Adresa: *Rruga Abdyl Frasheri, Nr 4/9+1, Tirana Albania.* tel/fax:
E-mail *www.fisa.pro*

SHTOJCA 3

RREGULLORE PËR ÇERTIFIKIMIN E SISTEMEVE TË MENAXHIMIT TË SIGURISË SË INFORMACIONIT NË PËRPUTHJE ME STANDARDIN ISO/IEC 27001:2025

3.1 TË PËRGJITHSHME

3.1.1 Kjo rregullore përcakton procedurat plotësuese dhe jo zëvendësuese të aplikuara nga FISA për certifikimin e sistemeve të menaxhimit të sigurisë së informacionit, në krahasim me atë që është përcaktuar tashmë në Rregulloren e Përgjithshme për Certifikimin e Sistemeve të Menaxhimit.
Pikat e këtyre rregulloreve u referohen pikave përkatëse të rregullores së përgjithshme për çertifikimin e sistemeve të menaxhimit për të cilat janë bërë shtesa.

3.1.2 NDRYSHIMI I RREGULLAVE TË PËRGJITHSHME

FISA lëshon certifikimin sipas kërkesave të ISO/IEC 17021:2015 dhe ISO/IEC 27006:2015 për organizatat, sistemi i menaxhimit, i të cilave, për sigurinë e informacionit është në përputhje me të gjitha kërkesat e Standardit ISO/IEC 27001:2025.

3.1.3 Sëbashku me Rregullat e Përgjithshme, terminologjia e përdorur në këtë rregullore tregohet gjithashtu në ISO/IEC 27001:2025.

3.2 CERTIFIKIMI FILLESTAR

(Pika 6.5.1 e Rregullores së përgjithshme të Certifikimit të SM)

3.2.1 Së bashku me rregullat e përgjithshme, organizatat, që dëshirojnë të marrin certifikim për sistemin e tyre të menaxhimit të sigurisë së informacionit, duhet, gjithashtu, t'i japin FISA-s të dhënat e tyre kryesore në lidhje me organizatën/prodhimin dhe vendndodhjen, duke plotësuar të gjitha pikat e formularit "Aplikim për certifikim" dhe "aneksin e formularit të aplikimit për ISO/IEC 27001 (certifikimi SMSI)", i disponueshëm në www.fisa.pro dhe dërgimi i tij tek FISA, e cila do ta përdorë atë për të përgatitur një kuotim.
Në veçanti, organizata duhet gjithashtu të informojë FISA-n nëse sistemi i menaxhimit të sigurisë së informacionit përfshin dokumentacion (procedura, regjistrime, etj.) të klasifikuara si "i rezervuar" dhe/ose në çdo rast është i padisponueshëm për qëllime certifikimi. FISA më pas do të vlerësojë nëse kushtet janë të përshtatshme për të vazhduar procesin e certifikimit.

3.3 KRYERJA E AUDITIMIT

(Pika 6.5.3 e Rregullores së Përgjithshme të Certifikimit të SM)

3.3.1 Sëbashku me rregullat e përgjithshme qëllimi i auditimit të fazës 1 është gjithashtu:

Adresa: *Rruga Abdyl Frasheri, Nr 4/9+1, Tirana Albania.* tel/fax:
E-mail *www.fisa.pro*

- të kontrollojë nëse vlerësimi i rrezikut,
  plani për trajtimin e rrezikut dhe deklarata e zbatueshmërisë (dhe çdo përjashtim i deklaruar) janë të përshtatshme në lidhje me fushën e aplikimit dhe aktiviteteve të organizatës.
- të kontrollojë nëse aktivitetet e nënkontraktuara janë identifikuar dhe monitoruar mjaftueshëm, duke konfirmuar, nëse është e nevojshme, domosdoshmërinë për të kryer një auditim tek palet e treta.

Faza 1 zakonisht kryhet në ambientet e klientit, mundësisht në zyrën e tij qendrore ose në çdo rast në një ambjent të përfshirë në fushën e certifikimit dhe ku do të kryhet auditimi i fazës 2. Mund të parashikohet, që në raste të veçanta, e vlerësuar rast pas rasti nga FISA , një pjesë e fazës 1 nuk nevojitet të kryhet në ambientet e organizatës.

3.4 MENAXHIMI I CERTIFIKATËS SË KONFORMITETIT
(Pika 6.5.4.1 e Rregullores së Përgjithshme të Certifikimit të SM)

3.4.1 Sëbashku me rregullat e përgjithshme, certifikatat e lëshuara i referohen deklaratës së zbatueshmërisë, botimit dhe datës së lëshimit të saj, që është në fuqi gjatë kryerjes së auditimeve në ambientet e organizatës.

3.5 SPECIFIKAT PËR ORGANIZATAT ME SHUMË VENDNDODHJE
(Pika 6.4 e Rregullores së përgjithshme të Certifikimit të SM)

3.5.1 Bashkë me rregullat e përgjithshme, të paktën aktivitetet e mëposhtme duhet të menaxhohen gjithashtu nga funksioni qendror i organizatës:

- përcaktimi dhe menaxhimi i politikës së sigurisë
- vlerësimi, analiza dhe trajtimi i rrezikut
- përcaktimi dhe menaxhimi i kontrolleve
- përcaktimi dhe menaxhimi i deklaratës për vlerësimin e zbatueshmërisë të kërkesave për trajnim.

3.5.2 Bashkë me rregullat e përgjithshme, FISA kontrollon gjithmonë mundësinë e marrjes së mostrave në të gjitha vendet dhe mund të vendosë nëse do ta kufizojë këtë kampionim në prani të:

- rezultatet e auditimeve të brendshme të zyrës qendrore dhe të vendndodhjeve ose të auditimeve të mëparshme të certifikimit;
- kompleksiteti i SMSI;
- kompleksiteti i sistemeve të IT-së në vendndodhje të ndryshme;
- ndërveprim i mundshëm me sistemet kritike të IT-së ose me sistemet e IT-së që menaxhojnë informacione sensitive;
- vlerësimi i rrezikut.

3.6 TRANSFERIMI I CERTIFIKATËS SË AKREDITUAR
(Pika 6.12 e Rregullores së përgjithshme të Certifikimit të SM)

Adresa: *Rruga Abdyl Frasheri, Nr 4/9+1, Tirana Albania.* tel/fax:
E-mail *www.fisa.pro*

3.6.1 Bashkë me rregullat e përgjithshme, organizata, nëse pranon ofertën ekonomike, duhet t'i dërgojë FISA "kërkesën për çertifikimin" së bashku me dokumentet e mëposhtme:

- kopje e kontrolluar e Deklaratës së Zbatueshmërisë e përmendur në certifikatë.