

Digital Services risk management tool

This tool can be used to assess the functional risks of social and healthcare remote and digital services from the client's and patient's perspective. The tool is based on the BowTie risk management model (BowTie).

The term digital service refers to a service implemented with the support of a digital communication channel or platform. Digital services also include remote services, which are real-time services based on an interaction between people.

Risks related to service processes must be identified, and measures to protect against risks must be defined. The evaluation of operational risks must be continuous and last for the entire lifetime of the service.

Structure of BowTie risk management

The BowTie risk management tool can be used to describe various chains of events. The model gets its name from the bowtie shape of the diagram (Figure 1).

In the centre of the diagram is a key event where a loss of control occurs, such as an accident. On the left are chains of events from threats that can lead to a key event. Chains of events can be broken with protections that prevent a key event from occurring. The right hand side presents potential consequences that can be mitigated or limited by responsive actions.

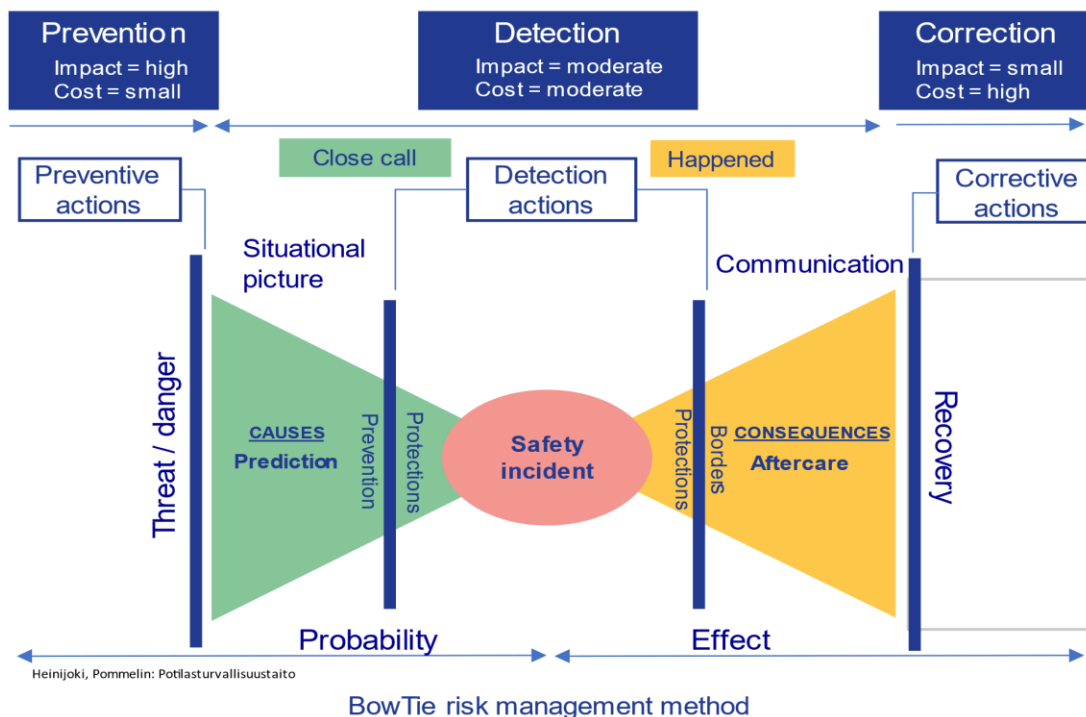


Figure 1. BowTie risk management method (Heinijoki, Pommelin 2019)

BowTie risk management in practice

The most common dangers that can threaten activities within digital services are described in Table 1. The factors that expose you to these risks are described in Table 2.

Table 3 is used to calculate the magnitude of the risk by estimating the probability of each hazard occurring and how large the impact of the occurrence would be. Table 4 is used to assess the need and urgency of the necessary measures. The Excel tool prepared by the Finnish Centre for Client and Patient Safety automatically calculates the magnitude of the risk.

After this, measures to reduce the risks will be reviewed. A record is made for each risk:

- current risk management methods, i.e. a description of preparedness
- assessment of the current management of the risk (adequate, to be developed, insufficient)
- proposals for improving risk management and decided development activities.

Table 1. The most common risks that can potentially threaten activities in remote and digital services:

<p>The client's or patient's dealings in the digital service are not successful, which results in one of the following:</p> <ul style="list-style-type: none"> • The service is interrupted • The service is implemented with incorrect information • Access to the service is delayed • The client or patient is completely deprived of services. <p>The client or patient may be harmed as a result.</p>
--

Table 2. Factors susceptible to risks

Client does not choose a digital service	Client cannot use the digital service	Client does not get the matter in question taken care of
The client has not received information about the service or cannot find the digital service	The client does not have the necessary equipment (computer, smartphone, internet connection)	The digital service is difficult to use or the service is not understandable
The client is concerned about data security or privacy protection	The client does not have tools for strong identification	A technical malfunction interrupts or prevents activities taking place
The client does not know whether the matter in question can be handled by the digital service	The client has insufficient digital skills	It is not possible to handle the matter in question with a digital service
The benefit of the digital service is unclear to the client	Dealing on someone else's behalf is not possible in the digital service	Deficiencies in the client's or Staff's remote interaction skills
	The client's functional limitation or reduced cognition prevents the use of the digital service	Not all relevant facts are identified or verified
	The digital service cannot be used in a language the client understands	The client cannot switch from one digital service or application to another
		The client does not receive written instructions at the end of the digital service

Table 3. Assessment of the magnitude of risk

		Probability				
		1 Rare	2 Unlikely	3 Possible	4 Likely	5 Almost certain
Impact	5 Severe	5	10	15	20	25
	4 Major	4	8	12	16	20
	3 Moderate	3	6	9	12	15
	2 Minor	2	4	6	8	10
	1 Insignificant	1	2	3	4	5

Table 4. Measures to reduce risk

Risk rating	Measures needed to mitigate risk
1-3 Low risk	No action required <ul style="list-style-type: none"> The risk is so low that no action is required
4-6 Moderate risk	Requires a long-term change to activities (6 months) <ul style="list-style-type: none"> The risk should be reduced Measures must be identified and scheduled for implementation If consequences are severe, it is necessary to discover how to reduce the likelihood of recurrence
8-12 High risk	Requires a change in operations in the short term (1 month) <ul style="list-style-type: none"> Risk reduction is essential Measures should be taken quickly Risky activities must be changed quickly or stopped until the risk is sufficiently reduced.
15-25 Extreme risk	Requires immediate change to continue activities <ul style="list-style-type: none"> Risk elimination is necessary Measures should be taken immediately Risky activities should be stopped immediately and should not restart until the risk has been eliminated

It should be noted that a review is always made from the perspective of the client and the patient. If necessary, risk identification can be refined and made more extensively, for example, by the service.

The bowTie risk management method can also be used to review a risk event that has already occurred. The starting point is the consequences of the event for the client or patient. The chain of events is explained by proceeding from right to left. At the same time, it is assessed whether protections had existed and whether they had been implemented.

Excel tool

A written record can be made with the help of an Excel tool prepared by the Finnish Centre for Client and Patient Safety, which contains the identified risk factors (Figure 2). The tool can be obtained by request from noharm@ovph.fi. (not yet in English, coming soon)

The tool also contains a more detailed description of the BowTie from the perspective of social welfare and healthcare digital services.

Vaarojen tunnistus		Riskin arviointi			Nykyinen hallinta	Hallinnan tilannearvio	Riskin hallinnan parantaminen	
Vaaran kuvaus	Vaaralle altistavat tekijät	Todennäköisyys	Vaikutus	Riski	Kuvaus varautumisesta	Riittävä Kehitettävää Riittämätön	Ehdotukset	Vastuuhenkilö
Asiakas ei valitse digipalvelua Asiakas ei ole saanut tietoa palvelusta tai hän ei löydä digipalvelua Asiakkaalla on huoli tietoturvan tai yksityisyyden suojaamisesta Asiakas ei tiedä voiko asian hoitaa digipalvelussa Digipalvelun hyöty on asiakkaalle epäselvä <i>Tyhjille riville voi kirjoittaa lisää tekijöitä</i> Asiakkaan tai potilaan asiointi digipalvelussa ei onnistu, ja palvelu keskeytyy, palvelu toteutetaan virheellisiillä tiedoilla, palvelun saanti viivästyy tai jää kokonaan vaille palveluja. Tämän seurauksena asiakkaalle tai potilaalle voi aiheutua haittaa.	Asiakas ei valitse digipalvelua Asiakas ei ole saanut tietoa palvelusta tai hän ei löydä digipalvelua	Harvinainen	Olematon	1		Riittävä		
	Asiakkaalla on huoli tietoturvan tai yksityisyyden suojaamisesta	Epätodennäköinen	Vähäinen	4		Riittämätön		
	Asiakas ei tiedä voiko asian hoitaa digipalvelussa	Mahdollinen	Vähäinen	6		Kehitettävää		
	Digipalvelun hyöty on asiakkaalle epäselvä	Todennäköinen	Vakava	20		Riittävä		
	<i>Tyhjille riville voi kirjoittaa lisää tekijöitä</i>							

Figure 2. Example screenshot of the Excel tool

This document has been made in the strategy group 3.2 of Client and Patient Safety strategy operational programme.

For more information: Finnish Centre for Client and Patient Safety (noharm@ovph.fi)

Published: 14.5.2024

Publisher: Finnish Centre for Client and Patient Safety

The need for updating the tool is checked annually.