



VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

Julkisen hallinnon digitaalisen turvallisuuden strateginen riskiarviomalli ja haastattelut

Digitaalisen turvallisuuden strateginen johtoryhmä
7.5.2020

Julkisen hallinnon digitaalisen turvallisuuden strateginen riskiarviomalli - luonnos

Julkisen hallinnon digitaalisen turvallisuuden strateginen riskiarviomalli - vaiheistus

DVV & Tietokiri

Tiedon keräys

Digiturvanäkökulma:

- Kansallinen riskiarvio
- Julk hall riskienhallinta
- TIKE, SUPO, Traficom, DVV/Vahti
- JTS, TTS
- Kv-riskidata: WEF, ISF, Enisa

DVV & Vahti

Tiedon luokittelu

Luokitellaan riskit (VM/riskienhallinta):

- Strateginen, operatiivinen, taloudellinen sekä vahinkoriski

Poimitaan digiturvan näkökulmasta vaikuttavat ja olennaiset riskit

VM & DVV & Vahti

Tiedon analysointi

Digiturvan näkökulmasta poimitut riskit käsitellään päätöksenteon pohjaksi riskikuvausmallin mukaisesti

STR JORY

Tiedon verifointi

Strateginen johtoryhmä käsittelee riskikartan

Ylimmän johdon asiantuntija-arvio riskikuvausmallin mukaisesti

DVV & Vahti

Analyyysin täydennys

DVV ja Vahti-verkosto täydentävät riskienhallintatoimenpiteet sekä niihin liittyvät kustannukset.

Arvioidaan riskienhallinnan riippuvuussuhteita

STR JORY

Toimeenpano

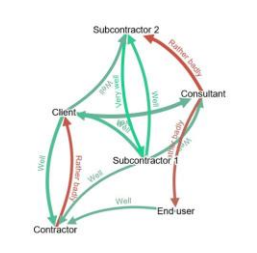
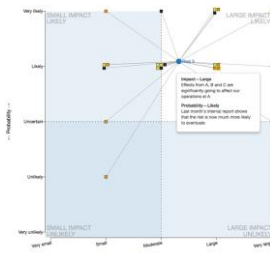
Strateginen johtoryhmä käsittelee riskit & riippuvuussuhteet ja seuraa toimenpiteitä

Strategisen johtoryhmän jäsenet sisällyttävät riskiarvion mukaiset toimenpiteet JTS ja TTS



Adversarial	Accidental	Environmental
Consumer	Supplier	Damage to or loss of external communications
Customer	Employee (general)	Sanctions
Business partner	Employee (specific)	Failure of environmental control systems
Equipment (hardware)	Supplier/vendor/partner	Fire (build)
Marketing group		Fire (structure)
Internal hacker		Hoax
Network		Hardware malfunction or failure
Organizational group		Human error
Supplier/vendor/partner		Malware (e.g. malware outbreak)
		Power failure or fluctuation
		Reputational risk (e.g. scandal and litigation)
		Service
		Terrorism
		Violence/espionage

Risk Ref #	Risk Description	Direction & Response Status
O.6	The risk that an unforeseen event or activity may impact a project's progress resulting in objectives not being fulfilled.	Dec 14 Mar 15
S.2.2	The risk that the Corporation may be unable to execute strategic goals and objectives in the LACIM market.	↑ ↓ → ←
T.2	The risk that the Corporation may be unable to adequately safeguard structure and customer data, specifically PII, resulting in fines, penalties, liabilities, legal claims, and/or reputational harm.	↑ ↓ → ←
O.2	The risk that sub-optimal processes may have an adverse effect on financial processes or business operations.	↑ ↓ → ←
S.1	The risk that the Corporation may be unable to identify, fund, and develop successful and timely new products and services.	↑ ↓ → ←
O.4	The risk that an inability to attract and retain qualified personnel may result in a loss of knowledge/capital or an adverse impact on the Corporation's business operations and results.	↑ ↓ → ←
S.5.1	The risk that increased competition in markets outside of Puerto Rico may result in an adverse effect on business operations and financial results.	↑ ↓ → ←
L.2	The risk that the Corporation or its partners may be non-compliant with existing or new laws, regulations or industry standards (e.g., penalties, fines, public censure, revocation of license) resulting in a financial loss or reputational harm.	↑ ↓ → ←
T.1	The risk that ineffective data governance may result in inaccurate, unstructured, or unavailable data.	↑ ↓ → ←
T.3	The risk that systems and applications to support current customer requirements as well as address emerging business demands may have a negative impact on the Corporation's ability to retain current customers and/or operate the business effectively, resulting in a potential material adverse effect on the business, financial condition, or results of operations.	↑ ↓ → ←



Risk Ref #	Risk Description	Direction & Response Status
O.6	The risk that an unforeseen event or activity may impact a project's progress resulting in objectives not being fulfilled.	↑ ↓ → ←
S.2.2	The risk that the Corporation may be unable to execute strategic goals and objectives in the LACIM market.	↑ ↓ → ←
T.2	The risk that the Corporation may be unable to adequately safeguard structure and customer data, specifically PII, resulting in fines, penalties, liabilities, legal claims, and/or reputational harm.	↑ ↓ → ←
O.2	The risk that sub-optimal processes may have an adverse effect on financial processes or business operations.	↑ ↓ → ←
S.1	The risk that the Corporation may be unable to identify, fund, and develop successful and timely new products and services.	↑ ↓ → ←
O.4	The risk that an inability to attract and retain qualified personnel may result in a loss of knowledge/capital or an adverse impact on the Corporation's business operations and results.	↑ ↓ → ←
S.5.1	The risk that increased competition in markets outside of Puerto Rico may result in an adverse effect on business operations and financial results.	↑ ↓ → ←
L.2	The risk that the Corporation or its partners may be non-compliant with existing or new laws, regulations or industry standards (e.g., penalties, fines, public censure, revocation of license) resulting in a financial loss or reputational harm.	↑ ↓ → ←
T.1	The risk that ineffective data governance may result in inaccurate, unstructured, or unavailable data.	↑ ↓ → ←
T.3	The risk that systems and applications to support current customer requirements as well as address emerging business demands may have a negative impact on the Corporation's ability to retain current customers and/or operate the business effectively, resulting in a potential material adverse effect on the business, financial condition, or results of operations.	↑ ↓ → ←

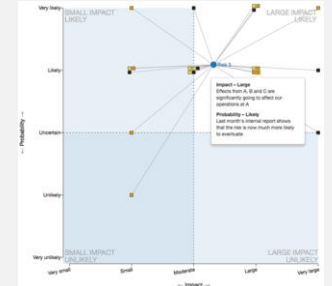
Digitaalisen turvallisuuden riskikuvausmalliluonnos

- Digitaalisen turvallisuuden riskien kuvaaminen ja seuranta edellyttävät toistettavuutta.
- Malli sisältää
 - digitaalisen turvallisuuden olennaiset ja vaikuttavat riskit,
 - arvion riskin kehityssuunnasta,
 - riskin arviointiin liittyvät mittarit/kontrollit sekä
 - hallintatoimenpiteet kustannusarvioineen.
- KPMG:n konsulttituki keskittyy riskikuvausmallin tarkentamiseen

Dynaaminen riskikartta

Digitaalinen työkalu monitahoisten strategisten riskien pohdintaan ja yhteiseen analyysiin.

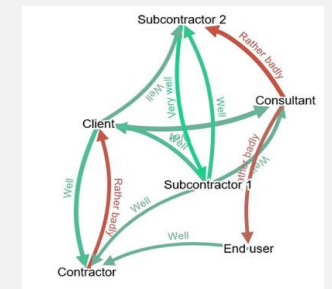
Analyyysin uusiminen säännöllisesti antaa kuvan siitä, miten esimerkiksi riskien hallintatoimet ovat vaikuttaneet.



Yhteistoimintakartta

Dynaaminen työkalu visualisoi esimerkiksi riippuvuussuhteet ja yhteistoimintaketjut osapuolten välillä.

Visualisoinnilla selkeytetään kokonaiskuvaa ja vastuita



Riskiluettelo

Malli riskien ja hallintatoimenpiteiden dokumentointiin

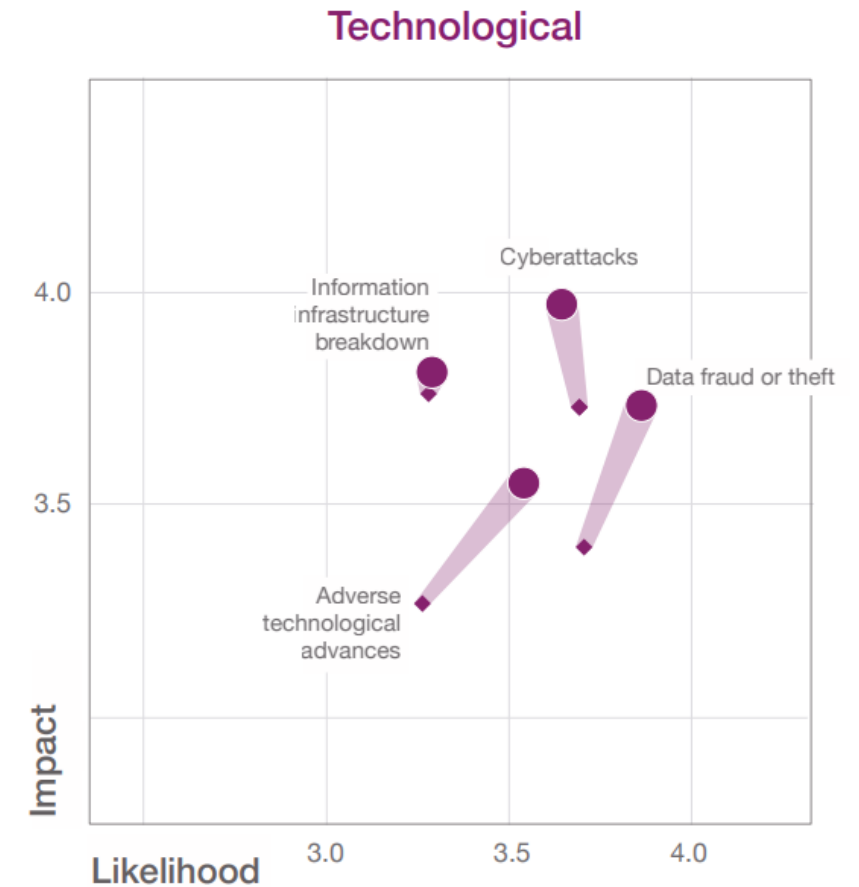
Riski	Kuvaus	Riskikkuu	Hallinta	Vastuu	Kustannus	Seuranta
Nimi	Riskin kuvaus ja laajuus	Riskin position, todennäköisyys ja vaikutus	Riskin tyypilliset hallintatoimenpiteet	Vastuussa oleva rooli	Hallintatoimenpiteiden esiohittama investointi	Hallintatoimenpiteiden status

Esimerkkejä tausta-aineistoista

Esimerkkejä riskianalyysin pohjadatasta – World Economic Forum

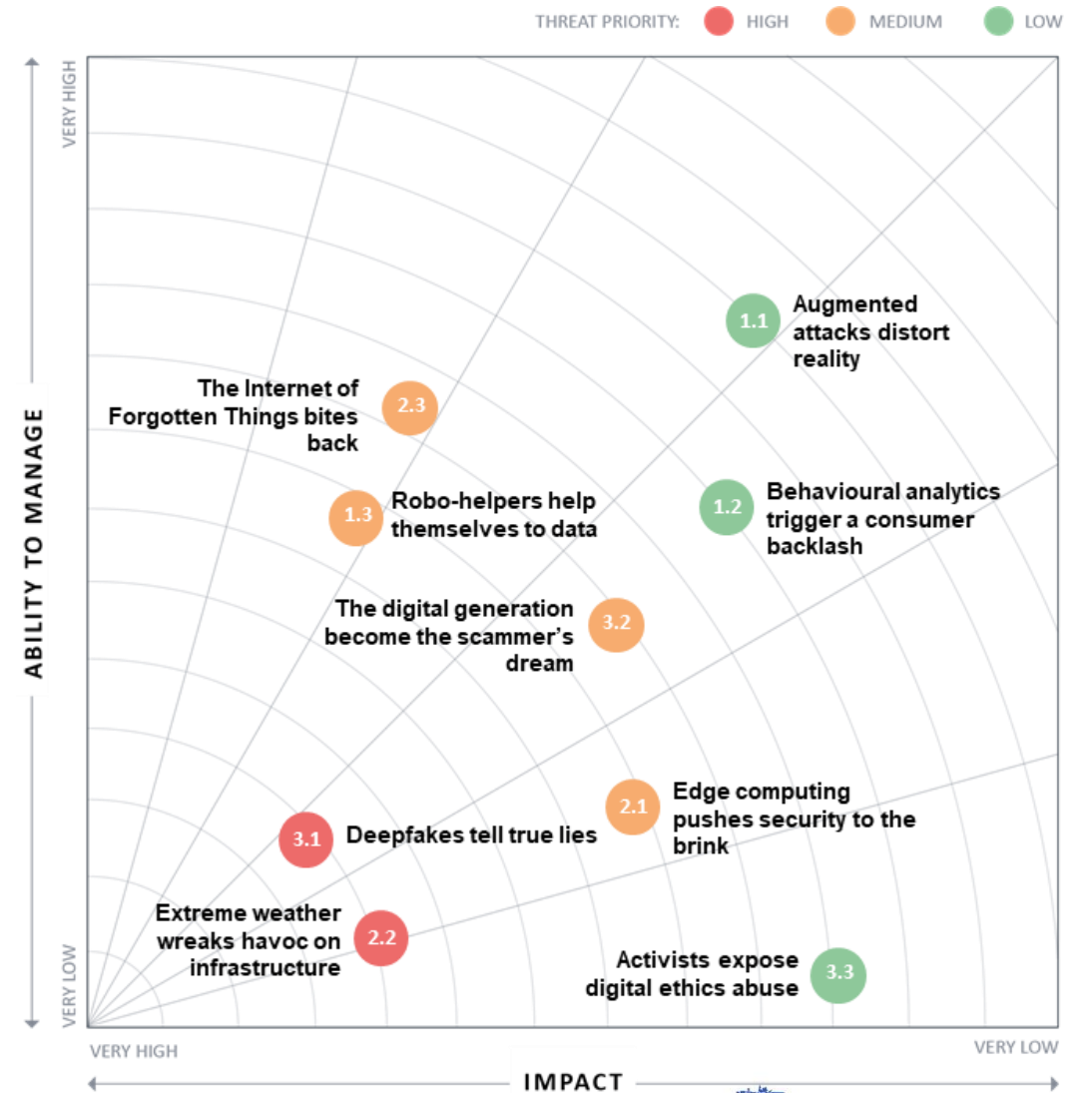
- World Economic Forum on nostanut neljä teknologiariskiä viimeisimpään raporttiin. Erityisesti digitaalisen infrastruktuurin vahingoittumisen nähdään yhtenä vaikuttavimmista riskeistä yhteiskunnan toiminnan kannalta.
- WEF raporttia voidaan hyödyntää strategisen tason kehittämistoimenpiteiden kohdentamiseen.

Risk	Description
Adverse consequences of technological advances	Intended or unintended adverse consequences of technological advances such as artificial intelligence, geo-engineering and synthetic biology causing human, environmental and economic damage
Breakdown of critical information infrastructure and networks	Cyber dependency that increases vulnerability to outage of critical information infrastructure (e.g. internet, satellites) and networks, causing widespread disruption
Large-scale cyberattacks	Large-scale cyberattacks or malware causing large economic damage, geopolitical tensions or widespread loss of trust in the internet
Massive incident of data fraud or theft	Wrongful exploitation of private or official data that takes place on an unprecedented scale



Esimerkkejä riskianalyysin pohjadatasta – Information Security Forum

- Information Security Forum julkaisee vuosittain yhdeksän lyhyen aikavälin uhkakuvaa perustuen jäsenorganisaatioiden uhka-arvioihin
- Uhkakuvia voidaan hyödyntää taktisella tasolla kehitystoimenpiteiden kohdentamiseen.
- Threat radar (oikealla) ei ole riskimatriisi. Tutka antaa kuvan siitä, miten valmiita organisaatiot ovat kohtaamaan tulevia uhkia.



Strategisen johtoryhmän jäsenten haastattelut kesäkuussa skypeissä

Alustavat haastattelukysymykset

- 1) Mitä tietoa digiturvan riskeistä ja mahdollisuuksista puuttuu tai on liian vähän?
 - 2) Kuka tämän tiedon voisi tuottaa? Kuinka usein tämä tieto päivittyy?
 - 3) Mitä digiturvan vaikuttavuudesta ei tiedetä riittävästi?
 - 4) Mitä muuta tietoa strategisen riskiarvion tulee sisältää? Mistä tämä tieto saadaan? Kuinka usein tieto päivittyy? Kuka tiedon tuottaa?
 - 5) Mitä näkemyksiä alustava riskiarviomallin vaiheistus ja riskiarviomallikuvaus herättävät?
- VM ottaa yhteyttä ja sopii haastatteluajan
 - Haastattelijat: Tuija Kuusisto, Jani Pyrrö ja Miika Hätinen VM:stä