SecMeter Audit

Arvioijan ohje

Sisällys

1 Arvioinnin toteutusta viitoittavia yleisiä neuvoja

- muutos on energia, jonka avulla liikutaan kohti päämäärää
- varmista, että arvioinnilla on linjajohdon tuki
- varmista, että arviointiin osallistuvilla henkilöillä on päämäärästä yhteinen ja myönteinen mielikuva
- edistä rakentavan ilmapiirin muotoutumista
- yhtenäistä menettelytapoja
- tue päätöksentekoa.

2 Arvioinnin suorittamiseen liittyviä yleisiä neuvoja

- laadi haastattelusuunnitelma ja sovi haastatteluajoista
- selvitä huolellisesti keneltä saat asiantuntijavastaukset
- lähetä turvallisuuskriteeristöt etukäteen haastateltaville
- suorita haastattelut asioita edistävässä positiivisessa hengessä.

3 Arvioinnin onnistumiskriteerit

Mittaa arvioinnin onnistumista seuraavilla kriteereillä:

1. aikataulussa pysyminen
2. tarkoituksenmukainen tiedonhankinta
3. kehittämistoimenpiteiden toteuttaminen
4. arviointikokemus ja ilmapiirin positiivisuus.

4 Arvioijien valinta

Yrityksestä voidaan valita yksi tai useampi henkilö arviointityöhön ja turvallisuuskriteeristöjen käyttäjiksi. Menetelmään perehtyminen voi tapahtua valinnan mukaan itseopiskeluna tai konsultin tukemana.

Valittavan henkilön tulee olla mahdollisimman riippumaton liiketoimintoyksiköiden toiminnasta ja edustaa arviointiin liittyvää parasta asiantuntemusta. Arvioija ei voi arvioida omaa työtään, tai oman työryhmänsä toimintaa.

5 Arviointikohteen valinta

Arvioinnin tulee kohdistua ensisijaisesti yrityksen palvelu- tai liiketoiminnan kannalta keskeisten resurssien käytettävyyden, luottamuksellisuuden ja eheyden turvaamiseen.

Arvioijan tulee olla selvillä arvioinnin kohteena olevan palvelu- tai liiketoimintayksikön operatiivisesta toiminnasta niin, että toiminnolle olennaiset kohteet tulevat arvoiduiksi.

Arviointiin liittyvien turvallisuuskriteeristöjen ja haastateltavien määrä tulee rajata kohtuulliseksi. Arvioijan on syytä muistaa, että tiedon kyllästymispiste saavutetaan saman turvallisuuskriteeristön kohdalla haastattelemalla kahta tai korkeintaan kolmea henkilöä. Lisähaastatteluilla ei yleensä saada uutta merkittävää tietoa. Tarpeettomat haastattelutapaamiset pitkittävät hanketta ja lisäävät kustannuksia.

6 Haastateltavien valinta

Oikeiden asiantuntevien henkilöiden löytäminen vastaajiksi kuhunkin turvallisuuskriteeristöön on keskeinen hankkeen onnistumiseen vaikuttava seikka. Ennen haastattelutilaisuuksien alkua on haastateltaville suositeltavaa järjestää infotilaisuus. Kerro osallistujille ainakin seuraavat asiat:

- hankkeen tavoite
- toteutustapa
- kuinka tulokset muodostuvat
- kuinka tuloksia tulkitaan
- milloin tulokset julkistetaan.

7 Haastattelusuunnitelma

Laadi haastattelutapaamisia varten mahdollisimman tarkka suunnitelma. Käytä suunnittelussa SecMeter Audit suunnittelulomaketta. Huolellinen haastattelusuunnitelma auttaa onnistumaan ja varmistaa haastattelujen tehokkaan läpimenon. Hyväksi haastattelijaksi oppii vain kokemuksen kautta analysoimalla omaa toimintaa.

8 Pilotointi

Ensimmäinen arviointi käynnistetään yleensä pilotoinnilla. Pilotointikohteeksi voidaan valita osasto, jossa valitut turvallisuuskriteeristöt voidaan suorittaa valvotusti. Pilotoinnista saatujen kokemusten perusteella on mahdollista päättää parhaasta yksityiskohtaisesta suoritustavasta ja laajuudesta.

9 Arvioinnista tiedottaminen

Ennen arvioinnin käynnistämistä asianomaisille henkilöille tulee tiedottaa arvioinnin tavoitteista, menetelmästä ja aikataulusta.

10 Vaihe I

Organisoi arviointityö

1. kohdista arviointi toimintoon tai yksikköön
2. valitse asianmukaiset turvallisuuskriteeristöt
3. rajaa arvioinnin laajuutta (kuinka monen henkilön on tarpeen vastata samaan turvallisuuskriteeristöön)
4. valitse haastateltaviksi henkilöt, jotka osaavat parhaiten vastata valittua turvallisuuskriteeristöä koskeviin asioihin
5. laadi haastattelusuunnitelma
6. lähetä turvallisuuskriteeristöt haastateltaville tutustumista varten (esim. sähköpostin liitteenä)
7. järjestä informaatiotilaisuus kaikille hankkeeseen osallistuville.

11 Vaihe II

Kerää tiedot ja arvioi

1. suorita haastattelut aikataulun mukaisesti
2. kirjaa havainnot suoraan turvallisuuskriteeristöön tai erillisen muistioon.

12 Vaihe III

Raportoi ja informoi tuloksista

1. varmista tulokset (laadunvarmistus)
2. raportoi tulokset
3. järjestä yhteinen tulostilaisuus (arvioinnin päätös).

13 Vaihe V

1. Hallinnolliset kehittämispäätökset (jatkohanke)
2. Suunnittele ja hyväksytä kehittämistoimenpiteiden toteutus.

14 Käsitteitä

14.1 Arvioija

Arvioija on henkilö, joka suorittaa arviointiin liittyviä käytännön tehtäviä.

14.2 Arviointi

Arviointi on järjestelmällinen tutkimusmenetelmä jossa toimintaa, toimintatapoja ja kokemuksia arvioidaan hyväksyttyjä turvallisuuskriteerejä vastaan. Arvioinnin kautta pyritään ymmärtämään, miksi asiat tapahtuvat tietyllä tavalla. Arviointi on keskeinen osa yritysturvallisuuden kehittämistyötä.

14.3 Arviointinäyttö

Tallenteet, tositteet ja muu dokumentaatio sekä informaatio (arvioijan keräämä), joka liittyy turvallisuuskriteereihin.

14.4 Turvallisuuskriteeristö

Turvallisuuskriteeristö koostuu yhdestä tai useammasta yrityksen johdon hyväksymästä tavoitetilasta, joita vastaan toiminnan arviointi tapahtuu.

SecMeter Audit turvallisuuskriteeristöihin perustuvalla arvioinnilla yrityksen johto voi todentaa ja osoittaa esimerkiksi sisäiselle tarkastukselle, että yritys on huolehtinut asianmukaisesti turvallisuudesta.

14.5 Arviointiryhmä

Arviointiryhmä on arviointia suorittava henkilö tai henkilöistä koostuva ryhmä, joka käytännössä toteuttaa arviointiprosessin.

14.6 Arviointisuunnitelma

Arviointisuunnitelma on dokumentti, josta ilmenee arvioinnin kohteet, tavoitteet, turvallisuuskriteerit ja tavoiteaikataulu.

14.7 Auditointi

Arvioinnin kohteesta riippumattoman ulkopuolisen tahon suorittama arviointi.

14.8 Kehittämiskohde

Kehittämiskohteella tarkoitetaan arviointiin perustuvaa havaintoa, jossa arvioija näkee mahdollisuuden tehdä jokin asia turvallisemmin, paremmin tai tehokkaammin.

14.9 Korjaava toimenpide

Korjaavalla toimenpiteellä tarkoitetaan toimenpidettä, jolla tekniikkaa, toimintaa, ohjetta tai vallitsevaa käytäntöä muuttamalla poikkeama poistetaan ja saavutetaan tavoitetila.

14.10 Poikkeama

Poikkeamalla tarkoitetaan tilannetta, jossa tavoitetila ja nykyinen menettelytapa eivät vastaa toisiaan. Poikkeamahavainnon osalta tulee kuvata

1. mitä havaittiin, millainen poikkeama löydettiin
2. aiheuttaja, mistä poikkeama johtuu
3. merkitys, mitä poikkeaman johdosta voi aiheutua
4. johtopäätös, mitä edellä todetusta voidaan päätellä
5. suositus, mitä poikkeaman korjaamiseksi suositellaan tehtäväksi.

14.11 Tavoitetila

Turvallisuuskriteeri on tavoitetila, jonka tulee heijastaa arvioinnin kohteena olevan yrityksen liiketoiminnan ja sitoumusten kannalta tarkoituksenmukaisinta ja kustannustehokkainta ratkaisua tai toimintatapaa.

Turvallisuuskriteeristöihin oletuksena sisältyvät tavoitetilat kuvaavat yritysturvallisuuteen liittyvien säädösten ja muiden yleisten velvoitteiden, hyvän tiedonhallintatavan ja hyvän johtamiskulttuurin vaatimuksia.