



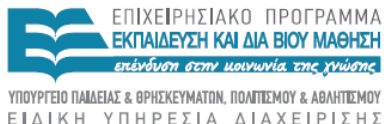
ΑΚΑΔΗΜΙΑ ΠΛΑΤΩΝΟΣ – ΑΝΑΠΤΥΞΗ ΤΗΣ ΓΝΩΣΗΣ ΚΑΙ ΚΑΙΝΟΤΟΜΩΝ ΙΔΕΩΝ

Υποέργο 6 «Τροφεία μεταπτυχιακών φοιτητών, θεμελίωση και λειτουργία Αποθετηρίου και
Επιστημονικοτεχνική Υποστήριξη του Έργου»

Δράση 2 «Θεμελίωση, Ενίσχυση και Λειτουργία Ψηφιακού Αποθετηρίου Ακαδημίας
Πλάτωνος»

Π 6.2.2.1 Μεθοδολογία Ελέγχου Συστήματος

Μάιος, 2013



Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης



Εικόνα Εγγράφου

Αριθμός Παραδοτέου	Π 6.2.2.1
Τίτλος Παραδοτέου	Μεθοδολογία Ελέγχου Συστήματος
Αριθμός Πακέτου Εργασίας	ΠΕ 6.2.2
Τίτλος Πακέτου Εργασίας	Μεθοδολογία Ελέγχου και Έλεγχος Συστήματος
Υποέργο	6 - Τροφεία μεταπτυχιακών φοιτητών, θεμελίωση και λειτουργία Αποθετηρίου και Επιστημονικοτεχνική Υποστήριξη του Έργου
Δράση	2 - Θεμελίωση, Ενίσχυση και Λειτουργία Ψηφιακού Αποθετηρίου Ακαδημίας Πλάτωνος
Πράξη	1 - Ανάπτυξη της Γνώσης και καινοτόμων ιδεών
Μήνας Συμβατικής Παράδοσης	Μάιος 2013
Ημερομηνία Ολοκλήρωσης	Μάιος 2013
Κατάσταση	Τελικό
Έκδοση	1
Σελίδες	61



Περιεχόμενα

Εικόνα Εγγράφου	3
Περιεχόμενα	5
1 Εισαγωγή	7
1.1 Σκοπιμότητα έκθεσης	7
1.2 Δομή κειμένου	8
2 Το Ψηφιακό Αποθετήριο	9
2.1 Περιγραφή	9
2.2 Στόχος και Αντικείμενο Έκθεσης και Ελέγχου	9
2.3 Προγραμματισμός Ελέγχου	9
2.4 Υποσυστήματα.....	10
3 Μεθοδολογία ελέγχων – Διεθνείς Πρακτικές	11
3.1 Στόχοι και προτεραιότητες	11
3.2 Προσέγγιση Σχεδιασμού Δοκιμών και Αξιολόγησης	12
3.3 Επίπεδα αξιολόγησης	19
4 Σενάρια Ελέγχων-Δοκιμών	23
4.1 Έρευνα γραφείου.....	23
4.2 Ελεύθερα σενάρια ελέγχου σε εργαστηριακό περιβάλλον	24
4.3 Έλεγχοι αποδοχής χρήστη	25
4.4 Έλεγχοι απόδοσης	26
5 Διάρθρωση ομάδων ελέγχου	29
6 Παράρτημα: Ενδεικτικές φόρμες καταγραφής ελέγχων.....	31
6.1 Πίνακας Ελέγχου Μετάπτωσης	31
6.2 Πίνακας Ελέγχου Συστημάτων	33
6.3 Πίνακας ελέγχου υπηρεσιών - υποσυστημάτων.....	42
6.4 Πίνακας καταγραφής ελέγχου συνιστωσών, προτύπων και τεχνολογιών	44
6.5 Υπόδειγμα φόρμας ελεύθερων σεναρίων ελέγχου	45
6.6 Φόρμες σεναρίων ελέγχου αποδοχής χρήστη και προκαθορισμένα σενάρια	46
6.7 Έλεγχοι απόδοσης	46
6.8 Φόρμες συλλογής πληροφοριών ελέγχων παρείσφρησης (Penetration tests).....	48



Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο



ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ, ΠΟΛΙΤΙΣΜΟΥ & ΑΘΛΗΤΙΣΜΟΥ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης



1 Εισαγωγή

1.1 Σκοπιμότητα έκθεσης

Είναι γενικά αποδεκτό ότι κάθε φορά που σχεδιάζεται αναπτύσσεται και εγκαθίσταται ένα Πληροφοριακό Σύστημα, ανεξάρτητα αν αυτό γίνεται από ένα άτομο ή από πολυπληθείς ομάδες, πάντα υπάρχουν περιπτώσεις που παρουσιάζονται σφάλματα κάθε είδους (σχεδιαστικά, υπολογιστικά, λειτουργικά κτλ.). Αυτό ιδίως σε συστήματα που περιλαμβάνουν δημιουργία νέου (ή παραμετροποίηση, εξειδίκευση, μετατροπή) λογισμικού.

Έτσι οι γνωστές δοκιμές και έλεγχοι αποτελούν αναπόσπαστο μέρος της δημιουργίας συστημάτων Πληροφορικής γενικά και Εφαρμογών Λογισμικού ειδικότερα. Οι Έλεγχοι και Δοκιμές είναι επίσης ένα κρίσιμο στοιχείο για την πιστοποίηση ποιότητας ενός παραδοτέου Π.Σ. για ευρεία χρήση και είναι ένας τρόπος επαλήθευσης ότι όλα τα προηγούμενα βήματα (π.χ. Ανάλυση, Σχεδιασμός συστήματος, κωδικοποίηση κλπ) έγιναν σωστά.

Η διαδικασία δοκιμών και ελέγχων αποτελεί ένα σημαντικό βήμα στη διαδικασία ολοκλήρωσης και αποδοχής του συστήματος. Για το λόγο αυτό, είναι σημαντικά τα ακόλουθα:

- Ο σωστός σχεδιασμός και η υλοποίηση των δοκιμών ελέγχου
- Η δημιουργία ισχυρής αίσθησης αποδοχής του συστήματος από τους τελικούς χρήστες, ώστε να είναι δυνατή η ενεργή συμμετοχή τους στη διαδικασία αποτύπωσης και υλοποίησης των σεναρίων τα οποία θα χρησιμοποιηθούν για τον έλεγχο των λειτουργιών.

Οι Έλεγχοι και Δοκιμές αποσκοπούν στο να περιορισθούν τα σφάλματα του παραδοτέου Π.Σ., πριν αυτό φθάσει στον τελικό χρήστη (Πολίτη, Ερευνητή, Μαθητή, Φοιτητή κτλ.). Πρόκειται για μία διαδικασία που αποσκοπεί στην βελτίωση της Ποιότητας του παραδοτέου που εξαρτάται και από άλλες παραμέτρους.

Σκοπός της έκθεσης αυτής είναι η σχεδίαση σεναρίων ελέγχων και δοκιμών τα οποία να καλύπτουν τους παρακάτω τύπους ελέγχων:

- Συμμόρφωσης με τις προδιαγραφές και προσδοκίες του κοινού του
- Σωστής λειτουργίας εφαρμογών και ακεραιότητας δεδομένων
- Ευχρηστίας
- Απόδοσης
- Ασφάλειας

1.2 Δομή κειμένου

Για να πραγματοποιηθεί η σχεδίαση σεναρίων ελέγχων, σημαντικά στοιχεία είναι η κατανόηση του υλοποιούμενου έργου και του περιβάλλοντος λειτουργίας, η μεθοδολογία υλοποίησής του και οι διεθνείς πρακτικές σχετικές με την αποδοχή ενός πληροφοριακού συστήματος. Η γνώση αυτών των πληροφοριών είναι απαραίτητη ώστε να οριστεί με πληρότητα η μεθοδολογία σχεδίασης των σεναρίων ελέγχων που θα ακολουθηθεί, λαμβάνοντας υπόψη τις ιδιομορφίες του υλοποιούμενου υποσυστήματος, τους σκοπούς του και το περιβάλλον λειτουργίας του. Με τη γνώση των παραπάνω στοιχείων και τον καθορισμό της μεθοδολογίας και των απαιτήσεων που απορρέουν απ' αυτή (απαιτούμενα έντυπα τεκμηρίωσης, δημιουργία κατάλληλων υποδομών δοκιμών, κλπ), μπορεί πλέον να γίνει ο τελικός σχεδιασμός των σεναρίων ελέγχου.

Στο Κεφάλαιο 2 με τίτλο «Ψηφιακό Αποθετήριο» δίνεται μια σύντομη περιγραφή του συνόλου των συστημάτων τα οποία αποτελούν αντικείμενο της εδώ παρουσιαζόμενης μεθοδολογίας.

Στο Κεφάλαιο 3 με τίτλο «Μεθοδολογία Ελέγχων - Διεθνείς πρακτικές» μελετώνται το ISO 9126 που είναι ένα διεθνές πρότυπο αξιολόγησης ποιότητας λογισμικού, καθώς και το Open Source Security Testing Methodology Manual (OSSTMM) το οποίο καλύπτει θέματα ασφάλειας πληροφοριών. Η έκθεση των διεθνών πρακτικών είναι σημαντική για τον καθορισμό της μεθοδολογίας των ελέγχων, καθώς παρέχουν σημαντική πληροφόρηση σχετικά με τομείς που πρέπει να ληφθούν υπόψη στο καθορισμό της μεθοδολογίας που τελικά θα ακολουθηθεί.

Στο Κεφάλαιο 4 με τίτλο «Μεθοδολογία ελέγχων» ορίζονται οι στόχοι και οι προτεραιότητες των ελέγχων που θα σχεδιαστούν, οι άξονες αξιολόγησης και τα επίπεδα αξιολόγησης. Μέσω της μεθοδολογίας καθορίζονται και τα προαπαιτούμενα, για τη διενέργεια των ελέγχων που θα σχεδιαστούν, στοιχεία, τα οποία και θα αξιοποιηθούν κατά την διενέργεια των ελέγχων. Τέτοια είναι το τεκμηριωτικό υλικό για τη δημιουργία του απαραίτητου περιβάλλοντος εκτέλεσης των ελέγχων, κλπ.

Στο Κεφάλαιο 5 με τίτλο «Σενάρια Ελέγχων-Δοκιμών» αναφέρονται ενδεικτικά σενάρια τα οποία και διαχωρίζονται σε α) Έρευνα γραφείου β) Ελέγχους μονάδων, γ) Ελεύθερα σενάρια χρήσης, δ) Ελέγχους αποδοχής χρηστών, ε) Ελέγχους απόδοσης και τέλος ελέγχους παρέισφρησης (penetration).

Τέλος στα Παραρτήματα περιλαμβάνονται φόρμες που αφορούν την εκτέλεση των σεναρίων ελέγχου του προηγούμενου κεφαλαίου (παρέχεται σύνδεσμος σε κάθε σενάριο προς τη φόρμα του παραρτήματος που θα συμπληρωθεί κατά την εκτέλεσή του).

2 Το Ψηφιακό Αποθετήριο

2.1 Περιγραφή

Το υποσύστημα του υλοποιούμενου αποθετηρίου ενσωματώνει τεχνολογίες αιχμής οι οποίες σήμερα εντοπίζονται σε έργα μεταβατικού χαρακτήρα, από τον τομέα έρευνας στον τομέα παραγωγής. Παράλληλα με την κύρια υλοποίηση δημιουργούνται μια σειρά από πρότυπες εφαρμογές προστιθέμενης αξίας οι οποίες αξιοποιούν τεχνολογίες αιχμής για την παράδοση υψηλού επιπέδου εξειδικευμένων υπηρεσιών στο χρήστη του ψηφιακού αποθετηρίου.

2.2 Στόχος και Αντικείμενο Έκθεσης και Ελέγχου

Στόχος της παρούσας έκθεσης είναι να θέσει τις βάσεις ώστε να εκτελεστεί ο έλεγχος του συστήματος ως προς την κάλυψη των προδιαγραφών των σχεδιαστών του και των προσδοκιών των χρηστών του.

Μέσω αυτής τίθενται οι προδιαγραφές των σεναρίων ελέγχου του συστήματος τα οποία στη συνέχεια, με την υλοποίηση του συστήματος, εφαρμόζονται για την πρόληψη και αντιμετώπιση των όποιων θεμάτων δύναται προκύπτουν, και ταυτόχρονα τροφοδοτούν τη διαδικασία ποιοτικού ελέγχου του έργου.

Το αντικείμενο του ελέγχου είναι:

- Το σύστημα το οποίο υλοποιείται από υποψήφιο ανάδοχο ως Ψηφιακό Αποθετήριο της Ακαδημίας Πλάτωνα.
- Το περιεχόμενο που συλλέγεται στο σύστημα ως αποτέλεσμα των διαδικασιών μετάπτωσης και συνάθροισης περιεχομένου.

2.3 Προγραμματισμός Ελέγχου

Τα σεναρία ελέγχου αφορούν σε εστιασμένους ελέγχους του παραδιδόμενου συστήματος με τη συμμετοχή χρηστών, εμπειρογνομόνων και εξειδικευμένων στελεχών του φορέα.

Κύρια σημεία ελέγχου είναι τα θέματα:

- Λειτουργικής πληρότητας
- Ασφάλειας και απόδοσης
- Ευχρηστίας
- Διαλειτουργικότητας

Η διαδικασία εκτελείται στα εξής στάδια:

Σύνταξη σεναρίων ελέγχου, η οποία ακολουθεί την αρχική σχεδίαση του συστήματος και αποτυπώνει τον τρόπο με τον οποίο θα ελεγχθούν τα παραπάνω θέματα και τη διαδικασία και

τις μετρικές με τις οποίες θα αξιολογηθούν τα αποτελέσματα. Τα σενάρια ελέγχου γνωστοποιούνται στον ανάδοχο του υποέργου προμήθειας του ψηφιακού αποθετηρίου και μάλιστα συμμετέχει στον εμπλουτισμό και την αξιολόγησή τους.

Εκτέλεση σεναρίων ελέγχου, η οποία πραγματοποιείται κυρίως κατά την περίοδο της πιλοτικής λειτουργίας και αναφέρεται στην βήμα προς βήμα διεκπεραίωση των εργασιών που αναφέρονται στα σενάρια από εξειδικευμένο προσωπικό ή/και τελικούς χρήστες. Η εργασία συνεχίζεται και κατά την περίοδο ελεγχόμενης παραγωγικής λειτουργίας. Τα ευρήματα της εκτέλεσης των σεναρίων ελέγχου αξιολογούνται συνεχώς και ακολουθεί σύνταξη αναφορών εκτέλεσης, η οποία προωθείται ως ανάδραση στον ανάδοχο του υποέργου προμήθειας του Ψηφιακού Αποθετηρίου για την αντιμετώπιση σοβαρών θεμάτων.

Η τελική αναφορά εκτέλεσης των σεναρίων ελέγχου αποτυπώνει τη διαδικασία, τα ευρήματα, τα αποτελέσματα των εργασιών και την αξιολόγηση του συστήματος ως προς την κάλυψη των σεναρίων αυτών.

2.4 Υποσυστήματα

Κύριο αντικείμενο ελέγχου αποτελεί το λογισμικό του ψηφιακού αποθετηρίου το οποίο προμηθεύει στο φορέα ανάδοχος. Οι ακριβείς προδιαγραφές αυτού δεν είναι γνωστές κατά τη συγγραφή της παρούσας καθώς καθορίζονται από την προσφορά του αναδόχου ο οποίος εξειδικεύει τις προδιαγραφές της σχετικής διακήρυξης.

Το ενδιάμεσο αποθετήριο, το οποίο θα τροφοδοτήσει αρχικά το κύριο αποθετήριο, υλοποιείται ως λογισμικό πάνω σε μια σειρά προϋπαρχόντων συστημάτων, τα οποία είναι τα παρακάτω:

- LifeRay
- Fedora Commons
- PostgreSQL
- Apache Tomcat
- Apache httpd

Τα υποσυστήματα αυτά δεν αντιμετωπίζονται αυτόνομα και άμεσα, αλλά έμμεσα μέσω του συνολικού ελέγχου του συστήματος.

3 Μεθοδολογία ελέγχων – Διεθνείς Πρακτικές

3.1 Στόχοι και προτεραιότητες

Το Ψηφιακό Αποθετήριο είναι ένα σύνολο υποσυστημάτων που στοχεύει στην παροχή υπηρεσιών σε εκπαιδευτικούς, μαθητές, φοιτητές και γενικότερα στους πολίτες. Ως εκ τούτου, πέραν της επιχειρησιακής λογικής, το σύστημα διαχειρίζεται, αποθηκεύει και διακινεί ένα μικρό πλήθος προσωπικών δεδομένων πολιτών (πχ στοιχεία επικοινωνίας, κοινωνικής δικτύωσης, σχόλια κλπ), όμως δεν διαχειρίζεται διαβαθμισμένες πληροφορίες.

Για τους λόγους αυτούς οι έλεγχοι αποδοχής με βάση και το αντικείμενο του έργου αφορούν:

➤ Σενάρια Ελέγχου Μετάπτωσης

- Έλεγχος της ευχρηστίας και αποδοχής του συστήματος από τους τελικούς χρήστες, καθώς είναι πολύ σημαντική παράμετρος για την επιτυχία και την επίτευξη των στόχων του οργανισμού.
- Έλεγχος για τυχόν κενά ασφαλείας που θα μπορούσαν να έχουν επίπτωση στην ακεραιότητα, εμπιστευτικότητα και ασφάλεια των δεδομένων.

➤ Σενάρια Ελέγχου Προσαρμογών – Παραμετροποιήσεων

- Έλεγχος της ποιότητας του κώδικα των εφαρμογών που αναπτύχθηκαν. Η ποιότητα του κώδικα είναι σημαντική για την απόδοση και ασφάλεια του συστήματος αλλά και για την επεκτασιμότητα αυτού
- Έλεγχος για τυχόν σφάλματα λογισμικού ή ελαττώματα (πχ κενά λογικής) που θα μπορούσαν να έχουν επίπτωση στην ακεραιότητα, εμπιστευτικότητα και ασφάλεια των δεδομένων.

➤ Σενάρια ελέγχου Web Services

- Έλεγχος για τυχόν κενά ασφαλείας που θα μπορούσαν να έχουν επίπτωση στην ακεραιότητα, εμπιστευτικότητα και ασφάλεια των δεδομένων.

➤ Σενάρια ελέγχου εξοπλισμού

- Έλεγχος του συστήματος ως προς την εγκατάσταση και συμβατότητά του με το υλικό στο οποίο έχει εγκατασταθεί.

➤ Σενάρια ελέγχου δικαιωμάτων χρηστών

- Έλεγχος της κάλυψης των επιχειρησιακών απαιτήσεων του συστήματος τόσο ως προς τις αρχικές απαιτήσεις του έργου όσο και ως προς τη λογική αυτών και πιθανών σφαλμάτων που μπορεί να υπήρξαν σε αυτές και τα οποία θα έπρεπε να ληφθούν υπόψη.

Οι έλεγχοι αποδοχής έχουν ως στόχο τη διασφάλιση ότι το ελεγχόμενο πληροφοριακό σύστημα ικανοποιεί τις ορισθέντες απαιτήσεις και τους επιχειρησιακούς στόχους του έργου και γενικότερα του φορέα.

Η διάρκεια εκτέλεσης των ελέγχων προτείνεται να είναι **δύο (2) μήνες** και βασική προτεραιότητά τους είναι ο έλεγχος της λειτουργικότητας και των υποστηριζόμενων διαδικασιών του πληροφοριακού συστήματος, η ασφάλεια και η απόδοσή αυτού.

3.2 Προσέγγιση Σχεδιασμού Δοκιμών και Αξιολόγησης

3.2.1 Προσέγγιση Ελέγχου Μετάπτωσης

Τα παρακάτω επίπεδα θεωρούνται απαραίτητα όσον αφορά τον έλεγχο της μετάπτωσης.

- **Συμφωνία/ταύτιση δεδομένων μετάπτωσης.** Στον έλεγχο αυτό θα πρέπει να γίνει καταμέτρηση με αυτοματοποιημένο τρόπο των δεδομένων στην πηγή και στην εφαρμογή στόχο. Η καταγραφή η οποία μπορεί, εφόσον το επιτρέπει η εφαρμογή πηγή, να προβλέπει και checksums θα πρέπει να γίνει σε κάθε επίπεδο στοιχείων (πίνακες) και επιχειρησιακή λειτουργία.
- **Δοκιμή μετρικών από την εφαρμογή πηγή στην εφαρμογή στόχο.** Εφόσον υπάρχει η δυνατότητα (ενδεχομένως με απλές τροποποιήσεις), προτείνεται η αναζήτηση μετρικών για τα ίδια μεγέθη από την παλιά και τη νέα εφαρμογή. (Πχ. Αριθμός Δημοτών, Αριθμός δημοτολογίων, Αριθμός μεταδημοτεύσεων σε συγκεκριμένη χρονική περίοδο, κλπ.).
- **Λειτουργική/Επιχειρησιακή συμβατότητα των δεδομένων μετάπτωσης.** Στη διάρκεια λειτουργίας του νέου συστήματος, προτείνεται η παράλληλη (εργαστηριακή) λειτουργία του παλαιού συστήματος, εφόσον είναι υπαρκτό για ένα διάστημα πχ. ενός μηνός. Στη διάρκεια αυτή θα γίνει έλεγχος και αντιπαραβολή των συγκεντρωτικών καταστάσεων και από τα δύο συστήματα.

3.2.2 Προσέγγιση Ελέγχου Υπάρχοντος Λογισμικού

Η προσέγγιση που θα ακολουθηθεί για τις δοκιμές των εφαρμογών που θα εγκαταστήσει η ομάδα εργασίας είναι αυτές που αφορούν σε ελέγχους και δοκιμές υπάρχοντος λογισμικού, δηλαδή εμπορικά διαθέσιμου off-the-shelf λογισμικού (COTS-Commercial-Off-The-Shelf) λύσης.

Ως εκ τούτου δεν θα ελεγχθεί η ακρίβεια αποτύπωσης των διαδικασιών που αποτυπώνονται στο λογισμικό, ούτε ο τρόπος ανάπτυξής του και οι δυνατότητες αυτών που το ανέπτυξαν, καθώς τα παραπάνω έχουν είτε ήδη ελεγχθεί είτε τυχόν λάθη έχουν διορθωθεί στις διάφορες φάσεις ανάπτυξης του λογισμικού. Συνεπώς, θέματα όπως η ακρίβεια του σχεδιασμού, η διαχείριση κινδύνων που ενσωματώνονται στο λογισμικό, η ωριμότητα και ο κύκλος ζωής ανάπτυξης του λογισμικού και η διαχείριση των δεδομένων από την εφαρμογή δεν θα μελετηθούν.

Το πλαίσιο ελέγχου και δοκιμών θα εστιάσει στις παρακάτω βασικές κατηγορίες:

1. Έλεγχος Πηγαίου Κώδικα
2. Δομικός Έλεγχος
3. Λειτουργικός Έλεγχος
4. Στατιστικός Έλεγχος
5. Έλεγχος Αντοχής
6. Έλεγχος Παλινδρόμησης (Regression Testing)

Οι ρόλοι και η σύσταση της ομάδας ελέγχου παρουσιάζονται στο Κεφάλαιο 5. Στο σημείο αυτό συνοψίζεται η συμμετοχή τους και τα χαρακτηριστικά τους:

	Έλεγχος Στοιχείων Προγράμματος	Έλεγχος Πακέτου	Έλεγχος Προγράμματος	Έλεγχος Υποσυστήματος	Έλεγχος Συστήματος
Μηχανικός Λογισμικού	ΝΑΙ	ΝΑΙ	ΙΣΩΣ	-	-
Υπεύθυνος Λογισμικού	ΙΣΩΣ	ΝΑΙ	ΝΑΙ	ΙΣΩΣ	ΙΣΩΣ
Τελικός Χρήστης				ΝΑΙ	ΝΑΙ
Ανεξάρτητος Ελεγκτής	ΙΣΩΣ	ΙΣΩΣ	ΝΑΙ	ΝΑΙ	ΝΑΙ

Οι παραπάνω ρόλοι διανέμονται στα ακόλουθα επίπεδα ελέγχου και δοκιμών:

	Μηχανικός Λογισμικού	Υπεύθυνος Λογισμικού	Τελικός Χρήστης	Ανεξάρτητος Ελεγκτής
Έλεγχος Πηγαίου Κώδικα	ΝΑΙ	ΙΣΩΣ		ΙΣΩΣ
Δομικός Έλεγχος	ΝΑΙ	ΝΑΙ		ΙΣΩΣ
Λειτουργικός Έλεγχος	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ

Στατιστικός Έλεγχος		ΙΣΩΣ	ΝΑΙ	ΝΑΙ
Έλεγχος Αντοχής	ΙΣΩΣ	ΝΑΙ	ΝΑΙ	ΝΑΙ
Έλεγχος Παλινδρόμησης	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ

3.2.2.1 Επιλογή Ελέγχων και Δοκιμών

Συνήθως ο έλεγχος ενός έτοιμου λογισμικού γίνεται στα πλαίσια μιας ευρύτερης διαδικασίας όπως ισχύει και στην προκείμενη περίπτωση.

Οι τυχόν ανάγκες για νέες εκδόσεις που θα προκύψουν από την εξέταση του προϊόντος στα πλαίσια των δοκιμών αποδοχής, θα εξετασθούν στα πλαίσια του κύκλου ζωής του προϊόντος. Αναμένεται ότι καθώς το προϊόν είναι εμπορικά διαθέσιμο για αρκετό χρονικό διάστημα, όσο πιο κρίσιμο είναι τυχόν θέμα που θα προκύψει από την δοκιμή αποδοχής, τόσο πιο πιθανό είναι, είτε να έχει δρομολογηθεί είτε να βρίσκεται στη φάση διόρθωσης σε εργαστηριακό επίπεδο.

Συμπερασματικά, εφόσον το προϊόν είναι καθιερωμένο έτοιμο, οι λειτουργίες του είναι προδιαμορφωμένες και (συνήθως) ποιοτικά ελεγμένες. Ως εκ τούτου, οι δοκιμές θα πρέπει να εστιασθούν σε καλά αλλά στενά καθορισμένες ιδιαίτερες λειτουργίες ή χαρακτηριστικά του.

Θέματα που δεν χαρακτηρίζονται κρίσιμα ή δεν προκύπτουν από την άμεση λειτουργία του προγράμματος μπορούν να ενταχθούν στο γενικότερο πλαίσιο αλλαγών και διορθώσεων που προβλέπεται.

Στο πίνακα που ακολουθεί παρουσιάζονται ενδεικτικά επιλογές ελέγχου με τα απαραίτητα δεδομένα και το εύρος ελέγχου. Αναλυτικά θα περιγραφούν στα παραρτήματα.

Επίπεδο Ελέγχου	Στόχος	Απαιτήσεις Πληροφορίας	Εύρος Ελέγχου και Ανάλυσης	Παράδειγμα
ΔΟΜΙΚΟΣ ΕΛΕΓΧΟΣ				
Ροή δεδομένων	Έλεγχος εσωτερικής ροής δεδομένων προγραμμάτων	Πηγαίος Κώδικας ή Λειτουργικές Προδιαγραφές	Επίπεδο εφαρμογής	
Βρόγχοι προγραμμάτων	Εσωτερικές λειτουργίες	Πηγαίος Κώδικας ή Λειτουργικές	Όρια επαναληπτικών	



Επίπεδο Ελέγχου	Στόχος	Απαιτήσεις Πληροφορίας	Εύρος Ελέγχου και Ανάλυσης	Παράδειγμα
	δομικών στοιχείων	Προδιαγραφές	λειτουργιών	
Ροή πληροφορίας	Έλεγχος συνεργασίας μεταξύ προγραμμάτων	Πηγαίος Κώδικας ή Λειτουργικές Προδιαγραφές	Όρια εφαρμογών	
Λογική εφαρμογών	Έλεγχος Εσωτερικής λογικής εφαρμογών	Πηγαίος Κώδικας ή Λειτουργικές Προδιαγραφές	Όλοι οι συνδυασμοί των ανωτέρω	
ΛΕΙΤΟΥΡΓΙΚΟΣ ΕΛΕΓΧΟΣ				
Transactions προγραμμάτων	Έλεγχος υλοποίησης εφαρμογών	Εκτελέσιμος Κώδικας, Απαιτήσεις λογισμικού	Έλεγχος transactions	§ 6.2.2.1
Εύρος δεδομένων	Έλεγχος λειτουργιών σε δεδομένα εισόδου	Εκτελέσιμος Κώδικας/Απαιτήσεις λογισμικού	Έλεγχος δυνατών τιμών εισόδου με οριακές τιμές ή μη αποδεκτές τιμές	§ 6.2.2.2
Σύνταξη προγράμματος	Έλεγχος διεπαφών χρήστη και μηνυμάτων	Εκτελέσιμος Κώδικας /Απαιτήσεις λογισμικού	Έλεγχος όλων των μηνυμάτων χρήστη	§ 6.2.2.3
Λογική Προγράμματος	Έλεγχος σε πραγματικό περιβάλλον χρήστη	Εκτελέσιμος Κώδικας /Απαιτήσεις λογισμικού	Έλεγχος σε συνδυασμό επιλογών πραγματικού χρήστη	§ 6.2.2.4
Κατάσταση Προγράμματος	Έλεγχος Καταστάσεων Προγράμματος	Εκτελέσιμος Κώδικας /Απαιτήσεις λογισμικού	Έλεγχος όλων των δυνατών καταστάσεων	§ 6.2.2.5

Επίπεδο Ελέγχου	Στόχος	Απαιτήσεις Πληροφορίας	Εύρος Ελέγχου και Ανάλυσης	Παράδειγμα
	σε συνδυασμό με άλλες εφαρμογές		για τις εφαρμογές	
ΣΤΑΤΙΣΤΙΚΟΣ ΕΛΕΓΧΟΣ				
Αξιοπιστία	Εκτίμηση αξιοπιστίας	Εκτελέσιμος Κώδικας /Απαιτήσεις λογισμικού/ Λειτουργικές Απαιτήσεις	Προκαθορισμός στόχων αξιοπιστίας	§ 6.2.3.1
ΕΛΕΓΧΟΣ ΑΝΤΟΧΩΝ				
Αντοχή εφαρμογών	Έλεγχος ευρωστίας	Εκτελέσιμος Κώδικας /Απαιτήσεις λογισμικού	Αντοχή ανά πόρο συστήματος ανά επίπεδο λειτουργίας	§ 6.2.4.1
Υποβάθμιση εφαρμογών	Έλεγχος επιπέδου υποβάθμισης εφαρμογών	Εκτελέσιμος Κώδικας /Απαιτήσεις λογισμικού	Υποβάθμιση ανά πόρο ανά επίπεδο λειτουργίας	§ 6.2.4.1
Μηχανισμοί Ανάκτησης εφαρμογών	Έλεγχος σημείων κατάρρευσης – Μηχανισμών ανάκτησης	Εκτελέσιμος Κώδικας /Απαιτήσεις λογισμικού	Συνεχής έλεγχος πόρων μέχρι σημείου κατάρρευσης /ανάκτησης	§ 6.2.4.2
ΕΛΕΓΧΟΣ ΠΑΛΙΝΔΡΟΜΗΣΗΣ				
	Έλεγχος επίδρασης αλλαγών στο λογισμικό	Διάφορα επίπεδα και είσοδοι	Έλεγχος μέχρι μηδενικού επιπέδου νέων σφαλμάτων	§ 6.2.5.1

3.2.2.2 Ορθότητα λειτουργίας εφαρμογών

Σκοπός των ελέγχων αυτών είναι αρχικά η επαλήθευση της κάλυψης της επιχειρησιακής λογικής που ζητείται από τον οργανισμό βάσει των προδιαγραφών του πληροφοριακού συστήματος και εν συνεχεία ο έλεγχος της πληρότητας αυτών. Οι έλεγχοι αυτοί βασίζονται τόσο στην ανάλυση της τεκμηρίωσης των εφαρμογών όσο και σε δοκιμές ελέγχου αυτού για το βαθμό κάλυψης των προδιαγραφών και της επίτευξης των στόχων του έργου.

3.2.2.3 Ευχρηστία

Η ευχρηστία, όπως αναφέρεται και στο ISO9126, αφορά στην προσπάθεια που απαιτείται για τη χρήση του συστήματος από πλευράς ευκολίας χρήσης και ευκολίας εκμάθησης. Ο έλεγχος της ευχρηστίας ενός συστήματος είναι μια τεχνική δοκιμής μαύρου κουτιού. Η ευχρηστία του συστήματος είναι βασικός παράγοντας της επιτυχίας του. Είναι σημαντικό να ελεγχθούν οι παρεχόμενες υπηρεσίες μέσω διαδικτύου καθώς η επιτυχία του εξαρτάται σε πολύ μεγάλο βαθμό από την αποδοχή που θα έχει από τους τελικούς χρήστες, καθώς η μη αποδοχή από μέρους τους θα σημάνει τη μη επίτευξη του γενικότερου στόχου του έργου.

Στην ευχρηστία μπορούν να συνεισφέρουν η ολοκλήρωση κάθε διαδικασίας με τα ελάχιστα δυνατά βήματα, η καθοδήγηση του χρήστη σε κάθε βήμα με κατάλληλα σημεία βοήθειας και πληροφόρησης, εμφανείς επιλογές και δυνατότητες σε κάθε βήμα καθώς και η ύπαρξη αναλυτικών και επεξηγηματικών μηνυμάτων.

Επίσης θα πρέπει να ελεγχθεί τήρηση διεθνών προτύπων προσβασιμότητας για χρήση των υπηρεσιών από ΑμεΑ αλλά και η κάλυψη προτύπων διαδικτυακών διεπαφών.

3.2.2.4 Απόδοση

Η απόδοση ενός συστήματος προσδιορίζεται σε σχέση με προκαθορισμένους στόχους και μη-λειτουργικές απαιτήσεις. Οι σημαντικότεροι παράγοντες που καθορίζουν την απόδοση ενός συστήματος είναι ο χρόνος απόκρισης, η κατανομή και η αποδοτική χρήση των πόρων του, η συχνότητα των λαθών και ο ρυθμός λήψης δεδομένων και παραγωγής αποτελεσμάτων.

Τα αποτελέσματα των ελέγχων απόδοσης μπορούν να χρησιμεύσουν και στην επαλήθευση άλλων ποιοτικών χαρακτηριστικών του συστήματος όπως η επεκτασιμότητα, η αξιοπιστία και η χρήση πόρων.

3.2.2.5 Ασφάλεια

Η ασφάλεια αποτελεί βασικό στοιχείο ενός πληροφοριακού συστήματος και αν δεν είναι επαρκής μπορεί να καταστεί μη λειτουργικό. Η ασφάλεια αφορά την ικανότητά του να προφυλάσσεται από μη εξουσιοδοτημένη πρόσβαση σε εφαρμογές ή δεδομένα, είτε αυτή είναι ακούσια είτε εσκεμμένη καθώς και να εξασφαλίζει τη συνέχεια της λειτουργίας του μετά από ακούσιες ή εκούσιες καταστροφές. Συνεπώς πρέπει να ελεγχθεί για την πρόβλεψη και ικανότητα



να παρέχει τον επιθυμητό βαθμό ασφάλειας καθώς και τους απαραίτητους μηχανισμούς για εύρεση και ενημέρωση σχετικά με ενέργειες που επηρεάζουν την ασφάλεια αυτού. Επίσης πρέπει να ελεγχθεί η ικανότητα ανάκαμψης από αστοχίες/καταστροφές.

Για λόγους ευχρηστίας αλλά και διαθέσιμου εξοπλισμού μπορεί να θυσιαστεί μέρος της ασφάλειας του συστήματος, καθώς συχνά έρχονται σε αντίθεση με την ασφάλεια, αλλά πρέπει πάντα να παρέχεται ένα αποδεκτό επίπεδο ασφαλείας βάσει των αγαθών που διαχειρίζεται το υπό έκθεση σύστημα και της αξίας αυτών. Βάσει του ότι οι εφαρμογές διαχειρίζονται οικονομικά δεδομένα και προσωπικά δεδομένα πολιτών και επιχειρήσεων, θα πρέπει να δοθεί μεγάλη σημασία στην ασφάλεια τους.

Μέσω της ασφαλείας επιδιώκεται η εμπιστευτικότητα και η ακεραιότητα των δεδομένων και η ανάκαμψη από αστοχίες υλικού ή άλλες καταστροφές. Ένας επιπρόσθετος στόχος της ασφαλείας ενός συστήματος είναι η κατά το δυνατόν καλύτερη επίτευξη αδιάλειπτης παροχής υπηρεσιών (μη-άρνησης παροχής υπηρεσίας), λαμβάνοντας υπόψη ότι είναι πρακτικά αδύνατον να επιτευχθεί σε περίπτωση επιθέσεων μεγάλης ισχύος ή υπερβολικά μεγαλύτερου φόρτου από τον αναμενόμενο.

Η ακεραιότητα αφορά την προστασία από μη εξουσιοδοτημένη τροποποίηση δεδομένων του συστήματος, τόσο κατά τη μεταφορά όσο και κατά την αποθήκευση. Αφορά τον έλεγχο κάθε περίπτωσης πρόσβασης ή εμπιστοσύνης στο επίπεδο που μπορεί να εξασφαλίσει ότι η διαδικασία αλληλεπίδρασης και η πρόσβαση στα αγαθά έχει τέλος και δεν μπορούν να υποστούν διαφθορά, να συνεχιστούν, να ανακατευθυνθούν, ή να αναιρεθούν χωρίς τη γνώση των εμπλεκόμενων μερών. Είναι απαραίτητη η εξασφάλιση της ακεραιότητας τόσο στα σημεία αποθήκευσης (σύστημα διαχείρισης βάσεων δεδομένων, αποθηκευτικά μέσα κλπ) όσο και κατά τη μεταφορά τους από άκρο σε άκρο. Πολύ σημαντικός είναι ο έλεγχος για ανεπάρκειες ακεραιότητας όπου χρησιμοποιούνται καταγεγραμμένες διαδικασίες, υπογραφές, κρυπτογράφηση, κατακερματισμός, για εξασφάλιση ότι το αγαθό δεν μπορεί να αλλαχθεί, συνεχιστεί, ανακατευθυνθεί, παρακρατηθεί, χωρίς να το γνωρίζουν τα εμπλεκόμενα μέρη.

Η ασφάλεια του πληροφοριακού συστήματος δεν εξαρτάται καθαρά και μόνο από την υλοποίηση της εφαρμογής αλλά και από την παραμετροποίηση του περιβάλλοντος στο οποίο θα λειτουργήσει, οπότε και είναι μέρος των ελέγχων που θα πραγματοποιηθούν.

Πρέπει να επισημανθεί ότι, πέραν των θεμάτων που αφορούν στην υλοποίηση και εγκατάσταση ενός πληροφοριακού συστήματος, σημαντικό ρόλο στην ασφάλεια του παίζει και ο ανθρώπινος παράγοντας, που σημαίνει ότι θα πρέπει ο κάθε οργανισμός να ορίζει συγκεκριμένες διαδικασίες που θα πρέπει να τηρούνται από το προσωπικό σχετικά με την ασφάλεια των πληροφοριακών συστημάτων, καθώς και να φροντίσει για την συνεχή ενημέρωση του προσωπικού σχετικά με ζητήματα ασφαλείας.



3.3 Επίπεδα αξιολόγησης

3.3.1 Εργοστασιακές δοκιμές αποδοχής (FAT)

Οι εργοστασιακές δοκιμές αφορούν στον έλεγχο των διακριτών υποσυστημάτων που αποτελούν το σύστημα του Ψηφιακού Αποθετηρίου όσον αφορά στα ελαττώματά τους στον χειρισμό των δεδομένων εισόδου τους, ανοχή σε σφάλματα καθώς και ελέγχους απόδοσης τόσο σε κανονική λειτουργία όσο και σε κατάσταση αυξημένου φόρτου.

Οι έλεγχοι αυτοί δεν στοχεύουν στην δοκιμασία πρώτου και δευτέρου επιπέδου του συστήματος (alpha και betatesting), οι οποίοι και είναι ευθύνη του αναδόχου κατά την φάση της ανάπτυξης του συστήματος αλλά, όπως ήδη αναφέρθηκε, πρόκειται για τελικούς ελέγχους σε επίπεδο διακριτού υποσυστήματος που αφορούν:

- Έλεγχο απαιτήσεων
- Έλεγχο προδιαγραφών
- Έλεγχο ανοχής σε σφάλματα,
- Έλεγχο εύρεσης ελαττωμάτων
- Έλεγχο απόδοσης και stresstest
- Πρωτογενή έλεγχο ευχρηστίας (ο βασικός εκτελείται στο περιβάλλον λειτουργίας)

Ο έλεγχος των απαιτήσεων αφορά τη συμβατότητα του πληροφοριακού συστήματος βάσει των τεχνικών προδιαγραφών του με τον εξοπλισμό στον οποίο θα εγκατασταθεί και τα υφιστάμενα συστήματα με τα οποία θα συνεργάζεται ή θα μοιράζεται το ίδιο υλικό. Τυχόν προβλήματα σε αυτούς τους ελέγχους είναι κρίσιμα για τη λειτουργία του συστήματος.

Ο έλεγχος των προδιαγραφών αφορά την πλήρη κάλυψη των προδιαγραφών του έργου και σε εργαστηριακό επίπεδο γίνεται σε δύο φάσεις. Η πρώτη φάση αφορά στην κάλυψη αυτών σε σχέση με τις προδιαγραφές που αναφέρονται στο υλικό τεκμηρίωσης του συστήματος και σε η δεύτερη φάση στον έλεγχο της πραγματικής παροχής αυτών μέσω των διεπαφών που παρέχονται. Μέσω της δεύτερης φάσης εκτός του ελέγχου της κάλυψης των προδιαγραφών πραγματοποιείται επίσης και πρωτογενής έλεγχος της ευχρηστίας του συστήματος.

Οι έλεγχοι ανοχής σε σφάλματα είναι πολύ σημαντικοί τόσο για την αξιοπιστία του πληροφοριακού συστήματος όσο και για την επιχειρησιακή συνέχεια του οργανισμού. Αποτυχία στους ελέγχους αυτούς θα μπορούσε να σημαίνει ότι το σύστημα δεν πληροί το σκοπό του, ασχέτως αν δεν ήταν σαφώς καταγεγραμμένο σαν απαίτηση του οργανισμού. Στους ελέγχους αυτούς δοκιμάζεται η ικανότητα του συστήματος να ανταπεξέρχεται σε σφάλματα υποσυστημάτων, περιβάλλοντος λειτουργίας και δεδομένων εισόδου. Οι έλεγχοι αυτοί βασίζονται τόσο στην ανάλυση της τεκμηρίωσης της αρχιτεκτονικής του συστήματος του Ψηφιακού Αποθετηρίου όσο και σε πρακτικές δοκιμές. Ελέγχονται περιπτώσεις μοναδικών σημείων σφάλματος, σημείων επαναφοράς από σφάλμα, διαδικασίες ανίχνευσης και περιορισμού σφάλματος. Επίσης πολύ σημαντική είναι η ικανότητα του συστήματος να



επανέρχεται σε κατάσταση κανονικής λειτουργίας χωρίς απώλεια δεδομένων και λειτουργικότητας, και σε σύντομο χρονικό διάστημα.

Άλλο ένα πολύ σημαντικό τμήμα των ελέγχων αποδοχής είναι ο έλεγχος εύρεσης ελαττωμάτων. Ελέγχεται η ακρίβεια της εφαρμογής, δηλαδή η απόκριση των υποσυστημάτων του σε ορθές και εσφαλμένες παραμέτρους εισόδου, και προβλήματα στην υλοποίηση της ασφάλειάς του. Γενικότερα αφορά στην ανίχνευση σφαλμάτων ή ατελειών του λογισμικού κατά τις οποίες η συμπεριφορά του είναι εσφαλμένη ή σε ασυμφωνία με τις προδιαγραφές του, την τεκμηρίωσή του και τις συνήθειες πρακτικές.

Ο έλεγχος απόδοσης και οι δοκιμές καταπόνησης (stresstests) του συστήματος αφορούν τους χρόνους απόκρισης του συστήματος στην εκτέλεση διαφόρων αιτημάτων τόσο σε συνθήκες αναμενόμενου φόρτου λειτουργίας όσο και σε συνθήκες βεβαρυμμένης λειτουργίας. Η απόδοση ενός πληροφοριακού συστήματος μπορεί να επηρεάσει και την ευχρηστία αυτού καθώς αν παρουσιάσει σημαντική καθυστέρηση τότε καθίσταται μη εύχρηστο και μη λειτουργικό.

3.3.1.1 Δημιουργία υποδομής δοκιμών

Για το σκοπό των εργαστηριακών ελέγχων η ομάδα εργασίας θα δημιουργήσει εξομοίωση του περιβάλλοντος λειτουργίας σε εναλλακτική υποδομή. Η βάση θα περιέχει κατάλληλα εικονικά δεδομένα που δεν θα περιέχουν ευαίσθητα δεδομένα. Αυτό μπορεί να γίνει με μαζική μεταβολή, από την ομάδα εργασίας, των ονομάτων, διευθύνσεων και λοιπών ευαίσθητων δεδομένων που θα περιέχονται σε βάση παραγωγής και η οποία θα χρησιμοποιηθεί για το σκοπό αυτό. Σημειώνεται ότι το σύστημα περιέχει ελάχιστα δεδομένα τα οποία μπορούν να κριθούν ως ευαίσθητα, πλην όμως και αυτά θα πρέπει να διασφαλιστούν.

Η υποδομή θα πρέπει να εξομοιώνει το σύνολο του συστήματος, το οποίο συνεπάγεται ότι θα πρέπει να υπάρξει μεταφορά και υφιστάμενων συστημάτων με τα οποία είναι απαραίτητη η διασύνδεση του συστήματος για την ομαλή λειτουργία του ή για τον έλεγχο των αποτελεσμάτων των ενεργειών του, εφόσον αυτές επηρεάζουν τα διασυνδεδεμένα συστήματα.

3.3.1.2 Δεδομένα εισόδου δοκιμών

Θα πρέπει να παραχθούν από την ομάδα εκπόνησης των σεναρίων ελέγχου, πίνακες πραγματικών δεδομένων εισόδου που να εγκριθούν από την ομάδα εργασίας και οι οποίοι θα περιέχουν τόσο σωστές όσο και λανθασμένες τιμές. Τα δεδομένα αυτά θα αποτελούνται από τις παραμέτρους εισόδου των προγραμματιστικών διεπαφών των υποσυστημάτων και θα δοθούν ως είσοδοι σε αυτές με αυτοματοποιημένες μεθόδους που θα δημιουργήσει η ομάδα ειδικά για το σκοπό αυτό. Τα δεδομένα αυτά θα πρέπει να περιέχουν τόσο εγγραφές με σωστό πλήθος ορισμάτων ανά προγραμματιστική διεπαφή και σωστά ή εσφαλμένα στοιχεία (κωδικός χρήστη, κωδικός ενέργειας, κλπ) όσο και με εσφαλμένο πλήθος ορισμάτων (λιγότερα και περισσότερα απ' τα αναμενόμενα ορίσματα). Επίσης θα πρέπει να περιέχονται περιπτώσεις με λανθασμένες



τιμές αναφορικά με το αναμενόμενο εύρος τιμών των παραμέτρων των προγραμματιστικών διεπαφών ή διεπαφών χρήστη.

Η εκτέλεση αυτών θα πρέπει πραγματοποιηθεί μαζικά και πολλές φορές για κάθε περίπτωση, ώστε εκτός της ορθότητας της λειτουργίας να μπορεί να ελεγχθεί η απόκριση του συστήματος από τα αρχεία καταγραφής και η λειτουργία αυτού σε περιπτώσεις αυξημένου φόρτου.

Θα πρέπει επίσης να γίνει δοκιμή των διεπαφών χρήστη του συστήματος με βάση τα δεδομένα αυτά ώστε να γίνουν οι αντίστοιχοι έλεγχοι της λειτουργικότητας μέσω των διεπαφών χρήστη καθώς και πρωτογενής έλεγχος ευχρηστίας του συστήματος.

Οι έλεγχοι μέσω διεπαφών χρήστη θα γίνουν από έμπειρους χρήστες και εκτός των ελέγχων βάσει σεναρίων θα πρέπει να πραγματοποιηθούν και ελεύθεροι έλεγχοι τόσο για περιπτώσεις κενών ασφαλείας όσο και για προβλήματα λειτουργικότητας που μπορούν να διαφύγουν από τα τυποποιημένα σενάρια ελέγχου.

3.3.1.3 Εξωτερικές υπηρεσίες

Καθώς το σύστημα υποστηρίζει τη σύνδεση με εξωτερικές υπηρεσίες, όπως πχ το ψηφιακό αποθετήριο και κοινωνικά δίκτυα, για την ολοκλήρωση των υπηρεσιών του, θα πρέπει για τους σκοπούς του ελέγχου να προσομοιώνει τις υπηρεσίες αυτές ή να συνδέεται με εναλλακτικές υπηρεσίες αν αυτές δεν είναι διαθέσιμες. Αυτό είναι απαραίτητο ώστε να ελεγχθούν οι διεπαφές που πραγματοποιούν την διασύνδεση με αυτές τις εξωτερικές υπηρεσίες.

3.3.2 Δοκιμές αποδοχής σε περιβάλλον λειτουργίας (SAT)

Οι δοκιμές αποδοχής σε περιβάλλον λειτουργίας (κατ' αναλογία της λειτουργίας σε περιβάλλον τελικού χρήστη κατά τις διαδικασίες ελέγχου λογισμικού παραδιδόμενου σε τρίτους) επικεντρώνονται κατά κύριο λόγο στο περιβάλλον χρήστη και αφορούν τα παρακάτω κριτήρια αξιολόγησης:

- έλεγχο για ανοχή σε σφάλματα
- έλεγχο εύρεσης ελαττωμάτων
- έλεγχο ευχρηστίας
- έλεγχο απόδοσης

Ο έλεγχος για ανοχή σε σφάλματα αφορά τον έλεγχο από έμπειρους χρήστες για την απόκριση του συστήματος σε εσφαλμένα στοιχεία εισόδου όπως εσφαλμένες τιμές και τιμές εκτός ορίων καθώς και στην δυνατότητα ανάκαμψης του συστήματος από καταστάσεις αστοχίας/καταστροφής όπως πτώση εξυπηρετητή διαδικτύου, διακοπή δικτύου, διακοπή παροχής υπηρεσίας υποσυστήματος κλπ.

Ο έλεγχος εύρεσης ελαττωμάτων πραγματοποιείται τόσο από έμπειρους χρήστες και τεχνικούς υποστήριξης που ελέγχουν σχετικά με ελαττώματα υλοποίησης όσο και από απλούς χρήστες σχετικά με κενά λογικής που παρατηρούν κατά την πραγματοποίηση των ελέγχων ευχρηστίας.

Ο έλεγχος ευχρηστίας πραγματοποιείται από απλούς χρήστες και αφορά προσχεδιασμένα σενάρια και την ευκολία υλοποίησής τους, την καθοδήγηση που προσφέρει το σύστημα και το αν κρίνονται κατανοητά και επεξηγηματικά τα μηνύματα του συστήματος σε περιπτώσεις επιλογών, λαθών, κλπ.

Ο έλεγχος της απόδοσης αφορά την απόκριση του συστήματος βάσει των αρχείων καταγραφής (logs) κατά την υλοποίηση των παραπάνω δοκιμών.

3.3.2.1 Δημιουργία υποδομής δοκιμών

Για την υλοποίηση των δοκιμών σε περιβάλλον λειτουργίας θα γίνει ακριβές αντίγραφο των απαιτούμενων δεδομένων για τις δοκιμές του συστήματος της Ψηφιακού Αποθετηρίου, σε εναλλακτικό χώρο του φορέα, ώστε να δοκιμαστεί το σύστημα με πραγματικά δεδομένα.

3.3.2.2 Δεδομένα εισόδου δοκιμών

Θα πρέπει να παραχθούν δεδομένα εισόδου τα οποία να έχουν σωστές (valid) και εσφαλμένες (invalid) τιμές. Θα πρέπει τα δεδομένα να αφορούν όλα τα υποσυστήματα και να καλύπτουν όλα τα δεδομένα που απαιτούνται για τον πλήρη έλεγχο κάθε υποσυστήματος αλλά και του συστήματος συνολικά. Τα δεδομένα θα πρέπει να περιλαμβάνουν τόσο χρήστες που περιέχουν δεδομένα σε όλα τα διασυνδεδεμένα υποσυστήματα, όσο και χρήστες που δεν υπάρχουν στα διασυνδεδεμένα υποσυστήματα. Επίσης θα πρέπει να περιλαμβάνουν ορθά στοιχεία, τέτοια ώστε να μπορεί να ελεγχθεί το σύνολο των παρεχόμενων υπηρεσιών του συστήματος, καθώς και λάθος στοιχεία ώστε να ελεγχθεί η απόκριση του συστήματος σε εσφαλμένες εισόδους και η απόκριση και καθοδήγηση που προσφέρει προς τους χρήστες. Εσφαλμένα στοιχεία θα μπορούσαν να είναι η χρήση λάθος ονόματος χρήστη ή κωδικού πρόσβασης, εσφαλμένα στοιχεία στα πεδία καταχώρησης μιας φόρμας, μη συμπλήρωση υποχρεωτικών πεδίων, εσφαλμένη τιμή σε αριθμητικά πεδία (πχ αρνητική ηλικία), κ.α.

3.3.2.3 Εξωτερικές υπηρεσίες

Καθώς το σύστημα υποστηρίζει τη σύνδεση με εξωτερικές υπηρεσίες, για την ολοκλήρωση των υπηρεσιών του, θα πρέπει για τους σκοπούς του ελέγχου να προσομοιώνει τις υπηρεσίες αυτές ή να συνδέεται με εναλλακτικές υπηρεσίες και κατόπιν επιλογής της ομάδας σχεδίασης. Αυτό είναι απαραίτητο ώστε να ελεγχθούν οι διεπαφές που πραγματοποιούν την διασύνδεση με αυτές τις εξωτερικές υπηρεσίες.



4 Σενάρια Ελέγχων-Δοκιμών

4.1 Έρευνα γραφείου

Κατά την έρευνα γραφείου θα μελετηθούν η τεκμηρίωση του συστήματος και η υλοποίηση αυτού σχετικά με τις δυνατότητες κλιμάκωσης, την απόδοσή του, την παρεχόμενη ασφάλεια και την επιχειρησιακή πληρότητα αυτού.

4.1.1 Έλεγχος κάλυψης μετάπτωσης και εφαρμογών

Ο έλεγχος αυτός αφορά την πλήρη κάλυψη των επιχειρησιακών προδιαγραφών του έργου σύμφωνα με τις προδιαγραφές που αναφέρθηκαν παραπάνω και οργανώνονται σε δυο βασικές κατηγορίες

- Έλεγχος Μετάπτωσης (σύμφωνα με τις φόρμες του παραρτήματος 6.1)
- Έλεγχος Εφαρμογών που ήδη είναι εμπορικά διαθέσιμες (σύμφωνα με τις φόρμες του παραρτήματος 6.2)
- Λοιποί έλεγχοι (σύμφωνα με όσα ορίζονται στο παράρτημα 6.2.1, 6.4, 6.5, 6.7 και 6.8)

Αν δεν καλύπτεται κάποια προδιαγραφή τότε αυτή θα πρέπει υποχρεωτικά να καλυφθεί. Επίσης ελέγχεται η ορθότητα της επιχειρησιακής λογικής.

Για τον έλεγχο αυτό θα χρησιμοποιηθεί η δομή της φόρμας του παραρτήματος 6.1.

Στη στήλη «ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ» αναγράφονται οι υπηρεσίες και το επίπεδο που απαιτείται ενώ στην στήλη «ΚΑΛΥΨΗ ΚΑΙ ΜΕΘΟΔΟΣ» το αν καλύπτεται πλήρως, μερικώς ή καθόλου καθώς και η μέθοδος, αν κρίνεται απαραίτητο. Στη στήλη «ΣΧΟΛΙΑ-ΠΑΡΑΤΗΡΗΣΕΙΣ» αναγράφονται τυχόν σχόλια/παρατηρήσεις των ελεγκτών σχετικά με πιθανά ελαττώματα της υπηρεσίας που προκύπτουν από την υλοποίηση αυτής ή άλλες παρατηρήσεις σχετικά με την κάλυψη ή τη μέθοδο κάλυψης της απαίτησης.

Στο τέλος του ελέγχου αναφέρονται τυχόν κενά υπηρεσιών που δεν υπήρχαν στις προδιαγραφές αλλά που κρίνονται απαραίτητα για την λειτουργικότητα του συστήματος και που θα έπρεπε να έχουν ληφθεί υπόψη κατά την υλοποίηση, ή άλλα θέματα επιχειρησιακής λειτουργίας που μπορούν να προκύπτουν.

4.1.2 Έλεγχος μοντέλου δεδομένων και αρχιτεκτονικής συστήματος

Σκοπός του ελέγχου της αρχιτεκτονικής των εφαρμογών καθώς και του μοντέλου δεδομένων σε μορφή entity relationship diagram, είναι να αναδείξει ελαττώματα ασφάλειας και απόδοσης του συστήματος. Θα ελεγχθεί η δυνατότητα του συστήματος για διασφάλιση της ικανότητας συνέχισης της λειτουργίας του σε περιπτώσεις αστοχιών υλικού ή προβλημάτων λογισμικού σε συγκεκριμένες μονάδες, θα ελεγχθούν οι μέθοδοι προφύλαξης πρόσβασης μέσω διαδικτύου και η αξιόπιστη και αποδοτική σχεδίαση της βάσης δεδομένων.

Σελίδα 23 από 61



Στο τέλος του ελέγχου θα πραγματοποιηθεί αναφορά με προβλήματα ή παρατηρήσεις που προέκυψαν, όπου θα αναφέρονται αναλυτικά τα σημεία που θεωρείται ότι μπορεί να παρουσιάσουν πρόβλημα στην λειτουργικότητα των συστημάτων ή στην κάλυψη των στόχων τους.

4.1.3 Έλεγχος εγχειριδίων χρήσεως

Στο στάδιο αυτό θα πραγματοποιηθεί έλεγχος του συνοδευτικού υλικού τεκμηρίωσης της εφαρμογής που αφορά τη χρήση του συστήματος. Θα ελεγχθεί το ότι καλύπτει το σύνολο των λειτουργιών των εφαρμογών τόσο από πλευράς απλού χρήστη όσο και από πλευράς διαχείρισης. Θα πραγματοποιηθεί επίσης δειγματοληπτικός έλεγχος για την πληρότητα της επεξήγησης και την ύπαρξη παραδειγμάτων.

Στο τέλος θα γίνει αναφορά του ελέγχου, που θα περιέχει τα σημεία που ελέγχθηκαν και τα προβλήματα/παρατηρήσεις που προέκυψαν με την αντίστοιχη αιτιολόγηση αυτών.

4.1.4 Έλεγχος πολιτικής ασφαλείας

Στο στάδιο αυτό θα παραληφθεί και θα μελετηθεί η πολιτική ασφαλείας του οργανισμού που επηρεάζει την ασφάλεια των εφαρμογών. Θα εξεταστεί η πολιτική ασφαλείας σχετικά με τη διαχείριση των κεντρικών εξυπηρετητών, η πολιτική κωδικών χρηστών, ο καθορισμός προστατευμένων περιοχών και δικαιωμάτων πρόσβασης σε αυτές (computerroom) και λοιπές παράμετροι που ορίζονται στη πολιτική ασφαλείας και επηρεάζουν τις εφαρμογές.

4.2 Ελεύθερα σενάρια ελέγχου σε εργαστηριακό περιβάλλον

Οι έλεγχοι αυτοί στοχεύουν σε έλεγχο για σφάλματα και ελαττώματα του συστήματος, κάλυψη προδιαγραφών και πρωτογενή έλεγχο ευχρηστίας του συστήματος.

Τα σενάρια εκτελούνται σε εργαστηριακό περιβάλλον από έμπειρους χρήστες και τεχνικούς που πλοηγούνται στο σύστημα και ελέγχουν την λειτουργία του συστήματος σε μη αναμενόμενες ενέργειες χρήστη, όπως καταχώρηση απ' ευθείας url, λάθος στοιχείων σε πεδία τιμών των διεπαφών χρήστη, διακοπή διεργασίας κατά την πραγματοποίηση υποβολής/καταχώρησης (αιτήματος, αρχείου, πληρωμής κλπ), είσοδο εσφαλμένων ή μη λογικών τιμών σε πεδία των φορμών του συστήματος, και άλλα σημεία κατά την εκτέλεση των οποίων υπάρχει περίπτωση ελαττώματος ή σφάλματος. Επίσης μέσω της πλοήγησης αυτής πραγματοποιείται και πρωτογενής έλεγχος ευχρηστίας του συστήματος.

Τα σενάρια που ελέγχονται καταγράφονται σε πίνακες βάσει του Παραρτήματος 6.5 όπου καταγράφονται το τμήμα της εφαρμογής που αφορούσε το σενάριο, τα βήματα που πραγματοποιήθηκαν, τα αποτελέσματα και τυχόν παρατηρήσεις/σχόλια. Για την πραγματοποίηση των ελέγχων χρησιμοποιούνται ως γενικές κατευθυντήριες γραμμές τα σενάρια ελέγχου αποδοχής χρήστη αλλά και δοκιμές για:

- Δειγματοληπτικό έλεγχο ιστοσελίδων του συστήματος ως προς την συμμόρφωση με τα πρότυπα και προδιαγραφές σχετικά με HTML, CSS και WAI

Σελίδα 24 από 61



- Έλεγχο ύπαρξης αρχείων βοήθειας στις εφαρμογές
- Έλεγχο σύνδεσης Single Sign On (SSO)
- Έλεγχο λειτουργίας πρόσβασης πύλης και των υπηρεσιών από διάφορα λειτουργικά (π.χ. Microsoft Windows, Mac OS, iOS, Linux, κλπ) και περιηγητές διαδικτύου (MS Internet Explorer, Mozilla Firefox, Google Chrome κλπ)
- Πρόσβαση στοιχείων μέσω διαδικτύου (internet)
- Πρόσβαση στοιχείων μέσω εσωτερικού δικτύου (intranet)

4.3 Έλεγχοι αποδοχής χρήστη

Οι έλεγχοι αποδοχής χρήστη θα εκτελεσθούν σε περιβάλλον λειτουργίας (SAT), σύμφωνα με την παράγραφο 3.3.2 της μεθοδολογίας, και στοχεύουν σε:

- Έλεγχο της ευχρηστίας των εφαρμογών από τους χρήστες
- Έλεγχο του περιεχομένου που έχει εισαχθεί (υπηρεσίες, πληροφόρηση σχετικά με τις υπηρεσίες, δικαιολογητικά υπηρεσιών)
- Έλεγχο της πληρότητας των βημάτων των διαδικασιών που καλύπτονται από τις εφαρμογές
- Έλεγχο της απόδοσης του συστήματος κατά την εκτέλεση των σεναρίων ελέγχου (σφάλματα που απαιτούν επανεκτέλεση κάποιου βήματος, ταχύτητα απόκρισης, ταχύτητα εκτέλεσης του συνόλου των βημάτων κάθε σεναρίου)

Η σχεδίαση/καταγραφή των σεναρίων γίνεται βάσει του πίνακα του Παραρτήματος 6.6.1. Για κάθε βήμα του σεναρίου αναφέρονται οι ενέργειες που περιλαμβάνει, τα αναμενόμενα αποτελέσματα, τυχόν απόκλιση/διαφοροποίηση κατά την εκτέλεση από τα αναμενόμενα και σχόλια/παρατηρήσεις.

Στις παρατηρήσεις κάθε βήματος αναφέρονται προβλήματα κατανόησης, λογικής, εμφάνισης ή και ελαττωμάτων της διαδικασίας και της παρεχόμενης πληροφορίας, καθυστέρησης απόκρισης, διαφορετικό αποτέλεσμα από το αναμενόμενο και περιπτώσεις αποτυχίας εκτέλεσης βήματος όπως σφάλματα που δεν μπορεί να επανακάμψει η διαδικασία ή και σφάλματα τα οποία μπορεί να επανακάμψει (επανεκτέλεση βήματος ή ανανέωση οθόνης). Επίσης στο τέλος γίνεται ανακεφαλαίωση των προβλημάτων/παρατηρήσεων καθώς και εκτίμηση της συνολικής απόδοσης του συστήματος ως προς την εκτέλεση του συγκεκριμένου σεναρίου (πχ. πολλά βήματα ή χρονοβόρος διαδικασία για την επίτευξη του στόχου της).



4.4 Έλεγχοι απόδοσης

4.4.1 Έλεγχος απόδοσης κανονικής λειτουργίας σε εργαστηριακό περιβάλλον

Για την πραγματοποίηση του ελέγχου αυτού χρησιμοποιούνται τα αρχεία καταγραφής (logs) που προκύψανε κατά την εκτέλεση των δοκιμών. Στον πίνακα του Παρατήματος 6.7.1 καταγράφονται η διεπαφή που ελέγχθηκε, ο μέσος χρόνος απόκρισης, ο βαθμός ικανοποιητικής απόδοσης και σχόλια των ελεγκτών σχετικά με την απόδοσή του.

Τα συμπεράσματα του ελέγχου αυτού θα χρησιμοποιηθούν ευριστικά για να προβλεφτούν προβλήματα λειτουργίας σε περιβάλλον κανονικής λειτουργίας και σε περιπτώσεις φόρτου καθώς και στην ταυτοποίηση ευπαθών σημείων.

4.4.2 Έλεγχος απόδοσης λειτουργίας αυξημένου φόρτου (stresstests) σε περιβάλλον κανονικής λειτουργίας (απομονωμένο περιβάλλον)

Για την πραγματοποίηση του ελέγχου αυτού χρησιμοποιούνται και πάλι τα εργαλεία και τα δεδομένα που χρησιμοποιήθηκαν για τον έλεγχο των προγραμματιστικών διεπαφών, αλλά αυτή τη φορά εκτελούνται παράλληλα πολλές επαναλήψεις κάθε κλήσης διεπαφής χρησιμοποιώντας κάθε μια διαφορετικό τμήμα των δεδομένων, ώστε να δοκιμαστεί η λειτουργία του συστήματος σε συνθήκες αυξημένου φόρτου. Ακολούθως εξάγονται μετρικές απόδοσης των υπο επίβλεψη υποσυστημάτων ακολουθώντας την μεθοδολογία που χρησιμοποιήθηκε στη παράγραφο 4.4.1 και συμπληρώνεται πίνακας βάσει του Παραρτήματος 6.7.1.

Κατά την εκτέλεση των παραπάνω ελέγχων, δηλαδή ενώ το σύστημα είναι σε κατάσταση φόρτου, εκτελούνται ενέργειες από τις διεπαφές χρήστη (μέσω φυλλομετρητή) και μετράται η απόκριση του συστήματος. Τα αποτελέσματα αυτού του τμήματος του ελέγχου καταχωρούνται στον πίνακα του παραρτήματος 6.7.2. Θα πρέπει ο μέσος χρόνος απόκρισης φορμών που περιλαμβάνουν εξαγωγή στατιστικών ή αναφορών να μην υπερβαίνει τα 10 δευτερόλεπτα σε εσωτερικό δίκτυο, ενώ η εμφάνιση των υπολοίπων φορμών να μην υπερβαίνει τα 4 δευτερόλεπτα.

4.4.3 Έλεγχος απόδοσης βάσει διεπαφών χρήστη σε περιβάλλον λειτουργίας

Πραγματοποιείται εκτέλεση ενεργειών από τις διεπαφές χρήστη (μέσω φυλλομετρητή) και μετράται η απόκριση του συστήματος. Τα αποτελέσματα του ελέγχου καταχωρούνται στον πίνακα του παραρτήματος 6.7.2 σε αντιπαραβολή με τα αποτελέσματα που προέκυψαν από τους αντίστοιχους ελέγχους της παραγράφου 4.4.2. Θα πρέπει ο μέσος χρόνος απόκρισης φορμών που περιλαμβάνουν εξαγωγή στατιστικών ή αναφορών να μην υπερβαίνει τα 10 δευτερόλεπτα



σε εσωτερικό δίκτυο, ενώ η εμφάνιση των υπολοίπων φορμών να μην υπερβαίνει τα 4 δευτερόλεπτα.



5 Διάρθρωση ομάδων ελέγχου

Οι ομάδες ελέγχου θα στελεχώνονται, ανάλογα με το είδος του ελέγχου που θα πραγματοποιείται, από τεχνικούς υποστήριξης, χειριστές εφαρμογής (απλούς και εξειδικευμένους χρήστες), αναλυτές και υπεύθυνους των ομάδων ελέγχων. Μια ή περισσότερες κατηγορίες μπορούν να εκπροσωπηθούν από το ίδιο φυσικό πρόσωπο.

Η κατανομή των αρμοδιοτήτων των μελών της ομάδας είναι η ακόλουθη:

- Μηχανικός Λογισμικού - Τεχνικός ελέγχου
 - Πραγματοποίηση απαιτούμενων εργασιών συστημάτων και εφαρμογών για την ομαλή εκτέλεση των εργασιών
 - Υλοποίηση αυτοματοποιημένων μεθόδων ελέγχου των συνιστωσών των εφαρμογών βάσει των απαιτήσεων των σεναρίων ελέγχου (όπου αυτό απαιτείται)
 - Παροχή και έλεγχος αρχείων και πληροφοριών που απαιτούνται από τους ελέγχους, όπως αρχείων log των εφαρμογών και συστημάτων
- Εξωτερικοί χειριστές
 - Εκτέλεση των σεναρίων ελέγχων που έχουν καθοριστεί
 - Παροχή πληροφοριών σε αναλυτές και υπεύθυνους ομάδας ελέγχου
- Απλοί χειριστές / Ανεξάρτητοι Ελεγκτές
 - Εκτέλεση των σεναρίων ελέγχων που έχουν καθοριστεί
 - Παροχή βοήθειας σε αναλυτές και υπεύθυνους ομάδας ελέγχου
- Έμπειροι χρήστες / Υπεύθυνοι Λογισμικού / Ανεξάρτητοι Ελεγκτές
 - Εκτέλεση ελέγχων που δεν ακολουθούν συγκεκριμένα σενάρια
 - Παροχή βοήθειας σε αναλυτές και υπεύθυνους ομάδας ελέγχου
- Αναλυτές / Σχεδιαστές Λογισμικού
 - Καθοδήγηση χειριστών της εφαρμογής για την εκτέλεση των ελέγχων
 - Τεκμηρίωση και χαρακτηρισμός των αποτελεσμάτων των ελέγχων
 - Εξασφάλιση της εγκυρότητας των διαδικασιών ελέγχου
 - Έλεγχος και τεκμηρίωση στοιχείων ελέγχων που στηρίζονται σε παράθεση στοιχείων και επιχειρηματολογίας και όχι σε εκτέλεση συγκεκριμένων ενεργειών
- Υπεύθυνοι ομάδας ελέγχου / Ανεξάρτητοι Ελεγκτές
 - Συντονισμός
 - Αντιμετώπιση δυσκολιών και προβλημάτων
 - Εξασφάλιση περιβάλλοντος ελέγχου
 - Εξασφάλιση αναγκαίων προϋποθέσεων
 - Εξασφάλιση επαρκούς τεκμηρίωσης ελέγχων



6 Παράρτημα: Ενδεικτικές φόρμες καταγραφής ελέγχων

Παρακάτω παρουσιάζονται μια σειρά από φόρμες οι οποίες καταδεικνύουν τις ανάγκες καταγραφής των ελέγχων και των αποτελεσμάτων τους.

6.1 Πίνακας Ελέγχου Μετάπτωσης

6.1.1 Έλεγχος Μετάπτωσης Δεδομένων

Μετά τη μετάπτωση των δεδομένων (όπου υφίσταται) θα πρέπει να συγκεντρωθούν τα ακόλουθα στοιχεία:

6.1.1.1 Έλεγχος Συμφωνίας Δεδομένων

Σενάριο Ελέγχου	Έλεγχος Γραφείου ή Πεδίου	
Κατηγορία Ελέγχου	Έλεγχος Μετάπτωσης	
Ελεγκτής	Μηχανικός Λογισμικού/Υπεύθυνος Λογισμικού	
Εφαρμογή/υποσύστημα		
Λειτουργία Ελέγχου	Έλεγχος Συμφωνίας Δεδομένων	
Επίπεδο Ελέγχου	Δεδομένα	

A/A	Χαρακτηριστικά /Λειτουργία Εφαρμογής	Παλαιά Εφαρμογή	Νέα Εφαρμογή	Βαθμός Συμφωνίας	Παρατηρήσεις
1.					
2.					
3.					

6.1.1.2 Έλεγχος Μετρικών Δεδομένων

Σενάριο Ελέγχου	Έλεγχος Γραφείου ή Πεδίου	
-----------------	---------------------------	--

Κατηγορία Ελέγχου	Έλεγχος Μετάπτωσης	
Ελεγκτής	Μηχανικός Λογισμικού/Υπεύθυνος Λογισμικού	
Εφαρμογή/υποσύστημα		
Λειτουργία Ελέγχου	Έλεγχος Μετρικών Δεδομένων	
Επίπεδο Ελέγχου	Δεδομένα	

A/A	Χαρακτηριστικά /Λειτουργία Εφαρμογής	Παλαιά Εφαρμογή	Νέα Εφαρμογή	Βαθμός Συμφωνίας	Παρατηρήσεις
1.	Αριθμός Πινάκων				
2.	Αριθμός Εγγραφών Πίνακας <>				
3.	Αριθμός Εγγραφών Πίνακας <>				
4.	Αριθμός Εγγραφών Πίνακας <>				
5.	Αριθμός Εγγραφών Πίνακας <>				
6.	Άθροισμα εγγραφών				

6.1.1.3 Έλεγχος Επιχειρησιακής Συμφωνίας Εφαρμογής

Σενάριο Ελέγχου	Έλεγχος Γραφείου ή Πεδίου	
Κατηγορία Ελέγχου	Έλεγχος Μετάπτωσης	
Ελεγκτής	Μηχανικός Λογισμικού/Υπεύθυνος Λογισμικού	
Εφαρμογή/υποσύστημα		
Λειτουργία Ελέγχου	Έλεγχος Επιχειρησιακής Συμφωνίας Εφαρμογής	
Επίπεδο Ελέγχου	Λειτουργίες Εφαρμογής	

A/A	Χαρακτηριστικά /Λειτουργία Εφαρμογής	Παλαιά Εφαρμογή	Νέα Εφαρμογή	Βαθμός Συμφωνίας	Παρατηρήσεις
1.					
2.					
3.					
4.					

6.2 Πίνακας Ελέγχου Συστημάτων

6.2.1 Δομικοί έλεγχοι

Όσον αφορά στη διαδικασία ελέγχου μπορούν να πραγματοποιηθούν οι παρακάτω έλεγχοι:

- Έλεγχος Ροής Δεδομένων
- Έλεγχος Ροής Πληροφορίας
- Έλεγχος Λογικής Εφαρμογής

πχ

Σενάριο Ελέγχου	Έλεγχος Γραφείου ή Πεδίου	
Κατηγορία Ελέγχου	Δομικός έλεγχος	
Ελεγκτής	Μηχανικός Λογισμικού	
Εφαρμογή/υποσύστημα		
Λειτουργία Ελέγχου	Έλεγχος Λογικής Εφαρμογής	
Επίπεδο Ελέγχου	Πηγαίος Κώδικας ή Προδιαγραφές Λογισμικού	

A/A	Χαρακτηριστικά/Λειτουργία	Κάλυψη	Σχόλια - Παρατηρήσεις
1.			
2.			

6.2.2 Λειτουργικού έλεγχου

Όσον αφορά τη διαδικασία ελέγχου της εφαρμογής θα πραγματοποιηθούν οι παρακάτω έλεγχοι:

6.2.2.1 Έλεγχος Transactions

Σενάριο Ελέγχου	Έλεγχος Γραφείου ή Πεδίου	
Κατηγορία Ελέγχου	Λειτουργικός έλεγχος	
Ελεγκτής	Υπεύθυνος Λογισμικού ή Τελικός Χρήστης ή Ανεξάρτητος Ελεγκτής	
Εφαρμογή/υποσύστημα		
Λειτουργία Ελέγχου	Έλεγχος Transactions Λογισμικού	
Επίπεδο Ελέγχου	Λογισμικό / Λειτουργικές Προδιαγραφές	

A/A	Χαρακτηριστικά/Λειτουργία	Κάλυψη	Σχόλια - Παρατηρήσεις
1.		Εφαρμογή	
2.		Εφαρμογή	
3.		Εφαρμογή	
4.		Εφαρμογή	
5.		Εφαρμογή	

6.2.2.2 Έλεγχος Εύρους Τιμών

Σενάριο Ελέγχου	Έλεγχος Γραφείου ή Πεδίου	
Κατηγορία Ελέγχου	Λειτουργικός έλεγχος	
Ελεγκτής	Υπεύθυνος Λογισμικού ή Τελικός Χρήστης ή Ανεξάρτητος Ελεγκτής	
Εφαρμογή/υποσύστημα		
Λειτουργία Ελέγχου	Έλεγχος Εύρους Δεδομένων	
Επίπεδο Ελέγχου	Λογισμικό / Λειτουργικές Προδιαγραφές	

A/A	Χαρακτηριστικά/Λειτουργία	Κάλυψη	Σχόλια - Παρατηρήσεις
1.		Εφαρμογή	
2.		Εφαρμογή	
3.		Εφαρμογή	
4.		Εφαρμογή	

5.		Εφαρμογή	
6.		Εφαρμογή	
7.		Εφαρμογή	

6.2.2.3 Έλεγχος Σύνταξης Εφαρμογής

Σενάριο Ελέγχου	Έλεγχος Γραφείου ή Πεδίου	
Κατηγορία Ελέγχου	Λειτουργικός έλεγχος	
Ελεγκτής	Υπεύθυνος Λογισμικού ή Τελικός Χρήστης ή Ανεξάρτητος Ελεγκτής	
Εφαρμογή/υποσύστημα		
Λειτουργία Ελέγχου	Έλεγχος Σύνταξης εφαρμογής	
Επίπεδο Ελέγχου	Λογισμικό / Λειτουργικές Προδιαγραφές	

A/A	Χαρακτηριστικά/Λειτουργία	Κάλυψη	Σχόλια - Παρατηρήσεις
1.	Καταγραφή μηνυμάτων χρήστη για μη αποδεκτές τιμές πεδίων	Εφαρμογή	
2.	Καταγραφή μηνυμάτων χρήστη για μη αποδεκτές λειτουργίες	Εφαρμογή	
3.	Καταγραφή μηνυμάτων χρήστη για αποδεκτές λειτουργίες	Εφαρμογή	
4.	Καταγραφή μηνυμάτων χρήστη για συνήθεις λειτουργίες	Εφαρμογή	
5.	Σήμανση κρισιμότητας μηνυμάτων	Εφαρμογή	

6.2.2.4 Έλεγχος Λογικής Εφαρμογής

Σενάριο Ελέγχου	Έλεγχος Γραφείου ή Πεδίου	
Κατηγορία Ελέγχου	Λειτουργικός έλεγχος	
Ελεγκτής	Υπεύθυνος Λογισμικού ή Τελικός Χρήστης ή Ανεξάρτητος Ελεγκτής	
Εφαρμογή/υποσύστημα		
Λειτουργία Ελέγχου	Έλεγχος Λογικής εφαρμογής	
Επίπεδο Ελέγχου	Λογισμικό / Λειτουργικές Προδιαγραφές	

A/A	Χαρακτηριστικά/Λειτουργία	Κάλυψη	Σχόλια - Παρατηρήσεις
1.	Καταγραφή κινήσεων χρήστη για εγγραφή νέου χρήστη	Εφαρμογή	
2.	Καταγραφή κινήσεων χρήστη για διαγραφή χρήστη	Εφαρμογή	
3.	Έναρξη πολλαπλών αντιγράφων εφαρμογής και εισαγωγή ταυτόσημων δεδομένων	Εφαρμογή	
4.	Διαγραφή χρήστη και Νέα εισαγωγή χρήστη	Εφαρμογή	
5.	Διαγραφή χρήστη και Νέα εισαγωγή χρήστη	Εφαρμογή	
6.			
7.			

6.2.2.5 Έλεγχος Κατάστασης Εφαρμογής

Σενάριο Ελέγχου	Έλεγχος Γραφείου ή Πεδίου	
Κατηγορία Ελέγχου	Λειτουργικός έλεγχος	
Ελεγκτής	Υπεύθυνος Λογισμικού ή Τελικός Χρήστης ή Ανεξάρτητος Ελεγκτής	
Εφαρμογή/υποσύστημα		
Λειτουργία Ελέγχου	Έλεγχος Κατάστασης εφαρμογής	
Επίπεδο Ελέγχου	Λογισμικό / Λειτουργικές Προδιαγραφές	

A/A	Χαρακτηριστικά/Λειτουργία	Κάλυψη	Σχόλια - Παρατηρήσεις
1.	Καταγραφή λειτουργίας εφαρμογής χωρίς τη βάση δεδομένων	Εφαρμογή	
2.	Καταγραφή λειτουργίας εφαρμογής μετά τη διαγραφή ενός ή περισσότερων πινάκων	Εφαρμογή	
3.	Έναρξη πολλαπλών αντιγράφων εφαρμογής και κατάσταση ανταπόκρισης	Εφαρμογή	
4.			
5.			

6.2.3 Στατιστικοί έλεγχοι

Όσον αφορά τη στατιστική διαδικασία ελέγχου της εφαρμογής θα πραγματοποιηθούν οι παρακάτω έλεγχοι

6.2.3.1 Έλεγχος Αξιοπιστίας

Σενάριο Ελέγχου	Έλεγχος Γραφείου ή Πεδίου	
------------------------	---------------------------	--

Κατηγορία Ελέγχου	Λειτουργικός έλεγχος	
Ελεγκτής	Υπεύθυνος Λογισμικού ή Τελικός Χρήστης ή Ανεξάρτητος Ελεγκτής	
Εφαρμογή/υποσύστημα		
Λειτουργία Ελέγχου	Έλεγχος Αξιοπιστίας	
Επίπεδο Ελέγχου	Λογισμικό / Λειτουργικές Προδιαγραφές	

A/A	Χαρακτηριστικά/Λειτουργία	Κάλυψη	Σχόλια - Παρατηρήσεις
1.	Καθορισμός στοιχείων αξιοπιστίας (ανά ημέρα, εβδομάδα, μήνα)	Εφαρμογή	
2.	Διαθεσιμότητα εφαρμογής ανά μήνα	Εφαρμογή	
3.	Χρόνος επαναφοράς εφαρμογής	Εφαρμογή	
4.	Χρόνος μεταξύ αποτυχιών	Εφαρμογή	
5.	Χρόνος ανταπόκρισης υποστήριξης	Εφαρμογή	

6.2.4 Έλεγχοι αντοχής

Όσον αφορά τη διαδικασία ελέγχου αντοχής της εφαρμογής μπορούν να πραγματοποιηθούν οι παρακάτω έλεγχοι:

6.2.4.1 Έλεγχος Αντοχής και Υποβάθμισης

Σενάριο Ελέγχου	Έλεγχος Γραφείου ή Πεδίου	
Κατηγορία Ελέγχου	Λειτουργικός έλεγχος	
Ελεγκτής	Υπεύθυνος Λογισμικού ή Τελικός Χρήστης ή	



	Ανεξάρτητος Ελεγκτής	
Εφαρμογή/υποσύστημα		
Λειτουργία Ελέγχου	Έλεγχος Αντοχής Εφαρμογής και Υποβάθμισης Εφαρμογής	
Επίπεδο Ελέγχου	Λογισμικό / Λειτουργικές Προδιαγραφές	

A/A	Χαρακτηριστικά/Λειτουργία	Κάλυψη	Σχόλια - Παρατηρήσεις
1.	Χρόνος ανταπόκρισης σε σύνθετη αναζήτηση με ένα αντίγραφο της εφαρμογής εν λειτουργία	Εφαρμογή	
2.	Χρόνος ανταπόκρισης σε σύνθετη αναζήτηση με δύο αντίγραφα της εφαρμογής εν λειτουργία	Εφαρμογή	
3.	Χρόνος ανταπόκρισης σε σύνθετη αναζήτηση με πέντε αντίγραφα της εφαρμογής εν λειτουργία	Εφαρμογή	
4.	Χρόνος ανταπόκρισης σε σύνθετη αναζήτηση με ένα αντίγραφο της εφαρμογής εν λειτουργία και δύο άλλες εφαρμογές εν λειτουργία	Εφαρμογή	
5.	Χρόνος ανταπόκρισης σε σύνθετη αναζήτηση με δύο αντίγραφα της εφαρμογής εν λειτουργία και δύο άλλες εφαρμογές εν λειτουργία	Εφαρμογή	
6.	Χρόνος ανταπόκρισης σε σύνθετη αναζήτηση με πέντε αντίγραφα της εφαρμογής εν λειτουργία και δύο άλλες εφαρμογές εν λειτουργία	Εφαρμογή	
7.	Αυξήστε ανά ένα τα αντίγραφα της εφαρμογής αλλά και των		



άλλων εφαρμογών εν λειτουργία και επαναλάβετε τα παραπάνω βήματα		
--	--	--

6.2.4.2 Έλεγχος Ανάκτησης Εφαρμογής

Σενάριο Ελέγχου	Έλεγχος Γραφείου ή Πεδίου	
Κατηγορία Ελέγχου	Λειτουργικός έλεγχος	
Ελεγκτής	Υπεύθυνος Λογισμικού ή Τελικός Χρήστης ή Ανεξάρτητος Ελεγκτής	
Εφαρμογή/υποσύστημα		
Λειτουργία Ελέγχου	Έλεγχος Ανάκτησης Εφαρμογής	
Επίπεδο Ελέγχου	Λογισμικό / Λειτουργικές Προδιαγραφές	

A/A	Χαρακτηριστικά/Λειτουργία	Κάλυψη	Σχόλια - Παρατηρήσεις
1.	Χρόνος ανάκτησης εφαρμογής σε μειούμενο αριθμό αντιγράφων εν λειτουργία	Εφαρμογή	
2.	Έλεγχος πόρων εφαρμογής μέχρι του σημείου κατάρρευσης/ανάκτησης εφαρμογής	Εφαρμογή	
3.	Έλεγχος «υγιεινής» δεδομένων μετά από ανάκτηση	Εφαρμογή	
4.			
5.			

6.2.5 Έλεγχος παλινδρόμησης

6.2.5.1 Έλεγχος Παλινδρόμησης Εφαρμογής

Σενάριο Ελέγχου	Έλεγχος Γραφείου ή Πεδίου	
Κατηγορία Ελέγχου	Λειτουργικός έλεγχος	
Ελεγκτής	Υπεύθυνος Λογισμικού ή Τελικός Χρήστης ή Ανεξάρτητος Ελεγκτής	
Εφαρμογή/υποσύστημα		
Λειτουργία Ελέγχου	Έλεγχος Παλινδρόμησης Εφαρμογής	
Επίπεδο Ελέγχου	Λογισμικό / Λειτουργικές Προδιαγραφές	

A/A	Χαρακτηριστικά/Λειτουργία	Κάλυψη	Σχόλια - Παρατηρήσεις
1.	Καταγραφή προβλημάτων λαθών σε κάθε αλλαγή της εφαρμογής	Εφαρμογή	
2.	Επανάληψη των παραπάνω δοκιμών μετά ένα μήνα λειτουργίας	Εφαρμογή	

6.3 Πίνακας ελέγχου υπηρεσιών - υποσυστημάτων

6.3.1 Διεκπεραίωση υπηρεσιών

ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ	ΚΑΛΥΨΗ ΚΑΙ ΒΑΘΜΟΣ ΕΠΙΠΕΔΟΥ	ΣΧΟΛΙΑ ΠΑΡΑΤΗΡΗΣΕΙΣ

Σελίδα 42 από 61

ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ	ΚΑΛΥΨΗ ΚΑΙ ΒΑΘΜΟΣ ΕΠΙΠΕΔΟΥ	ΣΧΟΛΙΑ ΠΑΡΑΤΗΡΗΣΕΙΣ

6.3.2 Σύστημα Διαχείρισης Χρηστών

ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ	ΚΑΛΥΨΗ ΚΑΙ ΜΕΘΟΔΟΣ	ΣΧΟΛΙΑ ΠΑΡΑΤΗΡΗΣΕΙΣ
Single Sign On		
Εγγραφή εξωτερικών χρηστών		

6.4 Πίνακας καταγραφής ελέγχου συνιστωσών, προτύπων και τεχνολογιών

6.4.1 Συνιστώσες και πρότυπα

ΣΥΝΙΣΤΩΣΕΣ	ΧΡΗΣΙΜΟΠΟΙΟΥΜΕΝΑ ΠΡΟΤΥΠΑ	ΣΧΟΛΙΑ – ΠΑΡΑΤΗΡΗΣΕΙΣ
Παρατηρήσεις:		

6.4.2 Πίνακας καταγραφής ελέγχου συνιστωσών και τεχνολογιών αυτών

ΣΥΝΙΣΤΩΣΕΣ	ΧΡΗΣΙΜΟΠΟΙΟΥΜΕΝΕΣ ΤΕΧΝΟΛΟΓΙΕΣ	ΣΧΟΛΙΑ – ΠΑΡΑΤΗΡΗΣΕΙΣ
Παρατηρήσεις:		

6.4.3 Πίνακας καταγραφής ελέγχου επαναχρησιμοποιούμενων συνιστωσών και σημείων επαναχρησιμοποίησης

ΣΥΝΙΣΤΩΣΕΣ	ΣΗΜΕΙΑ ΕΠΑΝΑΧΡΗΣΙΜΟΠΟΙΗΣΗΣ	ΣΧΟΛΙΑ – ΠΑΡΑΤΗΡΗΣΕΙΣ
Παρατηρήσεις:		

6.5 Υπόδειγμα φόρμας ελεύθερων σεναρίων ελέγχου

Σενάριο ελέγχου:			
A/A ΒΗΜΑΤΟΣ	ΠΕΡΙΓΡΑΦΗ ΕΝΕΡΓΕΙΑΣ	ΑΠΟΤΕΛΕΣΜΑ	ΣΧΟΛΙΑ - ΠΑΡΑΤΗΡΗΣΕΙΣ
Παρατηρήσεις:			

6.6 Φόρμες σεναρίων ελέγχου αποδοχής χρήστη και προκαθορισμένα σενάρια

6.6.1 Υπόδειγμα σεναρίων ελέγχου αποδοχής χρήστη

Σενάριο Ελέγχου Αποδοχής χρήστη:				
A/A	ΠΕΡΙΓΡΑΦΗ ΕΝΕΡΓΕΙΑΣ	ΑΝΑΜΕΝΟΜΕΝΑ ΑΠΟΤΕΛΕΣΜΑΤΑ	ΑΠΟΤΕΛΕΣΜΑ	ΣΧΟΛΙΑ - ΠΑΡΑΤΗΡΗΣΕΙΣ
1.				
2.				
3.				
Παρατηρήσεις:				

6.7 Έλεγχοι απόδοσης

6.7.1 Έλεγχοι απόδοσης προγραμματιστικών διεπαφών

ΠΡΟΓΡΑΜΜΑΤΙΣΤΙΚΗ ΔΙΕΠΑΦΗ:			
ΜΕΣΟΣ ΧΡΟΝΟΣ ΑΠΟΚΡΙΣΗΣ	ΧΡΟΝΟΣ	ΒΑΘΜΟΣ ΑΠΟΔΟΣΗΣ	ΣΧΟΛΙΑ – ΠΑΡΑΤΗΡΗΣΕΙΣ
Παρατηρήσεις:			

6.7.2 Έλεγχος απόδοσης διεπαφών χρήστη

ΔΙΕΠΑΦΗ		
ΚΑΝΟΝΙΚΗ ΛΕΙΤΟΥΡΓΙΑ	STRESS TEST	ΣΧΟΛΙΑ - ΠΑΡΑΤΗΡΗΣΕΙΣ

ΜΕΣΟΣ ΧΡΟΝΟΣ ΑΠΟΚΡΙΣΗΣ	ΒΑΘΜΟΣ ΑΠΟΔΟΣΗΣ	ΜΕΣΟΣ ΧΡΟΝΟΣ ΑΠΟΚΡΙΣΗΣ	ΒΑΘΜΟΣ ΑΠΟΔΟΣΗΣ	

6.8 Φόρμες συλλογής πληροφοριών ελέγχων παρείσφρησης (Penetration tests)

6.8.1 Φόρμα καταγραφής δικτύου

Εύρος IP που πρέπει να ελεγχθούν και πληροφορίες για αυτές

--

Πληροφορίες Τομέα και ρυθμίσεων

--

Zone Transfer Highlights

--

Λίστα Εξυπηρετητών

Διεύθυνση IP	Όνομα Τομέα	Λειτουργικό Σύστημα

6.8.2 Φόρμα πληροφοριών εξυπηρετητή

Διεύθυνση IP	Όνομα Τομέα

Σελίδα 48 από 61



ΟΙ ΔΡΟΜΟΙ ΤΗΣ ΓΝΩΣΗΣ



Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο



ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ, ΠΟΛΙΤΙΣΜΟΥ & ΑΘΛΗΤΙΣΜΟΥ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης



ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ

«Ακαδημία Πλάτωνος – Ανάπτυξη της Γνώσης και καινοτόμων ιδεών», MIS 364467
 Δράση 2 «Θεμελίωση, Ενίσχυση και Λειτουργία Ψηφιακού Αποθετηρίου Ακαδημίας Πλάτωνος»
 Π 6.2.2.1 Μεθοδολογία Ελέγχου συστήματος

Πόρτα	Πρωτόκολλο	Υπηρεσία	Πληροφορίες Υπηρεσίας

BANNER(S)

Πόρτα	Πρωτόκολλο	Banner

TCP SEQUENCING:

TCP Sequence Prediction
TCPISN Seq. Numbers
IPID Sequence Generation
Uptime

Σελίδα 49 από 61



Προβληματισμοί και Ευπάθειες

Προβληματισμός ή ευπάθεια
Παράδειγμα

6.8.3 Φόρμα ανάλυσης τείχους προστασίας

6.8.3.1 Λήψη αποτυπωμάτων (fingerprinting)

Προσδιορισμός της επιτυχίας διαφόρων μεθόδων λήψης αποτυπωμάτων από αποκρίσεις πακέτων μέσω του τείχους προστασίας.

Μέθοδος	Αποτέλεσμα

6.8.3.2 SYN stealth

Αποτέλεσμα

6.8.3.3 Σάρωση πορτών με χρήση συγκεκριμένης πηγαίας πόρτας

Σελίδα 50 από 61

Πρωτόκολλο	Πόρτα	Banner
UDP	53	
UDP	161	
TCP	53	
TCP	69	

6.8.3.4 Επικαλυπτόμενα τμήματα πακέτων

Πρωτόκολλο	Αποτέλεσμα

6.8.3.5 Διαχείριση μικρών τμημάτων

IP	Αποτέλεσμα

6.8.3.6 syn flood

IP	Αποτέλεσμα

6.8.3.7 rst flag

IP	Αποτέλεσμα

6.8.3.8 udp

IP	Αποτέλεσμα

6.8.3.9 ack

IP	Αποτέλεσμα

--	--

6.8.3.10 fin

IP	Αποτέλεσμα

6.8.3.11 null

IP	Αποτέλεσμα

6.8.3.12 win

IP	Αποτέλεσμα

6.8.3.13 xmas

Σελίδα 53 από 61

IP	Αποτέλεσμα

6.8.4 Φόρμα προχωρημένης ανάλυσης τείχους προστασίας

6.8.4.1 Συνεχείς συνδέσεις TCP

Σύνδεση	Περιγραφή	Μέγιστες συνδέσεις	Μέγιστος ανενεργός χρόνος

6.8.4.2 Σύντομες (φευγαλέες) συνδέσεις TCP

Σύνδεση	Περιγραφή	Μέγιστες συνδέσεις	Μέγιστος ανενεργός χρόνος

6.8.4.3 Ρυθμαπόδοση συνεχούς ροής UDP

Σύνδεση	Περιγραφή	Μέγιστες συνδέσεις

6.8.4.4 Αποκρίσεις ICMP

Τύπος	Περιγραφή τύπου	Απόκριση	RTT

6.8.4.5 Αποκρίσεις Snoop

Σύνδεση	Περιγραφή απόκρισης	Από	Προς

6.8.4.6 Πρωτόκολλο

Πρωτόκολλο	Αποτέλεσμα

Σελίδα 55 από 61

--	--

6.8.5 Φόρμα δοκιμής IDS

6.8.5.1 Τύπος IDS

Τύπος IDS	Εύρος προστατευόμενων IPs

6.8.5.2 Επίθεση Flood

Τύπος	Περιγραφή επίθεσης	διάρκεια	αποτέλεσμα

6.8.5.3 Τροποποιημένα URLs

Τύπος κωδικοποίησης	URL που στάλθηκε	αποτέλεσμα

6.8.5.4 Ρυθμίσεις ταχύτητας

	Περιγραφή πακέτου	καθυστέρηση	αποτέλεσμα
1 λεπτό			
5 λεπτά			
60 λεπτά			
24 ώρες			

6.8.5.5 Επιθέσεις Συμπεριφοράς

	Περιγραφή	Αποτέλεσμα
random speed attack		
random protocol attack		
random source attack		

6.8.5.6 Ταίριασμα μεθόδου

	Αποτέλεσμα
HEAD	
POST	
PUT	
DELETE	
PATCH	
PROPFIND	
PROPPATCH	
MKCOL	

Σελίδα 57 από 61

COPY	
MOVE	
LOCK	
UNLOCK	

6.8.5.7 Έλεγχος πηγαίας πόρτας

Πρωτόκολλο	Πόρτα	Banner
UDP	53	
UDP	161	
TCP	443	
TCP	22	

6.8.5.8 Sroof αποκρίσεις

Σύνδεση	Περιγραφή απόκρισης	Από	Προς

6.8.5.8.1 Τμήματα πακέτων

Αποτέλεσμα

--

6.8.6 Φόρμα ελέγχου ιδιωτικότητας

(Η φόρμα αυτή θα χρησιμοποιηθεί εφόσον έχει υλοποιηθεί και βρίσκεται σε λειτουργία πολιτική ασφαλείας)

Διεύθυνση IP	Όνομα τομέα
Πολιτική ιδιωτικότητας	
Παραβιάσεις ιδιωτικότητας	

Διεύθυνση IP	Όνομα τομέα
Πολιτική ιδιωτικότητας	
Παραβιάσεις ιδιωτικότητας	

Σελίδα 59 από 61

--

6.8.7 Φόρμα «σπασίματος» κωδικών

6.8.7.1 Προστατευόμενο αρχείο

Όνομα αρχείου	
Τύπος αρχείου	
Χρόνος «σπασίματος»	
Όνομα χρήστη	
Κωδικός	

6.8.7.2 Κωδικοποιημένο αρχείο κωδικών ασφαλείας

Διεύθυνση IP	
Πόρτα υπηρεσίας	
Τύπος υπηρεσίας	
Πρωτόκολλο	
Ονόματα αρχείου	
Τύπος αρχείου	
Χρόνος «σπασίματος»	
Ονόματα εισόδου	
Κωδικοί	

6.8.7.3 Προστατευόμενη online υπηρεσία

Διεύθυνση IP	
Πόρτα υπηρεσίας	
Τύπος υπηρεσίας	
Πρωτόκολλο	
Ονόματα εισόδου	
Κωδικοί	