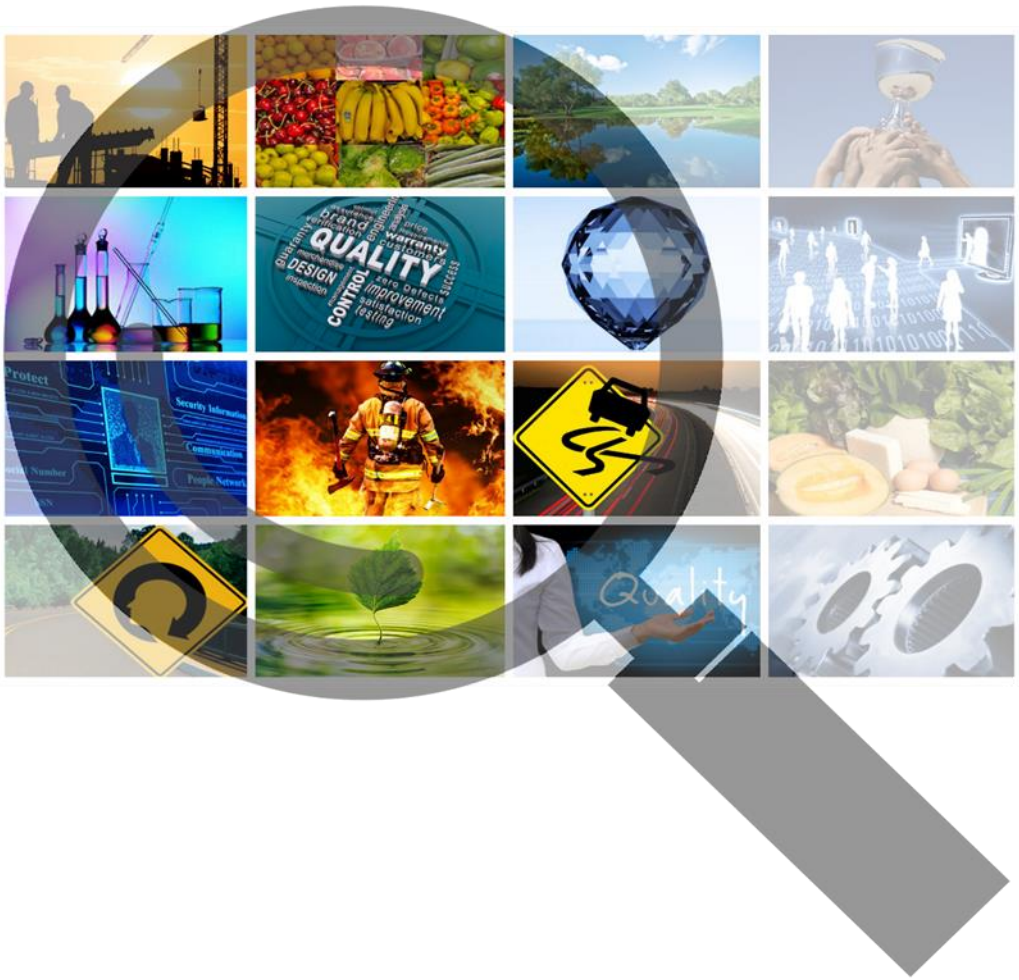


UDHËZIM NR.10
Tranzicioni i ISO 27001 në versionin e vitit 2022

2023

EQSC
European Quality & Safety Control
Rr. Sulejman Pasha, Pallati 70/1, Kati 1, Nr.1 1016 Tiranë

Ky dokument parashtron udhëzimet e EQSC për klientët e saj, për periudhën e tranzicionit të ndryshimit nga ISO 27001:2013 në ISO 27001:2022 të Sistemeve të Menaxhimit të Sigurisë së informacionit.

Siguria e informacionit

Përmbajtja

Siguria e informacionit

E përgjithshme

Informacioni është një element themelor në një organizatë, në të njëjtën mënyrë si punonjësit, ambientet dhe pajisjet. Informacioni shpreh njohurinë ose mesazhin në një formë konkrete. Ne mund të komunikojmë informacion, ne mund ta ruajmë atë, ne mund ta përsosim atë dhe ne mund të kontrollojmë proceset me të.
Prandaj, informacioni është i vlefshëm dhe duhet të mbrohet në bazë të nevojave. Informacioni mund të jetë i vlefshëm si për organizatat ashtu edhe për individin, ndonjëherë është edhe jetik. Nëse një informacion i tillë humbet ose është i pasaktë, mund të ketë pasoja katastrofike.

Çfarë do të thotë siguri e informacionit?
Siguria e informacionit ka të bëjë mbi të gjitha me parandalimin e rrjedhjes, shtrembërimit dhe shkatërrimit të informacionit. Ka të bëjë gjithashtu me disponimin e informacionit të duhur për njerëzit e duhur dhe në kohën e duhur. Informacioni nuk duhet të bjerë në duar të gabuara dhe të keqpërdoret. Siguria e informacionit vlen si për individët ashtu edhe për organizatat, si në biznes ashtu edhe në aktivitete publike. Prandaj, siguria e informacionit mbulon të gjithë aspektet e shoqërisë njerëzore.

Për këto arsye duhet të mbrojmë informacionin në mënyrë që:

- Të jetë gjithmonë i disponueshëm kur na nevojitet **(disponueshmëria)**
- Të mund të besojmë se është e saktë dhe jo i manipuluar apo i shkatërruar **(integriteti)**
- Të jetë i aksesuehëm vetëm nga personat e autorizuar **(konfidencialiteti)**

Siguria e informacionit

1. ISO/IEC 27001

Në 2005 u publikua versioni i parë i standardit ISO/IEC 27001 për sistemet e menaxhimit të sigurisë së informacionit (SMSI). Me zhvillimet teknologjike ky standard u rishikua në 2013 dhe së fundmi në Tetor 2022 është realizuar përditësimi i fundit i tij.

1.1 Çfarë është ISO/IEC 27001?

ISO/IEC 27001 është standardi më i njohur në botë për sistemet e menaxhimit të sigurisë së informacionit (ISMS). Ai përcakton kërkesat që duhet të plotësojë një ISMS.
Standardi ISO/IEC 27001 u ofron kompanive të çdo madhësie dhe nga të gjithë sektorët e veprimtarisë udhëzime për krijimin, zbatimin, mirëmbajtjen dhe përmirësimin e vazhdueshëm të një sistemi të menaxhimit të sigurisë së informacionit.
Pajtueshmëria me ISO/IEC 27001 do të thotë që një organizatë ose biznes ka ngritur një sistem menaxhimi për të menaxhuar rreziqet që lidhen me sigurinë e të dhënave që zotërohen ose trajtohen nga kompania, dhe se ky sistem respekton të gjitha praktikat dhe parimet më të mira të ISO 27001.

Zbatimi i kërkesave të sigurisë së informacionit të specifikuar në standardin ISO/IEC 27001 ju ndihmon të:

- Zvogëloni cenueshmërinë tuaj ndaj kërcënimit në rritje të sulmeve kibernetike.
- Përgjigjes ndaj rreziqeve në zhvillim të sigurisë së informacionit.
- Siguroni që asetet si pasqyrat financiare, pronësia intelektuale, të dhënat e punonjësve dhe informacioni i besuar nga palët e treta të mbeten të padëmtuara, konfidenciale dhe të disponueshme sipas nevojës.
- Siguroni një kornizë të menaxhuar nga zyra qendrore që siguron të gjitha informacionet që gjenden në një vend.
- Përgatitni njerëzit, proceset dhe teknologjinë në të gjithë organizatën tuaj për t'u përballur me rreziqet e bazuara në teknologji dhe kërcënime të tjera.
- Siguroni informacionin në të gjitha format, duke përfshirë të dhënat e bazuara në letër, të bazuara në cloud dhe të dhëna dixhitale.
- Kurseni para duke rritur efikasitetin dhe duke ulur shpenzimet për teknologjitë joefektive të mbrojtjes.
- Zbatoni deri në një nivel legjislacionin vendas dhe atë ndërkombëtar për sigurinë e informacionit dhe mbrojtjen e të dhënave.

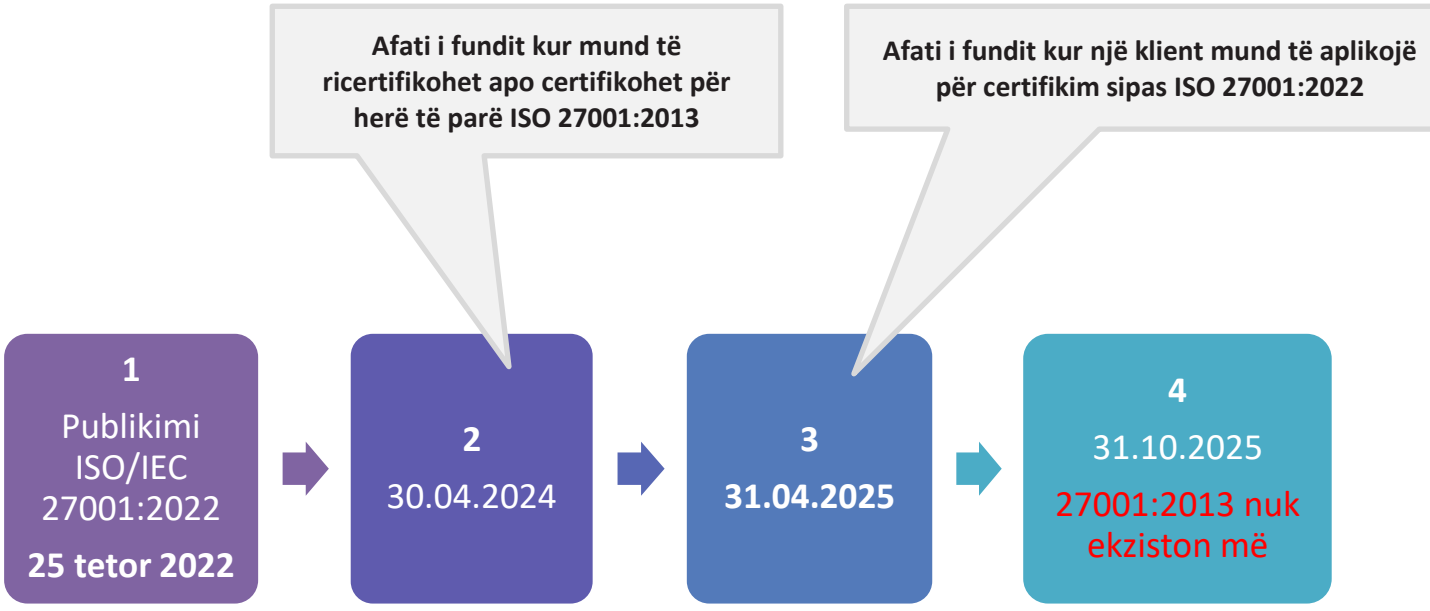
Siguria e informacionit

2. Periudha e tranzicionit

Me ndryshimin e ISO/IEC 27001 në 25 tetor 2022, një periudhë tranzicioni prej tre vjetësh planifikohet për organizatat e certifikuara sipas ISO/IEC 27001:2013. Pra kjo periudhë tranzicioni do të vazhdojë deri në datë 31 Tetor 2025.
Në përputhje me IAF MD 26:2023 për tranzicionin si dhe DA-IN-24, EQSC do të mundësojë brenda vitit 2023 të marrë akreditimi përkatës për këtë standard të përditësuar.

Në përputhje me sa më sipër EQSC ka përcaktuar rregullat e mëposhtme për tranzicionin.

Periudha 3 vjeçare e tranzicionit



Siguria e informacionit

2.1 Klientët ekzistues

EQSC ka përcaktuar që për klientët ekzistues, periudha nga publikimi i standardit deri në datën **31.04.2025** është e nevojshme që klientët të vlerësojnë mundësinë për tranzicionin e sistemit të tyre. Të gjitha certifikatat e lëshuara sipas ISO/IEC 27001:2013 e kanë vlefshmërinë deri më 31.10.2025, në rast se ky ka qenë dhe cikli i tyre i certifikimit.

Gjatë kësaj periudhe,

a) klientët kanë të drejtë që gjatë **auditimeve mbikëqyrëse dhe të ricertifikimit**, të kërkojnë auditimin sipas ISO/IEC 27001:2022. Kur auditimet e kalimit nga versioni i 2013 në versioni i 2022, kryhen gjatë auditimeve mbikëqyrëse ose të ricertifikimit, siç janë planifikuar më parë në ciklin e certifikimi, atëherë EQSC ju njofton se bazuar në IAF dhe në rregulloren e DPA, kohës normale të auditimit do ti shtohet një minimum prej:
   - auditimit mbikëqyrës: 1 ditë auditi/njeri.
   - auditimit ricertifikues: 0.5 ditë auditi/njeri

Në këtë mënyrë EQSC do të mundësojë auditimin e plotë të kërkesave ekzistuese dhe të reja, të versioni i 2013 dhe versioni i 2022.

b) në rast se klienti kërkon një auditim të veçantë, pasi e ka kaluar auditimin e planifikuar mbikëqyrës apo të ricertifikimit, ju njoftojmë se ky auditim **mund të kryhet** por do të ketë orë auditimi shtesë, krahasuar me pikën a) më sipër, në përputhje me rregulloret e IAF dhe DA-IN-24.
c) nëse klienti e kërkon, certifikatat versioni i 2013 dhe versioni i 2022, do të jenë paralelisht të vlefshme deri në 31.10.2025.
d) Certifikatat e akredituara sipas versioni e vitit 2022 do të lëshohen vetëm pasi EQSC të jetë akreditуar për të ofruar certifikim në standardin e ri dhe pasi sistemi i menaxhimit të klientit të ketë demonstruar konformitet me versionin e vitit 2022.
e) Nëse klienti kërkon të auditohet përpara se të akreditohet EQSC, dhe bie dakord me procedurat e EQSC, atëherë EQSC mund të lëshojë certifikatë të **pa-akredituar** në përputhje me ISO/IEC 27001:2022. Kjo certifikatë e pa-akredituar, do të rishikohet nga EQSC, pas akreditimit të tij.
f) Përpara auditimit të planifikuar sipas ISO/IEC 27001:2022, EQSC ju kërkon klientëve ti paraqesin të plotësuar: LiKP.310_9_LI kontrolli_ISO 27001_2022 faza 1. Në kolonën "Shënime" duhet të specifikojnë dokumentet e ndryshuara sipas kërkesave të ISO 27001:2022. Nëse klienti dëshiron, mund të zgjedhë të paraqesë në një dokument më vetë përshkrimin e ndryshimeve në sistemin e menaxhimit, por në çdo rast LiKP.310_9_LI kontrolli_ISO 27001_2022 faza 1 duhet të plotësohet dhe dërgohet pranë EQSC.
g) Certifikimi sipas ISO/IEC 27001:2022 nuk do të pranohet nga EQSC të realizohet vetëm me kontroll dokumentacioni, pa auditim prezent në kompani.

Siguria e informacionit

Rekomandimet e EQSC për procesin e tranzicionit

Kuptoni sa më mirë standardin e ri dhe ndryshimet krahasuar me versionin e mëparshëm!

Standardet kanë terma e koncepte të reja, ndaj është e rëndësishme studimi i tyre, marrja pjesë në trajnimet e organizuara nga EQSC apo kompani të tjera, si dhe të studiohen me vëmendje Anekset e standardeve të cilat japin shpjegime të rëndësishme.

Identifikoni pikat më të rëndësishme dhe përdorini ato në zhvillimin e sistemit tuaj

Në këtë kontekst disa nga ndryshimet më të rëndësishme dhe me vlerë për kompaninë, janë rreziku dhe mundësitë si dhe konteksti i organizatës: p.sh. plani i biznesit, planifikimi dhe kryerja e vlerësimit të kompetencës dhe/ose njohurive të organizatës. Këto janë pika të cilat duhet të adresohen sa më shpejt në mënyrë që të lehtësohet procesi i tranzicionit.

Përcaktuar momentin kur do të ndryshoni sistemin sipas standardeve të ndryshuara

Duhet të zgjidhni momentin më të përshtatshëm për ju, për të kryer ndryshimin. Ky moment duhet të vlerësohet duke pasur në konsideratë këtë udhëzim, por edhe kontakte për sqarime me EQSC.

Realizoni ndryshimet!

Zbatimi i kërkesave të rishikuara të standardeve kërkon një kohë të mjaftueshme për të dhënë rezultatet e saj. Për këtë arsye është e nevojshme që përpara se të aplikoni për certifikim sipas standardeve të reja, të kryeni një Auditim të brendshëm nëpërmjet të cilit do të keni një pasqyrë më të qartë të realizimit të ndryshimeve dhe nevojës për përshtatje të reja.

Aplikoni për Certifikim

Pasi të siguroheni se procesi i zbatimit të ndryshimeve është i finalizuar, EQSC ju mirëpret për aplikimin për certifikim sipas standardeve të ndryshuara. EQSC ka filluar procesin e akreditimit për këto standarde dhe në momentin e aplikimit të parë, do të mundësojë dhënien e certifikatave sipas standardeve të reja, të akredituara.

Këto janë thjesht Rekomandime!
Kini parasysh se vetë kompania juaj është përgjegjëse për procesin e tranzicionit dhe përputhjen e Sistemit tuaj të menaxhimit me kërkesat e standardit të përditësuar.

Siguria e informacionit

2.2 Klientët e rinj

Klientët e rinj, të cilët hyjnë në Sistemin e certifikimit të EQSC gjatë periudhës pas publikimit të standardit deri në datën **30.4.2024**, kanë mundësi të përzgjedhin nëse duan të certifikohen sipas versionit të 2013 ose versioni i 2022, ose të dyja.
Në rast se përzgjedhin direkt të zbatojnë vetëm sistemin e menaxhimit B sipas versionit të vitit 2022, klientët e rinj do të ndjekin procedurën e certifikimit të EQSC dhe nuk do të kenë kufizime në periudhën e tranzicionit, pasi do të ndiqet cikli i certifikimit në përputhje me versionin e vitit 2022 dhe standardet përkatëse.

Në rastin e përzgjedhjes së VERSIONI I 2013 + VERSIONI I 2022, ose vetëm të VERSIONI I 2013, kërkesat e përcaktuara në këtë dokument për periudhën e tranzicionit, janë të vlefshme.

3. Rishikimi i Sistemit të Menaxhimit nga Klientët

Të gjithë klientët aktualë dhe të rinj, të cilët aplikojnë për certifikim pranë EQSC sipas ISO/IEC 27001:2022, kanë afat deri në **6 muaj nga mbarimi i vlefshmërisë së versioni i 2013, pra 31.04.2025** të njoftojnë EQSC rreth statusit të zbatimit të kërkesave të standardit, në Sistemin e tyre të Menaxhimit.
EQSC i nxit klientët, që të konsiderojnë përpara datës së auditimit të çdo viti, njoftimin e EQSC se Sistemi i tyre i Menaxhimit është i gatshëm për tu audituar në përputhje me versionin e 2022. EQSC do të vlerësojë këto njoftime, dhe planifikojë auditimet sipas procedurave përkatëse të saj, për të gjithë klientët.
Afati më i fundit i zhvillimit të auditimit sipas versioni i 2013, për klientët e certifikuar versioni i 2013 dhe që duan të ruajnë ciklin e certifikimit, do të jetë data **31.04.2025**.
Kjo periudhë, do të shërbejë për të dhënë mundësinë kohore të duhur për mbylljen e jokonformiteteve të evidentuara gjatë auditimit si dhe përfundimin e procesit të vendimmarrjes së certifikimit. Në këtë mënyrë klientët dhe EQSC do të kenë mundësi të respektojnë afatin e mbarimit të certifikatave të lëshuara sipas standardit të shfuqizuar, dhe do të mundësoj që të gjithë klientët të jenë e pajisur me certifikatat sipas standardit të ri.

- EQSC **nuk do të pranojë auditime** sipas VERSIONI I 2013 pas datës **31.04.2025**.

Në rast se klienti nuk do të aplikojë për certifikim VERSIONI I 2022, pas datës 31.04.2025, Klienti do të mbajë vetë përgjegjësinë e mbarimit të afatit të certifikatës sipas VERSIONI I 2013 18001.

4. Përfundimi i periudhës së tranzicionit

Pas datës **31.10.2025** vlefshmëria e të gjitha certifikatave të lëshuara të akredituara, sipas versioni i 2013 **do të pushojë së ekzistuari**.

Pas kësaj date, nuk mund të pranohen nga EQSC certifikime sipas këtij standardi.

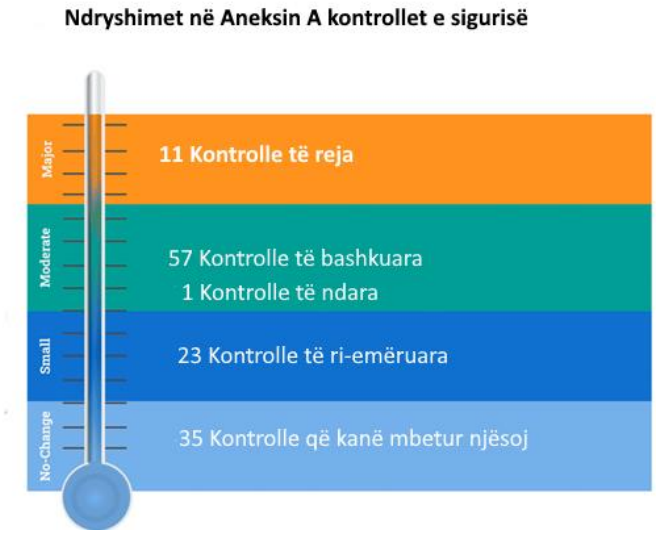
Siguria e informacionit

5. ISO/IEC 27001:2013 krahasuar me ISO/IEC 27001:2022.

5.1 Ndryshimet thelbësore

Krahasuar me ISO/IEC 27001:2013, ndryshimet kryesore të ISO/IEC 27001:2022 përfshijnë, por nuk kufizohen në:

i. Numri i kontrolleve ka rënë nga 114 në 93.
ii. Aneksi A tashmë ka të përcaktuar kontrollet në 4 seksione, në vend të 14 që ishin më parë.
iii. Janë përcaktuar 11 kontrolle të reja, ndërsa asnjë nga kontrollet nuk është fshirë dhe shumë kontrolle janë bashkuar.
iv. Aneksi A i referohet kontrolleve të sigurisë së informacionit në ISO/IEC 27002:2022, i cili përfshin informacionin e kontrollit, titullin dhe kontrollin.



v. Pika 6.1.3 c) është rishikuar duke përfshirë fshirjen e “objektivave të kontrollit” dhe përdorimin e "kontrollit të sigurisë së informacionit" për të zëvendësuar "kontroll".
vi. Formulimi i pikës 6.1.3 d) riorganizohet për të eliminuar paqartësitë e mundshme.
vii. Përdorimi i "procesit, produkteve ose shërbimeve të ofruara nga jashtë" për të zëvendësuar "proceset e jashtme" në pikën 8.1 dhe fshirja e termit "të jashtme".
viii. Mbajtja e konsistencës në foljen e përdorur në lidhje me informacionin e dokumentuar, për shembull, duke përdorur "Informacioni i dokumentuar do të jetë i disponueshëm si dëshmi e XXX" në pikat 9.1, 9.2.2, 9.3.3 dhe 10.2.
ix. Emërtimi dhe rirenditja e nënklauzolave në pikën 9.2 - Auditimi i brendshëm dhe 9.3 - Rishikimi i menaxhimit.
x. 9.3.3.c) ku përcaktohen inputete për mbledhjen e Rishikimit të menaxhimit janë ndryshuar nevojat dhe pritshmëritë e palëve të interesuara
xi. Shkëmbimi i rendit të dy nënklauzolave në pikën 10 - Përmirësimi.
xii. Përditësimi i edicionit të dokumenteve përkatëse të renditura në Bibliografi, si ISO/IEC 27002 dhe ISO 31000.
xiii. Disa devijime në ISO/IEC 27001:2013 në strukturën e nivelit të lartë HLS, tekstin bazë identik, termat e zakonshëm dhe përkufizimet thelbësore të standardeve të sistemeve të menaxhimit (SSM) janë rishikuar për përputhje me strukturën e harmonizuar për SSM, për shembull, neni 6.2 d).

Siguria e informacionit

5.2. Çfarë ka të re në standardin ISO/IEC 27001:2022?

ISO/IEC 27001:2022 paraqet disa kërkesa të reja:

- Shtimi i një pike të re 4.2 c) për të përcaktuar kërkesat e palëve të interesuara të adresuara nëpërmjet një sistemi të menaxhimit të sigurisë së informacionit (ISMS).
- Shtimi i një nënklauzole të re 6.3 - Planifikimi për ndryshime, i cili përcakton se ndryshimet në ISMS do të kryhen nga organizata në mënyrë të planifikuar.
- Shtimi te pika 8.1 i përcaktimit të proceseve dhe zbatimit të kontrolleve për to;

Modifikimet e paraqitura nga rishikimi i ri i 2022-ës nuk janë thelbësore, si rezultat nuk parashikohet që klientët të realizojnë shumë ndryshime në sistemin e tyre të menaxhimit.

Kjo është një përmbledhje e shkurtër e ndryshimeve thelbësore të standardit. Për tu njohur më tepër me ndryshimet e standardit, jeni të mirëpritur të merrni pjesë në **trajnimet profesionale të ofruara nga EQSC**.