DIGITAL AND CYBER SECURITY CHECKLIST FOR THE BOARD OF DIRECTORS

Instructions

STRATEGIA22 project

31 March 2022

HUOLTOVARMUUSORGANISAATIO
DIGIPOOLI

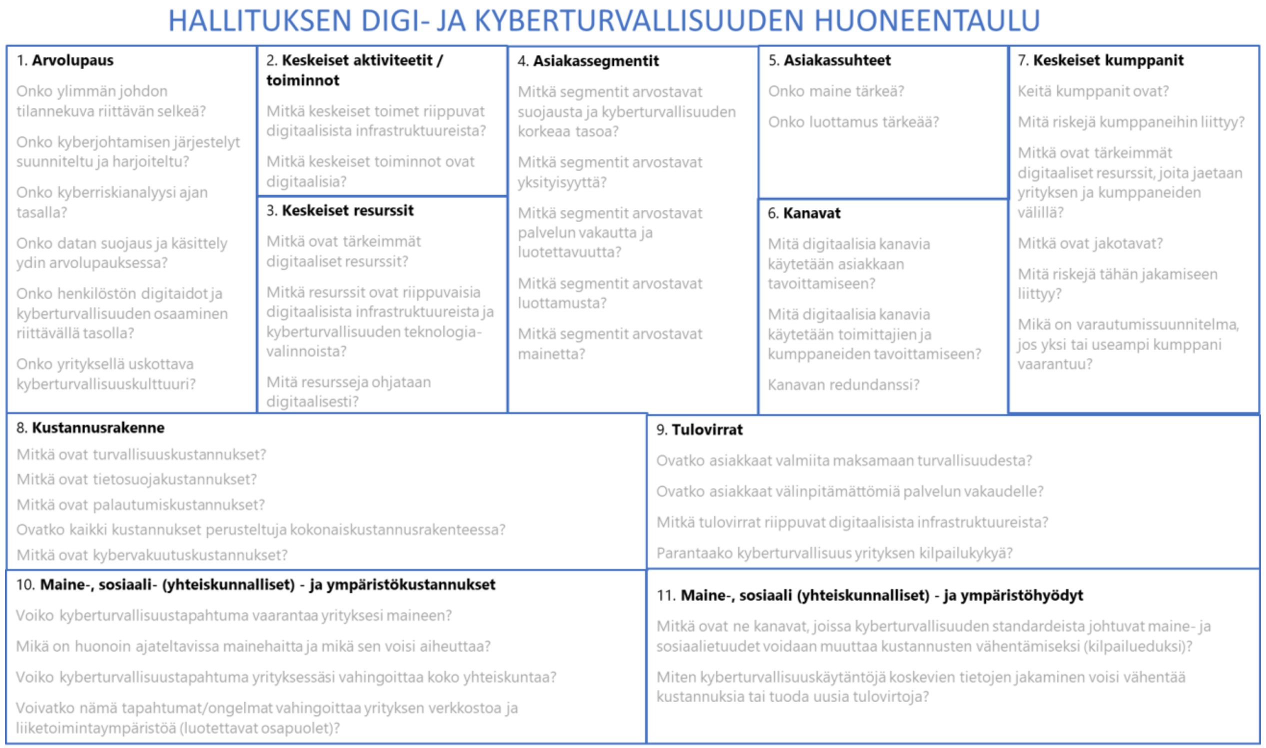
DIGITAL AND CYBER SECURITY CHECKLIST FOR THE BOARD OF DIRECTORS

Purpose of use

The checklist is based on the Business Model Canvas (BMC), which is a simplified tool for visualising the company's business model.

The key success factors created by digitalisation for the business and the relationships between them can be described in this context.

The checklist guides the company's own digital activities, and it can also be used to tell outsiders how the company's digital and cyber security is intended to be arranged and what the factors that create successful business are.



HALLITUKSEN DIGI- JA KYBERTURVALLISUUDEN HUONEENTAULU

1. **Arvolupaus**

Onko ylimmän johdon tilannekuva riittävän selkeä?

Onko kyberjohtamisen järjestelyt suunniteltu ja harjoiteltu?

Onko kyberriskianalyysi ajan tasalla?

Onko datan suojaus ja käsittely ydin arvolupauksessa?

Onko henkilöstön digitaidot ja kyberturvallisuuden osaaminen riittävällä tasolla?

Onko yrityksellä uskottava kyberturvallisuuskulttuuri?

2. **Keskeiset aktiviteetit / toiminnot**

Mitkä keskeiset toimet riippuvat digitaalisista infrastruktuureista?

Mitkä keskeiset toiminnot ovat digitaalisia?

3. **Keskeiset resurssit**

Mitkä ovat tärkeimmät digitaaliset resurssit?

Mitkä resurssit ovat riippuvaisia digitaalisista infrastruktuureista ja kyberturvallisuuden teknologia-valinnoista?

Mitä resursseja ohjataan digitaalisesti?

4. **Asiakassegmentit**

Mitkä segmentit arvostavat suojausta ja kyberturvallisuuden korkeaa tasoa?

Mitkä segmentit arvostavat yksityisyyttä?

Mitkä segmentit arvostavat palvelun vakautta ja luotettavuutta?

Mitkä segmentit arvostavat luottamusta?

Mitkä segmentit arvostavat mainetta?

5. **Asiakassuhteet**

Onko maine tärkeä?

Onko luottamus tärkeää?

6. **Kanavat**

Mitä digitaalisia kanavia käytetään asiakkaan tavoittamiseen?

Mitä digitaalisia kanavia käytetään toimittajien ja kumppaneiden tavoittamiseen?

Kanavan redundanssi?

7. **Keskeiset kumppanit**

Keitä kumppanit ovat?

Mitä riskejä kumppaneihin liittyy?

Mitkä ovat tärkeimmät digitaaliset resurssit, joita jaetaan yrityksen ja kumppaneiden välillä?

Mitkä ovat jakotavat?

Mitä riskejä tähän jakamiseen liittyy?

Mikä on varautumissuunnitelma, jos yksi tai useampi kumppani vaarantuu?

8. **Kustannusrakenne**

Mitkä ovat turvallisuuskustannukset?

Mitkä ovat tietosuojakustannukset?

Mitkä ovat palautumiskustannukset?

Ovatko kaikki kustannukset perusteltuja kokonaiskustannusrakenteessa?

Mitkä ovat kybervakuutuskustannukset?

9. **Tulovirrat**

Ovatko asiakkaat valmiita maksamaan turvallisuudesta?

Ovatko asiakkaat välinpitämättömiä palvelun vakaudelle?

Mitkä tulovirrat riippuvat digitaalisista infrastruktuureista?

Parantaako kyberturvallisuus yrityksen kilpailukykyä?

10. **Maine-, sosiaali- (yhteiskunnalliset) - ja ympäristökustannukset**

Voiko kyberturvallisuustapahtuma vaarantaa yrityksesi maineen?

Mikä on huonoin ajateltavissa mainehaitta ja mikä sen voisi aiheuttaa?

Voiko kyberturvallisuustapahtuma yrityksessäsi vahingoittaa koko yhteiskuntaa?

Voivatko nämä tapahtumat/ongelmat vahingoittaa yrityksen verkkostoa ja liiketoimintaympäristöä (luotettavat osapuolet)?

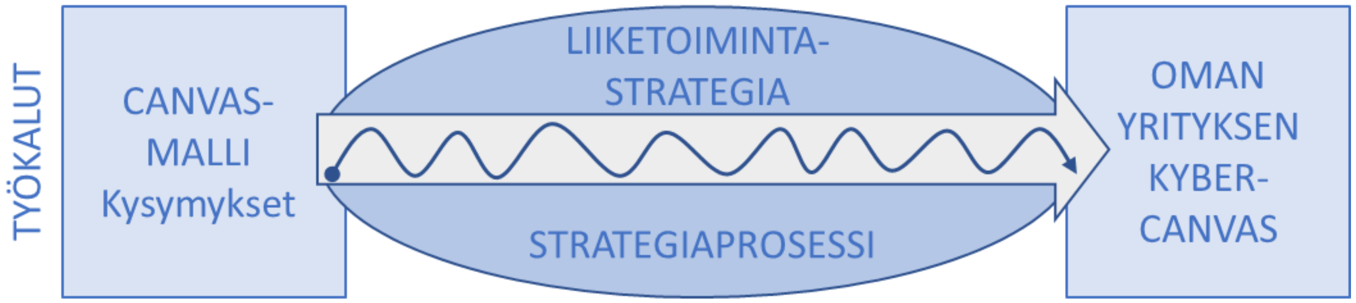
11. **Maine-, sosiaali (yhteiskunnalliset) - ja ympäristöhyödyt**

Mitkä ovat ne kanavat, joissa kyberturvallisuuden standardeista johtuvat maine- ja sosiaalietuudet voidaan muuttaa kustannusten vähentämiseksi (kilpailueduksi)?

Miten kyberturvallisuuskäytäntöjä koskevien tietojen jakaminen voisi vähentää kustannuksia tai tuoda uusia tulovirtoja?

DIGITAL AND CYBER SECURITY CHECKLIST FOR THE BOARD OF DIRECTORS

- The questions in the checklist targeted at different sections have been drawn up from the perspective of digital security.
- The business model and the digital security checklists can be used later to draw up a detailed business plan that uses more specific plans and calculations to describe how the company's business will become profitable with digitalisation.
- The digital and cyber security checklist for the board of directors can be used as a tool for developing the company's digital activities or reviewing the established implementation.
- The model can be worked on either alone or in a group, and the time spent on it can range from a few minutes to as long as several months.
- The company's management can use the model to support business planning.



STRATEGIAPROSESSIN KAUTTA KYBERTURVALLISUUS
TULEE OLEELLISEKSI OSAKSI LIIKETOIMINTASTRATEGIAA

DIGITAL AND CYBER SECURITY CHECKLIST FOR THE BOARD OF DIRECTORS

Contents of the structures

- The checklist can be filled in by answering the questions in numerical order with sentences or keywords.
- The following list includes questions for the different sections. Nine structural components have been added to the sections included in the traditional Business Canvas checklist in order to illustrate the underlying business model. You should answer them before the questions related to cyber security.
- Slides 16 and 17 have templates for filling in the checklist. On slide 16, ‘Value promise’ is the first one on the left, while on slide 17 it has been placed at the centre.
- The finished checklist can be printed out in size A0 or A1 for hanging on the wall.

Contents of the checklist

1. Value promise
2. Key activities/functions
3. Key resources
4. Customer segments
5. Customer relationships
6. Channels
7. Key partners
8. Cost structure
9. Income streams
10. Reputation, social (societal) and environmental costs
11. Reputation, social (societal) and environmental benefits

1. VALUE PROMISE

Business model

- The value promise is at the core of the business model as a whole. The value promise refers to how the customers benefit from our products or services.
  - More effective/cheaper/fast and reliable availability/comfort of use/design/risk-free
- What kind of value is produced for the customer?
- What kind of problem does it help the customer with solving?
- What product packages are offered to the different customer segments?
- Which customer needs do we meet?

Cyber security

- Is the operational picture of the top management clear enough?
- Has the planning and training of digital and cyber management arrangements been carried out?
- Is the cyber risk analysis up to date?
- Is the protection and processing of data realised in the value promise?
- Are the digital skills and cyber security expertise of the personnel at a sufficient level?
- Does the company have a credible cyber security culture?

2. KEY ACTIVITIES/FUNCTIONS

Business model

- The key activities answer the question: What are the tasks or functions to redeem the value promise and carry out business?
  - Production tasks/solutions for the problem
- Where is the work done, what are the distribution channels, where is the product purchased?
- What are the customer relationships like?

Cyber security

- What key activities are dependent on digital infrastructures?
- Which key functions are digital?

3. KEY RESOURCES

Business model

- The most important resources for realising the value promise are identified as key resources; they can be physical, immaterial, financial or human resources.
  - Information systems and devices/patents/brand/transport equipment/employees/financing

Cyber security

- What are the most important digital resources?
- Which resources are dependent on digital infrastructures?
- Which resources are controlled digitally?

4. CUSTOMER SEGMENTS

Business model

- The Customer segments section identifies the customers or customer groups for whom value is generated or offered.
- The groups can be divided based on different characteristics, for example.
  - Uniform mass market customer base/division based on e.g. wealth class/age/usage or importance

Cyber security

- Which segments value protection?
- Which segments value privacy?
- Which segments value the stability and reliability of the service?
- Which segments value trust?
- Which segments value reputation?

5. CUSTOMER RELATIONSHIPS

Business model

- The Customer relationships section answers the question: What kind of customer relationships does the organisation have with old, new or future customers, for example, and how are they maintained?
  - Service based on interaction/self-service/automatically maintained services/taking advantage of customer communities as a part of the purchase process and after it

Cyber security

- Is reputation important in the digitalisation processes?
- Is trust important in customer relationships?
- Does the loss of customer information constitute damage?
- Does the loss of the ability to function pose a threat to trust?

6. CHANNELS

Business model

- The Channels section identifies ways to reach the customer or the ways in which customers receive the value promise. For instance, elements that make it easier to make a purchase decision can be identified as channels.
  - Online shopping/sales personnel/brick-and-mortar shop/partners' distribution channels
- Which channels are cost-effective?

Cyber security

- Which digital channels are used to reach the customer?
- Which digital channels are used to reach the suppliers and partners?
- How much redundance does the channel have? (Refers to the extra data used to ensure the functioning of the system or make it easier to understand)

7. KEY PARTNERS

Business model

- The partners in cooperation necessary for the operation are identified as key partners.
  - Buyer–supplier agreements (competitiveness)/strategic partner (securing sufficient resources, sharing the risks caused by the business)

Cyber security

- Who are the partners?
- Are the priorities of business communicated via agreements?
- What risks are related to the partners?
- What are the most important digital resources shared between you and your partners?
- What are the sharing methods?
- What kind of risks are related to this sharing?
- What is the contingency plan, if one or more partners is at risk?

8. COST STRUCTURE

Business model

- The cost structure describes all costs created in the business related to the implementation process, marketing or distribution channels, among other things.
  - Fixed and variable costs/benefits of mass production
- What are the most important resources, which are the most expensive ones?
- What are the most important activities, which are the most expensive ones?

Cyber security

- What are the security costs of digitalisation?
- What are the data protection costs of digitalisation?
- What are the recovery costs?
- Are all costs justified in the overall cost structure?
- What are the cyber insurance costs?

9. INCOME STREAMS

Business model

- Income streams are linked to the pricing of products or services (value promises). There, the goal is to set a price for the value promise that the different customer segments are willing to pay.
  - Sales revenue/operational charging/activation charges/licensing/rental/advertising revenue

Cyber security

- Are the customers willing to pay for security?
- Are the customers indifferent about the stability of the service?
- Which income streams are dependent on digital infrastructures?
- Will digital and cyber security improve the company's competitiveness?

10. REPUTATION, SOCIAL (SOCIETAL) AND ENVIRONMENTAL COSTS

- Can a cyber security incident endanger the company’s reputation?
- What is the worst damage to reputation imaginable, and what could cause it?
- Can a cyber security incident in your company cause damage to society as a whole?
- Can these problems/incidents damage the company’s network and business environment (reliable parties)?

11. REPUTATION, SOCIAL (SOCIETAL) AND ENVIRONMENTAL BENEFITS

- What are the channels through which the social and reputation-related benefits due to cyber security standards can be transformed into a reduction in costs (competitive advantage)?
- How could sharing information on cyber security practices lower costs or bring in new income streams?

DIGITAL AND CYBER SECURITY CHECKLIST FOR THE BOARD OF DIRECTORS

1. **Value promise**

Is the operational picture of the top management clear enough?

Has the planning and training of digital and cyber management arrangements been carried out?

Is the cyber risk analysis up to date?

Is the protection and processing of data realised in the value promise?

Are the digital skills and cyber security expertise of the personnel at a sufficient level?

Does the company have a

2. **Key activities/functions**

What key activities are dependent on digital infrastructures?

Which key functions are digital?

3. **Key resources**

What are the most important digital resources?

Which resources are dependent on digital infrastructures and cyber security technology choices?

Which resources are controlled digitally?

4. **Customer segments**

Which segments value protection and a high level of cyber security?

Which segments value privacy?

Which segments value the stability and reliability of the service?

Which segments value trust?

Which segments value reputation?

5. **Customer relationships**

Is reputation important?

Is trust important?

6. **Channels**

Which digital channels are used to reach the customer?

Which digital channels are used to reach the suppliers and partners?

Redundancy of the channel?

7. **Key partners**

Who are the partners?

What risks are related to the partners?

What are the most important digital resources shared between the company and its partners?

What are the sharing methods?

What risks are related to this sharing?

What is the contingency plan, if one or more partners is at risk?

8. **Cost structure**

What are the security costs?

What are the data protection costs?

What are the recovery costs?

Are all costs justified in the overall cost structure?

What are the cyber insurance costs?

9. **Income streams**

Are the customers willing to pay for security?

Are the customers indifferent about the stability of the service?

Which income streams are dependent on digital infrastructures?

Will digital and cyber security improve the company's competitiveness?

10. **Reputation, social (societal) and environmental costs**

Can a cyber security incident endanger your company's reputation?

What is the worst damage to reputation imaginable, and what could cause it?

Can a cyber security incident in your company cause damage to society as a whole?

Can these incidents/problems damage the company's network and business environment (reliable parties)?

11. **Reputation, social (societal) and environmental benefits**

What are the channels through which the social and reputation-related benefits due to cyber security standards can be transformed into a reduction in costs (competitive advantage)?

How could sharing information on cyber security practices lower costs or bring in new income streams?

DIGITAL AND CYBER SECURITY CHECKLIST FOR THE BOARD OF DIRECTORS

2. **Key activities/functions**

What key activities are dependent on digital infrastructures?

Which key functions are digital?

3. **Key resources**

What are the most important digital resources?

Which resources are dependent on digital infrastructures and cyber security technology choices?

Which resources are controlled digitally?

4. **Customer segments**

Which segments value protection and a high level of cyber security?

Which segments value privacy?

Which segments value the stability and reliability of the service?

Which segments value trust?

Which segments value reputation?

1. **Value promise**

Is the operational picture of the top management clear enough?

Has the planning and training of digital and cyber management arrangements been carried out?

Is the cyber risk analysis up to date?

Is the protection and processing of data realised in the value promise?

Are the digital skills and cyber security expertise of the personnel at a sufficient level?

Does the company have a credible cyber security culture?

5. **Customer relationships**

Is reputation important?

Is trust important?

6. **Channels**

Which digital channels are used to reach the customer?

Which digital channels are used to reach the suppliers and partners?

Redundancy of the channel?

7. **Key partners**

Who are the partners?

What risks are related to the partners?

What are the most important digital resources shared between the company and its partners?

What are the sharing methods?

What risks are related to this sharing?

What is the contingency plan, if one or more partners is at risk?

8. **Cost structure**

What are the security costs?
What are the data protection costs?
What are the recovery costs?
Are all costs justified in the overall cost structure?
What are the cyber insurance costs?

9. **Income streams**

Are the customers willing to pay for security?

Are the customers indifferent about the stability of the service?

Which income streams are dependent on digital infrastructures?

Will digital and cyber security improve the company's competitiveness?

10. **Reputation, social (societal) and environmental costs**

Can a cyber security incident endanger your company's reputation?

What is the worst damage to reputation imaginable, and what could cause it?

Can a cyber security incident in your company cause damage to society as a whole?

Can these incidents/problems damage the company's network and business environment (reliable parties)?

11. **Reputation, social (societal) and environmental benefits**

What are the channels through which the social and reputation-related benefits due to cyber security standards can be transformed into a reduction in costs (competitive advantage)?

How could sharing information on cyber security practices lower costs or bring in new income streams?

THE SOURCES USED

- www.researchgate.net/publication/37426694_Clarifying_Business_Models_Origins_Present_and_Future_of_the_Concept
- www.varma.fi
- https://en.wikipedia.org/wiki/Business_Model_Canvas#/media/File:Business_Model_Canvas.png
- www.cyberbitsetc.org/post/the-samurai-approach-to-cyber-security-how-does -cyber-risk-fit-into-the-business-canvas

THANK YOU!

Contact information

National Emergency Supply Agency
Aleksanterinkatu 48A, 7th floor
FI-00100 HELSINKI

tel. +358 (0)2950 51000
fax +358 (0)9 260 9584

www.huoltovarmuus.fi
www.nesa.fi
www.varmuudenvuoksi.fi

VARMUUDEN
VUOKSI

HUOLTOVARMUUSORGANISAATIO
DIGIPOOLI