

ISO 27001:2022
UDHËZUES TRANZICIONI PËR KLIENTËT

ISO 27001:2022 "Siguria e informacionit, siguria kibernetike dhe mbrojtja e privatësisë- Sistemet e menaxhimit të sigurisë së informacionit- Kërkesat" u lëshua në tetor 2022 dhe po zëvendëson ISO 27001:2013 përmes një periudhe tranzicioni tre vjeçare.

Të gjitha Kompanitë që dëshirojnë të mbeten të certifikuar sipas ISO 27001 do të duhet të kalojnë në rishikimin e standardit të vitit 2022 brenda periudhës së caktuar të tranzicionit që përfundon në tetor 2025.

Qëllimi i AQSCERT-së është të mbajë një qasje të qartë tranzicioni që është e lehtë për klientët tanë të kuptojnë dhe zbatojnë. Qëllimi ynë është t'u ofrojmë kompaniave udhëzimet dhe mjetet për ta bërë sa më të lehtë kalimin nga ISO 27001:2013 në ISO 27001:2022.

Të dy versionet e standardit ISO 27001 mbeten të vlefshme dhe auditimet për secilin version të standardit mund të kryhen në përputhje me rregullat e përmendura më poshtë, por duhet të bëhen plane që kalimi i një kompanie të ndodhë plotësisht përpara përfundimit të periudhës së tranzicionit.

Periudha e Tranzicionit

- ISO/IEC 27001:2022- Data e publikimit: 25 tetor 2022; Botimi i 3-të;
- Fillimi i periudhës së tranzicionit: 31 tetor 2022
- Nga 30 prilli 2024, të gjitha certifikatat dhe rinovimet e reja duhet të lëshohen ekskluzivisht sipas ISO/IEC 27001:2022.

AQSCERT do të vazhdojë të pranojë aplikime për certifikim dhe të lëshojë certifikata të reja sipas standardit ISO 27001:2013 deri në 01 Maj 2024.

- Të gjitha auditimet e tranzicionit duhet të kryhen deri në 31 korrik 2025.
- Periudha e tranzicionit përfundon 31 tetor 2025. Certifikatat për ISO/IEC 27001:2013 nuk do të jenë më të vlefshme pas kësaj date. Pas kësaj date dhe të gjitha auditimet e ricertifikimit rekomandohen të përdorin botimin ISO 27001:2022.

Aktiviteti i rregullimit do të përfshijë një kohëzgjatje minimale prej 0,5 person/ditë shtesë nëse kryhet përmes një auditimi rinovues dhe 1 person/ditë nëse kryhet përmes një auditimi të veçantë ose mbikëqyrës

ISO 27001:2022 Analiza e ndryshimeve

Ndryshimet brenda strukturës të standardit ISO 27001 janë bërë për të harmonizuar më mirë strukturën e harmonizuar për standardet e sistemit të menaxhimit (d.m.th. Aneksi SL).

Vlen të përmendet se ndryshimet janë bërë në kërkesat e mëposhtme:

- 4.2 Kuptimi i nevojave dhe pritshmërive të palëve të interesuara;
- 4.4 Sistemi i menaxhimit të sigurisë së informacionit;
- 6.2 Objektivat e sigurisë së informacionit dhe planifikimi për arritjen e tyre;
- 6.3 Planifikimi i ndryshimeve;
- 9.1 Monitorimi, matja, analiza dhe vlerësimi;
- 9.3.2 Inputet e rishikimit të menaxhimentit;

- Kontrollat e Aneksit A janë rigrupuar nga 14 objektiva kontrolli në 4 tema të gjera që përfshijnë:
 - 1- Kontrollat Kompaniive,
 - 2- Kontrollat Njerëzore,
 - 3- Kontrollat Fizike dhe
 - 4- Kontrollat Teknologjike.
- Numri i përgjithshëm i kontrolleve brenda Aneksit A është 93 kontrolle krahasuar me 114 kontrolle në botimin e mëparshëm
- Megjithatë, disa kontrolle të mëparshme janë konsoliduar në kontrolle të reja më të gjera; dhe janë shtuar 11 kontrolle të reja, duke përfshirë:
 - Inteligjenca e Kërcënimit;
 - Siguria e informacionit për përdorimin e Shërbimeve Cloud;
 - Monitorimi i sigurisë fizike;
 - Menaxhimi i konfigurimit;
 - Fshirja e informacionit;
 - Maskimi i të dhënave;
 - Parandalimi i rrjedhjes së të dhënave;
 - Filtrimi i ëëbit;
 - Kodimi i Sigurt.
- Përveç kësaj, ISO 27002:2022 identifikon 5 attribute kontrolli për të kategorizuar kontrollet në mënyra të ndryshme; atributet përfshijnë:
 - Lloji i kontrollit;
 - Karakteristikat e Sigurisë së Informacionit;
 - Konceptet e sigurisë kibernetike;
 - Aftësitë operacionale;
 - Domenet e Sigurisë
- ISO 27002:2022 përcakton gjithashtu një qëllim për çdo kontroll individual për të shpjeguar më mirë qëllimin e çdo kontrolli.

Për të siguruar që klientët janë të suksesshëm me tranzicionin e tyre, AQSCERT këshillon hapat e mëposhtëm:

Përgatitja për tranzicionin tuaj ISO 27001

- Kompanitë duhet të kalojnë sistemin e tyre të menaxhimit në përputhje me kërkesat e ISO 27001:2022 përpara se të kryhet auditimi i tyre i tranzicionit. Kjo duhet të përfshijë çdo ndryshim të dokumentacionit, së bashku me dëshminë e çdo kërkesë të re ose të ndryshuar të procesit.
- Kompanitë duhet të kryejnë një auditim të brendshëm dhe rishikim të menaxhmentit të kërkesave të reja/ndryshuara përpara se të kryhet auditimi i tranzicionit të AQSCERT-së.
- Kompanitë mund të kenë një vlerësim të mangësive të tranzicionit të kryer nga AQSCERT përpara auditimit të tyre zyrtar të tranzicionit. Kjo mund të kryhet në lidhje me një mbikëqyrje të mëparshme ISO 27001:2013, ose në çdo kohë tjetër të pavarur përpara auditimit të tyre të tranzicionit.

AQScert ka hartuar një Udhëzues Gap dhe një Mjet të Analizës së Boshllëqeve për të ndihmuar me tranzicionin tuaj, prandaj ju lutemi shkarkoni këto dokumente për të mësuar më shumë dhe për të filluar tranzicionin tuaj.

Auditimi juaj i tranzicionit ISO 27001

- Të gjitha kompanitë duhet të kenë një auditim tranzicioni për të konfirmuar zbatimin e standardit të rishikuar. Auditimi i tranzicionit mund të kryhet në lidhje me një auditim ekzistues, ose mund të jetë një auditim i pavarur.
- Nëse auditimi i tranzicionit kryhet në lidhje me një mbikëqyrje ekzistuese (d.m.th. mbikëqyrja e tranzicionit) ose auditimi i ricertifikimit (d.m.th. rivlerësimi i tranzicionit), kohëzgjatjes së auditimit mund t'i shtohet kohë shtesë për të mbuluar kërkesat/konceptet e reja të paraqitura nga ISO 27001:2022.
- Nëse kryhet një auditim i pavarur për auditimin e tranzicionit, kohëzgjatja të llogaritet në bazë të një kompanie individuale.

Shënim: Kohëzgjatjet specifike të auditimit për tranzicionin do të varen nga situata aktuale e kompaniës, duke përfshirë madhësinë e kompaniës dhe kompleksitetin e ISMS. Përfaqësuesi juaj i klientit të AQSCERT-së do t'ju këshillojë për kohëzgjatjen specifike të auditimit të tranzicionit

Certifikatat e rishikuara ISO 27001:2022

- Si me çdo auditim, mospërputhjet e identifikuar gjatë një auditimi të tranzicionit do të kërkojnë që një veprim korigjues të dorëzohet dhe miratohet. Një certifikatë e përditësuar ISO 27001:2022 do të lëshohet pas miratimit të veprimeve korigjuese.
- Lëshimi dhe vlefshmëria e certifikatës së përditësuar ISO 27001:2022 do të jetë si më poshtë:
 - Mbikëqyrja e tranzicionit- "Vlefshmëria deri në datë" ekzistuese e kompaniës do të mbahet;
 - Rivlerësimi i tranzicionit – Do të lëshohet një 'Vlefshmëri deri në datën' e re për periudhën e rinovuar 3-vjeçare;
 - Tranzicion i pavarur – "Vlefshmëria deri në datë" ekzistuese e kompaniës do të ruhet.

Lista kontrolluese e tranzicionit AQSCERT ISO 27001:2022

AQSCERT është në procesin e zhvillimit të një liste kontrolli të tranzicionit ISO 27001:2022, e cila ofron një kornizë të thjeshtë për vlerësimin e sistemit tuaj të menaxhimit kundrejt kërkesave të ISO 27001:2022. Pasi të publikohet, ne inkurajojmë Kompanitë që të përdorin këtë listë kontrolli si një mjet për të lehtësuar dhe regjistruar ndryshimet brenda sistemit të tyre të menaxhimit dhe për ta mbajtur këtë dokument për rishikim në auditimin e tyre të tranzicionit.

Kontrolloni përsëri në javët e ardhshme ose regjistrohuni në InTouch, buletin tonë të rregullt për t'u njoftuar për publikimin e tij.

Mbështetje shtesë

Ekipi i AQSCERT-së është këtu për t'ju mbështetur gjatë gjithë procesit të tranzicionit. Nëse keni ndonjë pyetje ose keni nevojë për ndonjë ndihmë, ne mund t'ju mbështesim me:

- Analiza Teknike dhe Udhëzime. AQSCERT do të ofrojë përmbajtje të ndryshme shtesë gjatë muajve të ardhshëm; ju lutemi kontrolloni faqen e internetit të AQSCERT-së dhe regjistrohuni në buletin tonë për të qëndruar të informuar.
- Para-vlerësimi / Analiza e mangësive. AQSCERT mund të ofrojë një Para-Vlerësim ose Analizë të Mangësive të ISMS-së tuaj të rishikuar për të përcaktuar nivelin e përputhshmërisë së ISMS-së tuaj me kërkesat e ISO 27001:2022.
- Ëëbinare dhe seminare. AQSCERT do të ofrojë analiza të përgjithshme interpretuese dhe udhëzime për tranzicionin; ju lutemi kontrolloni faqen e internetit të AQSCERT-së dhe regjistrohuni në buletin tonë për të qëndruar të informuar.

- Trajnim. AQSCERT ofron një numër kursesh tranzicioni për të siguruar që pjesëmarrësit të kenë të gjithë informacionin përkatës që u nevojitet për të siguruar një tranzicion të qetë për kompaninë e tyre.

Nëse keni ndonjë pyetje ose keni nevojë të flisni me dikë në lidhje me tranzicionin tuaj, ju lutemi na kontaktoni.

Tirane me 04/03/2023