16.01.2024

Lausunto SFS:n standardointiryhmältä ”SFS/SR 211 Yhteiskunnan turvallisuus” CER-direktiivin kansallista toimeenpanotyötä tekeville viranomaisille ja muulle sidosryhmälle.

Aihe

Tähän dokumenttiin on koostettu CER-direktiiviä (2022/2557) ja sen artiklaa 16 koskevia standardeja, jotka ovat SFSn standardointiryhmän SFS/SR 211 mukaan hyödyllisiä tiedostaa direktiivin kansallisessa lainvalmistelu- ja muussa toimeenpanotyössä.

Suora lainaus artiklasta 16:

”..direktiivin johdonmukaisen täytäntöönpanon edistämiseksi jäsenvaltioiden on silloin, kun siitä on hyötyä, kannustettava käyttämään kriittisiin toimijoihin sovellettaviin toimenpiteisiin turvallisuuden ja häiriönsietokyvyn kannalta olennaisia eurooppalaisia ja kansainvälisiä standardeja…”

Standardien tunnuksista

Dokumentissa listatut standardit ovat kansainvälisiä standardeja, mikä tarkoittaa että ne on laadittu maailmanlaajuisessa standardointijärjestössä ISOssa tai eurooppalaisessa standardointijärjestössä CENissä. Mikäli standardin tunnuksessa esiintyy lyhenne ”ISO”, tämä tarkoittaa, että standardi on laadittu maailmanlaajuisessa standardointijärjestössä ISOssa. Mikäli standardin tunnuksessa esiintyy lyhenne ”EN”, tämä tarkoittaa, että standardi on laadittu eurooppalaisessa standardointijärjestössä CENissä. Mikäli standardin tunnuksessa esiintyy molemmat lyhenteet sekä ”EN” että ”ISO”, tämä tarkoittaa, että standardi on laadittu maailmanlaajuisessa standardointijärjestössä ja hyväksytty myös eurooppalaiseksi standardiksi eurooppalaisessa standardointijärjestössä CENissä. Mikäli standardissa on tunnus ”SFS”, tämä tarkoittaa että standardi kuuluu suomalaiseen standardikokoelmaan, ja on suomalainen standardi. SFS hyväksyy tarvearvioon, harkintaan ja julkiseen lausuntokierrokseen perustuen valittuja maailmanlaajuisessa standardointijärjestössä laadittuja ISO-standardeja suomalaisiksi SFS-ISO-standardeiksi. Eurooppalaisessa standardointijärjestössä eli CENissä laadittujen standardien tai sen erikseen hyväksymien ISO-standardien kohdalla SFS ei tee tarvearvioita, vaan nämä standardit hyväksytään sellaisenaan SFS-standardeiksi. Tämä toimintatapa on sääntö CENissä, joten kaikki sen kansalliset jäsenjärjestöt toimivat saman toimintatavan mukaisesti.

Eurooppalaisen standardin vahvuus on siinä, että se on automaattisesti myös kansallinen standardi kaikissa EU- ja ETA-maissa (CENin jäsenmaat). Alla olevassa listauksessa on muutamia eurooppalaisia standardeja, muutamia SFS-ISO-standardeja sekä muutamia ISO-standardeja. Standardien tunnusten yhteydessä esiintyy usein myös standardin voimaantulon vuosiluku. Tästä listauksesta ne on jätetty tarkoituksella pois siitä syystä, että tarkoituksena on ohjata lukija hyödyntämään aina kyseisen standardin uusinta painosta (standardeja uusitaan tyypillisesti muutamien vuosien välein). Mikäli vuosilukua ei ilmoiteta, viestitään että tarkoituksena on aina ensisijaisesti hyödyntää ko. standardin uusinta painosta.

Standardien hyödyntäminen osana lainsäädöntöä

Euroopan unioni toimii läheisessä yhteistyössä eurooppalaisten standardointijärjestöjen kanssa ja käyttää paljon standardeja säädöstensä tukena. Usein tuotteita koskeviin

säädöksiin kirjataan vain olennaiset vaatimukset, ja säädösten mukaisten tuotteiden valmistusta helpottamaan EU pyytää standardointijärjestöjä (CEN, CENELEC ja ETSI) laatimaan yksityiskohtaisia standardeja. Laadituille standardeille annetaan virallinen asema direktiivien jatkeina mainitsemalla ne Euroopan unionin virallisessa lehdessä. Standardit säilyvät luonteeltaan vapaaehtoisina, mutta valmistajat hyötyvät standardien käytöstä niin paljon, että haluavat useimmiten käyttää niitä. Tuotteiden katsotaan täyttävän säädösten eli asetusten ja direktiivien vaatimukset, kun ne on tehty säädöksissä viitattujen standardien mukaan. EU tai silloinen EY otti tämän ns. ”New Approach” -toimintatavan käyttöön jo 1980-luvulla. Toimintatapaa voidaan noudattaa myös muihin kuin tuotteiden säädöksiin ja standardeihin. Laissa säädetään oleelliset vaatimukset, ja standardissa esitetään tekniset ratkaisut tai toimintatavat näiden oleellisten vaatimusten täyttämiseksi. Standardit eivät kuitenkaan tässäkään tapauksessa ole velvoittavia, vaan ne säilyttävät vapaaehtoisen luonteensa. Jos tuote tai toiminta poikkeaa standardista, valmistajan tai toiminnasta vastuussa olevan on pystyttävä muulla tavoin osoittamaan, että se täyttää direktiivissä ja laissa esitetyt olennaiset vaatimukset.

Lainsäätäjä viittaa SFS-standardeihin monin paikoin suomalaisessa lainsäädöntökokoelmassa. Suomalaisen lainsäätäjän on tärkeää huomioida euroopassa vakiintunut hyvä viittaustekniikka, jossa standardeihin viitatessa ei velvoiteta lainkohteena olevaa soveltamaan standardia, vaan annetaan aina mahdollisuus jättää standardi soveltamatta, jolloin kuitenkin toiminnasta vastuussa olevan on pystyttävä muulla tavoin osoittamaan, että se täyttää toiminnassaan tai tuotteessaan laissa esitetyt olennaiset vaatimukset.

CER-direktiiviä koskevat standardit

1. SFS-ISO 28000 Turvallisuus ja kriisinkestävyys. Turvallisuuden hallintajärjestelmät. Vaatimukset
2. ISO 22316 Security and resilience — Organizational resilience — Principles and attributes
3. SFS-EN ISO 22301 Turvallisuus ja kriisinkestävyys. Liiketoiminnan jatkuvuuden hallintajärjestelmät. Vaatimukset
4. SFS-EN ISO 22313 Turvallisuus ja kriisinkestävyys. Liiketoiminnan jatkuvuuden hallintajärjestelmät. Ohjeistusta standardin ISO 22301 käyttöön
5. ISO/TS 22317 Turvallisuus ja kriisinkestävyys. Liiketoiminnan jatkuvuuden hallintajärjestelmät. Ohjeita liiketoiminnan vaikutusanalyysiin
6. ISO/TS 22332 Security and resilience — Business continuity management systems — Guidelines for developing business continuity plans and procedures
7. Riskienhallintaa
8. SFS-ISO 31000 Riskienhallinta. Ohjeet
9. SFS-EN ISO 22361 Security and resilience — Crisis management — Guidelines
10. ISO 22393 Security and resilience — Community resilience — Guidelines for planning recovery and renewal
11. SFS-EN ISO 22397 Yhteiskunnan turvallisuus. Yhteistyösopimusten solmimista koskevaa ohjeistusta
12. ISO 22396 Security and resilience — Community resilience — Guidelines for information exchange between organizations
13. SFS-EN 17483-1 Yksityiset turvallisuuspalvelut. Kriittisen infrastruktuurin suojaaminen. Osa 1: Yleiset vaatimukset
14. SFS-EN ISO/IEC 27001 Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset

16.01.2024

Yllä listatut standardit ryhmiteltynä aiheittain ja niitä koskevaa lisätietoa

Standardit yleistä turvallisuutta, toimitusketjuja sekä jatkuvuudenhallintaa koskevan johtamisjärjestelmän kehittämiseen

- SFS-ISO 28000
  - Standardissa annetaan vaatimuksia kokonaisvaltaisen turvallisuusjohtamisjärjestelmän rakentamiseksi mihin tahansa organisaatioon. Standardi kattaa turvallisuudenhallintajärjestelmälle osoitetut vaatimukset kokonaisvaltaisesti, mutta keskittyy tämän lisäksi erityisesti toimitusketjuihin ja niiden turvallisuuden johtamiseen.
- SFS-EN ISO 22301
  - Standardissa annetaan vaatimuksia turvallisuusjohtamisjärjestelmän rakentamiseksi mihin tahansa organisaatioon, joka keskittyy yksilöidysti toiminnan jatkuvuudenhallinnan varmistamiseen ja sen johtamiseen. Soveltamisala on siis kapeampi ja tarkempi kuin standardissa SFS-ISO 28000.
- SFS-EN ISO 22313
  - Standardissa annetaan ohjeita standardin SFS-EN ISO 22301 soveltamiseen, eli se tukee päästandardin käyttöä ja hyödyntämistä
- ISO/TS 22317
  - Tämä standardi on tekninen spesifikaatio (TS) ja siinä annetaan lisäohjeistusta päästandardissa (SFS-EN ISO 22301) mainittujen vaatimusten täyttämiseksi. Tässä tapauksessa lisäohjeistukset koskevat toiminnan vaikutusanalyysin tekoa, joka on yksi kulmakivistä tehokkaan jatkuvuudenhallinnan saavuttamiseksi.
- ISO/TS 22332
  - Tämä standardi on tekninen spesifikaatio (TS) ja siinä annetaan lisäohjeistusta päästandardissa (SFS-EN ISO 22301) mainittujen vaatimusten täyttämiseksi. Tässä tapauksessa lisäohjeistukset koskevat toiminnan jatkuvuudenhallintasuunnitelmia ja niissä kuvattavien menettelytapojen ja prosessien laatimista.

Standardit organisaation riskienhallinnan kehittämiseen

- SFS-ISO 31000
  - Standardissa esitetään kaikenlaisten riskien hallintaan soveltuvat riskienhallinan periaatteet, puitteet sekä yleisprosessi.

Standardeja kriisinkestävyydestä sen periaatteista ja terminologiasta

- ISO 22316
  - Standardissa esitetään kriisinkestävyyttä koskevia periaatteita ja ohjataan lukijaa kriisinkestävyyden kehittämisen kannalta olennaisten ominaisuuksien ja tekijöiden pariin.
  - Huom. tätä standardia ei ole vielä vahvistettu suomalaiseksi standardiksi (SFS-ISO), mutta vahvistamisprosessi on käynnissä, ja standardi on tätä koskevalla lausunnolla 15.01.2024-15.03.2024 välisenä aikana.

Standardeja koskien kriisinhallintaa

- SFS-EN ISO 22361
  - Standardissa esitetään kriisinhallintaohjeita, jotka auttavat organisaatioita suunnittelemaan, luomaan, ylläpitämään, tarkistamaan ja jatkuvasti parantamaan kriisinhallintakykyään.

Suomen Standardisoimisliitto SFS ry
Malminkatu 34, PL 130, 00101 Helsinki
p. 09 149 9331, www.sfs.fi, sfs@sfs.fi
Y-tunnus: 0202290-8

Standardeja kriisistä palautumiseen

- ISO 22393
  - Standardissa esitetään ohjeita kuinka kehittää ja suunnitella tehokkaita toimia kaikentyyppisistä kriiseistä, hätätilanteista, katastrofeista tai kriiseistä palautumiseen riippumatta siitä, millaisia ja kuinka laajoja vaikutuksia tai vahinkoja on aiheutunut. Standardissa korostuu ihmis- ja yhteisökeskeinen tulokulma, joten ohjeet ovat erityisen hyviä kolmannen sektorin organisaatiolle ja heidän keskinäiselle yhteistyölle.
  - Standardi kehitettiin koronan aikana vastaamaan koronapandemiasta kärsineiden yhteisöjen jälleenrakennustarpeisiin
  - Huom. tätä standardia ei ole vielä vahvistettu suomalaiseksi standardiksi (SFS-ISO), mutta vahvistamisprosessi on käynnissä, ja standardi on tätä koskevalla lausunnolla 15.01.2024-15.03.2024 välisenä aikana.

Yhteistyön kehittäminen, tiedonvaihto ja sopimusten solmiminen

- SFS-EN ISO 22397
  - Standardissa annetaan ohjeita organisaatioiden välisten yhteistyösopimusten solmimiseen. Näiden sopimusten avulla on tarkoitus hallita organisaatioiden välisiä suhteita yhteiskunnan turvallisuuteen vaikuttavien tapahtumien osalta. Standardi sisältää sopimuksia koskevat periaatteet ja siinä kuvataan sopimuksen suunnittelun, laatimisen, toteuttamisen ja katselmoinnin prosessi.
- ISO 22396
  - Standardi antaa ohjeita organisaatioiden väliseen tiedonvaihtoon. Se sisältää tiedonvaihdon periaatteet, puitteet ja prosessin. Se tunnistaa tiedonvaihdon mekanismeja, joiden avulla organisaatiot voivat oppia toistensa kokemuksista, virheistä ja onnistumisista.
  - Huom. tätä standardia ei ole vielä vahvistettu suomalaiseksi standardiksi (SFS-ISO), mutta vahvistamisprosessi on käynnissä, ja standardi on tätä koskevalla lausunnolla 15.01.2024-15.03.2024 välisenä aikana.

Kriittisen infrastruktuurin suojaamista koskevat turvallisuuspalvelut ja niiden laatu

- SFS-EN 17483-1
  - Standardissa asetetaan vaatimuksia kriittisen infrastruktuurin turvallisuuspalveluille ja niitä tarjoavalle organisaatiolle. Standardi on kehitetty nimensä mukaisesti kriittisen infrastruktuurin suojelua ja sen laatutasoa varmistamaan.

Tietoturvallisuuden hallinta

- SFS-EN ISO/IEC 27001
  - Standardi määrittelee ja ohjeistaa tietoturvallisuuden hallintajärjestelmän luomista ja käyttöä sekä tietoturvariskien huomioimista

Yhteenveto

CER-direktiivin toimeenpanotyössä on mahdollista hyödyntää olemassa olevia standardeja. Kansallisessa lainvalmistelussa tulisi tiedostaa tässä dokumentissa listatut standardit. Samaten tulisi tiedostaa paras mahdollinen viittaustekniikka.