KPMG IT Sertifiointi Oy

Palvelukuvaus

Elokuu 2021

kpmg.com/fi/it-sertifiointi

KPMG Public

KPMG
IT Sertifiointi Oy

Yrityksen nimi
KPMG IT Sertifiointi Oy

Y-tunnus
2469464-1

Osoite
Töölönlahdenkatu 3 A
PL 1037
00101 Helsinki

Yhteystiedot
+358 (0) 20 760 3000
etunimi.sukunimi@kpmg.fi

Toimitusjohtaja
Mika Laaksonen

Sisällys

1 Riippumattomuuden hallinta **2**
1.1 Eturistiriidat 3
1.2 Riippumattomuuden varmistaminen ja toimeksiantojen riskienhallinta 3
1.3 Riippumattomuuden varmistava toimielin 4
1.4 Luottamuksellisuus 4

2 Auditointiprosessi **5**
2.1 Sertifiointiin osallistuva henkilöstö 5
2.2 Ulkopuolisten auditoijien ja teknisten asiantuntijoiden käyttö 6
2.3 Suunnittelu 6
2.4 Esiauditointi 9
2.5 Sertifiointiauditointi 9
2.6 Sertifiointipäätös 10
2.7 Seuranta-auditoinnit 11
2.8 Valitusmenettely 12
2.9 Sertifikaattitodistus ja todistuksen käyttösäännöt 13
2.10 Sertifikaattirekisteri 13

Riippumattomuuden hallinta

KPMG IT Sertifiointi Oy toimii sertifiointielimenä ja tarkastuslaitoksena, ja se perustaa toimintansa itsenäisyyden, puolueettomuuden ja riippumattomuuden omaan tulorahoitukseen, toiminnan kannattavuuteen ja riittävään omavaraisuuteen.

Arvomme:

- Annamme toiminnallamme esikuvan muille.
- Työskentelemme yhdessä.
- Arvostamme toisiamme.
- Perustamme näkemyksemme tosiasioihin.
- Viestimme avoimesti ja rehellisesti.
- Kannamme yhteiskunnallisen vastuumme.
- Olemme riippumattomia.

Näihin arvoihin perustuen KPMG IT Sertifiointi Oy on sitoutunut puolueettomuuteen, eturistiriitatilanteiden hallintaan ja objektiivisuuteen. Riippumattomuuden varmistaminen on erityisen tärkeää KPMG IT Sertifiointi Oy:n toiminnassa, ja käytössämme on riippumattomuuden varmistamista tukevat menetelmät ja järjestelmät.

KPMG IT Sertifiointi Oy noudattaa KPMG-verkoston sääntöjä ja tukeutuu osaltaan verkoston tarjoamiin työvälineisiin riippumattomuuden ja toiminnan laadun varmistamiseksi.

1.1 Eturistiriidat

KPMG IT Sertifiointi Oy:lla on oikeus suorittaa seuraavia tehtäviä ilman, että ne katsotaan konsultoinniksi tai niistä syntyisi mahdollinen eturistiriita:

a.) Tietoturvajohtamiseen, siihen liittyviin johtamisjärjestelmiin tai auditointiin liittyvien valmennuskurssien järjestäminen tai luennoiminen yleisenä tiedon ja neuvonnan välittäjänä. KPMG IT Sertifiointi Oy ei tarjoa yrityskohtaista neuvontaa, joka on ristiriidassa alla olevan b-kohdan kanssa:

b.) Auditointistandardien vaatimusten tulkintaa kuvaavien tietojen asettaminen saataville tai julkaiseminen.

1.2 Riippumattomuuden varmistaminen ja toimeksiantojen riskienhallinta

Aina ennen kunkin toimeksiannon hyväksymistä KPMG IT Sertifiointi Oy:n riippumattomuus varmistetaan. Lisäksi toimeksiantojen riskit arvioidaan ja dokumentoidaan ennen toimeksiannon hyväksymistä. KPMG IT Sertifiointi Oy varaa oikeuden kieltäytyä toimeksiannoista, jotka

- uhkaavat KPMG Oy Ab:n tai KPMG IT Sertifiointi Oy:n riippumattomuutta (toimeksiannot, jossa jokin muu KPMG-verkostoon kuuluva yritys on suorittanut tarkastuksen kohteena olevaan toteutukseen liittyvää neuvontatyötä viimeisen kahden vuoden aikana),
- tapahtuvat maantieteellisesti sellaisella alueella, jossa KPMG:n henkilöstöön kohdistuu poikkeuksellisia työturvallisuus- tai turvallisuusriskejä (kriisialueet, geopoliittisesti epävakaat maat, epidemia-alueet),
- aiheuttavat muita uhkia KPMG Oy Ab:n tai KPMG IT Sertifiointi Oy:n toiminnalle, maineelle tai asiakkaille tai
- joissa auditoinnin kohteen ja KPMG IT Sertifiointi Oy:n näkemykset eivät kohtaa sertifioitavan toteutuksen laajuuden ja rajausten osalta. KPMG IT Sertifiointi Oy ei myönnä sertifikaattia silloin, mikäli sertifioitavan toteutuksen laajuus on olennaisilta osiltaan epätäydellinen.

1.3 Riippumattomuuden varmistava toimielin

Riippumattomuuden varmistamiseksi KPMG IT Sertifiointi Oy hyödyntää KPMG Oy Ab:n omaa erillistä Quality and Risk Management -yksikköä (QRM). KPMG IT Sertifiointi Oy noudattaa QRM-yksikön antamia määräyksiä ja ohjeita.

KPMG Oy Ab:n Ethics & Independence Partner/Risk Management Partner seuraa KPMG:n Independence Policyn noudattamista.

Toimeksiannot, jotka eivät vaaranna riippumattomuutta

ISO/IEC 27006 -standardin luku 5.2.1 määrittelee tehtävät, joita arviointilaitos voi tehdä ilman, että sen riippumattomuus vaarantuu. Sovellamme näitä sääntöjä KPMG IT Sertifiointi Oy:n toimeksiantoihin ja toimeksiantoja suorittaviin asiantuntijoihin.

KPMG IT Sertifiointi Oy ja sertifiointeihin osallistuvat henkilöt voivat tehdä seuraavia tehtäviä myös tarkastuksen kohteena olevissa organisaatioissa:

- auditointeja (ei kuitenkaan organisaation sisäisiä ISMS tai QMS auditointeja),
- koulutuksia (kunhan ne eivät sisällä yrityskohtaista neuvontaa),
- laatia ja julkaista sertifiointien pohjana oleviin vaatimuksiin liittyviä tulkintaohjeita tai muita vastaavia,
- esiauditointeja ja muita auditointi-/sertifiointivalmiuden toteamiseen liittyviä toimia (ei neuvontaa) sekä
- muihin standardeihin ja vaatimuksiin pohjautuvia auditointeja.

1.4 Luottamuksellisuus

KPMG IT Sertifiointi Oy saa sertifiointien yhteydessä tietoonsa luottamuksellista tietoa sertifioitavan toiminnasta. KPMG IT Sertifiointi Oy ei luovuta näitä luottamuksellisia tietoja kolmansille osapuolille muuten kuin laissa määritettyjen ehtojen mukaisesti.

Sertifiointitodistukseen merkitään toimeksiannon laajuus siinä muodossa kuin se on sertifioinnin laajuuden määrittelyn kannalta välttämätöntä ja asiakkaan kanssa yhdessä määritelty.

Auditointiprosessi

KPMG IT Sertifiointi Oy:n auditoinnit tehdään KPMG Oy Ab:n yleisen projektimallin mukaan. Haastattelut ja asiakkaalta tarvittavat dokumentit sovitaan jo suunnitteluvaiheessa, jotta projektin eteneminen ei viivästy.

Alla on kuvattu auditointien vaiheet ja auditointiprosessi, joka liittyy tietoturvallisuuden- tai laadunhallintajärjestelmän sertifiointiin, eli kaikkiin sellaisiin auditointeihin, joissa lopputuloksena on asiakkaalle myönnetty
ISO 27001 tai ISO 9001 -sertifiointi vaatimusten täyttyessä.

2.1 Sertifiointiin osallistuva henkilöstö

Kaikkiin auditointeihin osallistuu vähintään kaksi henkilöä, joista toinen on projektipäällikkö. Tarvittaessa auditoinneissa käytetään erityisosaamista esimerkiksi teknisempien tarkastuskohteiden osalta.

Mikäli kyseessä on sertifiointiauditointi, KPMG IT Sertifiointi Oy:n toimitusjohtaja tekee sertifiointipäätöksen kuultuaan auditointryhmän esityksen asiasta. Sertifiointipäätöksen tekijä ei itse osallistu aktiivisesti auditointiin.

2.1.1 Auditointitoimeksiantojen osaamisvaatimukset

KPMG IT Sertifiointi Oy noudattaa ISO 27006 sekä ISO 17021-1 -standardien vaatimuksia projekteihin osallistuvien henkilöiden osaamisen minimivaatimuksissa. KPMG IT Sertifiointi Oy varmentaa koulutusten ja perehdytyksen avulla auditointitiimin jäsenten tietämyksen soveltuvin osin

- tietoturvasta,
- laadunhallinnasta,
- teknisen tietämyksen auditoitavasta toiminnasta,
- johtamisjärjestelmistä,
- auditoinnin periaatteista sekä
- johtamisjärjestelmien monitoroinnista, mittaamisesta, analysoinnista ja arvioinnista.

Vaatimukset koskevat kaikkia auditointitiimin jäseniä, pois lukien tekninen tietämys auditoitavasta toiminnasta, joka voidaan jakaa tiimin jäsenten kesken.

2.1.2 Auditointitiimin työn ja osaamisen osoittaminen sekä laadunvarmistus

Auditointien suorittajien työn laatua ja osaamista valvotaan osana projektien laadunvarmistusprosessia. Toimeksiantoihin osallistuu Lead Auditor, joka tarkkailee muun tiimin suoritusta osana auditointia ja reagoi tarvittaessa. Jokaisen toimeksiannon jälkeen asiakkaalta pyydetään projektipalaute ja mikäli palautetta saadaan, se käydään läpi toimeksiantotiimin kanssa. Palautteet tulevat automaattisesti myös KPMG IT Sertifiointi Oy:n toimitusjohtajalle, joka voi tarvittaessa reagoida palautteeseen sen vaatimalla tavalla.

2.1.3 Turvallisuusselvitykset

Turvallisuusselvityshakemukset tehdään ennen toimeksiannon aloittamista. Jos auditoijalla on olemassa voimassaoleva turvallisuusselvitys, tätä ei tehdä uudestaan. Jos voimassa olevaa turvallisuusselvitystä ei ole tai siitä ei ole varmuutta, tehdään uusi turvallisuusselvitys.

2.2 Ulkopuolisten auditoijien ja teknisten asiantuntijoiden käyttö

Osa auditointityöstä voidaan ulkoistaa KPMG Oy Ab:n tehtäväksi niillä edellytyksillä, jotka esitetään ISO 17021 -standardissa. Tällöin kyse ei ole suoranaisesti ulkoistamisesta, vaan ulkoisten asiantuntijoiden käyttämisestä. Vastuu sertifioinnista ja koko sertifiointiprosessista säilyy KPMG IT Sertifiointi Oy:llä.

KPMG Oy Ab:n henkilöstö osallistuu sertifiointiauditointeihin teknisinä asiantuntijoina tai yksittäisinä auditoijina, kuten on esitetty ISO 17021-1 -standardin luvussa 7.3.

Luottamuksellisuuteen, eturistiriitoihin ja riippumattomuuteen pätevät samat säännöt, jotka on esitetty tämän palvelukuvauksen kohdassa 1 Riippumattomuuden hallinta.

2.3 Suunnittelu

2.3.1 Sertifiointihakemus

Ennen auditointia asiakasorganisaation tulee toimittaa sertifiointihakemus KPMG IT Sertifiointi Oy:lle. Erityisen tärkeää on sertifioinnin kohteen ja rajauksen määrittely, koska se vaikuttaa merkittävästi tulevaan auditointiin. Sertifiointihakemuksessa kuvataan organisaation toiminta, jolle sertifikaattia tullaan hakemaan mahdollisine rajauksineen. Hakemus sisältää lisäksi perustiedot organisaatiosta, prosesseista, aikaisemmista sertifioinneista sekä organisaatiota koskevat lait, määräykset ja asetukset. Sertifiointihakemukseen käytetään vakiomuotoista KPMG IT Sertifiointi Oy:n verkkosivuilta löytyvää hakemuspohjaa. Sertifiointihakemuksessa asiakasorganisaation tulee antaa seuraavat tiedot sertifiointia varten:

- sertifioinnin laajuus,
- sertifiointiskeeman kannalta olennaiset tiedot organisaatiosta, mukaan lukien nimi ja toimipisteiden osoitteet, prosessit ja toiminnot, henkilöstö- ja tekniset voimavarat, toimintayksiköt, sidosryhmäsuhteet ja olennaiset lainsäädännölliset vaatimukset,
- sellaisten ulkoistettujen prosessien identifiointi, jotka vaikuttavat vaatimusten säännönmukaiseen noudattamiseen,
- standardit tai muut vaatimukset, joille organisaatio hakee sertifiointia sekä
- mahdollinen sertifioitavaan johtamisjärjestelmään hankittu konsultaatio.

2.3.2 Auditoinnin suunnittelu

KPMG IT Sertifiointi Oy tarkastaa sertifiointihakemuksen ja sitä täydentävät tiedot varmistaakseen, että:

– tiedot hakijaorganisaatiosta ja sen johtamisjärjestelmästä ovat riittäviä auditointiohjelman läpiviemiseksi,

– kaikki KPMG IT Sertifiointi Oy:n ja hakijaorganisaation väliset ymmärryserot selvitetään,

– KPMG IT Sertifiointi Oy:llä on kyky ja pätevyys suorittaa sertifiointi ja

– sertifioinnin vaadittu laajuus, hakijaorganisaation toimintojen sijainnit, auditointeihin vaadittava aika ja muut sertifiointitoimiin vaikuttavat tekijät (muun muassa kieli, turvallisuusolot, uhat riippumattomuudelle) on otettu huomioon.

Suunnitteluvaihe aloitetaan, kun asiakas on hyväksynyt projektin. Viimeistään tässä vaiheessa projektille määritellään projektipäällikkö, yhteyshenkilö sekä laatuvastaava.

2.3.3 Auditoinnin laajuuden määrittäminen

Auditoinnin laajuutta ja kestoa määritettäessä nojaudutaan kokeneen henkilökunnan sekä pääauditoijien kokemuksiin vastaavista auditoinneista sekä ympäristöistä. Hallintajärjestelmiin liittyvissä auditoinneissa kokemusta täydennetään
ISO 27006 -standardin määrittelemillä vaatimuksilla, joita ovat muun muassa :

– auditoitavan hallintajärjestelmän ja käytetyn kriteeristön vaatimukset,

– asiakkaan koko ja kompleksisuus (käytettävien tietojärjestelmien/siirrettävän tiedon määrä, henkilöstön/käyttäjien lukumäärä, ylläpitäjien määrä ja eri verkkojen lukumäärä),

– käytetyt teknologiat sekä lainsäädännön ja muun säätelyn vaatimukset asiakkaan toimialaan liittyen,

– mahdolliset hallintajärjestelmään/ auditoinnin kohteeseen vaikuttavat ulkoistukset,

– edeltävien auditointien tulokset,

– auditoitavien toimipaikkojen lukumäärä ja etäisyys toisistaan sekä toimintojen vastaavuus tai erot päätoimipaikkaan (huomioidaan muun muassa eri työvuorot),

– auditoitavan organisaation toimintaan, tuotteisiin tai prosesseihin liittyvät erityiset riskit ja

– muiden menossa ja tulossa olevien auditointien mahdollinen yhdistäminen.

Auditoinnin laajuuden määrittäminen laadunhallintajärjestelmien sekä integroitujen hallintajärjestelmien osalta suoritetaan IAF MD 1:2018, IAF MD 5:2019 sekä IAF MD 11:2014 velvoittavien ohjeiden mukaisesti.

Arviomme auditoinnin laajuudesta ja määritellään aina kirjallisesti. Mikäli työn aikana havaitaan, että laajuus poikkeaa suunnitellusta huomattavasti, otetaan tämä välittömästi käsittelyyn asiakkaan kanssa.

2.3.4 Auditointi- ja työmenetelmät

Sertifiointiauditoinnit tehdään KPMG IT Sertifiointi Oy:n yleisen tarkastusmenetelmän mukaan, ja niissä käytetään viitekehyksenä voimassa olevaa ISO 27001 tai ISO 9001-standardia.

Kaikista tarkastettavista vaatimuksista tuotetaan dokumentaatio, jossa kuvataan vaatimusten toteutuminen ja todennustapa. Todentamisessa noudatetaan hyväksyttyjä todentamistapoja. Todentamistapoja ovat haastattelu, dokumentaatiokatselmoinnit, pistokokeet sekä tekninen varmentaminen. Mikäli vaatimus ei täyty, puutteisiin johtaneet syyt yksilöidään ja dokumentoidaan.

2.3.5 Tietojen kuljettamis- ja säilyttämiskäytännöt

Tietojen välitystapa kohteen (tietojen omistajan) ja KPMG IT Sertifiointi Oy:n välillä sovitaan aina ennen tietojen välittämistä. Tietojen kuljettamis- ja säilyttämiskäytännöt dokumentoidaan aloituspalaverin pöytäkirjaan.

Tietojen välittäminen tapahtuu millä tahansa tietojen omistajan hyväksymällä menettelyllä. KPMG IT Sertifiointi Oy:n asiantuntijat voivat kuitenkin tuoda ilmi erilaisiin viestinvälitystapoihin liittyviä riskejä ja suositella tiedon luokittelusta riippuen turvallisinta vaihtoehtoa.

Riippumatta tiedon muodosta ja säilytyspaikasta se kuljetetaan käsimatkatavarana/valvottuna kohteelta KPMG IT Sertifiointi Oy:lle.

2.3.6 Auditointidatan ja työpapereiden säilytys ja arkistointi

Kunkin sertifiointiasiakkaan osalta säilytämme riittävät ja tarvittavat tiedot tehdystä työstä KPMG Oy Ab:n dokumentinhallintajärjestelmässä johtopäätösten ja sertifiointipäätöksen perustelemiseksi. Säilytettävä dokumentaatio sisältää ainakin seuraavat dokumentit ja tiedot:

- hakemustiedot ja auditointiraportit,
- sopimukset,
- otoskoon määrittelyn perusteet,
- auditoinnin työmäärän arvioinnin perusteet,
- korjaavien toimenpiteiden varmentamisen (osana seuranta- tai uusinta-auditointien työpapereita),
- mahdolliset valitukset ja huomautukset sekä niiden perusteella tehdyt toimenpiteet,
- tehtyjen päätösten dokumentaatio (mikäli tarpeellista),
- sertifiointipäätöksen yksityiskohdat ja perustelut,
- kopio sertifikaatista sekä
- kaikki työpaperit.

Työpapereita säilytetään 10 vuotta sen vuoden päättymisestä, jonka aikana tehtyä työtä ne koskevat. Vaaditun säilytysajan umpeuduttua dokumentteja ei erikseen tuhota.

2.4 Esiauditointi

Esiauditointi on ensimmäinen varsinainen vaihe sertifiointiauditoinnissa. Vaiheen tavoitteena on tunnistaa puutteet, jotka vaativat toimenpiteitä ennen varsinaista sertifiointiauditointia. Esiauditoinnissa varmistetaan, että kohteella on riittävät ja vaatimukset täyttävät dokumentit.

Dokumentaation auditointi tulee olla suoritettuna ennen auditoinnin seuraava vaihetta. Auditoinnin tätä vaihetta täydennetään tarvittaessa tarkentavilla kysymyksillä/haastatteluilla, mutta tarkempi auditointi tehdään vasta sertifiointiauditointivaiheessa.

Esiauditoinnin tulokset dokumentoidaan kirjalliseen raporttiin. Auditoinnin kussakin vaiheessa tähän raporttiin lisätään tietoja/sisältöä siten, että lopulta lopputuloksena on ensimmäinen auditointiraportti.

2.5 Sertifiointiauditointi

Sertifiointiauditoinnin tavoitteena on varmistaa hallintajärjestelmän ja tietoturvapolitiikan tehokas ja vaatimustenmukainen implementointi, ja se tehdään sertifioitavan kohteen luona. Sertifiointiauditoinnin suunnitelma tehdään esiauditoinnin tulosten perusteella. Sertifiointiauditoinnin yhteydessä varmistetaan, että määritellyt prosessit, toimintatavat, mallit ja muut vastaavat on implementoitu, niitä noudatetaan ja ne toimivat. Samalla varmistetaan standardin pakottavien vaatimusten toteutuminen ja implementointi.

Sertifiointiauditoinnissa kiinnitetään erityisesti huomiota seuraaviin osa-alueisiin:

- riskienhallinta,
- dokumentointivaatimukset,
- kontrollitavoitteet ja organisaation riskianalyyseihin pohjautuvat kontrollit,
- tietoturvallisuuden hallintajärjestelmän toimivuus,
- organisaation sisäisten auditointien ja katselmointien suorittaminen,
- johdon roolit ja vastuut,
- soveltamissuunnitelma sekä valittujen kontrollien olemassaolo,
- kontrollien implementointi sekä
- tehtyjen toimenpiteiden ja päätösten dokumentointi.

2.6 Sertifiointipäätös

2.6.1 Sertifikaatin myöntäminen

Auditoinnin suorittanut tiimi tekee oman esityksensä siitä, onko sertifikaatin myöntämiselle olemassa edellytykset sekä esittää perustelunsa tälle näkemykselle. Tässä yhteydessä käydään läpi auditoinnin työpaperit ja auditointiraportti sekä varmistetaan, että auditointi on vaatimustenmukaisesti suoritettu.

Sertifikaatin myöntämisestä päättää aina KPMG IT Sertifiointi Oy:n toimitusjohtaja tai hänen sijaisensa kuultuaan auditointitiimin näkemyksen sertifioitavasta kohteesta auditoinnin jälkeisessä sertifiointipalaverissa. Edellytyksenä on, että sertifiointipäätöksen tekevä henkilö ei itse ole ollut suorittamassa auditointia.

Sertifikaattia ei voida myöntää, mikäli auditoinnissa on havaittu vakavia poikkeamia:

– Jokin standardin edellyttämä oleellinen asia on kuvaamatta tai puuttuu kokonaan.
– Jotakin standardin kohtaa vastaan tai jossakin toiminnossa on todettu monta lievää poikkeamaa.
– Järjestelmä todetaan olennaisilta osilta keskeneräiseksi.

Vakavien poikkeamien osalta todennetaan korjaustoimenpiteiden toimivuus ja implementointi ennen sertifikaatin myöntämistä.

Lieviä poikkeamia ovat yksittäiset vähäistä riskiä aiheuttavat puutteet standardin kohdassa tai toiminnossa. Myös lievien poikkeamien osalta korjaussuunnitelma ja sen toimivuus todennetaan ennen sertifikaatin myöntämistä.

2.6.2 Sertifioinnissa havaittujen poikkeamien korjaaminen

Sertifioinnissa havaitut vakavat poikkeamat tulee korjata ennen sertifioinnin myöntämistä. Kun kyseessä on ensimmäinen sertifiointi, asiakas voi suorittaa korjaukset ja esittää suoritetut korjaustoimenpiteet enintään kolmen kuukauden kuluessa auditoinnista.

Kun kyse on sertifioinnin ylläpitoauditoinnista tai sertifioinnin uusimisesta, korjaukset täytyy havaintojen vakavuudesta riippuen suorittaa nopeammassa ajassa. Vakavat havainnot on korjattava kahden viikon kuluessa ja vähemmän vakavat havainnot yhden kuukauden kuluessa niiden löytymisestä, jotta sertifiointi voidaan pitää voimassa tai uusia.

Auditoitavan tulee toimittaa poikkeamista riittävän tarkka korjaussuunnitelma, jossa korjaustoimenpiteet ovat uskottavia ja niiden voidaan arvioida täyttävän auditointivaatimukset. Jokaisen poikkeaman osalta on esitettävä yksityiskohtainen toimenpideluettelo korjaustoimenpiteistä aikatauluineen.

Poikkeamien korjaukset todetaan joko asiakkaan toimittaman dokumentaation katselmoinnilla tai verifioinnilla paikan päällä riippuen havaittujen poikkeamien määrästä ja vakavuudesta. Mikäli havaintoja on paljon ja niiden korjaamiseen menee yli kolme kuukautta, koko auditointi suoritetaan uudelleen.

2.7 Seuranta-auditoinnit

Seuranta-auditointien keskeisin tavoite on varmistaa, että tietoturvallisuuden hallintajärjestelmä toimii tehokkaasti myös sertifiointiauditointien välillä, eli koko sertifioinnin elinkaaren ajan. Seuranta-auditoinnissa käydään tyypillisesti läpi

- tietoturvallisuuden hallintajärjestelmän operointiin ja ylläpitoon liittyvät asiat,
- kommunikointi eri sidosryhmien välillä, erityisesti ulkoisiin tahoihin päin,
- muutokset dokumentteihin, toimintatapoihin ynnä muuhun samanlaiseen sekä
- otos standardin vaatimuksista (kaikki vaatimukset käydään läpi kertaalleen sertifikaatin elikaaren, kolmen vuoden, aikana).

Erityistä huomiota kiinnitetään edellisissä auditoinneissa havaittuihin puutteisiin ja siihen, mitä niiden korjaamiseksi on tehty. Tarkastuksen painotusta voidaan muuttaa riskilähtöisesti.

Seuranta-auditointeihin sisältyy paikan päällä tehtävää on-site-auditointia. Auditoinnilla saavutetaan riittävä varmuus siitä, että organisaatio toimii edelleen sertifioinnin vaatimusten mukaisesti ja on oikeutettu sertifiointiin.

Mikäli puutteita havaitaan, annetaan kohteelle sovittu aika korjata puutteet. Puutteiden korjaaminen todennetaan. Mikäli puutteita ei korjata, sertifiointi mitätöidään.

2.7.1 Menettely sertifioinnin voimassapitämisestä

Sertifioinnin voimassapidosta päättää aina KPMG IT Sertifiointi Oy:n toimitusjohtaja. Vaatimuksena sertifioinnin voimassapidolle on asiakkaan näyttö hallintajärjestelmän vaatimustenmukaisuudesta hallintajärjestelmästandardia vastaan. KPMG IT Sertifiointi Oy:n toimitusjohtaja voi nojata päätöksessään pääauditoijan antamaan positiiviseen sertifiointilausuntoon suoritetun tarkastuksen perusteella, jos sertifiointiauditoinnissa ei ole ilmennyt poikkeamia.

Mikäli sertifioinnin jäädyttämiseen tai peruuttamiseen vaikuttavia poikkeamia tai olosuhteita ilmenee ja asiakas kiistää ne, tarkastuksen suorittaneen pääauditoijan tulee raportoida nämä poikkeamat KPMG IT Sertifiointi Oy:n toimitusjohtajalle mahdollisen uusinta-auditoinnin järjestämiseksi. Uusinta-auditoinnissa tulee käyttää eri pääauditoijaa ja auditointiryhmää, jotta varmistutaan sertifioinnin peruuttamiselle/voimassapitämiselle olevista perusteista. Tällaisessa tilanteessa tavallisten laadunvarmistustoimenpiteiden lisäksi käydään jonkun toisen kuin tarkastuksen suorittaneen pääauditoijan johdolla alkuperäisen auditoinnin raportti ja työpaperit läpi, jotta varmistutaan siitä, että auditoinnissa ei tehty virheitä.

Vasta edellä mainitun käsittelyn jälkeen voidaan tehdä päätös sertifioinnin jäädyttämiseksi, peruuttamiseksi tai voimassapitämiseksi. Peruutettu sertifiointi on tilapäisesti pätemätön.

KPMG IT Sertifiointi Oy voi palauttaa sertifioinnin voimassaolon sen peruuttamisen jälkeen, mikäli peruuttamiseen johtaneet poikkeamat tai olosuhteet on korjattu. Mikäli korjaustoimenpiteitä ei suoriteta määräajassa (3 kk), peruutettu sertifiointi perutaan pysyvästi tai sertifioinnin laajuutta supistetaan.

2.7.2 Uudelleensertifiointi

Uudelleensertifiointi tehdään ennen kuin edellisen sertifikaatin voimassaolo päättyy. Uudelleensertifiointi edellyttää täydellistä uudelleenauditointia, kuten edellä esitetty.

2.7.3 Erityisauditoinnit

Mikäli organisaatiossa, sertifioinnissa tai ympäristössä tapahtuu merkittäviä muutoksia, voidaan joutua tekemään erityisauditointeja. Erityisauditoinneissa muutosten vaikutus organisaatioon, sertifiointiin ja/tai ympäristöön todennetaan ja päätös sertifioinnin jatkamisesta voidaan antaa.

2.7.4 Sertifikaatin supistaminen

Mikäli sertifioinnin kohde ei seuranta-auditoinnin tai muun tietoomme tulleen tosiasian mukaan täytä enää kaikilta osin alkuperäisen sertifioinnin vaatimuksia, voidaan sertifiointia joutua supistamaan. Käytännössä tämä tarkoittaa seuraavia asioita:

- sertifikaatin rajauksessa kohde määritellään niin, että osuudet, joiden osalta vaatimukset eivät enää toteudu, jäävät sertifioinnin ulkopuolelle,
- asiakkaalle toimitetaan uusi, rajaukseltaan supistetumpi sertifikaatti ja
- uuden rajoitetun sertifikaatin voimassaolo on sama kuin alkuperäisen.

2.8 Valitusmenettely

Mikäli sertifiointiin, tehtyyn työhön tai riippumattomuuteen kohdistuu epäilyjä tai niistä tehdään valitus, saatetaan tämä heti KPMG IT Sertifiointi Oy:n toimitusjohtajan sekä KPMG Oy Ab:n QRM-yksikön tietoisuuteen. Kaikkiin riippumattomuutta uhkaaviin tekijöihin ja riskeihin reagoidaan. Koska KPMG IT Sertifiointi Oy:n toimitusjohtaja osallistuu sertifiointipäätöksiin, valitusten käsittelyyn osallistuu riippumattomana tahona aina QRM-yksikkö.

Se, minkälaisiin toimiin valituksen toimesta ryhdytään, riippuu valituksen luonteesta. Kaikissa tilanteissa:

- valitus käsitellään KPMG IT Sertifiointi Oy:n toimitusjohtajan ja QRM-yksikön kesken,
- pyydetään lisätietoja kaikilta oleellisilta osapuolilta (mahdollisesti myös ulkopuoliselta asiantuntijalta),
- tehdään tarvittavat päätökset ja toteutetaan tarvittavat toimenpiteet sekä
- informoidaan kaikkia oleellisia osapuolia päätöksistä ja toimenpiteistä.

Mikäli valitus kohdistuu sertifioidun asiakkaan hallintajärjestelmän toimivuuteen, asia saatetaan asiakkaan tietoisuuteen ja asiakkaalta pyydetään lisätietoja. Tämän lisäksi voidaan joutua suorittamaan erillinen tarkastuskäynti.

Kaikki valitukset ja niiden perusteella tehdyt toimenpiteet ja päätökset arkistoidaan.

2.9 Sertifikaattitodistus ja todistuksen käyttösäännöt

Sertifikaatti on julkinen ja sen saa laittaa esille esimerkiksi asiakkaan www-sivuille ja tilojen seinälle. Alla esitetyt ehdot tulee kuitenkin huomioida sertifikaattiin viittaamiseen liittyen:

a.) Viittauksesta tulee käydä ilmi sertifikaatin myöntänyt taho ja sertifikaatin kattama alue.

b.) Viittauksessa ei saa antaa ymmärtää sertifikaatin kattavan muita alueita kuin mitä sertifikaatin alueeseen on määritelty tai olevan tae aukottomasta tietoturvallisuudesta.

c.) Viittauksessa ei saa antaa ymmärtää sertifioidun tahon olevan FINAS:n akkreditoima.

d.) Sertifiointiviittausta ei saa laittaa osaksi laboratorio-, kalibrointi- yms. raportteja, sillä tällöin raporttien saajat voisivat virheellisesti yhdistää sertifioinnin näiden mittaustulosten luotettavuuteen. Myöskään tuotteiden osalta asiakas ei saa viitata tuotteen olevan sertifioitu, koska kyseessä on hallintajärjestelmän, ei tuotteen, sertifiointi.

e.) Mikäli sertifioinnin kattama alue muuttuu, tulee kaikki viittaukset sertifiointiin muuttaa vastaamaan uutta sertifioinnin kattamaa aluetta. Tämä on tehtävä erityisesti silloin, kun sertifikaatin kattamaa aluetta on supistettu.

f.) Sertifiointiin ei saa viitata missään yhteydessä sen jälkeen, kun sertifioinnin voimassaolo on päättynyt.

g.) Mikäli sertifioinnin pohjana olevasta standardista on tullut uusi versio ja asiakkaan sertifikaattia ei ole konvertoitu standardin uuteen versioon, asiakas ei saa väittää olevansa sertifioitu uuden standardiversion mukaan.

h.) KPMG IT Sertifiointi Oy voi kieltää asiakasta käyttämästä sertifikaattia sellaisilla tavoilla, jotka rikkovat KPMG IT Sertifiointi Oy:n ja asiakkaan välisen sopimuksen ehtoja tai sertifioinnin myöntämiseen liittyvän akkreditoinnin vaatimuksia, joiden noudattamiseen KPMG IT Sertifiointi Oy on sitoutunut.

Myönnetty sertifikaatti on KPMG IT Sertifiointi Oy:n omaisuutta ja KPMG IT Sertifiointi Oy voi kumota sertifikaatin voimassaolon sekä kieltää sen käyttämisen, mikäli sertifikaatin myöntämisen edellytykset eivät ole voimassa.

2.10 Sertifikaattirekisteri

Kaikista myönnetyistä sertifioinneista pidetään kirjaa. Alla luetellut organisaation sertifiointia koskevat tiedot ovat pyynnöstä julkisesti saatavilla KPMG IT Sertifiointi Oy:lta. Sertifioinneista ilmoitetaan seuraavat tiedot:

- Sertifioidun organisaation nimi
- Sertifioinnin pohjana ollut vaatimusmäärittely (standardi)
- Sertifikaatin kattama alue (laajuus ja maantieteellinen alue)
- Sertifikaatin voimassaoloaika

Tapaa asiantuntijamme

Mika Laaksonen
Cyber Security, partner
T: 020 760 3337
E: mika.laaksonen@kpmg.fi

Olli Knuuti
Cyber Security
T: 020 760 3430
E: olli.knuuti@kpmg.fi

KPMG IT Sertifiointi Oy
PL 1037 | Töölönlahdenkatu 3 A
00101 Helsinki
P: 020 760 3000
E: etunimi.sukunimi@kpmg.fi

kpmg.com/fi/it-sertifiointi