TOPCERTIFIER
www.topcertifier.com

PALVELUMENETELMÄT ISO 27001:2013

TIEDOT TURVALLISUUDEN HALLINTA JÄRJESTELMÄ (ISMS)

TOPCERTIFIER
www.topcertifier.com

ISO 27001:2013 JOHDANTO

ISO 27001:2013 antaa organisaatiolle mahdollisuuden tunnistaa tietoturvariskit. Uhkien, haavoittuvuuksien, vaikutusten huomioiminen ja organisaation suojaaminen vaarantamatta sen CIA:n (Confidentiality Integrity Availability) tietoja hyväksymällä oikeat tiedot Turvallisuuden hallintajärjestelmä ISO 27001:2013:n yleinen asialista on kattaa alla olevat näkökohdat.

- Tarjoa malli perustamiseen, toteutukseen, toimintaan, seurantaan, tarkistamiseen, ylläpitoon ja tietoturvan hallintajärjestelmän parantaminen fyysisellä ja teknisellä ohjauksella.

- Varmista, että ISMS on integroitu organisaation liiketoimintaprosesseihin.

- Luo organisaatiokulttuuri, joka kannustaa työntekijöitä aktiivisesti osallistumaan Tietoturvan hallintajärjestelmä.

ALKU

Aloituskokous on olennainen työkalu kommunikoida ja suunnitella projektin toteutusta mahdollisimman vähän esteitä ja saada projekti päätökseen suunnitellussa ajassa ja kustannuksissa.Aloituskokouksen esityslista on:

- Projektisuunnitelmakeskustelu: Tämä sisältää keskustelun vastuullisuudesta ja vaarnan vastuusta haltijat. hankkeen virstanpylväät ja suoritteet

- Palveluiden laajuus ja sertifioinnin laajuus

- Lakisääteiset vaatimukset

YDINTIIMIN LUOMINEN

- CISO:n nimittäminen
- Tietoturvan hallintokomitean nimittäminen
- Sisäisten tarkastajien nimittäminen
- BCP-päällikkö
- ISO-johtajan nimittäminen

TOPCERTIFIER
www.topcertifier.com

GAP-ANALYYSI

Tämän vaiheen aikana teemme puuteanalyysin tarkistaaksemme, kuinka suuri osa nykyisistä käytännöistäsi on standardivaatimusten mukaisesti. käytännöt tarkistetaan näiden neljän vertailukriteerin perusteella

- ISO 27001:2013 -standardin vaatimukset
- SOA
- Lakisääteiset, lakisääteiset ja säännökset
- Asiakasvaatimukset
- Sisäiset käytännöt ja menettelyt

Tämän analyysin tulokset esitetään Gap Analysis Report -raportin muodossa. Tämä raportti toimii toimintokohteiden luettelona projektin muistutukselle.

ISMS-TIETOJEN KOULUTUS

ISMS-tietoisuuskoulutus järjestetään organisaatiosi työntekijöille. Koulutus istunnon tarkoituksena on auttaa työntekijöitä hankkimaan tietoa, ymmärtämään ISO 27001:2013:n käsitteet, ja linjata prosesseja ja käytäntöjä turvallisen ja uhkattoman työympäristön saavuttamiseksi. Kun henkilökunta on koulutettu, he voivat ajatella ja toimia sekä osallistua tavoitteiden saavuttamiseen maalit.

RISKIREKISTERI & SOA

Riskienhallintamenettely on dokumentoitava ja sitä on käytettävä viitteenä hallinnassa tunnistetut riskit kuullen kaikkia prosessin omistajia ja toiminnallisia johtajia. Käytämme I SO 31000 -standardia & ISO 27005 riskinhallintastandarditekniikat tunnistaa, analysoida, arvioida, dokumentoida, priorisoi, käsittele ja määritä tunnistetut riskit. Tämä vaihe luo riskirekisterin. Sopiva riski hoitosuunnitelmat yksilöidään yrityksen riskinhalutason ja CIA-tekijän perusteella. Tällaisten toimien tulokset lasketaan, kirjataan, arvioidaan ja dokumentoidaan. The Soveltuvuuslausunto (SOA) määrittelee ja yksilöi fyysiset ja tekniset hallintalaitteet sovellettavissa organisaatioosi liiketoimintaprosessien ja vaatimusten perusteella.

TOPCERTIFIER
www.topcertifier.com

OMAISUUSHALLINTA

Autamme varainhoidon periaatteiden ja menettelytapojen kehittämisessä koordinoimalla sitä toimivat päät ja ymmärrys prosessista. Omaisuuden päätavoite hallinta on:

- Tunnistaa organisaation omaisuus ja määritellä asianmukaiset suojavastuut
- Estää tallennettujen tietojen luvaton paljastaminen, muuttaminen, poistaminen tai tuhoaminen tiedotusvälineissä
- Varmistaa, että tiedot saavat asianmukaisen suojan tasonsa mukaisesti merkitystä organisaatiolle

VERKKO-/TIETOTURVA:

Autamme verkkoturvallisuuden hallintaperiaatteiden ja -menettelyjen kehittämisessä koordinoimalla toiminnallisten päiden kanssa ja ymmärrystä prosessista. Verkkoturvallisuuden päätavoite on:

- Varmistaa tietoturva verkoissa ja sitä tukeva tiedonkäsittely tilat
- Ylläpitää organisaation sisällä ja sen kanssa siirrettävien tietojen turvallisuutta mikä tahansa ulkoinen kokonaisuus

TAPAHTUMIEN HALLINTA

Autamme tapahtumanhallintaperiaatteiden ja -menettelyjen kehittämisessä koordinoimalla sitä toimivat päät ja ymmärrys prosessista. Tapahtuman päätavoite hallinta on:

- Varmistaa johdonmukainen ja tehokas lähestymistapa tietoturvan hallintaan tietoturvatapahtumia ja -heikkouksia koskevat tiedot mukaan lukien

TOPCERTIFIER
www.topcertifier.com

LIIKETOIMINNAN JATKUVUUDEN HALLINTA

Autamme kehittämään liiketoiminnan jatkuvuuden hallintaperiaatteita ja menettelytapoja koordinointi toiminnallisten johtajien kanssa ja ymmärrys prosessista. Päätavoite Liiketoiminnan jatkuvuuden hallinta on seuraava:

- Tietoturvan jatkuvuuden varmistaminen on sisällytettävä organisaation liiketoimintaan jatkuvuuden hallintajärjestelmät
- Tietojenkäsittelymahdollisuuksien saatavuuden varmistaminen

FYYSINEN TURVALLISUUS:

Autamme fyysisen turvallisuuden politiikkojen ja menettelytapojen kehittämisessä koordinoimalla toimivat päät ja ymmärrys prosessista. Fyysisen päätavoite turvallisuus on:

- Estää luvattoman fyysisen pääsyn, vahingot ja häiriöt organisaatiolle tieto- ja tietojenkäsittelylaitteet
- Estääkseen omaisuuden katoamisen, vahingoittumisen, varkauden tai vaarantumisen sekä organisaation toiminnan häiriöiden toiminnot

HENKILÖSTÖTURVALLISUUS:

Autamme henkilöstöpolitiikan ja toimintatapojen kehittämisessä koordinoimalla toimintopäälliköiden kanssa ja ymmärrystä prosessista. Henkilöstöturvan päätavoitteena on:

- Varmistaa, että työntekijät ja urakoitsijat ymmärtävät vastuunsa ja soveltuvat niihin roolit, joihin heitä harkitaan
- Suojella organisaation etuja osana muutos- tai lopettamisprosessia työllisyyttä
- Varmistaa, että kaikille työntekijöille ja myyjille on annettu riittävä koulutus tietoturvan suhteen

TOPCERTIFIER
www.topcertifier.com

DOKUMENTOINTI

Asiantuntijamme listaavat käytännöt, prosessit, SOP:t, sovellettavat SOA:t ja tietueet, jotka on oltava määritellään ja dokumentoidaan ISO 27001:2013 vaatimusten mukaisesti keskustelemalla kunkin kanssa osasto- ja toimintopäälliköt autamme sinua tarvittavan dokumentaation laatimisessa.

PERUSTA ISMS-OHJAUKSET

Kun käytännöt, prosessit, sovellettavuuslausunto (SOA) sen valvonta- ja SOP-ohjelmat ovat on dokumentoitu ja luettelo kerättävistä tietueista on listattu ja henkilöstö on ollut tunnistettu ja koulutettu tällaisiin toimiin, on tarpeen käyttää, seurata ja tarkistaa tällaisten prosessien tehokkuutta.

SISÄISEN TARKASTAJAN KOULUTUS

ISO 27001:2013 sisäinen tarkastaja (IA) -koulutus järjestetään tunnistetulle henkilökunnalle. Tämä koulutus antaa henkilöstölle valmiudet analysoida vaikutustenarvioinnin tarvetta, suunnitella ja ajoittaa IA sekä valmistautua tarkastaa tarkistuslistoja ja suorittaa vaikutustenarvioinnin sekä dokumentoida ja raportoida havainnot ylhäältä hallinta.

SISÄINEN TARKASTUS

Asiantuntijamme valvovat sisäisen tarkastuksen suorittamista sisäisen tarkastuksen tiimisi toimesta. Tämä sisäinen tarkastus tunnistaa järjestelmässä vielä olemassa olevat puutteet ja osoittaa niiden tason valmiutta kohdata sertifiointitarkastus. Tämä auditointi antaa organisaatiolle mahdollisuuden tunnista ja korjaa kaikki poikkeamat ennen kuin jatkat sertifiointiauditointiin. Huippujohto on tietoinen sisäisen tarkastuksen havainnoista.

TOPCERTIFIER
www.topcertifier.com

PERUSSYYANALYYSI (RCA) JA KORJAAVAT TOIMENPITEET

Kaikki poikkeamat, jotka on havaittu sisäisen tarkastuksen, asiakkaan tai kolmannen osapuolen auditoinneissa tai Riskien arviointi ja riskien käsittelymenetelmät, riskirekisteri Tapahtumarekisteri, haavoittuvuus Assessment & Penetration Test (VAPT) -raportti, haittaohjelmahyökkäykset, seisokkirekisteri, verkko asiat, pääsynvalvonta, omaisuusrekisteri, kolmannen osapuolen riskinarviointiraportit, CIA-tiedot luokitus, sisäiset ja ulkoiset hyökkäykset ja kaikki muut lähteet on lueteltava. RCA olla suoritetaan käyttämällä tekniikoita, kuten Brainstorming- ja Fish-Bone-menetelmiä. Optimaalinen korjaus toimet toteutetaan. Tällaisten toimien tehokkuus dokumentoidaan ja tarkistetaan a Korjausraportti (CAR).

JOHDON KATSAUSKOKOUS (MRM)

MRM tarjoaa kaikille ISMS:n sidosryhmille sopiva tavata määräajoin arvioidakseen, seuraavan ja suunnitella toimia alla olevissa asialistan kohdissa.

- Nykyisen hallintajärjestelmän tehokkuus ISMS:n ehdotus
- Riskinarviointi ja riskien hoitosuunnitelmat ja tiedot
- Tulokset tietojen CIA:sta (Confidentiality Integrity & Availability).
- Tarkastus vainnot ja poikkeamatha lähteistä
- Korjaava toimintasuunnitelma avoimien asia ratkaisemiseksi
- Jatkuvat parannukset järjestelmään
- Tarvittavat resurssit ja koulutukset
- Lakisääteiset ja uusia mukaisuusnäkökohtia

SERTIFIOINTITARKASTUS: VAIHE 1

Kun valmiusaste on saavuttanut riittävän tason, sertifiointiprosessi alkaa. Sertifiointielimen (CB) nimetty tarkastaja varmistaa standardin vaatimukset vaiheen 1 auditoinnilla. Tämä edellyttää, että tilintarkastaja tarkistaa politiikat, prosessit, SOP-, SOA-, kriittiset operatiiviset tietueet, IA- ja MRM-tietueet. Kaikki merkittävät poikkeamat CB-arvoista odotuksista ilmoitetaan tässä vaiheessa tarvittavien korjausten tekemiseksi. Tämä vähentää merkittävien poikkeamien mahdollisuudet sertifiointiauditoinnin aikana. TOP-varmentaja ottaa yhteyttä kaikkien sidosryhmien kanssa ja valvoa tarkastuksen sujuvaa loppuunsaattamista.

TOPCERTIFIER
www.topcertifier.com

SERTIFIOINTITARKASTUS: VAIHE 2

Vaiheen 1 auditoinnin onnistuneesti suoritettuaan tilintarkastaja keskittyy raportin ja raportin yksityiskohtaiseen tarkastukseen organisaation tietoturvan hallintajärjestelmän dokumentaatio. TOPCertifier olisi kouluttanut henkilöstösi auditointivaatimuksiin ja luottavaisesti tilintarkastuksen edessä. Asiantuntijamme ovat paikalla auttamaan kaikissa sujuvuuden edellyttämissä keinoissa tarkastuksen toimivuudesta. TOPCertifier auttaa tiimiäsi sulkemaan kaikki poikkeamat tarkastuksen aikana. Kun sertifiointiauditointi on suoritettu onnistuneesti, TOPCertifier on yhteydessä kaikkiin sidosryhmiin lopullisen todistuksen laatimiseksi, hyväksymiseksi ja julkaisemiseksi.

NOUDATTAMISEN JATKAMINEN

TOPCertifier on osa organisaatiosi vaatimustenmukaisuuspolkua ja auttaa sinua säännöllisesti välein tarvittavat koulutukset, järjestelmätuki ja päivitykset, sisäiset ja ulkoiset auditoinnit ja sertifiointisi säännöllinen uusiminen.