DEKRA

Vaatimustenmukaisuudesta kilpailueduksi:
ISO/IEC 27001 -standardin käyttöönotto liiketoiminnallisen arvon luomiseksi

Sisällysluettelo

Vaatimustenmukaisuudesta kilpailueduksi:
ISO/IEC 27001 -standardin käyttöönotto liiketoiminnallisen arvon luomiseksi

Elämme aikaa, jolloin tieto on yksi organisaatioiden tärkeimmistä voimavaroista. Samalla digitalisaatio, pilvipalvelut, etätyö ja jatkuvasti kehittyvät kyberuhat tekevät tietojen suojaamisesta aiempaa haastavampaa. Pelkät tekniset tietoturvaratkaisut eivät enää riitä, vaan tarvitaan järjestelmällinen ja kokonaisvaltainen tapa hallita tietoturvaa.

Tässä oppaassa tutustutaan ISO/IEC 27001 -standardiin, joka on kansainvälisesti tunnustettu tietoturvan hallintajärjestelmien (ISMS, Information Security Management System) viitekehys. Opas kertoo, kuinka ISO/IEC 27001 auttaa organisaatioita hallitsemaan tietoturvariskejä järjestelmällisesti, täyttämään vaatimustenmukaisuusvaatimukset sekä vahvistamaan asiakkaiden ja yhteistyökumppaneiden luottamusta. Samalla se osoittaa, miten tehokas tietoturvan hallinta tukee liiketoimintaa ja luo organisaatiolle kestävää kilpailuetua.

Johdanto:
Jatkuvasti muuttuva kybermaailma

Perinteiset digitaalisen toimintaympäristön rajat ovat hämärtyneet. Pilvipalveluiden, etätyön ja yhä kehittyneempien kyberuhkien myötä organisaatiot eivät voi enää tukeutua pelkästään verkkorajaukseen perustuvaan tietoturvamalliin. Perinteinen kehäpuolustusmalli ei yksin enää riitä vastaamaan nykyisiin tietoturvahaasteisiin.

Tietomurrot voivat aiheuttaa merkittäviä taloudellisia menetyksiä, keskeyttää liiketoiminnan ja vahingoittaa organisaation mainetta pitkäksi aikaa. Siksi pelkkä reaktiivinen ja tarkistuslistoihin perustuva lähestymistapa tietoturvaan ei enää riitä.

Organisaatiot tarvitsevat aiempaa enemmän järjestelmällisen, mukautuvan ja käytännössä toimivaksi osoitetun viitekehyksen tietoturvariskien hallintaan. ISO/IEC 27001 tarjoaa tähän kansainvälisesti tunnustetun ratkaisun.

Mikä on ISO/IEC 27001?

Enemmän kuin pelkkä sertifiointitunnus

ISO/IEC 27001 ei ole ohjelmisto eikä pelkkä tarkistuslista, jonka kohdat rastitaan suoritetuiksi. Se on kansainvälisesti tunnustettu standardi tietoturvan hallintajärjestelmän suunnitteluun, käyttöönottoon, ylläpitoon ja jatkuvaan parantamiseen.

Akkreditoidun sertifiointielimen myöntämä ISO/IEC 27001 -sertifikaatti osoittaa, että organisaation tietoturvan hallintajärjestelmä on toteutettu standardin vaatimusten mukaisesti ja että sen tietoturvaa hallitaan järjestelmällisesti kansainvälisten parhaiden käytäntöjen mukaisesti.

Liiketoimintariskit	ISO/IEC 27001 -ratkaisut	Liiketoiminnalliset edut
Tietoturvaloukkaukset	Riskien arviointi ja hallinta	Parannettu suojaus
Vaatimusten noudattamatta jättäminen	Turvallisuuskontrollit ja - käytännöt	Säännösten noudattaminen
Toiminnan häiriöt	Jatkuva valvonta	Asiakkaiden luottamus ja kasvu

Se on järjestelmällinen

Tietoturvan hallintajärjestelmä on järjestelmällinen viitekehys, joka koostuu toimintaperiaatteista, menettelyistä, prosesseista ja hallintakeinoista. Sen avulla organisaatio hallitsee luottamukselliseen tietoon kohdistuvia riskejä.

Se perustuu riskienhallintaan

ISO/IEC 27001-standardin ytimessä on tietoturvariskien arviointi ja käsittely. Riskienhallinta mukautetaan organisaation toimintaympäristöön, tavoitteisiin ja uhkakuvaan, jotta se vastaa juuri kyseisen organisaation tarpeita.

Se on kokonaisvaltainen

Tietoturvan hallintajärjestelmä kattaa ihmiset, prosessit ja teknologian. Näin varmistetaan yhtenäinen ja johdonmukainen tietoturvan toteuttaminen koko organisaatiossa.

ISO/IEC 27001 -viitekehys:
Vaiheittainen lähestymistapa käyttöönottoon

VAIHE 1 Suunnittelu (Tietoturvan hallintajärjestelmän perustaminen)

Määritä laajuus:
Määritä tietoturvan hallintajärjestelmän rajat (koko organisaatio tai asiakkaan kannalta merkitykselliset osat, esim. osastot, tuotteet).

Johtaminen ja toimintaympäristö:
Varmista ylimmän johdon sitoutuminen ja ymmärrä organisaatiosi kannalta merkitykselliset sisäiset ja ulkoiset asiat.

Tavoitteet:
Organisaation yleiset tavoitteet on otettava huomioon tietoturvan kannalta ja tarvittaessa sovitettava niihin.

Määritä riskienarviointimenetelmä:
Määritä organisaation riskienhallinnan menetelmät, arviointikriteerit, riskinottohalukkuus ja riskien hyväksymisperusteet.

VAIHE 2 Toteutus (Järjestelmän käyttöönotto ja ylläpito)

Suorita riskinarviointi ja toteuta riskienhallinta:
Tunnista tietojesi luottamuksellisuuteen, eheyteen ja saatavuuteen kohdistuvat riskit, analysoi ne ja sovella liitteessä A mainittuja asianmukaisia valvontatoimenpiteitä.

Toteuta hallintatoimenpiteet:
Toteuta valitut riskienhallintasuunnitelmat, mukaan lukien tekniset (salaus, pääsyn valvonta), fyysiset (pääsyrajoitukset) sekä organisaatio- ja henkilöstövalvontatoimenpiteet (esim. roolit ja vastuut, tietoisuuden lisäämiseen tähtäävät ohjelmat, koulutus).

Laadi dokumentaatio:
Laadi vaadittu dokumentaatio, mukaan lukien soveltuvuuslausunto (SoA), riskienhallintasuunnitelma (RTP) ja tietoturvakäytännöt.

Varmista, että kaikki työntekijät ymmärtävät roolinsa tietoturvan hallintajärjestelmässä.

VAIHE 3 Tarkastus (Valvonta ja arviointi)

Seuraa suorituskykyä:
Mittaa valvontatoimenpiteiden ja prosessien tehokkuutta keskeisten suorituskyvyn mittareiden avulla (KPI).

Sisäiset auditoinnit:
Suorita säännöllisiä sisäisiä tietoturvan hallintajärjestelmän tarkastuksia ISO/IEC 27001 -standardin mukaisesti varmistaaksesi, että järjestelmä täyttää omat vaatimuksesi ja standardin vaatimukset sekä että se on toteutettu tehokkaasti.

Johdon arviointi:
Ylimmän johdon on tarkasteltava tietoturvan hallintajärjestelmää säännöllisesti varmistaakseen sen jatkuvuus, riittävyys ja tehokkuus. Johtoryhmän on oltava saatavilla asiaankuuluvat tiedot, kuten riskianalyysien tilanne.

VAIHE 4 Toiminta (Ylläpito ja parantaminen)

Korjaa poikkeamat:
Toteuta korjaavia toimenpiteitä auditointien tai arviointien aikana havaittujen puutteiden korjaamiseksi.

Jatkuva parantaminen:
Käytä ”Tarkastus”-vaiheen tuloksia järjestelmän ennakoivaan parantamiseen ja reagoi ympäristön ja organisaation muutoksiin.

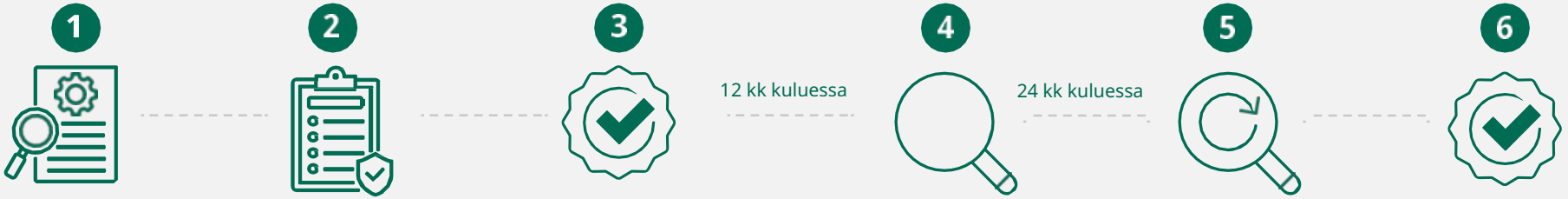
Tie sertifiointiin:
auditoinnin ymmärtäminen

Sertifiointiprosessin suorittaa akkreditoitu sertifiointielin kaksivaiheisessa auditoinnissa:

 Vaihe 1 (Asiakirjojen tarkastus/valmiusarviointi):
Auditoijat tarkastavat tietoturvan hallintajärjestelmän dokumentaation varmistaakseen, että se täyttää standardin vaatimukset, ja varmistavat olennaisten elementtien olemassaolon.

 Vaihe 2 (Paikan päällä suoritettava pääauditointi):
Auditoijat vierailevat organisaatiossanne tarkistaakseen, että järjestelmä on asianmukaisesti toteutettu ja toimii käytännössä. Kun prosessi on suoritettu onnistuneesti, mukaan lukien auditoijien tulosten riippumaton tarkastus, myönnetään sertifikaatti, joka on voimassa kolme vuotta. Vuosittaiset seuranta-auditoinnit varmistavat jatkuvan vaatimustenmukaisuuden.

Askeleet kohti onnistunutta ISO/IEC 27001 -sertifiointia



Auditointi

Vaihe 1: Arvioidaan dokumentoinnin vaatimustenmukaisuus.

Vaihe 2: Dokumentoinnin läpikäynti ja haastattelut.

Auditointiraportti

Johtamisjärjestelmän auditoinnin tulosten dokumentointi.

Sertifikaatti ja sinetti

Vaatimusten täyttyessä myönnetään sertifikaatti ja sinetti, joka on voimassa 3 vuotta.

Ensimmäinen seuranta-auditointi

Jatkuvan parantamisen ja kehittymisen arviointi.

Toinen seuranta-auditointi

Jatkuvan parantamisen ja kehittymisen arviointi.

Uudelleen sertifiointi

Vaatimusten täyttyessä myönnetään uusi sertifikaatti 3 vuodeksi ja toistetaan kohdat 2-6.

Asiakastarina:
Turvallisuuden ja luottamuksen vahvistaminen Innovatech Manufacturingissa

Innovatech Manufacturing on keskisuuri tarkkuuskomponentteja valmistava yritys, jonka tietoturvavaatimukset kasvoivat etätyön yleistymisen, kansainvälisen toimittajaverkoston sekä asiakkaiden luottamuksellisten tietojen käsittelyn myötä.

Tämän ratkaisemiseksi Innovatech Manufacturing otti käyttöön ISO/IEC 27001 -standardin PDCA-lähestymistapaa käyttäen:

 Suunnittelu: Yritys kartoitti kaikki kriittiset tietovarannot, tunnisti potentiaaliset riskit ja varmisti johdon tuen.

 Toteutus: IT-järjestelmiin, tuotantodokumentaatioon ja työntekijöiden prosesseihin otettiin käyttöön valvontatoimenpiteitä. Työntekijät kävivät pakollisen tietoturvakoulutuksen.

 Tarkastus: Säännölliset sisäiset auditoinnit ja avainlukujen seuranta auttoivat tiimiä seuraamaan toiminnan tehokkuutta ja havaitsemaan puutteet varhaisessa vaiheessa.

 Toimenpiteet: Jatkuvat parannukset ja korjaavat toimet vahvistivat tietoturvan hallintajärjestelmää ajan myötä.

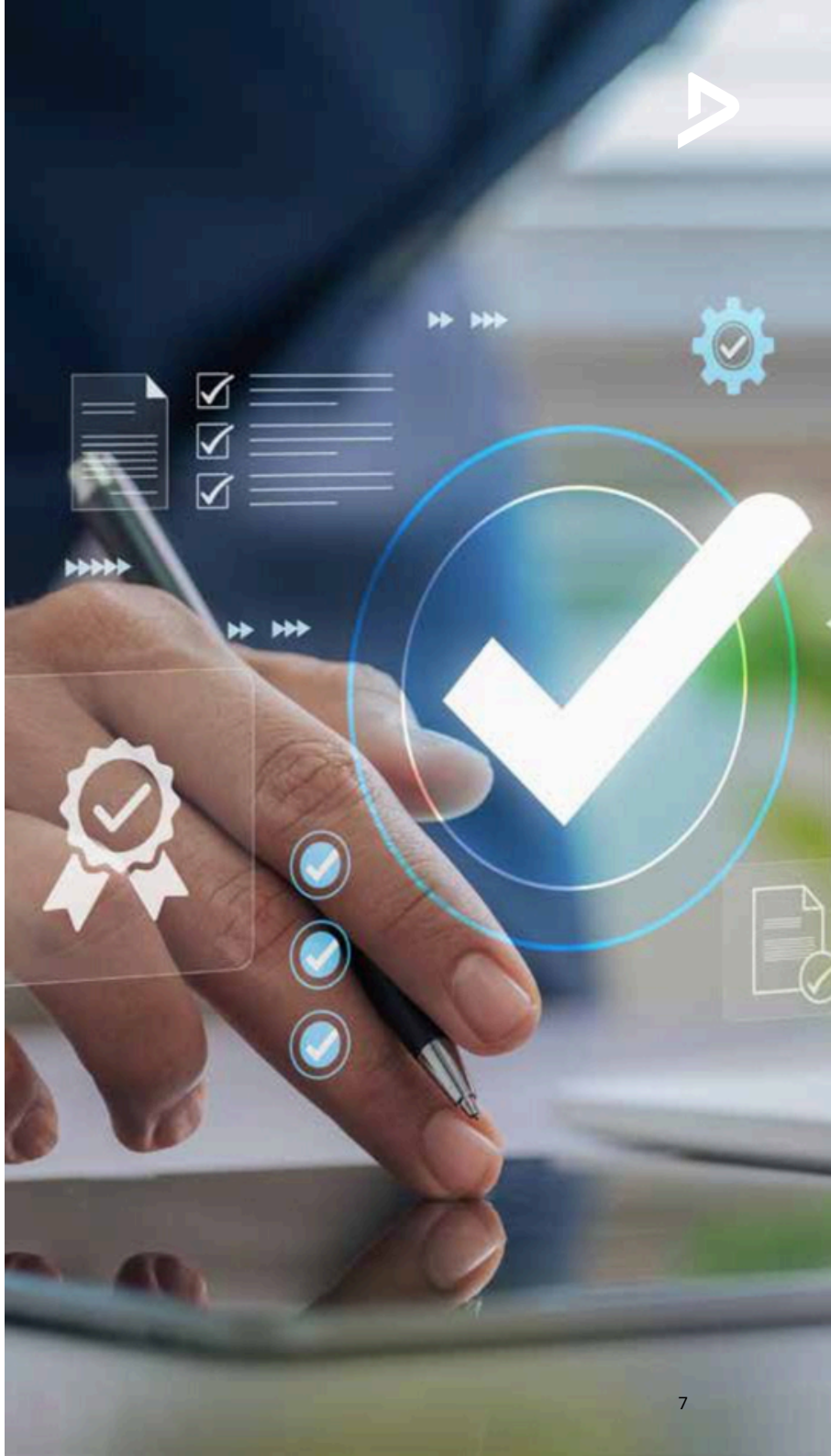
Tulokset:

 ISO/IEC 27001 -sertifiointi saavutettiin 12 kuukauden kuluessa.

 Turvallisuuspoikkeamat vähenivät 60 %, mikä esti mahdolliset toimintakatkokset ja taloudelliset menetykset.

 Vahvistettiin asiakkaiden luottamusta, mikä johti uusiin sopimuksiin merkittävien auto- ja ilmailualan kumppaneiden kanssa.

 Luotiin koko yrityksen kattava tietoturvatietoisuuden kulttuuri.



Johtopäätös:
Investointi joustavuuteen ja luottamukseen

ISO/IEC 27001 on paljon enemmän kuin keino täyttää vaatimustenmukaisuusvaatimukset. Se on strateginen investointi organisaation pitkän aikavälin menestykseen, toimintakykyyn ja kykyyn selviytyä muuttuvassa toimintaympäristössä.

Standardi tarjoaa selkeän ja järjestelmällisen viitekehyksen tietoturvariskien hallintaan sekä auttaa organisaatiota vastaamaan digitaalisen toimintaympäristön keskeisiin haasteisiin.

Ottamalla käyttöön ISO/IEC 27001 -viitekehyksen organisaatio rakentaa asiakkaiden ja yhteistyökumppaneiden luottamusta, osoittaa sitoutumisensa tietoturvan jatkuvaan kehittämiseen ja vahvistaa valmiuksiaan menestyä jatkuvasti muuttuvassa digitaalisessa toimintaympäristössä.

Haluatko lisätietoja? Ota yhteyttä!