Σύνταξη από	**Έγκριση από**
ΣΚΑΡΒΕΛΗΣ ΓΕΩΡΓΙΟΣ ΥΔΠ - ΑΝ. ΤΕΧΝΙΚΟΣ ΔΙΕΥΘΥΝΤΗΣ 01.11.2021	ΧΑΡΑΛΑΜΠΟΣ ΓΑΛΑΤΣΑΝΟΣ ΠΡΟΕΔΡΟΣ 01.11.2021

Αναθεωρήσεις

Ημερομηνία	**Νέα Έκδοση**	**Αιτιολογία**
01.11.2021	1.0	Αρχική Έκδοση

Περιεχόμενα

0. Σκοπός και Πεδίο Εφαρμογής

Σκοπός του παρόντος Ειδικού Κανονισμού Πιστοποίησης είναι η παροχή τεκμηριωμένων πληροφοριών προς κάθε ενδιαφερόμενο μέρος ή πελάτη του Φορέα Πιστοποίησης EQA HELLAS Α.Ε. σχετικά με τις απαιτήσεις πιστοποίησης του Συστήματος Διαχείρισης Επιχειρησιακής Συνέχειας κατά ISO 22301:2019.

Ο παρών Ειδικός Κανονισμός ισχύει σε συνδυασμό με τον Γενικό Κανονισμό Πιστοποίησης GRC (Γενικός Κανονισμός Πιστοποίησης) και τις λοιπές εφαρμόσιμες Διαδικασίες του Φορέα Πιστοποίησης.

1. Αναφορές

- Εγχειρίδιο Ποιότητας QM
- P01 Διαδικασία Διαχείρισης Δραστηριοτήτων πριν τη Πιστοποίηση
- P04 Διαδικασία Διαχείρισης Προσωπικού και Καθορισμού Κριτηρίων Επάρκειας για τις λειτουργίες Πιστοποίησης
- P05 Διαδικασία Επιθεωρήσεων, Έκδοσης Πιστοποιητικών, Αναστολής, Ανάκλησης ή Περιορισμού του Πεδίου Πιστοποίησης
- P11 Διαδικασία Χρήσης Σημάτων και Λογοτύπων
- GRC Γενικός Κανονισμός Πιστοποίησης
- ISO 22300, Security and resilience — Vocabulary
- ISO 22301:2019, Security and resilience — Business continuity management systems — Requirements
- ISO 22313, Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301
- ISO 22316, Security and resilience — Organizational resilience — Principles and attributes
- ISO/TS 22317, Societal security — Business continuity management systems— Guidelines for business impact analysis (BIA)
- ISO/TS 22318, Societal security — Business continuity management systems— Guidelines for supply chain continuity management
- ISO 22320, Security and resilience — Emergency management — Guidelines for incident management
- ISO 22395, Security and resilience — Community resilience — Guidelines for supporting vulnerable persons in an emergency
- ISO/IEC 17021-6 Απαιτήσεις επάρκειας για επιθεώρηση και πιστοποίηση Συστημάτων Διαχείρισης Επιχειρησιακής Συνέχειας
- GDPR ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2016/679 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων)
- ISO 31000, Risk management — Principles and guidelines
- ΕΛΟΤ ΕΝ ISO/IEC 17021-1:2015 Αξιολόγηση της συμμόρφωσης– Απαιτήσεις για φορείς επιθεώρησης και πιστοποίησης συστημάτων διαχείρισης - Μέρος 1: Απαιτήσεις
- Κανονισμοί και Κατευθυντήριες Οδηγίες του ΕΣΥΔ
- IAF MD Κατευθυντήριες Οδηγίες της Διεθνούς Διαπίστευσης

2. Όροι και Ορισμοί - Συντομογραφίες

δραστηριότητα : προγραμματισμένη ενέργεια ή σύνολο προγραμματισμένων ενεργειών με καθορισμένο αποτέλεσμα

επιχειρηματική/επιχειρησιακή συνέχεια : ικανότητα ενος οργανισμού να συνεχίσει την παράδοση προϊόντων και υπηρεσιών εντός αποδεκτών χρονικών περιθωρίων και σε προκαθορισμένο επίπεδο κατά τη διάρκεια μιας διακοπής

σχέδιο επιχειρησιακής συνέχειας : τεκμηριωμένη πληροφόρηση που καθοδηγεί έναν οργανισμό να ανταποκριθεί σε μία διακοπή και να επανεκκινήσει και να αποκαταστήσει την παράδοση προϊόντων και υπηρεσιών σε συνάφεια με τους στόχους επιχειρησιακής συνέχειας

ανάλυση επιχειρηματικών επιπτώσεων (Business Impact Analysis-BIA) : διεργασία ανάλυσης της επίπτωσης μιας διακοπής σε έναν οργανισμό με την πάροδο του χρόνου

διακοπή (disruption) : περιστατικό, αναμενόμενο ή μη αναμενόμενο, που προκαλεί μια εκτός προγραμματισμού, αρνητική απόκλιση από την προσδοκώμενη παράδοση προϊόντων και υπηρεσιών βάσει στόχων ενός οργανισμού

επίπτωση : το αποτέλεσμα μιας διακοπής που επηρεάζει τους αντικειμενικούς σκοπούς και στόχους ενός οργανισμού

περιστατικό : γεγονός που μορεί να προκαλέσει ή να οδηγήσει σε διακοπή, απώλεια, επείγουσα κατάσταση ή κρίση

αντικειμενικός σκοπός-στόχος : αποτέλεσμα που πρέπει να επιτευχθεί (στρατηγικό, τακτικό ή επιχειρησιακό)

ιεραρχημένη (προτεραιοποιημένη) δραστηριότητα : δραστηριότητα που αντιμετωπίζεται επειγόντως κατά τη διάρκεια διακοπής ώστε να αποφευχθούν μη αποδεκτές επιπτώσεις

προϊόν και υπηρεσία : εξερχόμενο αποτέλεσμα που παρέχεται από έναν οργανισμό στα ενδιαφερόμενα μέρη

αμεροληψία : παρουσία της αντικειμενικότητας (Αντικειμενικότητα σημαίνει ότι δεν υπάρχουν συγκρούσεις συμφερόντων ή ότι είναι επιλυμένες έτσι ώστε να μην επηρεάζουν αρνητικά τις μετέπειτα δραστηριότητες του φορέα πιστοποίησης. Άλλοι όροι που είναι χρήσιμοι σε σχέση με το στοιχείο της αμεροληψίας είναι: ανεξαρτησία, ελευθερία από σύγκρουση συμφερόντων, ελευθερία από προκατάληψη, έλλειψη ζημιάς από άδικη κρίση, ουδετερότητα, δικαιοσύνη, ευρύτητα, ομαλότητα χειρισμού, αποκόλληση, εξισορρόπηση.)

διακινδύνευση : η επίδραση της αβεβαιότητας στους αντικειμενικούς σκοπούς-στόχους

ενδιαφερόμενο μέρος : πρόσωπο ή ομάδα που ενδιαφέρεται ή επηρεάζεται από την επίδοση ενός οργανισμού

εμπιστευτικότητα : διατήρηση του εμπιστευτικού χαρακτήρα στοιχείων ή πληροφοριών

επιθεώρηση πιστοποίησης : επιθεώρηση που διεξάγεται από έναν οργανισμό επιθεώρησης ανεξάρτητο από τον πελάτη και τα μέρη που βασίζονται πάνω του, με σκοπό την πιστοποίηση του συστήματος διαχείρισης του πελάτη.

επιθεωρητής : πρόσωπο που διεξάγει μια επιθεώρηση

επάρκεια : ικανότητα εφαρμογής γνώσεων και δεξιοτήτων για την επίτευξη των αναμενόμενων αποτελεσμάτων

μη συμμόρφωση : μη εκπλήρωση μιας απαίτησης

κύρια μη συμμόρφωση : Μη συμμόρφωση που επηρεάζει την ικανότητα του συστήματος διαχείρισης να επιτύχει τα επιδιωκόμενα αποτελέσματα

δευτερεύουσα μη συμμόρφωση ή παρατήρηση: Μη συμμόρφωση που δεν επηρεάζει την ικανότητα του συστήματος διαχείρισης να επιτύχει τα επιδιωκόμενα αποτελέσματα

οδηγός : πρόσωπο που ορίζεται από τον πελάτη για να βοηθήσει την ομάδα επιθεώρησης

παρατηρητής : πρόσωπο που συνοδεύει την ομάδα επιθεώρησης αλλά δεν επιθεωρεί

πελάτης : οργανισμός του οποίου το σύστημα διαχείρισης επιθεωρείται για σκοπούς πιστοποίησης

πιστοποιημένος πελάτης : οργανισμός του οποίου το σύστημα διαχείρισης έχει πιστοποιηθεί

πιστοποίηση : είναι η επιβεβαίωση τρίτου μέρους που αναφέρεται σε προϊόντα, διεργασίες, συστήματα και πρόσωπα. Με τον όρο επιβεβαίωση τρίτου μέρους νοείται η έκδοση δήλωσης (δηλ. πιστοποιητικού), από ανεξάρτητο φορέα ως προς το πρόσωπο ή τον οργανισμό, που παρέχει το προς αξιολόγηση συμμόρφωσης αντικείμενο, ότι η επαλήθευση των καθορισμένων απαιτήσεων, έχει τεκμηριωθεί επαρκώς.

πλαίσιο λειτουργίας : επιχειρησιακό περιβάλλον. Συνδυασμός εσωτερικών και εξωτερικών παραμέτρων που μπορούν να επηρεάσουν την προσέγγιση του οργανισμού για τη καθιέρωση και επίτευξη των στόχων του.

πρότυπο : ονομάζεται ένα έγγραφο, που καταρτίζεται με συναίνεση και εγκρίνεται από αναγνωρισμένο φορέα, το οποίο παρέχει για κοινή και επαναλαμβανόμενη χρήση κανόνες, οδηγίες ή χαρακτηριστικά για δραστηριότητες ή τα αποτελέσματα τους, με σκοπό την επίτευξη του βέλτιστου βαθμού τάξης σε ένα συγκεκριμένο πλαίσιο εφαρμογής

συμβουλευτική συστήματος διαχείρισης : συμμετοχή στην εγκατάσταση, εφαρμογή ή τη διατήρηση ενός συστήματος διαχείρισης. (Προετοιμασία ή παραγωγή εγχειριδίων ή διαδικασιών, παροχή συγκεκριμένων συμβουλών, οδηγιών ή λύσεων προς την κατεύθυνση της ανάπτυξης και εφαρμογής ενός συστήματος διαχείρισης.)

σχήμα Πιστοποίησης : Σύστημα αξιολόγησης της συμμόρφωσης που σχετίζεται με συστήματα διαχείρισης στο οποίο εφαρμόζονται οι ίδιες εξειδικευμένες απαιτήσεις, ειδικοί κανόνες και διαδικασίες

τεχνική περιοχή : η τεχνική περιοχή χαρακτηρίζεται από ομοιότητες των διεργασιών που σχετίζονται με ένα συγκεκριμένο τύπο συστήματος διαχείρισης

τεχνικός εμπειρογνώμονας : Πρόσωπο που παρέχει εξειδικευμένη τεχνογνωσία ή εμπειρογνωμοσύνη στην ομάδα επιθεώρησης (εξειδικευμένη τεχνογνωσία ή εμπειρογνωμοσύνη είναι ότι αφορά τον οργανισμό, τις διεργασίες ή τις δραστηριότητες που επιθεωρούνται.)

χρόνος επιθεώρησης: χρόνος που απαιτείται για το σχεδιασμό και την ολοκλήρωση μιας πλήρους και αποτελεσματικής επιθεώρησης του συστήματος διαχείρισης του πελάτη

διάρκεια επιθεωρήσεων πιστοποίησης συστημάτων διαχείρισης : Μέρος του χρόνου επιθεώρησης που ξοδεύεται για τις δραστηριότητες επιθεώρησης από την εναρκτήρια συνεδρίαση έως τη καταληκτική συμπεριλαμβανομένης

προϊόν : Το αποτέλεσμα μίας διεργασίας (μπορεί να είναι υπηρεσία ή κατεργασμένο υλικό, το οποίο είναι απτό και η ποσότητά του είναι ένα μετρήσιμο ή ένα συνεχές χαρακτηριστικό)

διεργασία : Σύνολο από σχετικές μεταξύ τους εργασίες ή λειτουργίες ή δραστηριότητες, οι οποίες όταν εφαρμόζονται αποτελεσματικά και λαμβάνοντας ένα ή περισσότερα εισερχόμενα (inputs) δημιουργούν εξερχόμενα (outputs), τα οποία προσθέτουν αξία στον οργανισμό.

υπηρεσία: αποτέλεσμα τουλάχιστον μία δραστηριότητας που εκτελείται αναγκαστικά στη διεπαφή μεταξύ του προμηθευτή και πελάτη, που είναι γενικά άυλη.

δεδομένα προσωπικού χαρακτήρα: κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»)· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου,

ΥΔΠ: Υπεύθυνος Διαχείρισης Ποιότητας

ΣΔΠ: Σύστημα Διαχείρισης Ποιότητας

ΣΔΕΣ: Σύστημα Διαχείρισης Επιχειρησιακής Συνέχειας

ΦΠ: Φορέας Πιστοποίησης EQA HELLAS A.E.

3. Υπευθυνότητες και Αρμοδιότητες

Υπεύθυνος εφαρμογής του παρόντος ειδικού κανονισμού είναι ο Τεχνικός Διευθυντής του Φορέα Πιστοποίησης σε συνεργασία με τον Υπεύθυνο Διαχείρισης Ποιότητας και τους Αναπληρωτές τους. Ο ΥΔΠ είναι αρμόδιος για την έκδοση και αναθεώρηση του παρόντος εγγράφου με την έγκριση της Ανώτατης Διοίκησης.

4. Ανάπτυξη Ειδικού Κανονισμού

4.1 Γενικά

Το προσωπικό του Φορέα Πιστοποίησης διαθέτει την απαιτούμενη τεχνική ικανότητα, αξιολογείται τακτικά (P04 Διαδικασία Διαχείρισης Προσωπικού και Καθορισμού Κριτηρίων Επάρκειας για τις Λειτουργίες της Πιστοποίησης) και προετοιμάζει και διενεργεί την επιθεώρηση, εφαρμόζοντας όλες τις σχετικές Διαδικασίες και συμπληρώνοντας τα αντίστοιχα καθιερωμένα Έντυπα. Οι σχετικές διαδικασίες εδράζουν στις απαιτήσεις των τυποποιητικών εγγράφων περί διενέργειας επιθεωρήσεων συστημάτων διαχείρισης.

Για τις ενέργειες πριν την επιζητούμενη πιστοποίηση εφαρμόζουν οι προβλέψεις της Διαδικασίας P01 του ΦΠ. Στην Αίτηση Πιστοποίησης ο οργανισμός δηλώνει τον αριθμό προσωπικού που εμπλέκεται με την εφαρμογή του ΣΔΕΣ και την υλοποίηση των σχεδίων επιχειρηματικής/επιχειρησιακής συνέχειας (πχ. ανώτατη Διοίκηση, Υπευθύνους Τμημάτων του οργανισμού, μέλη των ομάδων ανταπόκρισης κλπ.) καθώς και τους υπεργολάβους/εξωτερικούς συνεργάτες.

Η αξιολόγηση συμμόρφωσης, διενεργείται σε συμμόρφωση με τον Γενικό Κανονισμό Πιστοποίησης και τη Διαδικασία P05 του ΦΠ, όπου κατά την αρχική επιθεώρηση συνίστανται σε δύο διακριτά Στάδια, την επιθεώρηση 1ου Σταδίου και την επιθεώρηση 2ου Σταδίου, τα οποία διενεργούνται με προσχεδιασμένο και προγραμματισμένο τρόπο στο πλαίσιο σχετικής επίσκεψης στις εγκαταστάσεις του υπό πιστοποίηση οργανισμού.

Κατά τα λοιπά ισχύουν οι πρόσθετες προβλέψεις που παρατίθενται στον Γενικό Κανονισμό Πιστοποίησης και στις εφαρμόσιμες Διαδικασίες του Φορέα Πιστοποίησης.

4.2 Περιεχόμενο Επιθεώρησης

Οι ενέργειες που συνθέτουν την επιθεώρηση στο πλαίσιο της επιζητούμενης πιστοποίησης, καθώς και οι μέθοδοι και τεχνικές που εφαρμόζονται, περιγράφονται στον Γενικό Κανονισμό Πιστοποίησης του Φορέα Πιστοποίησης. Στα παρακάτω εξειδικεύεται το περιεχόμενο (κριτήρια και αντικειμενικοί σκοποί) της επιθεώρησης και αναφέρονται συνοπτικά οι πτυχές του Συστήματος Διαχείρισης Επιχειρησιακής Συνέχειας κατά ISO 22301:2019, που ελέγχονται και των οποίων αξιολογείται ο βαθμός συμμόρφωσης με τις αντίστοιχες απαιτήσεις που θέτει το διεθνές πρότυπο.

Αρχική Επιθεώρηση Πιστοποίησης

Επισημαίνεται ότι η διενέργεια αρχικής αξιολόγησης της συμμόρφωσης περιλαμβάνει δύο διακριτά Στάδια (Στάδιο 1 και Στάδιο 2) τα οποία διενεργούνται υποχρεωτικά στις εγκαταστάσεις του επιθεωρούμενου οργανισμού.

Το χρονικό διάστημα μεταξύ 1ου και 2ου Σταδίου δεν μπορεί να υπερβεί τους έξι (6) μήνες και σε αντίθετη περίπτωση επαναλαμβάνεται πλήρως το Στάδιο 1. Επισημαίνεται ρητά, ότι αποτυχία του επιθεωρούμενου οργανισμού να συμμορφώνεται με βασικές απαιτήσεις, ο βαθμός συμμόρφωσης με τις οποίες διερευνάται κατά το Στάδιο 1, μπορεί να σηματοδοτήσει αδυναμία εκτέλεσης του Σταδίου 2. Τούτο καθίσταται σαφές και γραπτώς στον επιθεωρούμενο οργανισμό, ο οποίος δια του εκπροσώπου του λαμβάνει ενυπόγραφα γνώση περί των αποτελεσμάτων της επιθεώρησης 1ου Σταδίου. Το Στάδιο 1 έχει σαν κύριο αντικειμενικό σκοπό να διαπιστωθεί ο βαθμός ετοιμότητας που επιδεικνύει ο επιθεωρούμενος οργανισμός για την επιθεώρηση του Σταδίου 2, καθώς επίσης και να συλλεγούν όλα εκείνα τα αναγκαία δεδομένα και στοιχεία ώστε να σχεδιαστεί κατάλληλα και επαρκώς το πρόγραμμα της επιθεώρησης του Σταδίου 2, το οποίο σε κάθε περίπτωση θα επιβεβαιώσει και τα ευρήματα του Σταδίου1.

Ειδικότερα κατά το Στάδιο 1 αξιολογούνται και ελέγχονται :

- Η συμμόρφωση του οργανισμού με το ισχύον νομοθετικό πλαίσιο που διέπει τη λειτουργία του και τα προϊόντα ή/και υπηρεσίες του,
- Η καταλληλότητα του σχεδιασμού του Συστήματος Διαχείρισης Επιχειρησιακής Συνέχειας (ΣΔΕΣ) σε ότι αφορά τη δυνατότητα κάλυψης των σχετικών σκοπών, στόχων και της καθιερωμένης πολιτικής της επιχείρησης. Ελέγχεται η τεκμηρίωση του οργανισμού που απαιτείται στο ISO 22301, η επαρκής κατανόηση του σχεδιασμού του BCMS στο πλαίσιο λειτουργίας και εντός της οργάνωσης του πελάτη, η εκτίμηση κινδύνου και ο μετριασμός (συμπεριλαμβανομένων των ελέγχων που καθορίζονται), η ανάλυση επιπτώσεων τόσο όσον αφορά τη μεθοδολογία αλλά και τα αποτελέσματα, η πολιτική επιχειρησιακής συνέχειας και οι στόχοι, το πεδίο εφαρμογής, οι στρατηγικές και λύσεις, η αναγνώριση των νομικών και κανονιστικών

απαιτήσεων που σχετίζονται με την επιχειρησιακή συνέχεια του οργανισμού και την παροχή υπηρεσιών / προϊόντων.

- Η επάρκεια της γραπτής τεκμηρίωσης του ΣΔΕΣ
- Η δέσμευση, η επάρκεια, η εγρήγορση και η ικανότητα του προσωπικού που εμπλέκεται στην εφαρμογή των προβλέψεων του ΣΔΕΣ (Διοίκηση, Υπεύθυνος ΣΔΕΣ, προσωπικό ομάδων αμταπόκρισης κλπ)
- Κατά πόσον η διαπιστωμένη έκταση εφαρμογής των προβλέψεων του Συστήματος Διαχείρισης Επιχειρησιακής Συνέχειας δικαιολογεί τη διενέργεια της επιθεώρησης Σταδίου 2,
- Ο βαθμός συμμόρφωσης των καθιερωμένων σχεδίων επιχειρησιακής συνέχειας και των προγραμμάτων επαλήθευσης, επικύρωσης και βελτίωσης της αποτελεσματικότητας του εφαρμοζόμενου Συστήματος Διαχείρισης Επιχειρησιακής Συνέχειας, με τις απαιτήσεις του εφαρμόσιμου προτύπου και τις επιλεγείσες σταρτηγικές και λύσεις επιχειρησιακής συνέχειας,
- Η διενέργεια αξιόπιστης εσωτερικής επιθεώρησης και ανασκόπησης από τη Διοίκηση,
- Η ανάγκη για ανασκόπηση πρόσθετης γραπτής τεκμηρίωσης και διάθεσης πρόσθετων πόρων ή τεχνογνωσίας κατά τη διενέργεια του Σταδίου 2 της επιθεώρησης,
- Ο εντοπισμός περιπτώσεων και αδυναμιών στην εφαρμογή του Συστήματος Διαχείρισης Επιχειρησιακής Συνέχειας, που μπορεί να προκαλέσουν εμφάνιση δυνητικών μη συμμορφώσεων και χρήζουν ιδιαίτερης προσοχής κατά τη διεξαγωγή της αξιολόγησης συμμόρφωσης Σταδίου 2.

Με βάση τα ευρήματα που τεκμηριώνονται στο Στάδιο 1 στη σχετική αναφορά επιθεώρησης, αναπτύσσεται ένα σχέδιο επιθεώρησης για τη διεξαγωγή της επιθεώρησης Σταδίου 2. Εκτός από την αξιολόγηση της αποτελεσματικής εφαρμογής του BCMS, οι αντικειμενικοί σκοποί του δεύτερου σταδίου είναι να επιβεβαιωθεί ότι ο επιθεωρούμενος οργανισμός εφαρμόζει τεκμηριωμένα και τηρεί τις δικές του καθιερωμένες πολιτικές, στόχους και διαδικασίες.

Για να γίνει αυτό, η επιθεώρηση θα επικεντρωθεί στα παρακάτω θέματα:

α) αναγνώριση του πλαισίου λειτουργίας του οργανισμού και τνω προσδοκιών των ενδιαφερομένων μερών

β) δέσμευση της Ανώτατης Διοίκησης για την πολιτική επιχειρηματικής/επιχειρησιακής συνέχειας και τους στόχους της επιχειρησιακής συνέχειας, πολιτική επιχειρηματικής/επιχειρησιακής συνέχειας και κοινοποίησή της, ρόλοι και υπευθυνότητες

β) απαιτήσεις τεκμηριωμένης πληροφορίας που προβλέπονται στο πρότυπο ISO 22301,

γ) αξιολόγηση της μεθοδολογίας για τη διενέργεια της εκτίμησης επιχειρηματικών/επιχειρησιακών επιπτώσεων (Business Impact Analysis) και των σχετικών αποτελεσμάτων,

δ) αξιολόγηση της μεθοδολογίας και των εξαγόμενων κινδύνων που σχετίζονται με την επιχειρησιακή λειτουργία του οργανισμού και την επιχειρησιακή του συνέχεια ,

ε) πληροφορίες επιδόσεων επιχειρησιακής συνέχειας και αποτελεσματικότητα του BCMS, αξιολόγηση σε σχέση με τους καθιερωμένους στόχους που σχετίζονται με την επιχειρησιακή συνέχεια,

στ) αξιολόγηση του σχεδιασμού και της υλοποίησης των σχεδίων επιχειρησιακής συνέχειας και των σχετικών προβλέψεων, καθώς και διαθεσιμότητα αναγκαίων πόρων για την αποτελεσματική εφαρμογή των σχεδίων,

ζ) εφαρμογή των σχετικών διαδικασιών και σχεδίων λαμβάνοντας υπόψη το εσωτερικό και εξωτερικό πλαίσιο λειτουργίας και τους συναφείς κινδύνους, την παρακολούθηση, μέτρηση και ανάλυση των διεργασιών επιχειρησιακής συνέχειας του οργανισμού, για να προσδιορισθεί αν τα στοιχεία ελέγχου είναι εφαρμοστέα και ανταποκρίνονται στους δεδηλωμένους στόχους της επιχειρησιακής συνέχειας,

η) τα προγράμματα, διεργασίες, διαδικασίες, αρχεία, εσωτερικές επιθεωρήσεις και ανασκοπήσεις της αποτελεσματικότητας του BCMS για να εξασφαλιστεί ότι αυτά είναι ανιχνεύσιμα στις αποφάσεις της Ανώτατης Διοίκησης και την πολιτική επιχειρησιακής συνέχειας και τους στόχους.

θ) τις στρατηγικές και λύσεις που έχουν επιλεγεί και εφαρμοστεί για την επιχειρησιακή συνέχεια.

ι) τον προγραμματισμό και τις ασκήσεις που έχουν αποτυπωθεί και πραγματοποιηθεί από τον οργανισμό για την επιχειρησιακή συνέχεια και τα αποτελέσματα αυτών

κ) την επάρκεια, εγρήγορση και ικανότητα του εμπλεκόμενου προσωπικού και τις σχετικές εκπαιδεύσεις του προσωπικού και την αποτελεσματικότητα τους

Η Ομάδα Επιθεώρησης πρέπει να:

α) απαιτεί από τον πελάτη να αποδείξει ότι οι λειτουργίες, τα σχέδια, η ανάλυση επιχειρησιακών επιπτώσεων και τα μέτρα είναι επαρκή για την επίτευξη των στόχων επιχειρησιακής συνέχειας του οργανισμού.

β) διαπιστώσει κατά πόσον οι καθιερωμένες διαδικασίες για την αναγνώριση, επιλογή και κατάρτιση των απαιτήσεων και σχεδίων για την επιχειρησιακή συνέχεια καθώς και των αναγνωρισμένων και ιεραρχημένων διακινδυνεύσεων, είναι συνεπείς με την πολιτική, τους σκοπούς και τους στόχους του οργανισμού, είναι κατάλληλες και εφαρμόζονται σωστά.

Εκτός από τις απαιτήσεις για την αναφορά επιθεώρησης στο ISO/IEC 17021-1, 9.4.8, η έκθεση επιθεώρησης παρέχει και τις ακόλουθες πληροφορίες ή μια σχετική αναφορά:

α) έναν απολογισμό της επιθεώρησης συμπεριλαμβανομένης της σύνοψης της ανασκόπησης των εγγράφων σε ότι αφορά την επάρκειά τους,

β) έναν απολογισμό της επιθεώρησης πιστοποίησης σε ότι αφορά συνολικά το σύστημα διαχείρισης επιχειρησιακής συνέχειας του επιθεωρούμενου οργανισμού και της καταλληλότητάς του,

γ) αποκλίσεις από το πρόγραμμα επιθεώρησης (π.χ. περισσότερο ή λιγότερο χρόνο που δαπανάται σε ορισμένες τακτικές δραστηριότητες),

δ) το πεδίο εφαρμογής του συστήματος διαχείρισης επιχειρησιακής συνέχειας που επιθεωρήθηκε (BCMS).

ε) παρατηρήσεις που έγιναν, τόσο θετικές (π.χ. αξιοσημείωτα χαρακτηριστικά) όσο και αρνητικές (π.χ. πιθανές μη συμμορφώσεις/αποκλίσεις)

στ) σχόλια σχετικά με τη συμμόρφωση του BCMS του πελάτη με τις απαιτήσεις πιστοποίησης με μια σαφή δήλωση περί της ενδεχόμενης μη συμμόρφωσης, και επιπλέον, οποιαδήποτε χρήσιμη σύγκριση με τα αποτελέσματα της προηγούμενης επιθεώρησης αξιολόγησης συμμόρφωσης του οργανισμού.

ζ) την πρόταση της ομάδας επιθεώρησης ως προς το κατά πόσον θα πρέπει να πιστοποιηθεί το BCMS του πελάτη ή όχι, με επαρκή παράθεση τεκμηριωμένων πληροφοριών για να αιτιολογηθεί αυτή τη σύσταση.

Η έκθεση επιθεώρησης είναι επαρκώς λεπτομερής ώστε να διευκολύνει και να υποστηρίζει την απόφαση πιστοποίησης. Αναλυτικά στοιχεία σε σχέση με τα σημαντικά δεδομένα και πληροφορίες που ιχνηλατήθηκαν και αξιολογήθηκαν κατά την επιθεώρηση (audit trails) καθώς και σε σχέση με τα αποδεικτικά στοιχεία (verifiable evidence) που συλλέχθηκαν, περιλαμβάνονται μέσα στο έντυπο της αναφοράς της επιθεώρησης. Πληροφορίες σχετικά με τα δειγματοληπτικά δεδομένα που αξιολογούνται κατά τη διάρκεια της επιθεώρησης περιλαμβάνονται επίσης μέσα στο έντυπο της αναφοράς της επιθεώρησης. Η αναφορά της επιθεώρησης συμπληρώνεται από τους επιθεωρητές που συμμετέχουν στην ομάδα επιθεώρησης, ελέγχεται και εγκρίνεται από τον Επικεφαλής της Ομάδας Επιθεώρησης και παραδίδεται στον αρμόδιο εντεταλμένο για χορήγηση του Φορέα Πιστοποίησης μαζί με τα υπόλοιπα έγγραφα της επιθεώρησης, παραθέτοντας όλη την απαιτούμενη πληροφόρηση για τη λήψη της σχετικής απόφασης χορήγησης πιστοποίησης.

Επιθεώρηση Επιτήρησης

Σκοπός της επιθεώρησης (αξιολόγησης συμμόρφωσης) επιτήρησης είναι να επιβεβαιώσει ότι το πιστοποιημένο BCMS εξακολουθεί να είναι κατάλληλο και αποτελεσματικό σε σχέση με το πεδίο εφαρμογής (fit for purpose), να εφαρμόζεται, να διατηρείται και να ανασκοπείται σε ότι αφορά τις δυνητικές επιπτώσεις τυχόν επιφερόμενων αλλαγών.

Η επιθεώρηση επιτήρησης για να επιβεβαιώσει τη συνεχή συμμόρφωση με τις απαιτήσεις και τα κριτήρια πιστοποίησης πρέπει να καλύπτει κατ' ελάχιστον:

α) τα σημαντικά στοιχεία διατήρησης του ΣΔΕΣ όπως η αξιολόγηση των διακινδυνεύσεων και του έλεγχου των απειλών για την επιχειρησιακή συνέχεια, των αποτελέσματων της ανάλυσης επιχειρησιακών επιπτώσεων, των σχεδίων επιχειρησιακής συνέχειας (ανταπόκρισης και αποκατάστασης/επαναφοράς ομαλής λειτουργίας), των σκήσεων και δοκιμών αποτελσματικότητας των σχεδίων επιχειρησιακής συνέχειας, των στρατηγικών και λύσεων επιχειρησιακής συνέχειας που έχει επιλέξει και καθορίσει ο οργανισμός, της εσωτερικής επιθεώρησης του BCMS, της ανασκόπησης από τη Διοίκηση και των διορθωτικών δράσεων,

β) τη συνεχιζόμενη συμμόρφωση του οργανισμού με τις εφαρμόσιμες νομοθετικές και τυποποιητικές απαιτήσεις,

γ) την επικοινωνία με τα εξωτερικά μέρη όπως απαιτείται από το πρότυπο ISO 22301,

δ) τις σημαντικές μεταβολές στις διεργασίες και στο περιβάλλον λειτουργίας του οργανισμού και τις ενδεχόμενες αλλαγές που σηματοδοτούνται στην τεκμηρίωση του ΣΔΕΣ,

ε) στις περιοχές επιχειρηματικής και επιχειρησιακής λειτουργίας που υπόκεινται σε αλλαγές (πχ αλλαγές στην εφοδιαστική αλυσίδα, αλλαγές στη μέθοδο παραγωγής προϊόντων και παροχής υπηρεσιών κλπ),

στ) σε επιλεκτικές απαιτήσεις του ISO 22301,

ζ) σε άλλες περιοχές λειτουργίας ανάλογα με την περίπτωση και την περιπλοκότητα και το μέγεθος του επιθεωρούμενου οργανισμού.

Ως ελάχιστο, σε κάθε επιτήρηση η ομάδα επιθεώρησης ανασκοπεί τα εξής:

α) την αποτελεσματικότητα του BCMS όσον αφορά την επίτευξη των στόχων της πολιτικής επιχειρησιακής συνέχειας του οργανισμού,

β) τη λειτουργία των διαδικασιών για την περιοδική αξιολόγηση και επανεξέταση της συμμόρφωσης με τις σχετικές νομοθεσίες και κανονισμούς για την επιχειρησιακή συνέχεια,

γ) τις αλλαγές στους ελέγχους που καθορίζονται, και τα αποτελέσματα αυτών των αλλαγών,

δ) την εφαρμογή και αποτελεσματικότητα των μέτρων για την αντιμετώπιση αποκλίσεων, κινδύνων και προβλέψεων σχετικών με την επιχειρησιακή συνέχεια,

ε) τα παράπονα, αγωγές, προσφυγές και καταγγελίες των ενδιαφερομένων μερών που σχετίζονται με το σύστημα διαχείρισης επιχειρησιακής συνέχειας

στ) τυχόν μη συμμορφώσεις και παρατηρήσεις από προηγούμενη επιθεώρηση αξιολόγηση συμμόρφωσης του BCMS/ΣΔΕΣ

Οι επιθεωρήσεις επιτήρησης μπορεί να συνδυαστούν με επιθεωρήσεις επιτήρησης άλλων συστημάτων διαχείρισης, σύμφωνα με τα προβλεπόμενα στον Γενικό Κανονισμό Πιστοποίησης. Η αναφορά επιθεώρησης πρέπει να παραθέτει με σαφήνεια τις πτυχές που σχετίζονται με κάθε σύστημα διαχείρισης.

Επιθεώρηση Επαναπιστοποίησης

Σκοπός της επιθεώρησης επαναπιστοποίησης είναι η επιβεβαίωση της συνεχιζόμενης συμμόρφωσης και αποτελεσματικότητας του συστήματος διαχείρισης επιχειρησιακής συνέχειας στο σύνολό του, καθώς και της συνεχιζόμενης καταλληλότητας και ισχύος του πεδίου εφαρμογής της πιστοποίησης. Μέσω της επιθεώρησης επαναπιστοποίησης αξιολογείται η διαρκής ικανοποίηση όλων των απαιτήσεων του Συστήματος Διαχείρισης Επιχειρησιακής Συνέχειας. Η αξιολόγηση συμμόρφωσης επαναπιστοποίησης πρέπει να σχεδιάζεται και να διενεργείται σε κατάλληλο χρόνο, ικανό για την έγκαιρη ανανέωση της πιστοποίησης, πριν από την ημερομηνία λήξης του πιστοποιητικού.

Η επιθεώρηση επαναπιστοποίησης περιλαμβάνει οπωσδήποτε και την ανασκόπηση των αναφορών των προηγούμενων επιθεωρήσεων επιτήρησης του κύκλου πιστοποίησης με σκοπό να αξιολογηθεί η συνολική επίδοση του επιθεωρούμενου οργανισμού.

Η επιθεώρηση επαναπιστοποίησης πρέπει να περιλαμβάνει μία επιτόπια επιθεώρηση, η οποία να καλύπτει, μεταξύ άλλων, τα ακόλουθα:

- την αποτελεσματικότητα του συστήματος διαχείρισης επιχειρησιακής συνέχειας συνολικά, αναφορικά με εσωτερικές και εξωτερικές αλλαγές και τη συνεχιζόμενη σχετικότητα και εφαρμοσιμότητα του πεδίου της πιστοποίησης,

- την αποδεδειγμένη δέσμευση για διατήρηση της αποτελεσματικότητας και της βελτίωσης του συστήματος διαχείρισης επιχειρησιακής συνέχειας, ώστε να βελτιώνεται η συνολική επίδοση του οργανισμού,
- την αποτελεσματικότητα του συστήματος διαχείρισης επιχειρησιακής συνέχειας, με αναφορά στην επίτευξη των αντικειμενικών σκοπών του πιστοποιημένου οργανισμού και τα επιδιωκόμενα αποτελέσματα.

Συγκεκριμένα για το Σύστημα Διαχείρισης Επιχειρησιακής Συνέχειας θα ελεγχθούν:

α) τα σημαντικά στοιχεία διατήρησης του ΣΔΕΣ όπως η αξιολόγηση των διακινδυνεύσεων και του έλεγχου των απειλών για την επιχειρησιακή συνέχεια, των αποτελέσματων της ανάλυσης επιχειρησιακών επιπτώσεων, των σχεδίων επιχειρησιακής συνέχειας (ανταπόκρισης και αποκατάστασης/επαναφοράς ομαλής λειτουργίας), των σκήσεων και δοκιμών αποτελσματικότητας των σχεδίων επιχειρησιακής συνέχειας, των στρατηγικών και λύσεων επιχειρησιακής συνέχειας που έχει επιλέξει και καθορίσει ο οργανισμός, της εσωτερικής επιθεώρησης του BCMS, της ανασκόπησης από τη Διοίκηση και των διορθωτικών δράσεων,

β) η συνεχιζόμενη συμμόρφωση του οργανισμού με τις εφαρμόσιμες νομοθετικές και τυποποιητικές απαιτήσεις και η συνεχιζόμενη καταλληλότητα του πεδίου εφαρμογής της πιστοποίησης,

γ) η επικοινωνία με τα εξωτερικά μέρη όπως απαιτείται από το πρότυπο ISO 22301,

δ) οι σημαντικές μεταβολές στις διεργασίες και στο περιβάλλον λειτουργίας του οργανισμού και τις ενδεχόμενες αλλαγές που σηματοδοτούνται στην τεκμηρίωση του ΣΔΕΣ,

ε) οι περιοχές επιχειρηματικής και επιχειρησιακής λειτουργίας που υπόκεινται σε αλλαγές (πχ αλλαγές στην εφοδιαστική αλυσίδα, αλλαγές στη μέθοδο παραγωγής προϊόντων και παροχής υπηρεσιών κλπ),

στ) επιλεκτικές απαιτήσεις του ISO 22301,

ζ) άλλες περιοχές λειτουργίας ανάλογα με την περίπτωση και την περιπλοκότητα και το μέγεθος του επιθεωρούμενου οργανισμού.

Ως ελάχιστο, σε κάθε επιτήρηση η ομάδα επιθεώρησης ανασκοπεί τα εξής:

α) την αποτελεσματικότητα του BCMS όσον αφορά την επίτευξη των στόχων της πολιτικής επιχειρησιακής συνέχειας του οργανισμού,

β) τη λειτουργία των διαδικασιών για την περιοδική αξιολόγηση και επανεξέταση της συμμόρφωσης με τις σχετικές νομοθεσίες και κανονισμούς για την επιχειρησιακή συνέχεια,

γ) τις αλλαγές στους ελέγχους που καθορίζονται, και τα αποτελέσματα αυτών των αλλαγών,

δ) την εφαρμογή και αποτελεσματικότητα των μέτρων για την αντιμετώπιση αποκλίσεων, κινδύνων και προβλέψεων σχετικών με την επιχειρησιακή συνέχεια,

ε) τα παράπονα, αγωγές, προσφυγές και καταγγελίες των ενδιαφερομένων μερών που σχετίζονται με το σύστημα διαχείρισης επιχειρησιακής συνέχειας

στ) τυχόν μη συμμορφώσεις και παρατηρήσεις από προηγούμενη επιθεώρηση αξιολόγηση συμμόρφωσης του BCMS/ΣΔΕΣ

Αν κριθεί σκόπιμη η υλοποίηση πλήρους επαναξιολόγησης, είτε λόγω χαμηλού βαθμού συμμόρφωσης του Συστήματος Διαχείρισης BCMS/ΣΔΕΣ του οργανισμού με τις απαιτήσεις του προτύπου, είτε λόγω λήξης της τριετούς διάρκειας ισχύος της αρχικής

πιστοποίησης (επίσκεψη επαναπιστοποίησης του τρίτου έτους) τότε αυτή εκτελείται με τους όρους, τα κριτήρια και τις προϋποθέσεις που ισχύουν για την αρχική επιθεώρηση αξιολόγησης συμμόρφωσης, χωρίς απαραίτητα να πραγματοποιείται η επιθεώρηση σε δύο στάδια υποχρεωτικά.

Κατά την επαναπιστοποίηση στο τέλος τρέχοντος κύκλου πιστοποίησης, όταν συμβαίνουν σημαντικές μεταβολές στο εφαρμοζόμενο ΣΔΕΣ/BCMS και όποτε επιζητείται τροποποίηση/επέκταση του πεδίου πιστοποίησης είναι απαραίτητο να υποβληθεί η προβλεπόμενη Αίτηση Πιστοποίησης εκ νέου. Στην Αίτηση Πιστοποίησης ο οργανισμός δηλώνει τον αριθμό προσωπικού που εμπλέκεται με την εφαρμογή του ΣΔΕΣ και την υλοποίηση των σχεδίων επιχειρηματικής/επιχειρησιακής συνέχειας (πχ. ανώτατη Διοίκηση, Υπευθύνους Τμημάτων του οργανισμού, μέλη των ομάδων ανταπόκρισης κλπ.) καθώς και τους υπεργολάβους/εξωτερικούς συνεργάτες.

Για τις ανάγκες επαναπιστοποίησης δύναται η Ομάδα Επιθεώρησης που ορίζεται, να είναι διαφορετικής σύνθεσης ως προς τα πρόσωπα, από την Ομάδα που εκτέλεσε την αρχική επιθεώρηση ή/και τις ενδιάμεσες υποχρεωτικές επιτηρήσεις του πρώτου και του δεύτερου έτους ισχύος της αρχικής πιστοποίησης.

5 Έντυπα

Για τις ανάγκες της τεκμηρίωσης των επιθεωρήσεων που εκτελούνται, χρησιμοποιούνται τα έντυπα σε ηλεκτρονική ή τυπωμένη μορφή, που αναφέρονται στις Διαδικασίες P01 και P05 του Συστήματος Διαχείρισης Ποιότητας της EQA HELLAS A.E.