Udhëzues për kalimin nga standardi ISO/IEC 27001:2013 në ISO/IEC 27001:2022

Zbatues: Stafi i DPA-së, vlerësuesit teknik dhe organet certifikues të sistemeve të menaxhimit të sigurisë se informacionit

Përgjegjës për zbatim: Drejtori i Drejtorisë së Organeve Certifikuese dhe Inspektuese

Kontrolli: Menaxheri i Cilësisë
Ardita MELE

Miratoi: Drejtori i Përgjithshëm
Pranvera FAGU

1 Qëllimi

Ky dokument përshkruan udhëzime për kalimin nga ISO/IEC 27001:2013 në ISO/IEC 27001:2022. Ky dokument është i vlefshëm për DPA dhe vlerësuesit e saj si dhe për organet certifikuese të sistemeve të menaxhimit të sigurisë së informacionit të akredituar nga DPA, organet certifikuese të sistemeve të menaxhimit të sigurisë së informacionit që kanë aplikuar për akreditim apo që kanë për qëlllim të aplikojnë për akreditim. Ky dokument është i vlefshëm deri në datën 31 Tetor 2025.

2 Fusha e zbatimit

Ky udhëzues zbatohet nga vlerësuesit dhe stafi i DPA, nga nënkontraktuesit e saj për vlerësimin e organeve certifikuese që kryejnë certifikim të sistemeve të menaxhimit të sigurisë së informacionit në përputhje me këtë standard.

3 Përgjegjësitë

Ky udhëzues është pjesë e sistemit të menaxhimit të DPA dhe si i tillë është nën përgjegjësinë e Drejtorit të Drejtorisë së Zhvillimit rishikimi i vazhdueshëm në varësi të ndryshimeve të duhura dhe përmirësimeve të vazhdueshme në sistemin e menaxhimit të DPA. Drejtori i Drejtorisë së Organeve Certifikuese dhe Inspektuese ka detyrë të kontrollojë zbatimin e këtij udhëzimi.

4 Referimet

Kjo procedurë referohet**:**

- Standardi S SH ISO 17011:2017,

- IAF MD 26:2023, versioni 2, Kërkesat e tranzicionit të ISO 27001:2022

5 Përkufizime

Në këtë udhëzues është përdorur terminologjia e standardit SSH ISO/IEC 17011:2017

IAF Forum Ndërkombëtar i Akreditimit
DPA Drejtoria e Përgjithshme e Akreditimit

6. PËRMBAJTJA

6.1. Të përgjithshme

Forumi Ndërkombëtar i Akreditimit (IAF) ka vendosur një periudhë tranzitore 3 vite (36 muaj) për kalimin nga

standardi ISO/IEC 27001:2013 në standardin ISO/IEC 27001:2022. Referuar dokumentit IAF MD 26:2023, versioni 2, periudha e tranzicionit për standardin ISO/IEC 27001:2022 do të vazhdojë deri më datë 31 Tetor 2025. DPA do të jetë gati për të kryer vlerësime sipas ISO/IEC 27001:2022 që nga data 1 Prill 2023. DPA do të filloje të kryeje vlerësime fillestare sipas ISO/IEC 27001:2022 që nga data 1 Prill 2023. Duke filluar nga data 1 Prill 2023, DPA nuk pranon më asnjë kërkesë të re për akreditim ose zgjerim të fushës së akreditimit, që i referohet standardit ISO 27001:2013. DPA duhet ta përfundojë vlerësimin e procesit të tranzicionit të organeve certifikuese të sistemeve të menaxhimit nga ISO 27001:2013 në ISO/IEC 27001:2022 deri më datë 31 Tetor 2023. Nëse një organ certifikues i akreditуar nuk përfundon në mënyrë të suksesshme vlerësimin e tranzicionit deri në datën 31 Tetor 2023, vlefshmëria e akreditimit sipas ISO/IEC 27001:2013 përfundon në datën 31 Tetor 2025.

Organi certifikues i akreditуar do të fillojë ofrimin e certifikimit fillestar të kompanive sipas standardit ISO/IEC 27001:2022 jo më vonë se data 31 Tetor 2023 . OVK duhet ta përfundojë procesin e tranzicionit nga ISO/IEC 27001:2013 në ISO/IEC 27001:2022 të klientëve të saj të certifikuar deri më datë 31 Tetor 2025.

6.2 VEPRIMET E ORGANIZMIT AKREDITUES.

DPA do të trajnojë vlerësuesit, kryevlerësuesit, specialistët e dosjeve, vendimmarrësit, anëtarët e komitetit teknik përkatës në lidhje me kërkesat e ndryshuara dhe të reja të ISO 27001:2022 si dhe me procesin e tranzicionit.

Për rastin e organeve certifikuese që aplikojnë për akreditim sipas ISO 27001:2022, DPA do të kryej vlerësimin fillestar të tyre duke filluar nga 1 Prill 2023.

Për organet certifikuese të akredituara më ISO/IEC 27001:2013, DPA do të shqyrtojë ndryshimet në ISO/IEC 27001, analizat e mangësive të cdo organi certifikues të akreditуar sipas skemës së certifikimit ISO 27001:2013, planet e tranzicionit/zbatimit të ISO 27001, dokumentacionin e ndryshuar ku të reflektohen ndryshimet sipas versionit të ri të ISO 27001, autorizimet e personelit për ISO/IEC 27001:2022, evidenca të zbatimit të versionit të ri të ISO 27001 dhe cdo informacion tjetër që DPA mund tju kërkojë organeve certifikuese. Organet certifikuese tëë akredituara nga DPA do të dërgojnëë dokumentacionin e mësipërm jo më vonë se data 3 Prill 2023.

Nëse rezultati i vlerësimit të dokumentacionit është pozitiv (organi certifikues ka demostruar plotësimin e kërkesave të versionit të ri të ISO 27001), DPA nuk organizon vizitë në zyrat e organit certifikues. Shqyrtimi i dokumentacionit nga ana e DPA do të llogaritet minimum një ditë pune dhe do të paguhet nga organi certifikues i akreditуar.
Nëse rezultati i vlerësimit të dokumentacionit nuk është pozitiv (organi certifikues nuk demostron plotësimin e kërkesave të versionit të ri të ISO 27001), DPA organizon vizitë në zyrat e organit certifikues. Kohezgjatja e vizitës bazohet në analizën e riskut. Vizita në organin certifikues për vlerësimin e tranzicionit të ISO 27001 do të jetë gjatë vizitës mbikëqyrëse ose në një vizitë shtesë. Vlerësim me dëshmi nuk është i nevojshëm.

DPA do të përditësojë informacionin e akreditimit të organeve certifikuese të akredituara (p.sh. certifikatën e akreditimit), nëse kompetenca e tyre për ISO/IEC 27001:2022 është demonstruar.

Vlerësimi në zyrën e OVK-së duhet të fokusohet në verifikimin e zbatimit të marrëveshjes së tranzicionit pavarësisht se kjo marrëveshje nuk është zbatuar plotësisht. Vlerësimi në zyrë duhet të përfshijë të paktën:
• Zbatimi i proceseve dhe procedurave të rishikuara të organit certifikues-së.
• Kompetenca e personelit përkatës është demonstruar para se të ishin përfshirë në aktivitetet e certifikimit kundrejt ISO/IEC 27001:2022.
• Ecuria e tranzicionit për klientët e certifikuar kundrejt standardit ISO/IEC 27001:2022.

Vlerësimet me dëshmi të planifikuara për tu zhvilluar pas vendimit për kalimin e tranzicionit do të bazohen në standardin ISO/IEC 27001:2022 duke vënë fokusin në vlerësimin e kompetencës së auditorëve për të kryer auditimet kundrejt ISO/IEC 27001:2022.

6.3 VEPRIMTARITË E ORGANEVE CERTIFIKUESE

Organi certifikues duhet të krijojë planin e tranzicionit për ISO/IEC 27001:2022 duke marrë parasysh kërkesat e këtij standardi dhe rregullat e përcaktuara për tranzicionin nga DPA. Plani i tranzicionit do të përcaktojë se çfarë do të bëjë organi certifikues dhe çfarë do të bëjë klienti.

Rekomandohet që Organet e Certifikimit të:

a) Planifikojnë dhe të përgatiten për të aplikuar tek DPA për tranzicionin dhe të bëhen gati për zbatimin e kërkesave të reja sipas afateve të përcaktuara në këtë udhëzues.

b) Zhvillojnë një plan tranzicioni duke përfshirë cështjet e mëposhtme:

– idenfikimin e ndryshimeve ndërmjet versionit të ri dhe atij të vjetër të standardit ISO/IEC 27001 dhe analizën e mangësive;
-analizimin e impaktit të ndryshimeve në aktivitetet/proceset përkatëse dhe identifikimin e veprimeve të kërkuara për të siguruar përputhshmërinë me kërkesat e versionit të ri të standardit (psh. Sistemi i menaxhimit/dokumentat, IT, etj);
- sigurimin që personeli përkatës eshte kompetent sipas versionit të rishikuar dhe procesin e tranzicionit;
-grupi i auditimit, në tërësi, duhet të ketë njohuri për të gjitha kontrollet e sigurisë së informacionit të përfshira në ISO/IEC 27002:2022 dhe zbatimin e tyre (shih ISO/IEC 27006:2015, 7.1.2.1.3 b));

- programi i auditimit të tranzicionit;

-percaktimin e komunikimit në kohë me klientin për programin e tranzicionit, të tilla si afati kohor, percaktimin e auditimit të tranzicionit dhe pasojat nëse klienti nuk arrin të kalojë përpara përfundimit të periudhës së tranzicionit;

c) fillimin e veprimeve të nevojshme sa më shpejt që të jetë e mundur.

Organet certifikuese mund të kryejë auditimin e tranzicionit gjatë autimeve të mbikqyrjes, të ricertifikimit ose nëpërmjet një auditimi të veçantë. Auditimi i tranzicionit nuk duhet të mbështetet vetëm në rishikimin e dokumentave, veçanërisht për rishikimin e kontrolleve teknologjik të sigurisë së informacionit.

Auditimi i tranzicionit përfshin, por nuk kufizohet në:
• Analiza e boshllëqeve të ISO/IEC 27001:2022, si dhe nevoja për ndryshime në ISMS të klientit.
• Përditësimi i deklaratës së zbatueshmërisë (SoA).
• Nëse është e aplikueshme, përditësimi i planit të trajtimit të rrezikut.
• Zbatimi dhe efektiviteti i kontrolleve të reja ose të ndryshuara të sigurisë së informacionit të zgjedhura nga klientët

Organi certifikues mund të kryejë edhe nje auditim në distancë mjafton që të plotësohen objektivat e auditimit të

tranzicionit.

Organet e certifikimit mund të përcaktojnë afatin kohor për dorëzimin e aplikimit për tranzicionin nga klientët e certifikuar në programin e auditimit të tranzicionit. Organi certifikues duhet të marrë vendimin e tranzicionit bazuar në rezultatin e auditimit të tranzicionit, Organi certifikues duhet të përditësojë dokumentet e certifikimit për klientët i certifikuar nëse ISMS-ja e tij plotëson kërkesat e ISO/IEC 27001:2022. Të gjitha certifikatat e lëshuara kundrejt ISO/IEC 27001:2013 duhet të skadojnë ose tërhiqet në fund të periudhës së tranzicionit.

6.4. Certifikimet e organeve certifikuese.

Certifikimet e reja dhe ricertifikimet:

Organet certifikuese duhet të përdorin versionin e ISO/IEC 27001:2022 për certifikim fillestar apo ricertifikim vetëm pas akreditimit të tyre sipas ISO/IEC 27001:2022.