Heli Pietiläinen
CIA, CISA
Senior Manager, Internal Audit
Stockmann Oyj Abp

Liiketoiminnan jatkuvuussuunnittelu (Business Continuity Planning)

Mitä tarkoittaa jatkuvuussuunnittelu

Vaikka organisaation riskit olisivat hyvin hallinnassa, joskus yllättävät tapahtumat voivat aiheuttaa toiminnan keskeytyksen. Tällaisia tapahtumia voivat olla esimerkiksi tulipalo, tulva, laiterikot tai kyberhyökkäykset. Jotta toimintaa pystyttäisiin jatkamaan mahdollisimman pian ja mahdollisimman sujuvasti tapahtuman jälkeen, on suositeltavaa suunnitella etukäteen, miten erilaisissa poikkeustilanteissa toimitaan. Tätä toimintaa kutsutaan jatkuvuussuunnitteluksi (business continuity planning). Usein käytetään myös käsitettä business continuity management eli jatkuvuuden hallinta, joka tarkoittaa samaa asiaa hiukan laajemmasta näkökulmasta.

Jatkuvuussuunnitteluun liittyy läheisesti myös käsite disaster recovery plan, jonka voidaan kääntää suomeksi esimerkiksi termillä toipumissuunnitelma. Sillä tarkoitetaan suunnitelmaa, jota seuraamalla saadaan tietojärjestelmät korjattua ja toimimaan keskeytyksen jälkeen. Ero käsitteiden merkityksissä on se, että kun jatkuvuussuunnittelulla tarkoitetaan kokonaisten liiketoimintaprosessien jatkuvuuden turvaamista, toipumissuunnitelmissa keskitytään puhtaasti tietojärjestelmiin. Voikin ajatella, että toipumissuunnitelma on osa jatkuvuussuunnitelmaa.

Miksi jatkuvuussuunnittelu on tärkeää

Jokainen yllättävä toiminnan keskeytyminen aiheuttaa yleensä kuluja, ja tyypillisesti kuluja syntyy sitä enemmän, mitä pidempään poikkeustilanne kestää. Kuluja syntyy sekä toiminnan korjaamisen aiheuttaman lisätyön myötä että välillisesti esimerkiksi kärsineen maineen tai vaikkapa aiheutuneiden ympäristövahinkojen vuoksi. Toisaalta keskeytykset aiheuttavat yleensä myös tulonmenetyksiä, kun liiketoimintaa ei pystytä harjoittamaan normaalilla tavalla. Jatkuvuussuunnittelun avulla voidaan merkittävästi pienentää vahinkojen aiheuttamia kustannuksia ja tulonmenetyksiä.

Jos organisaatiolla on toimiva riskienhallintaprosessi ja riskienhallintatoimenpiteet ovat ajan tasalla, voi herätä kysymys, onko jatkuvuussuunnitelma tällaiselle organisaatiolle tarpeellinen. Jatkuvuussuunnittelua ei kuitenkaan pitäisi nähdä vaihtoehtona riskienhallinnalle, vaan pikemminkin työkaluna, joka täydentää riskienhallintaa. Jatkuvuussuunnitelma otetaan käyttöön silloin, kun riski toteutuu: joko riskiä ei ole pystytty kokonaan poistamaan muilla hallintakeinoilla tai esimerkiksi kustannussyistä näin ei ole haluttukaan tehdä.

Jatkuvuussuunnitelman laatiminen

Jos organisaatiolla ei ole ajantasaista jatkuvuussuunnitelmaa, on työ hyvä aloittaa käymällä läpi keskeiset liiketoimintaprosessit ja listaamalla niiden heikot tai riskialttiit kohdat. Työssä kannattaa hyödyntää olemassa olevia prosessikuvauksia ja –kaavioita sekä niiden henkilöiden asiantuntemusta, jotka työskentelevät kyseisen prosessin parissa. Kun heikot kohdat on tunnistettu, arvioidaan, kuinka paljon aiheutuisi kustannuksia kunkin kohdan pettämisestä eripituisina ajanjaksoina (esimerkiksi tunti, päivä, viikko, kaksi viikkoa). Laskelmia tehdessä kannattaa pohtia, mikä on omalle toimialalle kriittistä: esimerkiksi mittavia projekteja toimittavalle organisaatiolle muutaman tunnin toimintakatkos laskutusjärjestelmässä ei välttämättä aiheuta merkittävää haittaa, kun taas vähittäiskaupassa vaikkapa jonakin joulunaluspäivänä tunninkin kestävä häiriö kassajärjestelmässä voi aiheuttaa mittavat kustannukset. Prosessien läpikäynnin ja laskelmien laatimisen perustella pystytään määrittelemään, mihin alueille vähintäänkin suunnitelma tulee laatia.

Seuraavaksi tehdään varsinainen suunnitelma aloittaen kriittisimmistä prosesseista ja toiminnoista. Jokainen heikko kohta käydään läpi ja suunnitellaan, miten kyseinen vaihe voidaan poikkeustapauksessa hoitaa toisella tavoin. Erilaisia vaihtoehtoja voivat olla esimerkiksi manuaaliset työvaiheet järjestelmissä tehtävien työvaiheiden sijaan, työvaiheiden tai kokonaisten prosessien ulkoistukset, varahenkilöjärjestelyt ja vaihtoehtoisten toimipaikkojen käyttäminen. Suunnitelman on hyvä olla mahdollisimman yksityiskohtainen, ja siinä kannattaa dokumentoida myös vastuuhenkilöt. Prosessien ja järjestelmien väliset riippuvuudet on syytä huomioida toimenpiteitä suunnitellessa.

Tärkeä vaihe suunnitelman laatimisessa on sen testaaminen. Testaustapoja on erilaisia, eikä mikään testitilanne vastaa täysin todellista poikkeustilannetta, mutta siitä huolimatta testausta ei kannata jättää tekemättä: tositilanteessa on mukava olla edes jonkinlainen varmuus siitä, että suunnitelma toimii niin kuin on ajateltu. Testaus voidaan toteuttaa esimerkiksi asiantuntevan tiimin kesken kirjoituspöytätyönä käymällä suunnitelma huolellisesti läpi ja tunnistamalla ja korjaamalla mahdolliset aukkokohdat ja epärealistiset toimenpiteet. Hyvän varmuuden antava testausvaihtoehto on luoda simuloimalla poikkeustilanne, edetä jatkuvuussuunnitelman mukaan ja havainnoida toimimattomat osiot. Simuloinnin huono puoli on, että se vaatii usein huomattavasti resursseja organisaation eri osista.

Suunnittelu- ja testaustyöhön tulisi osallistua ainakin kyseisen prosessinomistajan sekä keskeisten järjestelmien omistajien. Työtä voi koordinoida esimerkiksi henkilö, joka organisaatiossa koordinoi myös riskienhallintaa. Mukaan suunnitteluun kannattaa kutsua asiantuntijoita tarpeen mukaan mm. henkilöstöosastolta, kiinteistöhallinnosta, lakiosastolta sekä ympäristöosastolta. Myös ulkoisten asiantuntijoiden käyttö on mahdollista, ja joskus ulkopuolinen henkilö saattaa nähdä prosessien heikkoudet paremmin kuin prosessin parissa päivittäin työskentelevä henkilö.

Johdon tuki ja sitoutuminen

Keskeinen asia jatkuvuussuunnittelussa, niin kuin riskienhallinnassa ylipäätään, on johdon tuki ja sitoutuminen. Huolellisesti tehty jatkuvuussuunnittelu testauksineen vaatii etenkin ensimmäisellä toteutuskerralla paljon resursseja, ja siksi johto kannattaa sitouttaa asiaan mahdollisimman hyvin. Johdon tuki ei välttämättä ole itsestäänselvyys, koska useinkaan jatkuvuussuunnittelun arvoa ei nähdä ennen kuin suunnitelmaa tarvitaan käytännössä. Johdon olisi kuitenkin hyvä ymmärtää, että pahimmassa tapauksessa jatkuvuussuunnittelun puuttuminen voi tarkoittaa jopa liiketoiminnan päättymistä. Tietyillä toimialoilla kuten esimerkiksi terveydenhuollossa ja rahoitusalalla jatkuvuussuunnittelun testaaminen onkin säädetty pakolliseksi.

Sisäinen tarkastus ja jatkuvuussuunnittelu

Miten sisäisen tarkastuksen tulisi tarkastaa jatkuvuussuunnitelmia? Jokaisella tarkastajalla on oma lähestymistapansa, mutta karkeasti voidaan sanoa, että jatkuvuussuunnitelmien tarkastamiseen on kolme erilaista näkökantaa:

1) Kun liiketoimintaprosessiin tehdään sisäinen tarkastus, samalla tarkastetaan kyseisen prosessin jatkuvuussuunnitelma.
2) Jos sisäinen tarkastus arvioi riskienhallintaa erillisenä toimeksiantona, jatkuvuussuunnitelmat eri liiketoiminta—alueille ja –prosesseihin käydään samassa yhteydessä läpi.
3) Jatkuvuussuunnittelu ja –suunnitelmat valitaan omaksi aiheeksi vuosisuunnitelmaan ja ne muodostavat siis oman tarkastusprojektinsa.

Käytännön ohjeita tarkastustyöhön löytyy esimerkiksi IIA:n GTAG –sarjan julkaisusta Business Continuity Management, joka on julkaistu heinäkuussa 2008. Sama julkaisu tarjoaa myös viitekehyksen jatkuvuussuunnittelun eri osa-alueiden kypsyyden arviointiin organisaatiossa.

Lähteet:

IIA GTAG Business Continuity Management (David Everest, Roy E.Garber, Michael Keating ja Brian Peterson, heinäkuu 2008)

How to create an effective business continuity plan (Kim Lindros ja Ed Tittel, heinäkuu 2017, www.cio.com)