μπορεί να έχει περισσότερους από ένα ρόλους. Για παράδειγμα, τα καθήκοντα του υπεύθυνου διαμόρφωσης και του υπεύθυνου αλλαγών μπορεί να ασκούνται από το ίδιο πρόσωπο. Ο όρος «ρόλος» αναφέρεται επίσης σε αυτό στο οποίο αποσκοπεί ή για το οποίο χρησιμοποιείται κάτι.

server (διακομιστής)

Ηλεκτρονικός υπολογιστής που είναι συνδεδεμένος σε δίκτυο και παρέχει λειτουργίες λογισμικού τις οποίες χρησιμοποιούν άλλοι ηλεκτρονικοί υπολογιστές.

service (υπηρεσία)

Τρόπος με τον οποίο παρέχεται αξία στους πελάτες, οι οποίοι εξασφαλίζουν τα αποτελέσματα που επιθυμούν χωρίς να εμπλέκονται στα οικονομικά και το ρίσκο της υπηρεσίας. Ο όρος «υπηρεσία» χρησιμοποιείται ενίοτε ως συνώνυμο της κεντρικής υπηρεσίας, της υπηρεσίας πληροφορικής και τηλεπικοινωνιών ή του πακέτου υπηρεσιών.

service level agreement (SLA) (Σύμβαση Επιπεδου Παρεχόμενης Υπηρεσίας (SLA))

Συμφωνία μεταξύ ενός παρόχου υπηρεσιών πληροφορικής και τηλεπικοινωνιών και ενός πελάτη. Σε μια συμφωνία επιπέδου υπηρεσιών περιγράφεται η παρεχόμενη υπηρεσία πληροφορικής και τηλεπικοινωνιών, καταγράφονται οι στόχοι επιπέδου υπηρεσιών και καθορίζονται οι ευθύνες τόσο του παρόχου υπηρεσιών πληροφορικής και τηλεπικοινωνιών, όσο και του πελάτη. Μια συμφωνία μπορεί να καλύπτει πολλαπλές υπηρεσίες πληροφορικής και τηλεπικοινωνιών ή πολλαπλούς πελάτες. *Βλέπε επίσης* σύμβαση επιχειρησιακού επιπέδου.

single point of failure (SPOF) (μοναδικό σημείο αστοχίας (SPOF))

Στοιχείο διαμόρφωσης το οποίο εάν παρουσιάσει αστοχία μπορεί να προκαλέσει συμβάν και για το οποίο δεν έχει προβλεφθεί αντίμετρο. Μοναδικό σημείο αστοχίας μπορεί να είναι ένα πρόσωπο ή ένα βήμα μιας διεργασίας ή δραστηριότητας, ή ένα

συστατικό στοιχείο μιας υποδομής πληροφορικής και τηλεπικοινωνιών. *Βλέπε επίσης* αστοχία.

snapshot (στιγμιότυπο)

Η τρέχουσα κατάσταση στοιχείου διαμόρφωσης, διεργασίας ή άλλου συνόλου δεδομένων, όπως αυτή αποτυπώνεται μια δεδομένη χρονική στιγμή. Στιγμιότυπα καταγράφονται μέσω εργαλείων ανακάλυψης (discovery tools) ή μη αυτόματων τεχνικών, όπως η διενέργεια αξιολόγησης. *Βλέπε επίσης* επίπεδο αναφοράς, μέτρο σύγκρισης.

stakeholder (ενδιαφερόμενο μέρος)

Πρόσωπο που το ενδιαφέρει ή το επηρεάζει ένας οργανισμός, ένα έργο, μια υπηρεσία πληροφορικής και τηλεπικοινωνιών κ.λπ. Το ενδιαφέρον των ενδιαφερόμενων μερών μπορεί να επικεντρώνεται στις δραστηριότητες, στους στόχους, στους πόρους ή στα παραδοτέα. Ενδιαφερόμενα μέρη μπορεί να είναι πελάτες, εταίροι, εργαζόμενοι, μέτοχοι, ιδιοκτήτες κ.λπ.

standard (πρότυπο)

Υποχρεωτική απαίτηση. Π.χ. το ISO/IEC 20000 (διεθνές πρότυπο), ένα εσωτερικό πρότυπο ασφάλειας για την παραμετροποίηση σε περιβάλλον Unix ή ένα κρατικό πρότυπο για την τήρηση των χρηματοοικονομικών αρχείων. Ο όρος αναφέρεται επίσης στους κώδικες πρακτικής και στις προδιαγραφές που δημοσιεύουν οργανισμοί τυποποίησης, όπως οι ISO και BSI. *Βλέπε επίσης* κατευθυντήριες γραμμές.

standby (ετοιμότητα)

Αναφέρεται στους πόρους που δεν είναι απαραίτητοι για την επιχειρησιακή λειτουργία των υπηρεσιών πληροφορικής και τηλεπικοινωνιών, αλλά είναι διαθέσιμοι για την υποστήριξη των σχεδίων συνέχειας υπηρεσιών πληροφορικής και τηλεπικοινωνιών. Για παράδειγμα, ένα εφεδρικό κέντρο δεδομένων μπορεί να διατηρείται σε ετοιμότητα για την υλοποίηση σχεδιασμού υψηλής ή θερμής ετοιμότητας (hot standby), μέσης ετοιμότητας (warm standby) ή χαμηλής ετοιμότητας (cold standby).

system (σύστημα)

Μια συνάθροιση πραγμάτων που συσχετίζονται μεταξύ τους και συνεργάζονται για την επίτευξη ενός συνολικού στόχου. Για παράδειγμα:

- Ένα σύστημα ηλεκτρονικού υπολογιστή, το οποίο περιλαμβάνει υλικό, λογισμικό και εφαρμογές.
- Ένα σύστημα διαχείρισης, το οποίο περιλαμβάνει το πλαίσιο της πολιτικής, των διεργασιών, των λειτουργιών, των προτύπων, των κατευθυντήριων γραμμών και των εργαλείων που έχουν κοινό σχεδιασμό και τελούν υπό κοινή διαχείριση, όπως για παράδειγμα ένα σύστημα διαχείρισης ποιότητας.
- Ένα σύστημα διαχείρισης βάσης δεδομένων ή ένα λειτουργικό σύστημα, το οποίο περιλαμβάνει πολλές υπομονάδες λογισμικού που είναι σχεδιασμένες να επιτελούν ένα σύνολο συναφών λειτουργιών.

system management (διαχείριση συστημάτων)

Το σκέλος της διαχείρισης υπηρεσιών πληροφορικής και τηλεπικοινωνιών που επικεντρώνεται στη διαχείριση υποδομών πληροφορικής και τηλεπικοινωνιών και όχι διεργασιών.

third party (τρίτος)

Πρόσωπο, οργανισμός ή άλλη οντότητα που δεν ανήκει στην οργανωτική δομή του παρόχου υπηρεσιών και δεν είναι πελάτης, όπως για παράδειγμα ένας προμηθευτής λογισμικού ή μια εταιρεία συντήρησης υλικού. Οι απαιτήσεις που οφείλει να εκπληρώνει ένας τρίτος καθορίζονται κατά κανόνα στο πλαίσιο συμβάσεων που υποστηρίζουν συμφωνίες επιπέδου υπηρεσιών. *Βλέπε επίσης* υποστηρικτική σύμβαση.

threat (απειλή)

Απειλή είναι οτιδήποτε μπορεί να εκμεταλλευτεί μια ευπάθεια. Καθετί που δύναται να προκαλέσει συμβάν μπορεί να θεωρηθεί απειλή. Για παράδειγμα, μια πυρκαγιά είναι απειλή που μπορεί να εκμεταλλευτεί την ευπάθεια των εύφλεκτων δαπέδων. Ο όρος αυτός χρησιμοποιείται κατά κόρον στη διαχείριση της ασφάλειας πληροφοριών και στη διαχείριση της συνέχειας υπηρεσιών πληροφορικής και τηλεπικοινωνιών, αλλά τυγχάνει εφαρμογής και σε άλλους τομείς, όπως η διαχείριση προβλημάτων και διαθεσιμότητας.

threshold (όριο)

Η τιμή ενός δείκτη μέτρησης που πρέπει να προκαλεί τη δημιουργία προειδοποίησης ή τη λήψη διαχειριστικών μέτρων. Για παράδειγμα, «Μη επίλυση συμβάντος 1ης προτεραιότητας εντός τεσσάρων ωρών», «Περισσότερα από πέντε παροδικά σφάλματα στο δίσκο σε διάστημα μίας ώρας» ή «Περισσότερες από 10 αποτυχημένες αλλαγές σε διάστημα ενός μηνός».