IT-palvelutoiminnan ja jatkuvien palvelujen riskienhallinta

Miten riskienhallintaa toteutetaan jatkuvassa palvelutoiminnassa? Esityksen skouppi on lähinnä sähköisissä palveluissa ja niihin liittyvässä palvelutoiminnassa.

UPDATE 2010

Matti Vuori, www.mattivuori.net

Sisällysluettelo 1/3

Sisällysluettelo 2/3

Sisällysluettelo 3/3

Esityksen tarkoitus

- Nostaa esille palvelutoiminnan riskeihin liittyviä näkökulmia ja menettelyjä, joiden avulla
  - Voidaan varmista ihmisten ja sähköisten palvelujen ja vähäriskisyys ja siten mahdollisimman luotettava toimitus
  - Voidaan antaa asiakkaille lisäarvoa tukemalla heidän liiketoimintansa ja verkkotoimintansa riskienhallintaa ja siten heidän menestystään
- Jokaiseen tilanteeseen voidaan löytää sopivia riskienhallinnan menettelyjä, joiden avulla asiat ja tilanteet saadaan ymmärrettyä ja hallittua
- Kuulijat saavat eväitä omien riskienhallintatoimiensa suunnitteluun

Keskeiset prinsiipit 1/2

- Kaikkein tärkein asia on riskien tunnistaminen
  - Vain tunnistettuja riskejä voidaan hallita
- Riskienhallinta ja palvelujen laatu kulkevat käsi kädessä
  - Riskienhallinnalla hallitaan laatua ja laatukokemusta heikentävien tapahtumien vaikutusta ja todennäköisyyttä ja luodaan suunnitelmia niiden kanssa pärjäämiseksi
- Palveluissa ja asiakaslähtöisessä toiminnassa riskien keskeisin näkövinkkeli on aina asiakkaan näkökulma, tarpeet, kokemus
- Riskienhallinta edellyttää yhteistyötä
- Riskejä ei saa tunnistaa aina samalla vakiosapluunalla, vaan on löydettävä ketterästi kuhunkin tilanteeseen sopivat keinot
- Yhteisesti hyväksytyt riskit ovat osa yhteistä sopimusta
  - Tiedetään "maailman reunaehdot", joiden puitteissa toimitaan

Keskeiset prinsiipit 2/2

- Riskienhallinnalla ei aina minimoida riskejä, vaan sen avulla tehdään oikeita päätöksiä ja tekoja
  - Riskianalyysin pitää johtaa tekoihin, joita valvotaan
  - Riskianalyysit tuottavat tietoa asioiden prioriteeteista
  - Riskienhallinnassa on paljolti kyse viestinnästä – asioiden nostamisesta esille, tiedon jakamisesta, keskustelusta asioista
- Tunnistettujen riskien käsittely ja päätöksenteko edellyttää jämäkkää johtamista
- On merkki organisaatiopatologiasta, jos kaikki riskit otetaan
- Mikään palvelu tai järjestelmä ei ole 2000-luvun tuotantokäyttöön kelpaava, jos sen riskejä ei ole tunnistettu
- Tarjottavien palvelujen riskejä voidaan useimmiten pienentää palveluja kehittämällä, silloin niiden laatu paranee ja tehokkuus saattaa kasvaa

Palvelutoiminnan riskien pääkohteet

Asiakassuhde

- Asiakkaan tyytyväisyys
- Tarpeiden ja vaatimusten täyttyminen
- Suhteen jatkuvuus

Palveluliiketoiminta

- Liiketoiminnan onnistuminen
- Kannattavuus
- Jatkuvuus

Palvelun kohteena olevat asiat (esim. sähköinen palvelu)

- Kohteen laadukkuus
- Keskeytysriskit
- Laaturiskit
- Vahinkoriskit
- Tietoturvariskit
- Jne…

Palvelun riskienhallinnan näkökulmia

Loppuasiakkaan / käyttäjän tarpeet

Loppuasiakkaan / käyttäjän riskit

Asiakkaan tarpeet

Asiakkaan liiketoiminnan riskit

Tietoriskit, keskeytysriskit, vahinkoriskit

Asiakkaan operaatioiden ja muutosten riskit

Operatiiviset uhat

Sopimukset

Asiakaspalvelu-näkökulma

Palvelun prosessien laatu

Verkkopalvelun tuotanto

Palvelu konseptina

Yksittäiset palvelutehtävät

Henkilöstö

Asiakkuus, luottamus, yhteistyö

Vahinkojen torjunta

Vahinkosuunnitelmat

Palvelu konseptina

- Näkökulma:
  - Palvelun keskeiset piirteet
  - Sen perusratkaisujen toimivuus
  - Liiketalous
  - Asiakasnäkökulma
- Olennaista riskien tunnistamisessa:
  - Palvelun piirteiden käsittely asiakasnäkökulmasta
  - Heikkoudet palvelukyvyssä
- Tiimi:
  - Liiketoimintajohto, palveluvastaavat jne…
- Välineitä riskien tunnistamiseen:
  - SWOT-analyysi
  - Palvelun riskien tarkistuslista

RH:n "pakollista" ydintä

Palvelun prosessien riskit

- Näkökulma:
  - Työn ja toiminnan analyysi
  - Teknisen järjestelmän analyysi
  - Asiakaspalvelunäkökulma
- Olennaista riskien tunnistamisessa:
  - Tarkkuus, detaljit, realismi
- Tiimi:
  - Palvelusta vastaava, prosesseihin osallistuvat henkilöt
- Välineitä riskien tunnistamiseen:
  - Prosessin analysointi
  - Prosessin riskikartta
  - Poikkeamatarkastelu
  - Laatujärjestelmä- ja muut prosessistandardit (ISO 9001, ITIL / ISO 20000)
    - ISO 9001 –auditointi paljastaa aivan avainasioita palvelutoiminnankin laadusta
    - ITIL / ISO 20000 antavat täsmätukea operatiiviseen ylläpitoon ja hostaukseen
  - Tietoturvallisuusstandardit (ISO 27001)

RH:n "pakollista" ydintä

Luottamuspääoma

- Näkökulma:
  - Luottamus on palveluihin liittyvä keskeinen suojattava pääoma
- Olennaista riskien tunnistamisessa:
  - Analysoitava, mistä luottamus syntyy
  - Tunnistettava luottamusta uhkaavat asiat
- Tiimi:
  - Palvelujen ja asiakkuuden avainhenkilöt
- Välineitä riskien tunnistamiseen:
  - Asiakkaan tarpeiden ja vaatimusten selvittäminen ja määrittäminen
  - Yhteistyön ja luottamuksen riskikartta

Sopimukset

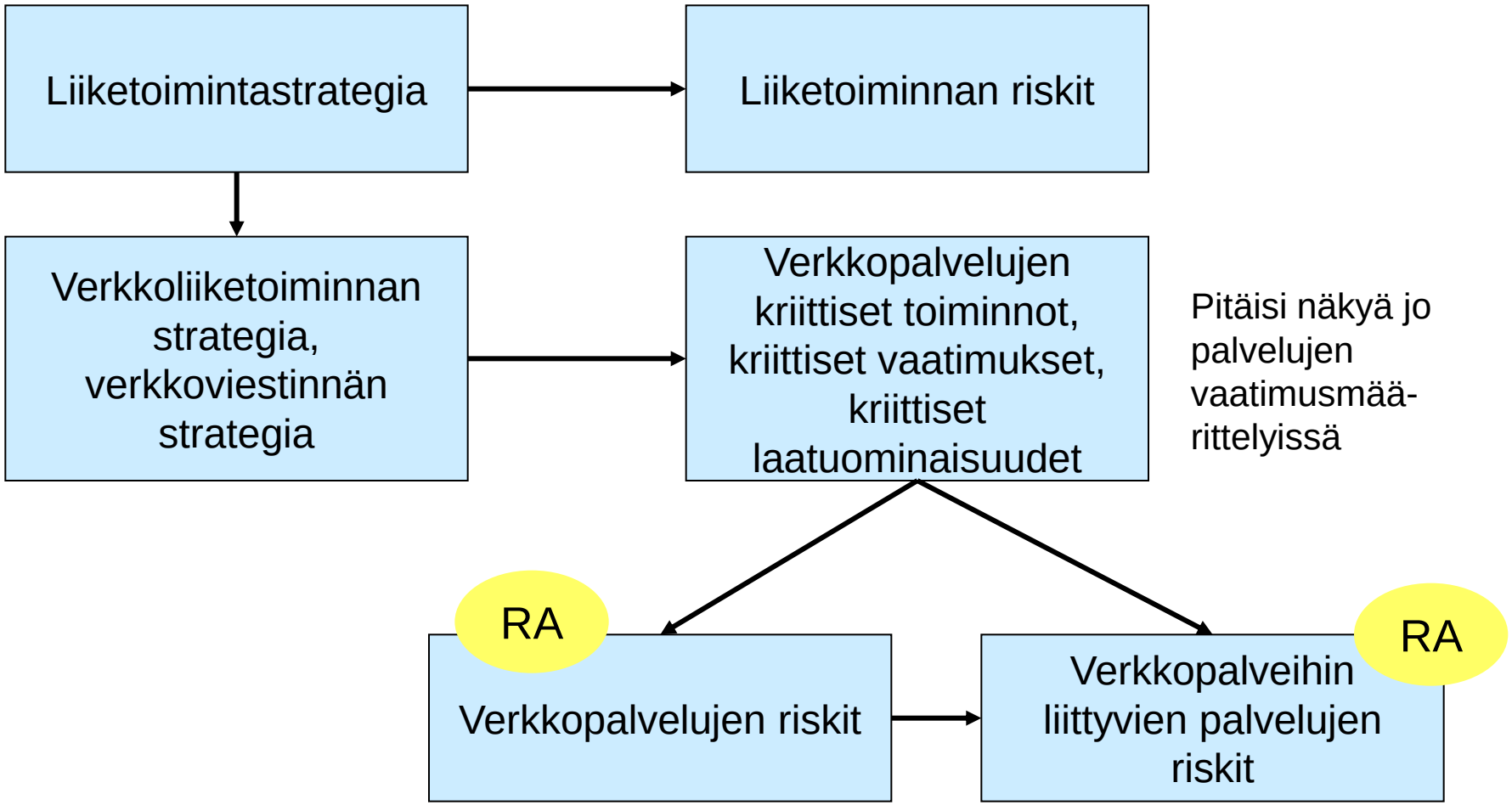
- Näkökulma:
  - Lupaukset
  - Juridiikka
  - Tietoisuus sopimusten sisällöstä
- Olennaista riskien tunnistamisessa:
  - Sopimusten tarkastaminen ja analysointi (lakimies)
  - Sopimusten katselmointi
- Olennaista riskien hallinnassa
  - Sopimusosaaminen
  - Kaikkien on tiedettävä, mitä on sovittu
- Tiimi:
  - Liiketoiminnasta ja asiakkuuksista vastaavat; myynti
  - Tarjousprosessin mukaan
- Välineitä riskien tunnistamiseen:
  - Sopimusten tarkistuslistat (ks. esim. Pk-yrityksen riskienhallinta – välinesarja http://www.pk-rh.fi/tyovalineet/tyovalineiden-tulostettavat-versiot/)

RH:n "pakollista" ydintä

Asiakkaan liiketoiminnan riskit 1/2

- Näkökulma:
  - Mikä asiakkaan liiketoiminnassa (ja sähköisessä palvelussa) on tärkeää?
  - Mitkä ovat uhat, varjeltavat asiat?
  - Mitkä ovat siis sähköisen palvelun kriittiset asiat ja palvelutoiminnan riskit?
  - Lisäarvoa tuottava analyysi asiakkaalle, jos asiat eivät ole selvillä
- Olennaista riskien tunnistamisessa:
  - Asiakkaan auttaminen miettimään oman liiketoimintansa riskejä
  - Asiakasnäkökulma
  - Keskustelut asiakkaan kanssa
  - Yhteinen riskianalyysi
  - Asiakkaan strategian selvittäminen (liiketoimintastrategia, verkkoviestinnän strategia)
  - Yleinen asiakkaan toimialan toiminnan, vaatimusten, riskien ymmärtäminen
- Tiimi:
  - Omat liiketoimintatason avainhenkilöt
  - Asiakkaan avainhenkilöt
- Välineitä riskien tunnistamiseen:
  - Riskikartat, tarkistuslistat

Asiakkaan liiketoiminnan riskit 2/2



Asiakkaan riskien vähentäminen

- Näkökulma:
  - Riskienhallinnan paradigman ulkopuolella alihankkija voi auttaa asiakasta osaamisellaan
  - Konsultointia tavallisen palvelutoiminnan yli
- Mahdollisuuksia
  - Konsultointi verkkoviestintästrategian kehittämisessä
  - Teknologiaselvitykset
  - Kilpailija- ja markkinaselvitykset – miten muut toimivat
  - Asiakkaan konsultointi riskianalyyseissä, riskianalyysikoulutus, jne…
  - Jne…
- Etuja
  - Asiakkaan riskit vähenevät
  - Strategisen tason yhteistyö
  - Asiakkaan sitouttaminen kaikilla tasoilla
  - Profiilimme nosto

Asiakkaan operaatioiden ja muutosten riskit

- Näkökulma:
  - Asiakkaan auttaminen ymmärtämään, mitä kaikkea operaatioihin ja muutoksiin liittyy ja millaisten asioiden onnistuminen on varmistettava
  - Esimerkiksi uusi viestintäratkaisu, tietojärjestelmä, ulkoistaminen
- Olennaista riskien tunnistamisessa:
  - Tilanteen kokonaisvaltainen käsittely
- Tiimi:
  - Asiakkaan avainhenkilöt
  - Riskianalyysikonsultti
  - Operaatioon toimittajalla liittyvät avainhenkilöt
- Välineitä riskien tunnistamiseen:
  - Riskikartat (esim. tietojärjestelmähankinnan riskien riskikartta), tarkistuslistat

Loppukäyttäjän riskit

- Näkökulma:
  - Sähköisten palvelujen loppuasiakkaan ja loppukäyttäjän riskit
  - Merkittävä näkökulma palvelun riskeihin
  - Tietosuoja, tietoturva, tuotevastuu oleelliset
  - Mikä tieto on kriittistä, mitä tietoa on suojattava
- Olennaista riskien tunnistamisessa:
  - Loppukäyttäjien tunteminen
- Tiimi:
  - Riskianalyysikonsultti, käyttäjiä tunteva, palvelun asiantuntijat
- Välineitä riskien tunnistamiseen:
  - Tiivis menetelmä: Asiakkaan/käyttäjän riskianalyysi
  - Muut riskikartat ja tarkistuslistat; järjestelmästä riippuen

Muutosten / pienten töiden riskit

- Näkökulma:
  - Epäonnistuneet muutokset, pienet työt, ovat juuri palvelutoiminnassa oleellinen asia
- Olennaista:
  - Muutos/työprosessissa muutoksen formaali, sovittu käsittelyprosessi; ml. muutosraati tarpeen mukaan
  - Muutoksen vaikutusten analysointi (ja jälki siitä)
  - Muutoksen pakollinen testaus / onnistumisen muu tarkistus
  - Konfiguraationhallinta, jonka avulla muutos voidaan tarvittaessa perua nopeasti
- Välineitä riskien tunnistamiseen:
  - Tarkistuslistat
  - Ohjelmiston riippuvuustarkastelut ohjelmallisesti ja manuaalisesti

RH:n "pakollista" ydintä

Projektiriskit

- Näkökulma:
  – "Projekteina" toteutettavat asiat
- Olennaista:
  – Moninäkökulmaisuus
- Välineitä riskien tunnistamiseen:
  – Tarkistuslistat, riskikartat
  – Tapauksen mukaan muut riskianalyysimenetelmät
- Huom!
  – Projektien riskienhallinnasta on omia esityksiään

RH:n "pakollista" ydintä

Henkilöstö

- Näkökulma:
  - Henkilöstö on aina palvelutoiminnan keskeisin toimija
  - Olivatpa prosessin miten mietittyjä tahansa, ihmiset ovat avainasemassa
- Olennaista:
  - Kokonaisvaltainen riskien tunnistaminen – osaamisesta yrityskulttuuriin; avainhenkilöriskeistä kansallisiin eroihin
- Välineitä riskien tunnistamiseen:
  - Riskikartat ja tarkistuslistat (ks. esim. (ks. esim. Pk-yrityksen riskienhallinta –välinesarja)
  - Työtyytyväisyys- ja motivaatiokyselyt

Operatiiviset uhat

- Näkökulma:
  - Verkkopalvelun tai muun systeemin operatiiviset uhat
  - Tietoriskit, keskeytysriskit, vahinkoriskit
  - Johdetaan asiakas- ja loppukäyttäjätarpeista
- Olennaista riskien tunnistamisessa:
  - Kaikkien riskilajien tarkastelu
  - Syvällinen syiden ja vaikutusmekanismien tunnistaminen
- Tiimi:
  - Riskianalyysikonsultti, IT-hallinto, tekniikan ihmiset
- Välineitä riskien tunnistamiseen:
  - Tarkistuslistat ja riskikartat
  - Kaikki riskianalyysimenetelmät SWOT:sta FMEA:an

RH:n "pakollista" ydintä

Verkkopalvelun tekninen laatu

RH:n "pakollista" ydintä

- Näkökulma:
  - Teknisen järjestelmän robustius
  - Varautuminen rikkoutumisiin, tilojen vahinkoihin jne…
  - Tekninen tietoturvallisuus
- Olennaista riskien tunnistamisessa:
  - Peruslähtökohdat tulevat turvallisuussuunnitelman yhteydessä tehtävästä riskianalyysistä, siitä jatkaen eteenpäin
  - Turvallisuussuunnittelu on yritys- ja yksikkötason työtä
  - Tekniikan tuntijat mukana
- Tiimi:
  - Riskianalyysikonsultti, IT-hallinto, tekniikan ihmiset
- Välineitä riskien tunnistamiseen:
  - Turvallisuussuunnittelun prosessi
  - Tietoturva-tarkastukset ja auditoinnit
  - FMEA – vika- ja vaikutusanalyysi

Vahinkosuunnitelmat

- Kun jotain tapahtuu…
- Turvallisuussuunnitelman taso isoille asioille
- Konerikkojen, palvelinrikkojen varasuunnitelmat
  - Onko varapalvelimia, varalaitteita?
- Insidenssien hallinnan taso hostauksen tason asioille
  - Mitä tehdään, jos asiat eivät onnistu
  - Miten palautetaan edeltävä tila (esim. tietokannan tila, jos päivitys menee pieleen)
- Varmistettava, että
  - Menettelyt on koulutettu
  - Vastuut määritetty
  - Valmiudet ja resurssit ovat olemassa
  - Laitteet ovat oikeasti olemassa
  - Viestintäprosessit kunnossa

RH:n "pakollista" ydintä

Oleellista riskin tunnistamisessa

- Panostukset tunnistamiseenkin palvelun kriittisyystason mukaan
- Moninäkökulmaisuus
- Eri abstraktiotasot – palvelu konseptina ja pienet työt
- Eri riskilajit
- Liiketoiminnan, tuotteen ja projektin kontekstin ymmärtäminen
- Laadukas riskianalyysisessio

Palvelujen kriittisyysluokat

- ”Toiminteen” kriittisyyden suuruutta kuvaava luokitus
  - Toiminne = liiketoiminnat, liiketoimintojen osat, projektit ja tuotteet
- Käytetään menettelytapojen valinnassa ja riskien priorisoinnissa
  - Kriittisiin asioihin järeämmät menettelyt.
  - Auttaa resursoimaan riskienhallintaa.
- Ohessa kuvattu eräs yleinen kriittisyysluokittelu

Kriittisyysluokka III

- III – kriittinen taso
  - Liiketoimintakriittiset toiminteet, erittäin suuri strateginen tai taloudellinen merkitys oman yrityksen tai asiakkaan liiketoiminnalle
  - Ydinsisällöistä ei ole kokemuksia, toiminta-alue tai ydinteknologia on uusi.
  - Poikkeuksellisen suuret suorituskykyvaatimukset / asiakasvaatimukset, esimerkiksi aikataulu on poikkeuksellisen tiivis

Kriittisyysluokka II

- II – normaalitaso
  - Liiketoimintayksikön ”tavalliset” toiminteet, toisin sanoen toiminteet joista on kohtuullisesti aiempaa kokemusta / osaamista,
  - Esim. keskikokoiset projektit, joissa on vain kohtuullisesti uusia asioita tai tuotteet, joihin liittyy vain kohtuullisesti uusia ominaisuuksia ja kohtuullinen kehityspanos

Kriittisyysluokka I

- I – alhainen taso
  - Pienikokoiset toiminteet, joiden tulosvaikutus on vähäinen, esim. projektit, jotka perustuvat aiempaan osaamiseen / tuotteet, joiden kehityspanos on vähäinen
  - Vakiomuotoinen palvelutoiminta

Kriittisyysluokan vaikutus riskien tunnistamisessa 1/2

- III – kriittinen taso
  - Käytetään jotain ideoivaa riskien tunnistamistekniikkaa (aivoriihi, SWOT, potentiaalisten ongelmien analyysi) sekä tarkistuslistoja
  - Riskien tunnistamiseen osallistuu riskiryhmän lisäksi riskialueen tai -teknologian asiantuntijoita ryhmän ulkopuolelta
  - Vastuuhenkilö tai tarvittaessa riskianalyysikonsultti toimii puheenjohtajana tunnistamiskokouksissa

Kriittisyysluokan vaikutus riskien tunnistamisessa 2/2

- II – normaali taso
  - Riskien tunnistamiseen osallistuu määritelty ryhmä
  - Asiantuntijoiden osallistumista suositellaan, mutta ei edellytetä.
  - Riskien tunnistamisessa käytetään systemaattisena työvälineenä vähintään tarkistuslistaa, mutta systemaattisten ideoivien menetelmien käyttöä suositellaan.
- I – alhainen taso
  - Riskien tunnistaminen ja esittely edellytetään
  - Riskianalyysi tehdään harkinnan mukaan sopivalla, tarkoituksenmukaisella tavalla
  - Menetelmien käyttöä ei edellytetä

Riskien tunnistamisen tilanteet

- Vakioidun palvelun (palvelutoiminta) määrittely
  - Uudenlainen ylläpitopalvelu, hostauspalvelu, jne…
- Räätälöidyn palvelun (palvelutoiminta) kehittäminen
- Merkittävän asiakkuuden alkaessa
- Palvelun prosessien kehittäminen
- Palvelun laadun arviointi
- Yksittäinen suuri palvelusopimus
- Projektoidut tehtävät
- Muutokset
- Määräajoin

Tiimit tekemään riskianalyysejä

- Perinteinen patologia on se, että projektipäällikkö miettii riskejä.
- Kaikki tiimit on saatava tekemään systemaattisia riskianalyysejä ja tuomaan kokemuksensa ja osaamisensa esille
  - Vaatimusmäärittelijät
  - Ohjelmistokehitystiimit
  - Testaustiimit
  - Asiakas
  - Ohjausryhmä!

Riskianalyysin perusmalli

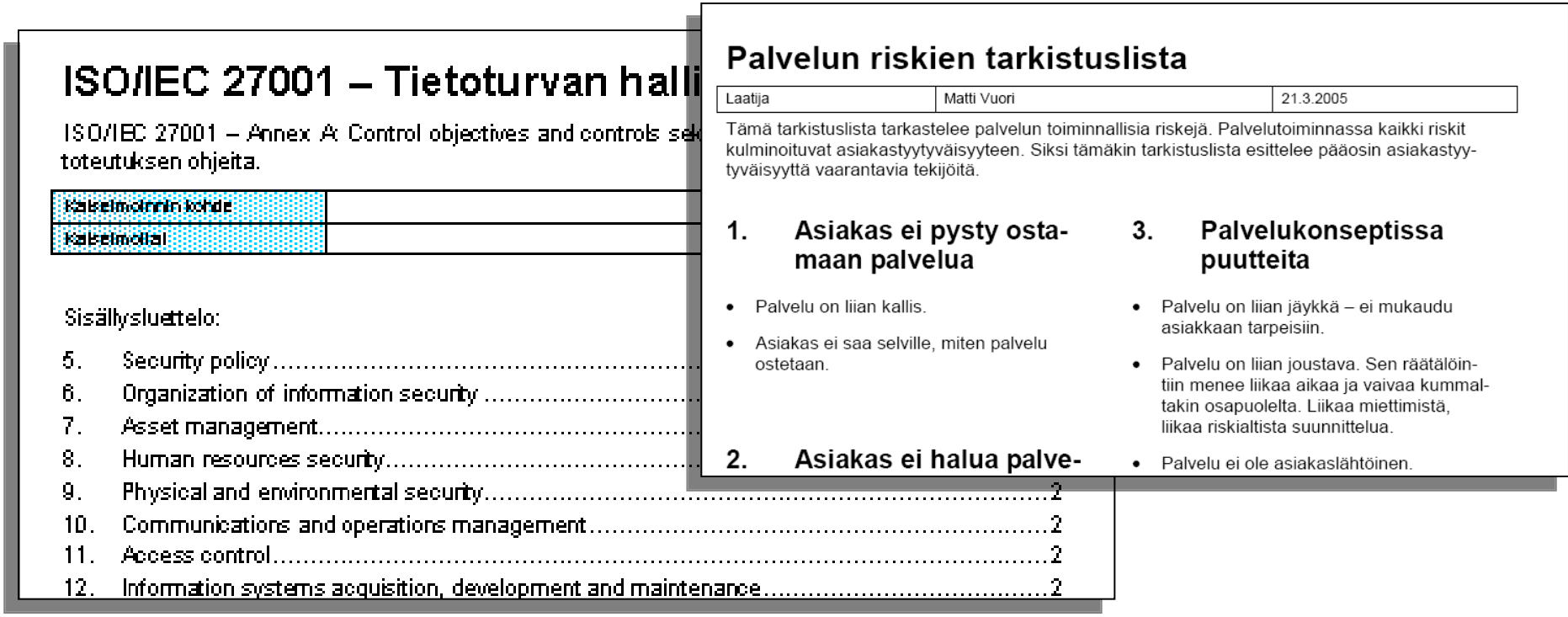
- Tiimin parituntinen sessio
- Ideoiva osuus ja asioita systemaattisesti läpikäyvä osuus
- Kolme keskeistä tunnistamisen välinettä
  - Riskikartat – avaavat tilannetta eri näkökulmista
  - Tarkistuslistat – varmistetaan, että tyypilliset ongelmat on käsitelty
  - Riskianalyysimenetelmät – FMEA, SWOT, poikkeamatarkastelu, erilaiset herkkyysanalyysit jne…
- Hyvästä riskianalyysisessiosta on oma kalvosetti

Riskikartat

- Riskikartta hedelmällinen väline
  - Auttaa jäsentämään tarkastelun kohdetta
  - Keskeiset elementit ja haavoittuvuudet
  - Avaa riskien maailmaa
  - Tukee luovaa riskien tunnistamista
  - Tarjoaa yhteisen objektin, jonka kautta riskejä tarkastellaan
  - Käydään läpi laatikko kerrallaan
  - Helppo laatia erilaisiin tarkoituksiin

Tarkistuslistat

- Yleisiä riskejä
- Toistuviin asioihin kannattaa organisaatiolla räätälöidä omat tarkistuslistat, joissa otetaan huomioon toteutuneet ja tunnistetut riskit



ISO/IEC 27001 – Tietoturvan halli

ISO/IEC 27001 – Annex A: Control objectives and controls sel
toteutuksen ohjeita.

Kalvelmoinnin kohde	
Kalvelmoijat	

Sisällysluettelo:

5. Security policy 2
6. Organization of information security 2
7. Asset management 2
8. Human resources security 2
9. Physical and environmental security 2
10. Communications and operations management 2
11. Access control 2
12. Information systems acquisition, development and maintenance 2

Palvelun riskien tarkistuslista

Laatija	Matti Vuori	21.3.2005

Tämä tarkistuslista tarkastelee palvelun toiminnallisia riskejä. Palvelutoiminnassa kaikki riskit kulminoituvat asiakastyytyväisyyteen. Siksi tämäkin tarkistuslista esittelee pääosin asiakastyytyväisyyttä vaarantavia tekijöitä.

1. Asiakas ei pysty ostamaan palvelua

- Palvelu on liian kallis.
- Asiakas ei saa selville, miten palvelu ostetaan.

2. Asiakas ei halua palve-

3. Palvelukonseptissa puutteita

- Palvelu on liian jäykkä – ei mukaudu asiakkaan tarpeisiin.
- Palvelu on liian joustava. Sen räätälöintiin menee liikaa aikaa ja vaivaa kummaltakin osapuolelta. Liikaa miettimistä, liikaa riskialtista suunnittelua.
- Palvelu ei ole asiakaslähtöinen.

Varsinaiset riskianalyysimenetelmät

- Systemaattiseen kohteen läpikäyntiin
- Vaativat enemmän aikaa ja panostusta
- SWOT – Strengths, Weaknesses, Opportunities, Threats. Monille tuttu. Soveltuu kaikenlaisten asioiden yleiseen ja nopeaan tarkasteluun.
- Potentiaalisten ongelmien analyysi
  - Hyödyntää avainsanalistoja, usein kohteelle räätälöityjä.
  - Sen lisäksi kohteen elementtien systemaattinen läpikäynti.
- FMEA, FMECA. Vika- ja vaikutusanalyysi.
  - Teknisen järjestelmän analysointiin
- Poikkeamatarkastelu
  - Prosessien analysointiin
- Työn turvallisuusanalyysi / tehtäväanalyysi
  - Työtehtävien analysointiin
- Jne…

Kokemustiedon hyödyntäminen

- Tutustuminen historiaan
  - Aiemman toiminnan riskit
- Lähteitä
  - Organisaation tietokannat
  - Riskilistat
  - Projektien loppuraportit
  - Lessons Learned –raportit
  - Kokeneet päälliköt
  - Riskienhallintapäällikkö, laatuihmiset

Riskitietojen dokumentointi riskilistaan

- Yleisintä: Riskilista laaditaan Excel-taulukkona
- Tehostaa riskienhallintaa, helpottaa riskien kirjaamista
- Näkyvyys suunniteltava – riskitieto ei saa jäädä ”pöytälaatikkoon”
- Yksinkertaistaa riskienhallinnan kokonaisvaltainen seurantaa ja raportointia

Riskien raportointi ja käsittely

- Raportointi ideaalisesti portfolionäkökulmasta
  - Riskit asiakkuuksittain
  - Riskit palveluittain
  - Riskit järjestelmittäin
- Käytännössä
  - Riskianalyyseittäin
    - Aktiivinen: sähköpostiin
    - Passiivinen: riskilistan tallennus
  - Keskeiset muutokset
  - Ylemmän tason (linjaorganisaatiossa) käsittelyä edellyttävät isot asiat

Riskien katselmointi ja käsittely

- Tilanteen katselmointi avainhenkilöiden kesken
- Tilanteen katselmointi oman johdon kanssa
- Tiimien palavereissa
- Raportointi asiakkaalle
- Käsittely asiakkaan kanssa ohjausryhmässä

Riskeistä oppiminen

- Riskilistojen kokoaminen ja analysointi
  - Yhteiset asiat
  - Uudet ilmiöt
  - Tilastot – perusteluiksi
- Tulokset
  - Tietoa
  - Päälliköiden preppausmateriaalia
  - Prosessien parantaminen
  - Riskien tunnistustyökalujen päivitys