Sata ajatusta riskeistä ja niiden hallinnasta

Matti Vuori

Olemme ajassa, jolloin epävarmuus on hyväksytty maailman luonteeksi ja olemme oppineet tunnistamaan erilaisia konteksteja erilaisiksi tässä suhteessa. Se merkitsee riskien läsnäolon tervettä hyväksymistä. Tällöin myös riskien käsittely erilaisissa toiminnoissa saa osin uudenlaisen tarpeen ja uudenlaisia mahdollisuuksia.

Mitä riskit ovat?

1. Riskeissä on kyse hallitsemattomista tapahtumista, joiden vuoksi lopputulos ei ole toivottu.
2. Silloin jokin laatu on heikompi kuin on sovittu, toivottu tai odotettu tai tapahtuu jotain vielä pahempaa – vaikkapa todellinen onnettomuus.
3. Riskiajattelun historia onkin "missioissa", joiden onnistumista jokin uhkaa – ei kenties päästäkään kuuhun, vaan raketti räjähtää.
4. Nämä vahinkoriskit johtuvat siitä, että jokin ei toimikaan kuin ajateltiin, tulee jokin hallitsematon ulkoinen häiriö, suunnitelma ei vastaakaan todellisuutta, kuva todellisuudesta on väärä tai se muuttuukin matkan varrella. Tai ihmiset laiminlyövät jostain syystä asioita. Syitä on monia.
5. Toisaalta on positiivisten riskien olemus. Silloin on kyse liiketoiminnasta ja innovaatioista. Onnistuminen on epävarmaa lisäarvoa. Liikeriskeillä on myös positiivinen syy: ottamatta riskejä ei menesty. Mutta jos liikeriskejä otetaan hallitsemattomasti...
6. Erilaisista riskeistä puhutaan riskilajeina – on projektiriskejä ja tuoteriskejä, vahinkoriskejä ja liikeriskejä, tietoturvariskejä, keskeytysriskejä ja poliittisia riskejä jne... Ajattelun ja toiminnan konteksti määrittää relevantit riskilajit. Samoin se, kenen kannalta asiaa katsellaan.
7. Riskejä on aina kaikilla toiminnan tasolla. Ohjelmoijaa mietityttää, että toimiiko joku ohjelmanpätkä oikein. Asiakasta uuden tietojärjestelmän toimivuus muiden järjestelmien kokonaisuudessa.
8. Yhden toimijan ykkösprioriteettiriski on toisen sekundäärinen nippeliasia.

9. Vahinkoriskien perusmatematiikka kuuluu: riskin suuruus vahingollisen tapahtuman vahingon suuruuden ja todennäköisyyden tulo. Niinpä riskien maailma on lähellä luotettavuustekniikkaa, jonka ydintä todennäköisyydet ovat.
10. Todennäköisyydet riippuvat tietysti kontekstista. Globaalia ohjelmistovalmistajaa kiinnostaa se määrä, jolla ohjelman asennus epäonnistuu koko käyttäjäkunnassa, mutta yksittäisen käyttötapauksen yhteydessä kiinnostaa sen onnistumisen todennäköisyys.
11. Riskimatematiikka on yleensä karkeaa ja luonteeltaan laadullista – kumpaakin elementtiä arvioidaan esim. sopivalla 1-5 skaalalla. Kuitenkin se auttaa jäsentämään riskien suuruutta yksinään ja suhteessa toisiin. Siten voidaan keskittyä isoimpiin riskeihin ensimmäisenä ja hyväksyä vähäpätöiset riskit – tai sellaiset, joille ei voi tehdä mitään.
12. Hyvää riskeissä on se, että ne tulevat ja menevät. Teknologiariski on läsnä epätietoisuudessa, mutta kun teknologia validoidaan testauksella, sen riski vähenee. Ja Y2K-riskit häipyvät, kunhan kaikki kellot ovat reilusti uudella vuosituhannella.
13. Joskus riskit tietysti "laukeavat", eli muuttuvat vahingoiksi... Silloin punnitaan suunnitelmat niiden hallitsemiseksi.

Riskeistä voi ajatella eri tavoilla

14. Riskeissä on kyse epävarmuudesta ja epätäydellisyydestä. Kun nämä hyväksyy, riskien olemassaolon ja niistä puhumisen kokee luontevana.
15. Toisaalta, moni ajattelee, että riskeihin ei voi vaikuttaa. Silloin ei riskeistä kannata murehtia.
16. Ammattilaisen lähtökohta on kuitenkin, että useimmiten ja suurimpaan osaan riskejä voi vaikuttaa jollain toiminnan tasolla: välttäen, todennäköisyyttä tai seurauksia minimoiden, heikkojakin indikaattoreita seuraten, hypäten vaihtoehtoiseen toimintamalliin jne... Silloin riskeistä kannattaa puhua kokonaisvaltaisina skenaarioina.
17. Se, millainen on kuvamme ihmisistä ja organisaatioista, vaikuttaa keskeisinä koettuihin riskeihin ja myös käsitteisiin.

18. Joku organisaatio huolehtii "avainhenkilöriskeistä" ja tärkeiden henkilöiden vaihtuvuudesta, toinen taas henkilöstökokemuksesta ja yhteisen kasvamisen uhista. Yhtä huolestuttaa innovointiin kuluva rahamäärä, toista taas se, mitä tapahtuu, jos organisaatio jämähtää paikalleen eikä osaa uudistua ja disruptoitua.
19. Joku yritys huolehtii tietoturvariskeistä oikeusjuttujen ja maineen näkökulmasta, toinen taas pohtii asiakkaille aiheutuvia ongelmia.
20. Nämä ovat eri ajattelun ja aikakauden ajattelumalleja ja strategioita.
21. Esiintyy myös tietämättömyyttä, joka rajoittaa koettua riskien avaruutta.
22. Yleinen maailman ja teknologian muuttuminen muuttaa riskien kenttää. Aiempina vuosikymmeninä ei tietoturvasta ja tietosuojasta tarvinnut kantaa määräänsä enempää huolta, mutta nyt ne ovat ykkösasioita.
23. Ja valtioidenkin tilanteet vaihtelevat. Poliittinen riski voi tulla ajankohtaiseksi maassa, jossa sitä ei hetki sitten koettu relevantiksi.
24. Lintukodossa ei tarvitse miettiä kybersabotaaseja, mutta käärmeiden pesässä pärjää vain, jos on kaikkeen varautunut ja kaikkea vastaan suojautunut.
25. Teollisessa yhteiskunnassa huolestuttivat tapaturmat ja työperäiset sairaudet, mutta nyt työpaikan kiinnostavuus työmarkkinoilla.

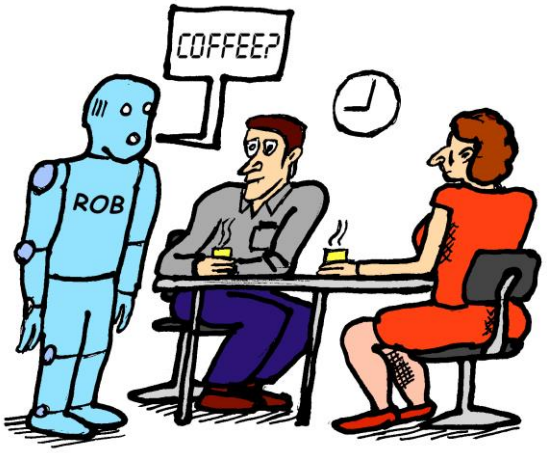
26. Mediayhteiskunnassa on maineriski aina läsnä. Hutilointi vaikkapa tietoturvassa ei aiheuta vain tietovahinkoja.
27. Ihmiset ovat aina sokeita riskeille ja näkevät vain asioita, jotka ovat tuttuja omassa kontekstissa ja omassa historiassa. Se on "mentaalista kiertotaloutta". Uusien kontekstien ja tulevaisuuden ympäristön riskejä on vaikea käsitellä.
28. Posin kautta -ajattelu on riskiajattelun ja todellisen suorituskyvyn vihollinen.
29. "Mokailun hyväksyminen" ja siitä oppiminen pitää myös ymmärtää oikein. Hölmöily on hölmöä, mutta virheet ovat väistämättömiä vähänkään ei-triviaalissa toiminnassa ja liiketoimintariskejä on pakko ottaa.
30. Riskiajattelu on läsnä kaikissa organisaation toiminnoissa ja ajattelumalleissa – johtaminen, liiketoiminta, uudistuminen, laatu, tietohallinto, etiikka... jne...

Riskien ja laadun suhde

31. Laatua voidaan aina ajatella riskien kautta. Joskus se on dominoiva näkökulma, joskus siinä vain vieraillaan välillä tekemällä vaikkapa riskianalyysi.
32. Teollisessa palvelutoiminnassa on variaatiokin riski ja palvelun muuta laatua kannattaa alentaa, jotta variaatio saadaan kuriin, sillä negatiiviset poikkeamat odotuksista ovat aina ikävä vahinko.
33. "Pakollinen laatu" muodostaa perinteisen laaturiskin, jota hallitaan hyvällä suunnittelulla ja toteutuksella.
34. "Ylimääräinen laatu" on jotain, mikä erottaa kilpailijoita. Sen onnistuminen, innovaatioiden onnistuminen, muodostaa liiketoimintariskin, jota ei ole niin helppoa hallita, sillä uusi ja erilainen on aina vähän hallitsematonta.
35. Liiketoimintariskien ottaminen edellyttää laadukasta perustoimintaa – vanhaa pohjaa, joka kannattaa kurotellessa.

Elämme hypen ajassa

36. Elämme hypen ja uuden aikaa. Disruptoivia teknologioita tarjotaan koko ajan. Organisaatio- ja projektimallitkin muuttuvat. Startupien pitäisi mullistaa oma alansa uusilla liiketoimintamalleilla.
37. Kaikki hype on iso riski. Mitä on uusi asia ei toimikaan?
38. Hypen epäily ei ole uuden vastaisuutta, vaan tervettä järkeä.
39. Mitä, jos vaikka tekoäly ei toimikaan luotettavasti? Miten se voisi vikaantua? Miten vahdimme sen toimintaa?
40. Robotiikan ensimmäisessä teollisessa käyttöönottovaiheessa (muutama vuosikymmen sitten), niiden riskianalyyseissä oli oleellista tunnistaa uudella tavalla liikkuvan mekaniikan vaaroja (tein itse korkeakoulussa erityistyön robottien turvallisuudesta – ikävä kyllä sitä ei ole tallella) ja toisaalta automaation keskeytysriskejä.
41. Nykyään tiedostetaan, että älykäs robotiikka on dataintensiivistä ja tietoriskit ovat mukana riskien paletissa. Mutta kun kuvioihin tulee humanoidirobotteja, paletti laajenee ja sosiaaliset riskit kontekstissa – työpaikka, laitos, koti – ovat hyvin olennaisia.
42. Riskienhallinnan ensiaskel on kriittinen ajattelun uusista asioista ja uuden idean kokonaisvaltainen analysointi.



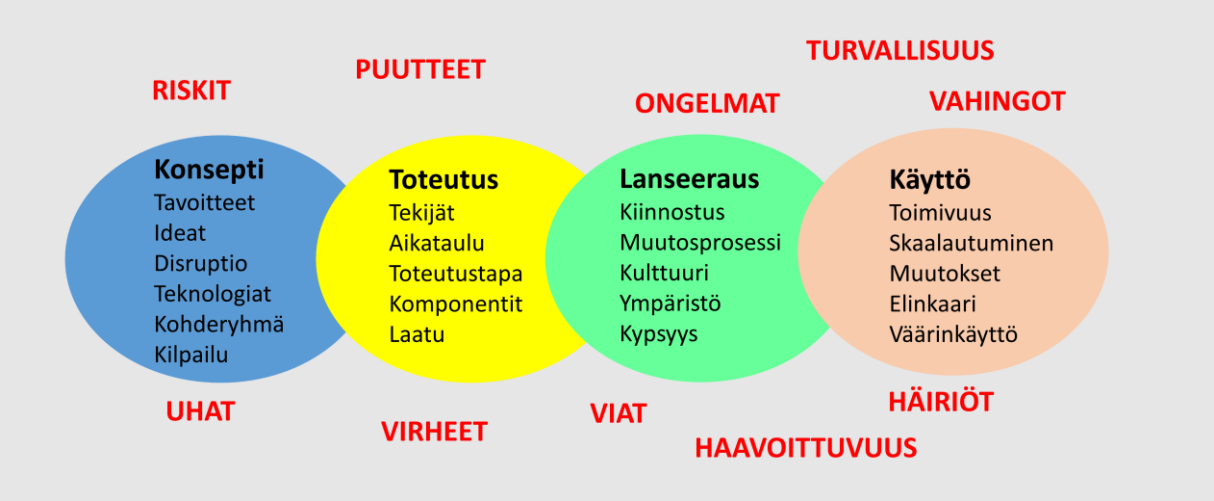
Riskienhallinnasta

43. Riskien kanssa pitää tehdä töitä, jotta ne eivät laukea.
44. Riskienhallinta on omanlainen paradigmansa, jossa järjestelmällisesti, yleensä ryhmätyönä, riskejä tunnistetaan, niiden suuruutta arvioidaan, mietitään niiden kontrollointia ja jaetaan vastuita. Ja sitten seurataan ja välillä katselmoidaan tilannetta ja päivitetään käsityksiä.

45. Riskienhallinta on ammattilaisuutta ja merkki eettisestä toimijasta – yksilöstä ja organisaatiosta. Se on vastuullisuutta. Ja riskienhallinnasta tinkiminen on vastuuttomuutta.
46. Riskeissä on kuitenkin kyse tärkeistä asioista – liiketoiminnasta, työpaikoista, terveydestä ja jopa hengestä tai yhteiskunnan tulevaisuudesta.
47. Riskienhallinnalla myös hallitaan vastuuta. Kun projektin riskit tunnistetaan, projektipäällikkö siirtää henkilökohtaisen riskinsä pykälää ylemmäksi.
48. Riskienhallinta ei ole excelien täyttämistä, vaan ajattelua.
49. Kun riskejä tunnistetaan ryhmässä, jossa on eri ammattiryhmien ihmisiä, ulkoistetaan ja prosessoidaan erilaisia käsityksiä kohteesta ja toimintaympäristöstä. Se on nykyaikaista yhteiskehittämistä.
50. Riskeihin pitää sitoutua. Niiden hallinta pitää myydä. Se onnistuu parhaiten tunnistamalla ne yhdessä ja sopimalla yhdessä niiden hallinnasta.
51. Tämän ohella tarvitaan johtajuutta ja johtopuhetta, jotta organisaation yhteiset riskit saadaan käsittelyyn.
52. Riskienhallinta on tietojohtamista. Riskitietoa jaetaan, käsitellään ja sen perusteella toimitaan.
53. Riskien tunnistaminen on luovaa skenaarioiden kuvittelua lähtien jostain kohdasta, ei väliä mistä: puute/vaikutus -> häiriö -> tapahtuma -> seuraus.
54. Esim.: murtautuminen järjestelmään -> tietokannan kryptaus -> palvelunesto -> liiketoiminnan keskeytys. Riskin jäsennys voidaan aloittaa mistä kohdasta tahansa, menetelmästä ja mindsetistä riippuen.
55. Riskien tunnistaminen on hieno mahdollisuus oppia järjestelmän toiminnasta. Joskus se tehdään rutiininomaisesti, vaikka olisi mahdollisuus tehdä avauksia uudelle ymmärrykselle ja ajattelulle.
56. Niinpä järjestelmän suunnitteluvaiheessa tehdyt analyysit ovat tärkeä suunnitteluprosessin osa. Kun riskejä ja potentiaalisia ongelmia tunnistetaan, nähdään mahdollisuuksia parantaa suunnitelmia. Suunnittelussa on aina reflektiivinen osa ja systeemeillä, joihin liittyy todellisia riskejä, reflektioon tarvitaan moninäkökulmaista yhteistä prosessia.
57. Monenlaisia etsittäviä asioita: Riskit uhkaavat, vaarantavat, tuottavat lauetessaan vahinkoa. Ongelmat haittaavat, estävät, vähentävät kokemusta. Puutteet estävät jotain, haittaavat, voivat olla ongelma. Virheet tuottavat ongelmia ja riskejä. Häiriöt ovat tilapäisiä ongelmia. On suunnittelun tai toiminnan laadun puutetta, jos häiriöitä ei hallita. Vaarat aiheuttavat turvallisuusriskin. Haavoittuvuudet ovat alemman tason syitä tietoturvariskeille – monen muun muassa. Jne...
58. Joskus mietitään, että onko joku asia niin iso, että se on riski ja että siitä kannattaa puhua? Ei kannata miettiä rajoja, vaan tunnistaa mahdollisia ongelmia.
59. Asian suuruus tulee relevantiksi vasta, kun mietitään, miten siihen suhtaudutaan? Yritetäänkö se kiertää (uusi suunnitelma, komponentin vaihto), voiko sitä vähentää (parempi disaini, turvajärjestelmä), voisiko riskin siirtää (vaikka alihankkijalle) tai onko asia sellainen, että sen kanssa pitää vain elää – asia, johon ei voida vaikuttaa tai pieni riski.
60. Hyvä riskianalyysi tarkastelee aina asioita useasta näkökulmasta ja tyylillä – elementit, toiminta; yleiset ongelmat, simulointi. Varsinainen työ tehdään tietenkin muualla kuin analyysisessioissa – arkisessa työssä.
61. Riskianalyysikin on riski! Mikään ei olisi kyberrikolliselle arvokkaampi kuin tietoriskianalyysi, joka paljastaa organisaation käsityksen sen suurimmista uhista! Niinpä pitää tarkkaan katsoa, miten riskilistoja jaellaan.

Projektitoiminnassa

62. Klassikkosanonta: "Risk management is how adults manage projects" – Tim Lister and Tom DeMarco. Riskienhallinta on projektinhallinnan ydintä. Samalla se muodostaa laadunvarmistuksen ison osan.
63. Kun vahinkoriskit hallitaan, voidaan ottaa innovaatioriskejä.



64. Koska riskejä on monen tasoisia, on projekteissakin tehtävä riskienhallintaa kaikilla tasoilla.
65. Painotus vaihtelee. Liiketoimintariskejä mietitään eniten alussa projektin skouppia miettiessä ja taas myöhemmin sen tuloksia käyttöönottaessa. Sillä välillä keskitytään projektiriskeihin ja tuoteriskeihin – ml. teknologiariskeihin.
66. Projektinhallinnan taso on kuitenkin avoin kaikenlaisille riskeille – vain projektiriskit ovat aina vakioelementtinä mukana.
67. Niinpä projekteihin pitää riskienhallinta rakentaa projektin tavoitteiden ja skoupin mukaan.
68. Koska toiminnan eri tasot vaikuttavat toisiinsa, on niihin luotava näkyvyyttä ja kytkentöjä. Pienetkin systeemien toteutusten tekniset valinnat vaikuttavat liiketoimintariskeihin. Ilman ylätason asioiden miettimistä ei voi tehdä hyvää suunnittelua eikä hallita riskejä.
69. Toimittajan kannalta riskit ovat joko omia tai asiakkaan tai yhteiskunnan (yleisemmin ympäristön) riskejä.
70. Oma lehmä on aina lähinnä katsetta ja siksi toimittaja miettii ensin omia riskejään: saako toimitettua halutun asian riittävän hyvin. Mitkä asiat voisivat uhata sitä? Miten niiltä suojaudutaan?
71. Turvallisuuskriittisissä sovelluksissa onnettomuus- ja tapaturmariskit ovat tietysti keskeiset ja edellyttävät turvallisuussäädösten ja -standardien mukaisia menettelyjä systeemin kehittämisessä. Mutta niilläkin riskien maailma kattaa paljon muuta eikä esim. testaus saa perustua vain pakollisten vaatimusten täyttämiseen ja sitä myöten markkinakelpoisuuteen.
72. Vaikutustenarviointi on monien asioiden yhteydessä nimitys tietynlaiselle edellytetylle riskianalyysille. Esim. tietosuoja-asetus edellyttää sellaista.
73. Se on hyvä idea tehtynä tavalla, joka auttaa ymmärtämään kokonaissysteemiä, sen toiminnan muuttumista, mahdollisia ongelmia ja myös uusia mahdollisuuksia. Vaikutusten pitäisi tietysti olla myös positiivisia...
74. Sosioteknisen järjestelmän dynamiikka on sellaista että vaikutusten analysointi ei saa olla suoraviivaista ja keskittyä vain muutettavaan systeemin elementtiin.
75. Sanotaan, että inkrementaaliset projektimallit ovat hyviä riskienhallinnalle. Näin on vain, jos niissäkin muistetaan tehdä hyvää kokonaisuuden suunnittelua konseptitasolla, eikä sorruta koodauskulttuuriin.
76. Inkrementaalinen toiminta on tärkeää vähänkin kaoottisessa ympäristössä, koska edes sellaisen riskejä ei osata tunnistaa ennakolta. Inkrementit antavat ymmärtämismahdollisuuden kontekstille, tilannepäivityksen ja uusien mentaalisten "hälyttimien asentamisen".
77. Joskus sanotaan, että vasta testaus paljastaa tuotteen riskit. Testaus viittaa yleensä ja silloinkin toiminnalliseen testaukseen. Se testaus paljastaa testattavan version julkaisemisen riskit.

78. Konseptin testaus prototyypeillä ja MVP-versioilla paljastaa koko tuoteliiketoiminnan riskit.
79. Paljon puhutaan käyttäjä- ja asiakaskokemuksista. Käytettävyys- ja käyttäjäkokemustestaus auttaa näkemään niihin liittyviä riskejä.
80. Turvallisuusriskit paljastetaan turvallisuus- ja luotettavuusanalyyseillä ja niihin liittyvien tilanteiden hallinnan testeillä.
81. Järjestelmän käyttöönoton ja hyväksynnän riskien viimeinen testausportti on hyväksymistestaus.
82. Lanseerauskampanjan riskien välttämistä auttaa kuormitustestaus.
83. Tietoturvariskit arvioidaan analyyttisesti ja testaus selvittää vain niiden hallinnan tason.
84. Mutta kypsä toimittaja miettii asiaa asiakkaan kannalta. Miten toteutettava asia muuttaa asiakkaan toimintaa? Mitä riskejä liittyy muutokseen, uuteen? Silloin pitää tehdä asiakkaan toiminnalle riskianalyysi.
85. Hektisessä toiminnassa tarkastellaan nykyhetkeä, mutta tulevaisuus on aina tuleva vastaan joskus. Siksi on mietittävä, miten järjestelmä toimii tulevaisuuden skenaarioissa. Onko sen muuttaminen triviaalia, vai isoriskinen remontti? Onko perusta luja, vai juoksuhiekkaa?
86. Arkkitehtuurin skenaariopohjainen arviointi on riskianalyysiä.

Tapahtumista oppiminen

87. Joskus riskit laukeavat. Silloin on paikka katsoa, mitä tapahtui ja oppia siitä.
88. Tietenkin kunnollinen analyysi kannattaa tehdä vain tietyn rajan ylittäville tapahtumille. Yleensä raja menee jollain tavalla vahingon suuruudessa.
89. Tapahtuneitakin asioita pitää käsitellä toiminnan eri tasoilla. Tiimeissä, projektien ja toimintojen johdossa, organisaation johdossa.
90. Olennaista on oppia menneestä tulevaisuutta varten, ei etsiä syyllisiä, vaan syitä.
91. "Syyt" ovat harvoin kausaalisia syistä. Kaiken taustalla olevia "juurisyitä" ei ole. On vain joukko tapahtuneeseen vaikuttavia asioita.
92. Vaikuttavat tekijät toimivat joko systeemin eri elementtien tai erilaisten mekanismien kautta.
93. Mitä systeemisempi konteksti on, sitä enemmän pitää miettiä systeemin eri osien erilaisia vaikutuksia. Sosioteknisten järjestelmien yhteydessä on mietittävä esim. ihmisiä, välineitä, yhteistyötä, sääntöjä ja normeja, työnjakoa, tiedonkulkua jne...
94. Oppiminen siis edellyttää jo hieman oppineisuutta: sitä ymmärrystä, että toimintajärjestelmä ei ole aina niin simppeli kuin miltä se näyttää.

Lopuksi

95. Riskien maailma on monimuotoinen kehikko.
96. Mitä enemmän olemme riippuvaisia tietotekniikasta, sitä enemmän siihen liittyvät riskit voivat vaikuttaa elämäämme.
97. Niinpä riskejä pitää systemaattisesti tunnistaa ja hallita perusteellisemmin kuin aiemmin. Tunnistamisessa tarvitaan moninäkökulmaisuutta (toimijat, toiminnot; systeemien rakenne ja toiminta; tutut ja vieraat asiat), systeemisyyttä (vuorovaikutteiset systeemin elementit ja eri systeemit) ja kokonaisvaltaisuutta (toiminnan ylätaso aina näkyvillä).
98. Niiden taustalla on kontekstin ja sen luonteen oikea asemointi ja ymmärtäminen.
99. Kaikki tämä on sellaista ajattelua, jota muutenkin tarvitaan nykymaailmassa. Siksi riskienhallinnan tilaa ja käytäntöjä kannattaa juuri nyt arvioida jokaisessa organisaatiossa.
100. Iso osa sitä on toiminnan aikuinen, kriittinen kulttuuri ja läsnä oleva riskiajattelu – kaikkien ei tarvitse olla riskienhallintaihmisiä, mutta se elementti pitää olla vastapainona sopivalle intoilulle. Diversiteetti ja dynamiikka ovat päivän sanat.

Matti Vuori on tehnyt riskien parissa töitä varsinkin tutkijana ja kehitellyt organisaatioille välineitä riskienhallinnan tueksi. Jutun julkaisuhetkellä hän on etsimässä töitä Tampereella.