MASTER'S THESIS

Een raamwerk voor het vaststellen van risico's voor de bedrijfsvoering van het mkb op basis van genomen weerbaarheidsmaatregelen, procesvolwassenheid en mate van digitalisering

de Vries, R.

Award date:
2021

Een raamwerk voor het vaststellen van risico's voor de bedrijfsvoering van het mkb op basis van genomen weerbaarheidsmaatregelen, procesvolwassenheid en mate van digitalisering

A framework for establishing SMEs business risks based on resilience measures, business process maturity and degree of digitization

Opleiding:	Open Universiteit, faculteit Management, Science & Technology Masteropleiding Business Process Management & IT
Programme:	Open University of the Netherlands, faculty of Management, Science & Technology Master Business Process Management & IT
Cursus:	IM0602 Voorbereiden Afstuderen BPMIT IM9806 Afstudeertraject Business Process Management and IT
Student:	Rob de Vries
Datum:	13-04-2021
Afstudeerbegeleider	Prof. dr. ir. Johan Versendaal
Meelezer	Prof dr. Rob Kusters
Versienummer:	0.93
Status:	Concept

Abstract

Het bewustzijn rondom cybercriminaliteit is zeer beperkt binnen mkb-bedrijven in Nederland. Hierdoor ontstaat een onjuiste risicoperceptie bij deze bedrijven. Dit terwijl de schade van cybercriminaliteit toeneemt, aanvallen succesvol blijven door ontbreken van basismaatregelen en aanvallen vaker voorkomen en geavanceerder worden. Het doel van dit onderzoek was het opstellen van een raamwerk waarmee de (cyber) risico's voor de bedrijfsvoering van mkb-bedrijven inzichtelijk kunnen worden gemaakt. Hierbij is gekeken naar de invloed van de constructen mate van volwassenheid procesinrichting, de mate van digitalisering en de mate van genomen digitale weerbaarheidsmaatregelen op (cyber) risico's. Door middel van een enquête is data verzameld van 61 mkb-bedrijven in Nederland. Uiteindelijk zijn hiermee tien risico's geïdentificeerd welke correlatie vertonen met de eerdergenoemde constructen. Vervolgens is een raamwerk opgebouwd waarmee inzichtelijk is gemaakt in welke mate de tien risico's worden beïnvloed door de constructen.

Sleutelbegrippen

Cyberrisico's, mkb-bedrijven, risico, procesvolwassenheid, weerbaarheid, digitalisering, maturity model

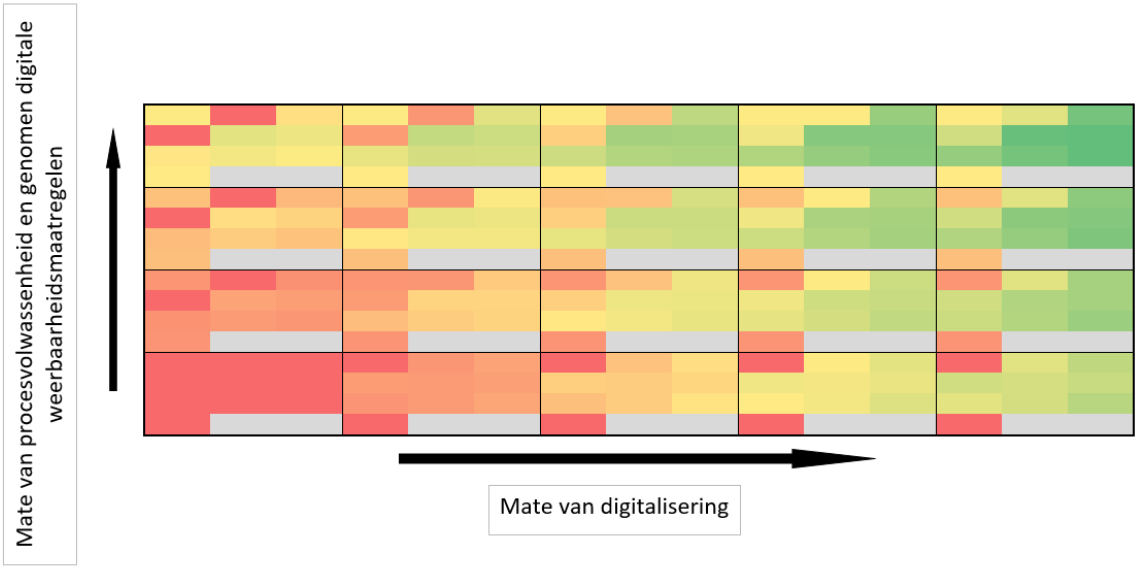
Samenvatting

In het project Cyberweerbaarheid in Limburg van het Platform Veilig Ondernemen (PVO) Limburg en de Brightlands Smart Service Campus wil men ondernemers meer weerbaar maken tegen cybercriminaliteit. Uit onderzoek van PVO Limburg blijkt namelijk dat het bewustzijn rondom cybercriminaliteit zeer beperkt is in mkb-bedrijven, dit terwijl de schade van cybercriminaliteit toeneemt, aanvallen succesvol blijven door ontbreken van basismaatregelen en aanvallen vaker voorkomen en geavanceerder worden. Er is dus sprake van een onjuiste risicoperceptie door deze mkb-bedrijven. Door weerbaarheidsscans te ontwikkelen wil men vanuit het project Cyberweerbaarheid het mkb in Limburg meer bewust en weerbaar maken tegen cybercriminaliteit. Met een weerbaarheidsscan krijgt een ondernemer inzicht in de kritieke punten, risicofactoren en belangrijkste maatregelen met betrekking tot cybercriminaliteit. Niet duidelijk is echter op welke manier de onderdelen van de scan vertaald kunnen worden naar risico's voor de bedrijfsvoering. Eveneens bestaat het vermoeden dat risico's beïnvloed worden door de mate van procesvolwassenheid, de mate van digitalisering en de mate van genomen weerbaarheidsmaatregelen.

Dit onderzoek heeft als doel om een raamwerk te ontwikkelen waarmee de risico's voor de bedrijfsvoering van mkb-bedrijven inzichtelijk kunnen worden gemaakt. Deze risico's worden inzichtelijk gemaakt aan de hand van drie constructen: mate van procesvolwassenheid, mate van digitalisering en mate van genomen digitale weerbaarheidsmaatregelen. Met behulp van een enquête is data verzameld van 61 mkb-bedrijven in Nederland, waarbij is vastgesteld welk niveau van procesvolwassenheid, digitalisering en genomen digitale weerbaarheidsmaatregelen het bedrijf heeft en vervolgens zijn 13 risico-categorieën uitgevraagd of de genoemde categorie van risico voor de bedrijfsvoering van het bedrijf is of niet. Met de resultaten zijn vervolgens correlaties berekend. De mate van procesvolwassenheid en mate van genomen digitale weerbaarheidsmaatregelen vertoont in dit onderzoek een sterke positieve correlatie en is daarom in het model samengenomen. Op basis van de sterkte van correlatie is vervolgens het model ingevuld.

Onderstaand in Figuur 1 is het model opgenomen. Tabel 1 bevat de risico's welke over het model gelegd kunnen worden. De kleurgradatie (rood – groen) geeft aan in hoeverre een risico correlatie vertoont met de genoemde constructen op de X en Y-as. Het ontwikkelde model kan worden gebruikt om op basis van de mate van digitalisering en de mate van procesvolwassenheid en genomen digitale weerbaarheidsmaatregelen te bepalen óf en in welke mate een risico van toepassing kan zijn voor een mkb-bedrijf.

Figuur 1 - Model



Tabel 1 - Risico-mapping

Acties van personen: Per ongeluk	Acties van personen: Opzettelijk	Acties van personen: Inaction
Falen van systemen en technologie: Hardware	Falen van systemen en technologie: Software	Falen van interne processen: Procesontwerp of uitvoer
Falen van interne processen: Procescontrols	Falen van interne processen: Ondersteunende processen	Externe gebeurtenissen: Rampen
Externe gebeurtenissen: Juridische problemen		

Een verdere verdieping zou gemaakt kunnen worden door in plaats van de gebruikte 13 risicocategorieën de onderliggende elementen uit te vragen. Op die manier ontstaat een lijst van 57 elementen welke 13 cyberrisico categorieën invullen. Ook zou een gedetailleerd information security risk assessment kunnen worden uitgevoerd. Eveneens kan als aanbeveling worden opgenomen het onderzoek uit te voeren met een grotere groep mkb-bedrijven om zo meer generaliseerbare resultaten te verkrijgen.

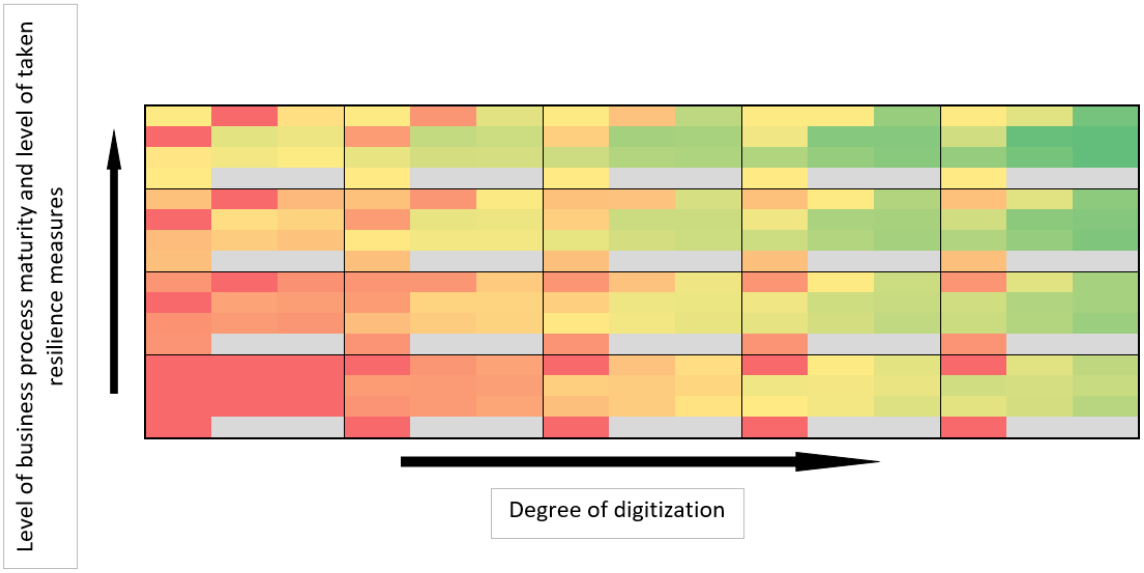
Summary

The project Cyberweerbaarheid (cyberresilience) in Limburg (The Netherlands) started by the PVO Limburg and Brightlands Smart Service Campus has as goal to make SME businesses more resilient against cybercrime. According to research from PVO Limburg, the awareness for cybercrime is very low in SMEs, while the damage from cybercrime increases, attackers keep being successful because lack of basic measures and attacks occur more often and are becoming increasingly more advanced. Therefore, there is an incorrect risk perception by these SMEs. By creating a resilience scan the project Cyberweerbaarheid would like to make SMEs in Limburg more aware and resilient against cybercrime. By using a resilience scan, a SME gains insight in its critical factors, risk factors and most important measures against cybercrime. However, unclear is how these parts of the resilience scan can be translated into business risks. The presumption also arises that business risks are influenced by business process maturity, degree of digitization and resilience measures taken.

This research focusses on the development of a framework that provide insight to SME business risks based on three constructs: business process maturity, degree of digitization and resilience measures taken. By using a survey data was collected from 61 SMEs in The Netherlands. Using the survey, the SMEs level of business process maturity, degree of digitization and level of taken resilience measures was established. Subsequently, 13 risk categories were questioned to establish to what extent the category is a risk for the SME or not. By using the results from the survey correlations were calculated. The level of business process maturity and degree of resilience measures show a strong positive correlation and were therefor taken together as a new construct in the framework. Based on the correlation scores the framework was filled in.

In Figuur 2 below the model is shown. Tabel 2 contains the risks which can be applied as overlay to the model. De colour gradient (red – green) indicates to what extent a risk relates to the mentioned constructs on the X and Y-axis. The developed model can be used to determine whether and to what extent a risk possibly applies to a SME, based on the level of business process maturity and taken resilience measures and the degree of digitization.

Figuur 2 - Model



Tabel 2 - Risk mapping

Actions of People: Inadvertent	Actions of People: Deliberate	Actions of People: Inaction
Systems and Technology Failures: Hardware	Systems and Technology Failures: Software	Failed Internal Processes: Process design or execution
Failed Internal Processes: Process controls	Failed Internal Processes: Supporting processes	External Events: Disasters
External Events: Legal issues		

The framework could be further expanded by extending the 13 risk categories by the underlying elements. In that way a list of 57 elements is created, which fill in 13 cyber risk categories. A detailed information security risk assessment could also be performed. It may also be recommended to carry out the research with a larger group of SMEs to obtain more generalizable results.

Inhoudsopgave

1. Introductie

1.1. Achtergrond

Uit onderzoek (Platform Veilig Ondernemen Limburg & Campus, 2018) blijkt dat het bewustzijn rondom cybercriminaliteit zeer beperkt is, rond de 60% van de ondernemers geeft aan dat het onwaarschijnlijk of niet relevant is slachtoffer te worden van cybercriminaliteit. Er is dus sprake van een onjuiste risicoperceptie door deze mkb-bedrijven.

In het project Cyberweerbaarheid in Limburg van het PVO Limburg en de Brightlands Smart Service Campus wil men deze ondernemers meer weerbaar maken tegen cybercriminaliteit. Onderdeel hiervan is het ontwikkelen van weerbaarheidsscans waarmee het bedrijfsproces en de daarbij ingezette IT-infrastructuur wordt doorgelicht. Op die manier worden kritieke punten, risicofactoren en belangrijkste maatregelen die de ondernemer zou moeten (laten) nemen om meer weerbaar te worden tegen cybercriminaliteit inzichtelijk gemaakt.

Binnen het project is reeds een weerbaarheidsscan opgezet waarbij wordt gekeken naar vier onderdelen: een technische scan, een WiFi-scan, de digitale voetafdruk en een veilige website. Echter is tot op heden onduidelijk op welke manier de onderdelen van de scan vertaald kunnen worden naar (cyber) risico's voor de bedrijfsvoering en op welke manier deze risico's aangepakt kunnen worden. Vanuit de praktijkervaring van het PVO Limburg bestaat een vermoeden dat de risico's voor de bedrijfsvoering ook afhankelijk zijn van de mate van digitalisering binnen een bedrijf en de mate van volwassenheid van de procesinrichting.

Het doel van dit onderzoek is om een wetenschappelijk onderbouwd raamwerk te ontwikkelen waarmee de (cyber) risico's voor de bedrijfsvoering van mkb-bedrijven door onvoldoende genomen digitale weerbaarheidsmaatregelen inzichtelijk gemaakt kunnen worden.

1.2. Gebiedsverkenning

In de inleiding wordt gesproken over cybercriminaliteit, het inzichtelijk maken van de digitale weerbaarheid op basis van een weerbaarheidsscan en (cyber) risico's voor de bedrijfsvoering op basis van de mate van digitalisering en de mate van volwassenheid van procesinrichting.

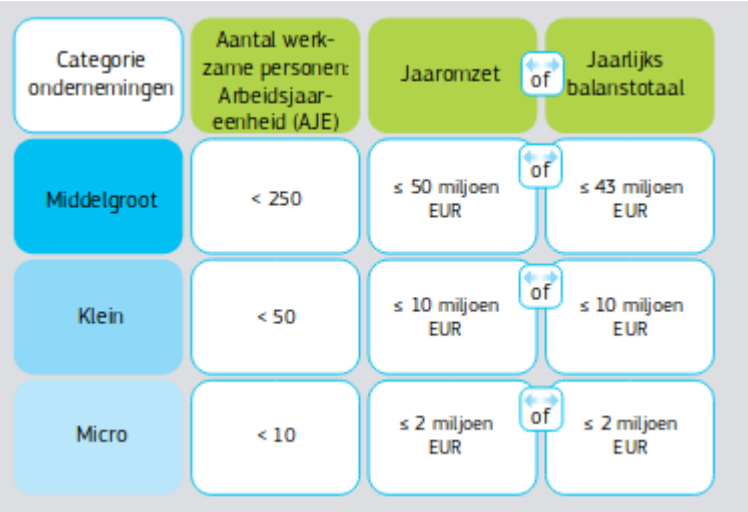
De term cybercriminaliteit, ook wel cybercrime, heeft geen uniforme definitie. De term wordt meestal gebruikt om verschillende vormen van criminaliteit te beschrijven die gericht zijn op computers en andere apparaten of traditionele criminaliteit die gesteund wordt door het gebruik van technologie en internet (Donalds, Kweku-Muata, & Osei-Bryson, 2018). De mate waarin een organisatie een aanval kan voorkomen, detecteren, reageren en herstellen met minimale impact voor de reputatie wordt ook wel digitale weerbaarheid genoemd (Wilding, 2016).

De mate van volwassenheid procesinrichting kan worden vastgesteld aan de hand van een volwassenheidsmodel (Becker, Knackstedt, & Pöppelbuß, 2009) zoals het Business Process Maturity Model (Lee, Lee, & Kang, 2007). De mate van digitalisering wordt ook wel uitgedrukt in het digitaal volwassenheidsniveau (Schwer, Hitz, Wyss, Wirz, & Minonne, 2018; Xu, 2014) waarbij eveneens sprake kan zijn van volwassenheidsmodellen voor het vaststellen van het volwassenheidsniveau (Becker et al., 2009).

Aangezien de focus van dit onderzoek ligt op het midden- en kleinbedrijf (mkb) is het noodzakelijk deze definitie te verduidelijken. Volgens de Nederlandse overheid wordt een onderneming als mkb-

er aangemerkt op basis van drie kenmerken: aantal werknemers, jaaromzet en/of jaarbalans (Rijksdienst voor Ondernemend Nederland, 2004). Aan de grondslag van deze kenmerken ligt de definitie van de Europese Commissie, zoals weergegeven in onderstaand figuur.

Figuur 3 - MKB-toets (Europese Commissie, 2015)



1.3. Probleemstelling

Met het project Cyberweerbaarheid in Limburg wil men het mkb in Limburg meer bewust maken van en weerbaar maken tegen cybercriminaliteit. Onderdeel hiervan is het uitvoeren van zogenaamde weerbaarheidsscans. Hiermee krijgt een ondernemer inzicht in de kritieke punten, risicofactoren en belangrijkste maatregelen met betrekking tot cybercriminaliteit. Niet duidelijk is echter op welke manier de onderdelen van de scan vertaald kunnen worden naar risico's voor de bedrijfsvoering.

Vanuit het project bestaat het vermoeden dat de risico's die een ondernemer loopt bij het niet voldoende nemen van weerbaarheidsmaatregelen beïnvloed worden door de mate van procesvolwassenheid, de mate van digitalisering en de mate van genomen weerbaarheidsmaatregelen. Vanuit de wetenschap is weinig actuele literatuur beschikbaar over de risico's voor de bedrijfsvoering bij het niet voldoende nemen van digitale weerbaarheidsmaatregelen en de invloed van de mate van procesvolwassenheid en mate van digitalisering hierop. Verder onderzoek is dus gewenst.

1.4. Opdrachtformulering

Dit onderzoek heeft als doel om een wetenschappelijk onderbouwd raamwerk te ontwikkelen waarmee de risico's voor de bedrijfsvoering door onvoldoende genomen digitale weerbaarheidsmaatregelen inzichtelijk gemaakt kunnen worden. Hierbij staat de volgende onderzoeksvraag centraal:

Uit welke onderdelen bestaat een raamwerk waarmee een mkb-bedrijf inzichtelijk krijgt welke risico's het loopt voor zijn bedrijfsvoering, vanwege onvoldoende genomen digitale weerbaarheidsmaatregelen?

Binnen het project Cyberweerbaarheid bestaat het vermoeden dat de risico's voor de bedrijfsvoering worden beïnvloed door de mate van procesvolwassenheid, de mate van digitalisering en de mate van genomen weerbaarheidsmaatregelen. Dit leidt tot het opstellen van de volgende

deelvragen welke behandeld worden vanuit het theoretische kader uit vak- en wetenschappelijke literatuur:

1. Op welke manier kan invulling worden gegeven aan de 'mate van volwassenheid procesinrichting' als determinant voor de risico's voor de bedrijfsvoering?
2. Op welke manier kan invulling worden gegeven aan de 'mate van digitalisering' als determinant voor de risico's voor de bedrijfsvoering?
3. Op welke manier kan invulling worden gegeven aan de 'mate van genomen weerbaarheidsmaatregelen' als determinant voor de risico's voor de bedrijfsvoering?
4. Op welke manier kan een raamwerk worden opgesteld waarbij bovenstaande drie variabelen samen met de variabele 'risico's voor de bedrijfsvoering' inzichtelijk kan worden gemaakt?

Vervolgens wordt in het empirische deel van het onderzoek invulling gegeven aan de volgende deelvraag:

5. Hoe kan op basis van het raamwerk invulling worden gegeven aan risico's voor de bedrijfsvoering behorende bij de verschillende niveaus van procesvolwassenheid, digitalisering en genomen weerbaarheidsmaatregelen?

1.5. Motivatie / relevantie

Uit recent onderzoek blijkt dat de financiële impact en daarmee schade van cybercriminaliteit toe neemt (Blythe & Coventry, 2018), dat aanvallen vaker voorkomen en geavanceerder worden (Bailey, Del Miglio, & Richter, 2014), dit in combinatie met het feit dat aanvallers succesvol blijven door het ontbreken van basismaatregelen (NCSC, 2018). Uit eigen onderzoek (Platform Veilig Ondernemen Limburg & Campus, 2018) blijkt daarnaast dat ondernemers zich niet voldoende bewust zijn van de risico's omtrent cybercriminaliteit. Dit terwijl financiële impact en schade toenemen en basismaatregelen uitblijven. Het beter weerbaar maken van ondernemers tegen cybercriminaliteit is dus nodig. Een voorbeeld van een aanval die grote economische en maatschappelijk impact heeft gehad is de WannaCry aanval in 2017. Bij deze aanval zijn computers in 150 landen geïnfecteerd geraakt met een gijzelvirus dat bestanden versleuteld en daarmee ontoegankelijk maakt. Een deel van deze systemen waren de computers in een ziekenhuis in het Verenigd Koninkrijk (NCSC, 2018).

Over de onderdelen van een raamwerk waarmee een mkb-bedrijf inzichtelijk krijgt welke risico's hij loopt voor zijn bedrijfsvoering, vanwege onvoldoende genomen digitale weerbaarheidsmaatregelen is weinig actuele wetenschappelijke literatuur beschikbaar. Eerdere onderzoeken behandelen het onderwerp veelal in de vorm van welke digitale weerbaarheidsmaatregelen er te nemen zijn door bedrijven (Renaud, 2016), methoden om risico te bepalen (Rees, Deane, Rakes, & Baker, 2011) en een raamwerk om een investeringsstrategie te bepalen voor te nemen digitale weerbaarheidsmaatregelen (Fielder, Panaousis, Malacaria, Hankin, & Smeraldi, 2016). In deze onderzoeken zijn de invloed van de mate van digitalisering en de mate van procesvolwassenheid op de risico's voor de bedrijfsvoering niet expliciet opgenomen. Verder onderzoek is dus gewenst.

1.6. Aanpak in hoofdlijnen

In dit onderzoek wordt gebruik gemaakt van de principes van Design Science Research waarbij het ontwikkelen van nieuwe en innovatieve artefacten centraal staan (Hevner, March, Park, & Ram, 2004). Design Science Research maakt een opdeling in drie hoofdonderdelen in het Information Systems Research Framework: Business Needs (relevance), Knowledge Base (rigor) en IS Research. Het onderdeel IS Research omvat het ontwikkelen/ bouwen van theorieën en/of artefacten en het evalueren van deze. Deze opdeling komt in dit onderzoek terug in hoofdstuk 1 (relevance), hoofdstuk 2 (rigor) en hoofdstuk 3 (IS research).

Onderstaand wordt een globale beschrijving per hoofdstuk gegeven:

In hoofdstuk 1 wordt beschreven dat er een praktische relevantie bestaat voor het onderzoek afkomstig uit het project Cyberweerbaarheid in Limburg van het PVO Limburg en de Brightlands Smart Service Campus. Ook wordt beschreven dat de wetenschappelijke relevantie bestaat vanwege weinig actuele wetenschappelijke literatuur over de risico's voor de bedrijfsvoering bij het niet voldoende nemen van digitale weerbaarheidsmaatregelen en de invloed van de mate van procesvolwassenheid en mate van digitalisering hierop.

Hoofdstuk 2 beschrijft het theoretische raamwerk waarbij bestaande kennis uit literatuur wordt gebruikt om een eerste antwoord te kunnen geven op de onderzoeksvragen. Daarmee vormt de kennis opgedaan gedurende het literatuuronderzoek de brug tussen hoofdstuk 1 en hoofdstuk 3.

Hoofdstuk 3 beschrijft de gehanteerde methodologie. Hierbij wordt ingegaan op de gemaakte keuzes met betrekking tot de onderzoeksmethode en validiteit, betrouwbaarheid en ethische aspecten.

Hoofdstuk 4 beschrijft de resultaten van het uitgevoerde onderzoek.

Hoofdstuk 5 sluit het onderzoek met discussie, conclusie en aanbevelingen voor vervolgonderzoek.

2. Theoretisch kader

Het theoretische kader wordt opgebouwd aan de hand van een review van de literatuur. Met behulp van deze review wordt inzicht verkregen in relevante eerder uitgevoerde onderzoeken en trends (Saunders, Lewis, & Thornhill, 2016) en wordt daarmee de basis van dit onderzoek gevormd door de gestelde deelvragen te beantwoorden. Het literatuuronderzoek heeft een deductief karakter, op basis van literatuur worden theorieën gevormd en later verder geoperationaliseerd in het empirisch deel (Saunders et al., 2016).

2.1. Onderzoeksaanpak

Onderstaand wordt de aanpak voor het literatuuronderzoek weergegeven. Het doel van het literatuuronderzoek is kennis verkrijgen voor het beantwoorden van de eerste onderzoeksvragen om vervolgens een conceptueel model op te kunnen bouwen wat gevalideerd gaat worden gedurende het empirische onderzoek. De volgende deelvragen worden beantwoord vanuit de literatuur:

1. Op welke manier kan invulling worden gegeven aan de 'mate van volwassenheid procesinrichting' als determinant voor de risico's voor de bedrijfsvoering?
2. Op welke manier kan invulling worden gegeven aan de 'mate van digitalisering' als determinant voor de risico's voor de bedrijfsvoering?
3. Op welke manier kan invulling worden gegeven aan de 'mate van genomen weerbaarheidsmaatregelen' als determinant voor de risico's voor de bedrijfsvoering?

Per deelvraag zijn zoekquery's opgesteld om relevante wetenschappelijke literatuur te vinden. Voor het opstellen van de zoekquery's zijn *key phrases* opgesteld (Dreher & Dreher, 2011) waarbij aan de hand van de deelvraag een lijst met zoektermen gegenereerd is. De onderstaande zoekquery's zijn gebruikt, weergegeven per deelvraag:

1. TitleCombined:("business process maturity");
   TitleCombined:("process maturity") AND NOT TitleCombined:("business");
   TitleCombined:("process maturity") AND Abstract:(sme);
2. TitleCombined:("digital maturity");

TitleCombined:("degree of digitalisation");
TitleCombined:("digital transformation") AND maturity;

3. TitleCombined:("cyber security maturity");
   TitleCombined:("cyber security capability");
   TitleCombined:("cyber resilience").

Deze zoekquery's zijn vervolgens gebruikt in zoekopdrachten in de universiteitsbibliotheek van de Open Universiteit en Google Scholar. Hierbij zijn de query's zowel in het Engels als in Nederlandse vertaling gezocht. Als voorwaarden aan de gevonden artikelen is gesteld dat het wetenschappelijke literatuur moest zijn, in de vorm van journals (peer-reviewed, non-refereed en professional) en dat deze artikelen in Pdf-formaat te downloaden moesten zijn vanwege gebruik van software Endnote. Vervolgens is voor de systematische selectie van de gevonden onderzoeksliteratuur gebruik gemaakt van de PRISMA methodiek (Moher, Liberati, Tetzlaff, & Altman, 2009).

Vervolgens wordt in de conclusie met de informatie afkomstig uit deelvraag 1, 2 en 3 een voorlopig model opgesteld in deelvraag 4:

4. Op welke manier kan een raamwerk opgezet worden waarbij bovenstaande drie variabelen samen de variabele 'risico's voor bedrijfsvoering' kan worden getoetst?

2.2. Uitvoering

Op basis van de zoekquery's genoemd onder 2.1 zijn zoekopdrachten uitgevoerd. Onderstaand worden de gevonden resultaten weergegeven, opgedeeld per deelvraag.

Deelvraag 1: Op welke manier kan invulling worden gegeven aan de 'mate van volwassenheid procesinrichting' als determinant voor de risico's voor de bedrijfsvoering?

Tabel 3 - PRISMA deelvraag 1

Stappen PRISMA:	**Aantal artikelen:**
Records identified through database searching	95
Additional records identified through other sources	1
Records after duplicates removed	96
Records screened	59
Full-text articles assessed for eligibility	6
Studies included in qualitative synthesis	5

Deelvraag 2: Op welke manier kan invulling worden gegeven aan de 'mate van genomen weerbaarheidsmaatregelen' als determinant voor de risico's voor de bedrijfsvoering?

Tabel 4 - PRISMA deelvraag 2

Stappen PRISMA:	**Aantal artikelen:**
Records identified through database searching	195
Additional records identified through other sources	2
Records after duplicates removed	194
Records screened	39
Full-text articles assessed for eligibility	9
Studies included in qualitative synthesis	6

Deelvraag 3: Op welke manier kan invulling worden gegeven aan de 'mate van genomen weerbaarheidsmaatregelen' als determinant voor de risico's voor de bedrijfsvoering?

Tabel 5 - PRISMA deelvraag 3

Stappen PRISMA:	**Aantal artikelen:**
Records identified through database searching	182
Additional records identified through other sources	2
Records after duplicates removed	182
Records screened	44
Full-text articles assessed for eligibility	7
Studies included in qualitative synthesis	4

2.3. Resultaten en conclusies

Onderstaand worden de deelvragen beantwoord op basis van de gevonden literatuur.

2.3.1. Mate van volwassenheid procesinrichting

De eerste deelvraag heeft betrekking op invulling van mate van volwassenheid procesinrichting. Van belang is te bepalen hoe invulling gegeven kan worden aan het bepalen van de mate van volwassenheid procesinrichting. De mate van volwassenheid kan worden vastgesteld aan de hand van een volwassenheidsmodel (Becker et al., 2009). Het Business Process Maturity Model (BPMM) is een conceptueel model dat de volwassenheid van processen vergelijkt met een bepaalde standaard (Lee et al., 2007). Het BPMM-model lijkt dus een geschikt model om het volwassenheidsniveau van processen te kunnen bepalen. Echter blijkt uit onderzoek (Tarhan, Turetken, & Reijers, 2016) dat ondanks de grote hoeveelheid verschillende BPMM-modellen de validiteit en bruikbaarheid van de modellen gering is. Eveneens stelt dit onderzoek dat er twee verschillende typen BPMM-modellen bestaan: modellen die focussen op het volwassenheidsniveau van business procesmanagement (BPM) en modellen die focussen op het volwassenheidsniveau van processen zelf.

Daar de focus van dit onderzoek ligt in het kunnen toepassen van de volwassenheidsniveaus van BPMM in de context van risico's voor de bedrijfsvoering in relatie tot genomen digitale weerbaarheidsmaatregelen is ervoor gekozen om geen actueel overzicht van de literatuur over BPMM te genereren. Daarentegen wordt een BPMM gekozen die goed aansluit bij de behoefte van dit onderzoek: het bepalen van het volwassenheidsniveau van de processen.

Uit onderzoek naar een overzicht van volwassenheidsmodellen (Röglinger, Pöppelbuß, & Becker, 2012) blijkt dat er 6 modellen bestaan welke zowel gericht zijn op BPM en volwassenheid van processen zelf. Echter zijn niet alle modellen uitgebreid gevalideerd (Tarhan et al., 2016): alleen BPO-MM (McCormack & Johnson, 2001) en BPMM-OMG (Weber, Curtis, & Gardiner, 2008) zijn zowel gevalideerd als gericht op BPM en processen. Opgemerkt moet worden dat BPMM-OMG slechts beperkt is gevalideerd empirisch onderzoek naar de daadwerkelijke toepassing ervan. BPO-MM lijkt daarom het meest geschikt vanwege focus op processen en validatie in onderzoeken.

BPO-MM hanteert vijf volwassenheidsniveau 's voor mate van procesvolwassenheid (Lockamy & McCormack, 2004; McCormack et al., 2009): *ad hoc*, *defined*, *linked*, *integrated* en *extended*. Deze niveaus zullen verderop worden gebruikt bij het opstellen van het conceptueel model.

2.3.2. Mate van digitalisering

De tweede variabele in dit onderzoek is de mate van digitalisering. Van belang is vast te stellen op welke manier er invulling gegeven kan worden aan de mate van digitalisering. Onder de mate van digitalisering wordt verstaan: ' The extent to which a firm accomplishes day-to-day business

activities electronically' (Barua, Konana, Whinston, & Yin, 2004). In recenter onderzoek wordt de mate van digitalisering ook wel omschreven als de *digital transformation* (Xu, 2014).

Onderzoek op het gebied van *digital transformation* is met name aanwezig in de vorm van samenwerking tussen professionele experts en onderzoekscentra (Ivančić, Vukšić, Vesna, & Spremić, 2019). Wel is recent wetenschappelijk onderzoek uitgevoerd waarbij een scenario Industry 4.0 wordt behandeld waarbij meer waarde gecreëerd kan worden door digitalisering (Alejandro, Mendes, Ayala, & Ghezzi, 2019). In het onderzoek (Alejandro et al., 2019) wordt een conceptueel raamwerk voorgesteld voor de convergentie van Industry 4.0 en Servitization waarbij gesproken wordt over drie verschillende niveaus van digitalisering: Low (Manual services), Moderate (Digital services) en High (Industry 4.0 related services). Deze drie niveaus kunnen verder verdiept worden in de vorm van niveaus van *digital maturity*. *Digital maturity* speelt een rol bij het kunnen bepalen van een strategie voor digitalisering en *digital transformation* (Schwer et al., 2018).

Uit onderzoek van (Schwer et al., 2018) zijn 15 modellen voor het vaststellen van *digital maturity* geïdentificeerd. Uit analyse van deze modellen blijkt dat slechts een aantal van deze modellen daadwerkelijk afkomstig is uit gevalideerd wetenschappelijk onderzoek. In dit onderzoek is ervoor gekozen gebruik te maken van het 'Digital Maturity Model' (Valdez-de-Leon, 2016) om de niveaus van *digital maturity* uit te verkrijgen. Dit vanwege de uitgebreide operationalisering van de variabelen in de vorm van interviewvragen.

De volgende vijf niveaus van *digital maturity* (Valdez-de-Leon, 2016) worden in dit onderzoek gebruikt: *initiating, enabling, integrating, optimizing en pioneering*. Deze niveaus zullen verderop worden gebruikt bij het opstellen van het conceptueel model.

2.3.3. Mate van genomen digitale weerbaarheidsmaatregelen

De derde variabele in dit onderzoek is de mate van genomen digitale weerbaarheidsmaatregelen. Ook hier is het van belang te bepalen op welke manier invulling gegeven kan worden aan dit begrip. Als basis hiervoor dient de Scan Digitaal Veilig Ondernemen (ROC Friese Poort, Stichting Cyber Safety Noord Nederland, & Digital Trust Centrum, 2018) welke bestaat uit 4 categorieën: een technische scan, Wifi-scan, Digitale voetafdruk en veilige website. Per categorie zijn vragen opgenomen om deze te operationaliseren en uiteindelijk per categorie een antwoord te geven in de vorm van Ja/Nee op de stellingen. Onderstaand is in Figuur 4 een voorbeeld opgenomen van de stellingen voor het onderdeel 'Technische scan'.

Figuur 4 - Voorbeeld stellingen 'Technische scan' met Ja/Nee antwoorden (ROC Friese Poort et al., 2018)

Samenvatting:

Stelling	*Ja/ Nee*	*Aanbeveling*	*Verwijzing*
1 Het bedrijf gaat veilig met back-ups om			
2 Het bedrijf gaat veilig met smartphones en tablets om			
3 Het bedrijf voorkomt malware			
4 Het bedrijf voorkomt phishing en fraude			
5 Het bedrijf gebruikt wachtwoorden om data te beschermen			

Opmerking bij invullen: de samenvatting invullen nadat onderstaande thema`s zijn ingevuld.

Onduidelijk is echter welk volwassenheidsniveau van digitale weerbaarheid gekoppeld kan worden aan antwoorden op de stellingen. Een verdere verdieping van digitale weerbaarheid en volwassenheidsniveaus is daarmee noodzakelijk.

Digitale weerbaarheid kan omschreven worden als de mogelijkheid die een organisatie heeft om een aanval te mitigeren in vijf categorieën: *Identify*, *Protect*, *Detect*, *Respond* en *Recover* (Wilding, 2016) (National Institute of Standards and Technology, 2018). Als hulpmiddel om daadwerkelijk te kunnen toetsen in welke mate een organisatie voldoet aan de invulling van deze categorieën bestaan er cyber security volwassenheidsmodellen (Bilge, Yildirim, & Baykal, 2016) (Miron & Muita, 2014). Een analyse (Le & Hoang, 2016) toont aan dat er 12 verschillende cyber security volwassenheidsmodellen geïdentificeerd kunnen worden. Het raamwerk van IBM (Buecker, Borrett, Lorenz, & Powers, 2010) lijkt het meest toepasbaar voor dit onderzoek vanwege de nadruk op het uitvoeren van een *security gap analysis* en daarmee de praktische toepasbaarheid voor dit onderzoek. De overige genoemde onderzoeken (Le & Hoang, 2016) leggen met name de nadruk op specifieke onderwerpen in plaats van het bepalen van een algeheel weerbaarheidsniveau of zijn van toepassing op sectoren anders waar voor dit onderzoek de nadruk ligt.

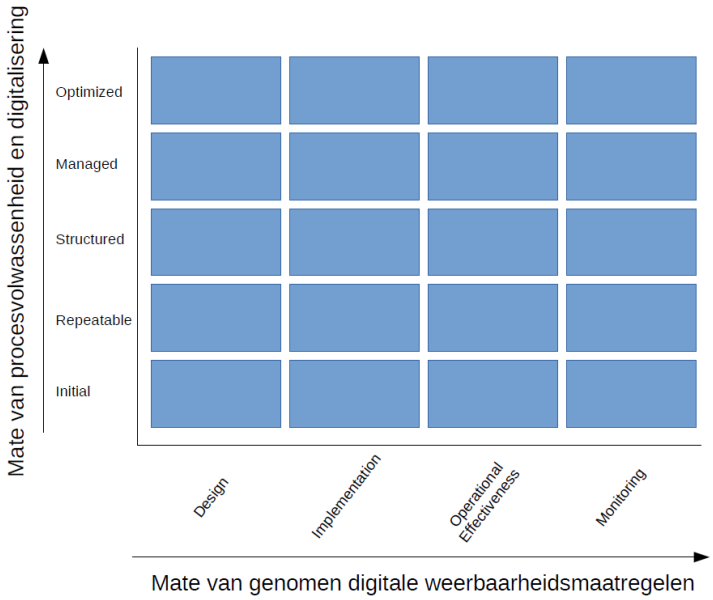
Uit een andere analyse (Spruit & Roeling, 2014) blijkt dat het raamwerk van IBM echter niet volledig is doordat niet alle deelgebieden van information security worden behandeld. Eveneens ontbreekt een duidelijke operationalisering van de weerbaarheidsniveaus wat het vaststellen van deze niveaus bemoeilijkt (Le & Hoang, 2016). Daar de focus van dit onderzoek ligt in het daadwerkelijk vaststellen van een weerbaarheidsniveau lijkt het ISFAM-model (Roeling, 2010; Spruit & Roeling, 2014) vanwege de opgenomen operationaliseringen dan ook het meest toepasbaar.

De volgende vier niveaus (Roeling, 2010; Spruit & Roeling, 2014) van mate van genomen digitale weerbaarheidsmaatregelen worden in dit onderzoek gebruikt *Design, Implementation, Operational Effectiveness en Monitoring*. Deze niveaus zullen hierna worden gebruikt bij het opstellen van het conceptueel model.

2.3.4. Conclusies

Voor het vaststellen van zowel mate van procesvolwassenheid, mate van digitalisering en mate van genomen digitale weerbaarheidsmaatregelen bestaan volwassenheidsmodellen. Uit het literatuuronderzoek zijn drie modellen geselecteerd welke gebruikt worden om invulling te geven aan de genoemde variabelen. Op basis van de geselecteerde modellen uit voorgaande literatuuronderzoek wordt het voorlopig conceptueel model voorgesteld, zoals weergegeven in Figuur 5. Hierbij is gebruik gemaakt van de mate van procesvolwassenheid (McCormack et al., 2009), mate van digitalisering (Valdez-de-Leon, 2016) en mate van genomen digitale weerbaarheidsmaatregelen (Roeling, 2010; Spruit & Roeling, 2014). Vanwege de overeenkomsten in deelgebieden van mate van procesvolwassenheid en mate van digitalisering zijn de twee variabelen samengenomen in het voorlopig conceptuele model. Gekozen is om voor deze samengenomen variabelen de vijf niveaus *Initial, Repeatable, Defined, Managed* en *Optimized* afkomstig uit het Capability Maturity Model (Humphrey, 1988) toe te kennen.

Figuur 5 - Voorlopig conceptueel model



In bovenstaand model kunnen vervolgens (cyber) risico's voor de bedrijfsvoering worden ingevuld bij de vierkanten. Risico's voor de bedrijfsvoering kunnen worden gedefinieerd als de kans op een bepaalde gebeurtenis die schade veroorzaakt x de omvang van de schade (Kaplan & Garrick, 1981) (Böhme, Laube, & Riek, 2018) waarbij risico's ontstaan omtrent beschikbaarheid, vertrouwelijkheid en integriteit van informatie (Wangen, Hallstensen, & Snekkenes, 2017). Deze risico's kunnen in kaart worden gebracht door middel van een risk assessment (ISO/IEC, 2018). Om een dergelijk assessment zo volledig mogelijk uit te kunnen voeren kan gebruik worden gemaakt van een zogenaamde taxonomie (Lindqvist & Jonsson, 1997) waarvan er verschillenden bestaan (Chanchala, Kumar, & Tarey, 2015). De taxonomie voor operationele cyber security risico's (Cebula & Young, 2010) lijkt het meest toepasbaar voor dit onderzoek vanwege de focus op het identificeren en organiseren van bronnen van operationele cyber security risico's. In dit onderzoek (Cebula & Young, 2010) zijn de risico's opgedeeld in vier hoofdklassen: Acties van personen, fouten in systemen en technologie, falen van interne processen en externe gebeurtenissen. Iedere hoofdklasse wordt beschreven door subklassen met elementen. Op deze manier ontstaat een lijst van 57 elementen als cyberrisico's.

In het empirisch onderzoek kunnen deze 57 elementen als van toepassing zijnde (cyber) risico's voor de bedrijfsvoering bij een bepaald niveau van procesvolwassenheid en digitalisering en mate van genomen digitale weerbaarheidsmaatregelen worden ingevuld in het conceptueel model.

2.4. Doel van het vervolgonderzoek

In het empirische deel van het onderzoek wordt invulling gegeven aan welke risico's voor de bedrijfsvoering bestaan bij een bepaald niveau van genomen weerbaarheidsmaatregelen, procesvolwassenheid en mate van digitalisering. Op basis van deze risico's kan vervolgens het raamwerk verder worden ingevuld waarmee het onderzoeksdoel, het opstellen van een raamwerk waarmee wetenschappelijk onderbouwd de risico's voor de bedrijfsvoering van mkb-bedrijven, bij het niet voldoende nemen van weerbaarheidsmaatregelen afkomstig uit de scan, kan worden ingevuld.

3. Methodologie

In dit onderzoek worden de principes van Design Science Research (Hevner et al., 2004) toegepast. Waar in voorgaande hoofdstukken zowel praktische- als wetenschappelijke informatie is verkregen voor het opstellen van een conceptueel model worden de risico's ingevuld vanuit het empirisch onderzoek. Voor het empirisch onderzoek staat de deelvraag 'Hoe kan op basis van het raamwerk invulling worden gegeven aan risico's voor de bedrijfsvoering behorende bij de verschillende niveaus van procesvolwassenheid, digitalisering en genomen weerbaarheidsmaatregelen?' centraal. Dit hoofdstuk beschrijft de onderzoeksopzet van dit empirisch onderzoek.

3.1. Conceptueel ontwerp: keuze van onderzoeksmethode(n)

Om invulling te kunnen geven aan welke risico's voor de bedrijfsvoering bestaan bij een bepaald niveau van genomen weerbaarheidsmaatregelen, procesvolwassenheid en mate van digitalisering is het noodzakelijk informatie te verzamelen binnen de doelgroep van mkb-bedrijven. (Edmondson & McManus, 2007) geven aan dat gegeven de mate van volwassenheid van eerder onderzoek in de verschillende gebieden die als constructen worden gebruikt in het conceptueel model het verzamelen van data mogelijk door middel van een survey. Een dergelijke onderbouwing voor een survey kan ook worden gevonden in het verklarende karakter van de onderzoeksvraag (Wohlin, Höst, & Regnell, 2012). Een survey kan uitgevoerd worden op drie manieren: enquête, gestructureerde observatie en gestructureerde interviews (Saunders et al., 2016). Om op gestandaardiseerde manier gegevens te verzamelen van mkb-bedrijven is gekozen dit te doen op basis van een enquête. Het gebruiken van een enquête heeft twee voordelen (Saunders et al., 2016): 1. Er kan een grotere groep mkb-bedrijven benaderd worden; 2. De gegevens zijn eenvoudiger te analyseren met behulp van statistische programmatuur.

Een nadeel van deze gekozen methode is dat verkregen data uit de survey minder breed is ten opzichte van data verkregen bij andere onderzoeksstrategieën, omdat er een limiet gesteld moet worden aan hoeveel vragen er gesteld kunnen worden aan de respondenten (Saunders et al., 2016). Bij het opstellen van de enquêtes is hiermee rekening gehouden door het aantal vragen te beperken en door specifieke risico's uit te vragen in plaats van open vragen. Verderop worden deze keuzes onderbouwd.

3.2. Technisch ontwerp: uitwerking van de methode

Een eerste versie van de enquête is opgezet op basis van 12 vragen voor mate van procesvolwassenheid (McCormack & Johnson, 2001) met bijbehoren Likertschaal, 131 vragen voor mate van digitalisering (Valdez-de-Leon, 2016) in de vorm van Ja/Nee stellingen en 161 vragen voor mate van genomen digitale weerbaarheidsmaatregelen (Roeling, 2010) ook in de vorm van Ja/Nee stellingen. Ter verificatie van de geënquêteerde, behoort deze daadwerkelijk tot de doelgroep van mkb-bedrijven, is een vraag opgenomen om te bepalen in welke categorie (CBS, 2019) en sector (CBS, 2020) op basis van de top 5 sectoren de ondernemer behoort. Vervolgens zijn aan de enquête de 57 elementen van cyberrisico's (Cebula & Young, 2010) toegevoegd waarbij een Likertschaal toegevoegd is om op schaal van 1 tot 5 te kunnen beoordelen in hoeverre een cyberrisico voor een mkb-bedrijf van toepassing is.

Om deze eerste versie van de enquête op haalbaarheid te toetsen is deze telefonisch met één mkb-bedrijf doorgenomen waarbij de enquêtevragen op het scherm werden gedeeld (via Microsoft Teams). Doel van deze eerste pilottest was het vaststellen van mogelijke probleempunten voordat de enquête wordt verspreid naar een groter aantal mkb-bedrijven. Uit deze eerste toets bleek dat de enquête in bovengenoemde vorm te lang was om digitaal of telefonisch af te nemen. In een

tijdsperiode van 1 uur was het mogelijk 36 van de 361 vragen te behandelen. Ook bleek de specifieke terminologie uit de volwassenheidsmodellen soms lastig te begrijpen voor de geënquêteerde.

Vervolgens is een nieuwe versie van de enquête opgesteld waarbij gekozen is om de niveaus van procesvolwassenheid, mate van digitalisering en digitale weerbaarheid uit te vragen in een samengevatte vorm. Een zelfde aanpak is gebruikt in een eerder onderzoek (Aberle & Henkel, 2017) waarbij onderzocht is of een maturity model uitgevraagd kan worden met minder detaillering Deze samengevatte volwassenheidsmodellen zijn opgenomen in bijlage 7.2. Met behulp van de niveaus zijn vragen opgesteld in de vorm van *category questions* (Saunders et al., 2016) waarbij de respondent kiest uit het voor de organisatie het meest van toepassing zijnde niveau van procesvolwassenheid, mate van digitalisering en digitale weerbaarheid. Om de enquête verder in te korten is gekozen om de cyberrisico's uit te vragen op het niveau van subcategorie waar per categorie de elementen zijn samengevat. De samengevatte categorieën zijn opgenomen in bijlage 7.1. In de nieuwe enquête zijn drie vragen opgenomen voor procesvolwassenheid, mate van digitalisering en digitale weerbaarheid, vijf vragen voor cyberrisico's en twee vragen voor vaststelling mkb-bedrijf en sector. De volledige enquête is opgenomen in bijlage 7.3. De enquête is opgezet met behulp van een onlineprogramma, Easion.

Om de haalbaarheid van deze tweede versie van de enquête te toetsen is wederom een pilottest opgezet. Deze versie van de enquête is verspreid via LinkedIn met een uitnodiging tot deelname. Door deze werkwijze van self-selection sampling (Saunders et al., 2016) zijn in totaal 1201 mogelijke respondenten bereikt en totaal 33 enquêtes ingevuld in de periode van 12-07-2020 tot 12-08-2020. Van deze 33 enquêtes zijn 5 geheel ingevuld. Uit reacties en deels ingevulde enquêtes bleek dat het lastig was een inschatting te geven van risico's door respondenten welke in mindere mate op de hoogte zijn van risico's (bijvoorbeeld een specifieke respondent die een ZZP mkb-bedrijf heeft).

Vervolgens is een derde versie van de enquête opgesteld waarbij specifiek gericht wordt op rollen/ personen binnen mkb-bedrijven waarvan verondersteld wordt dat deze personen beter in staat zijn een inschatting kunnen geven van risico's binnen de organisatie. Deze derde versie is opgesteld in een onlineprogramma, LimeSurvey en vervolgens verzonden naar directieleden, CEO's, ISO's en risk officers via een uitnodiging op LinkedIn en e-mail door gebruik te maken van eigen connecties en connecties van connecties (convenience sampling en snowball sampling (Saunders et al., 2016)). De gebruikte enquete komt overeen met de enquête zoals opgenomen in bijlage 7.3, alleen zijn de vragen voor vaststelling mkb-bedrijf en sector verwijderd aangezien dit al bekend was bij het aanschrijven van de respondent. Hierbij zijn in totaal 135 personen aangeschreven met een persoonlijke uitnodiging om de enquête in te vullen. In totaal zijn gedurende de periode 09-11-2020 en 07-12-2020 61 enquêtes ingevuld.

De resultaten zijn vervolgens geanonimiseerd opgeslagen voor verdere analyse.

3.3. Gegevensanalyse

Kwantitatieve data, zoals verkregen uit de enquête, moet verder verwerkt worden met kwalitatieve technieken voordat deze nuttig gebruikt kan worden (Saunders et al., 2016). Allereerst is de data ingeladen in SPSS en zijn 14 rijen met ontbrekende data verwijderd. Vervolgens zijn de variabelen omgezet van tekst (afkomstig uit LimeSurvey) naar een ordinale waarde. Deze omgezette variabelen zijn toegevoegd als nieuwe variabele met toevoeging "_RECODE" als naam (bijvoorbeeld PV_RECODE voor procesvolwassenheid). De volgende variabelen zijn gecodeerd:

- PV_RECODE: Mate van procesvolwassenheid;

- DS_RECODE: Mate van digitalisering;
- DW_RECODE: Mate van genomen digitale weerbaarheidsmaatregelen;

Eveneens zijn de variabelen voor de risico's gecodeerd:

- RC1001_RECODE: Acties van personen: per ongeluk;
- RC1002_RECODE: Acties van personen: opzettelijk;
- RC1003_RECODE: Acties van personen: inaction;
- RC2001_RECODE: Falen van systemen en technologie: hardware;
- RC2002_RECODE: Falen van systemen en technologie: software;
- RC2003_RECODE: Falen van systemen en technologie: systemen;
- RC3001_RECODE: Falen van interne processen: procesontwerp of uitvoer;
- RC3002_RECODE: Falen van interne processen: procescontrols;
- RC3003_RECODE: Falen van interne processen: ondersteunende processen;
- RC4001_RECODE: Externe gebeurtenissen: rampen;
- RC4002_RECODE: Externe gebeurtenissen: juridische kwesties;
- RC4003_RECODE: Externe gebeurtenissen: Bedrijfsproblemen;
- RC4004_RECODE: Externe gebeurtenissen: Afhankelijkheid van diensten.

Vervolgens is op basis van het conceptueel model getoetst in welke mate de variabelen mate van procesvolwassenheid en mate van digitalisering samengenomen kunnen worden. Hierbij is gekeken naar de Cronbach's alpha en gezien het ordinale niveau van deze variabelen (non-parametrisch) en de daarmee ontbrekende normale verdeling (bijlage 7.4) is gebruik gemaakt van Spearman's rank correlation coëfficiënt (Wohlin et al., 2012) waarbij een verband wordt gemeten tussen -1 en +1 (Agresti & Finlay, 2009) (Saunders et al., 2016). Bij een sterke mate van samenhang kan vervolgens met behulp van een Principal Component Analysis (PCA) een samengestelde factor worden bepaald (Prokop, 2011). Deze is opgeslagen in variabele 'FAC1_1'.

Met behulp van Spearman's rank correlation coëfficiënt zijn vervolgens coëfficiënten uitgerekend op basis van de 13 risico's en de variabelen. De coëfficiënten zijn vervolgens gebruikt om het conceptueel model in te vullen met behulp van de risico's.

3.4. Reflectie t.a.v. validiteit, betrouwbaarheid en ethische aspecten

Onderstaand wordt een reflectie gegeven op welke manier met validiteit, betrouwbaarheid en ethische aspecten is omgegaan in dit onderzoek.

Interne validiteit

Om de interne validiteit te kunnen vergroten is de eerste versie van de opgestelde enquête getoetst met één mkb-bedrijf. Deze eerste versie van de enquête bevatte de volledige lijst met geoperationaliseerde variabelen bestaande uit in totaal 361 vragen. Uit deze toets bleek dat de enquête te lang was om digitaal of telefonisch af te nemen. Vervolgens is een verkorte versie opgesteld waarbij de variabelen samengevat zijn op hun volwassenheidsniveaus. Eenzelfde aanpak is gehanteerd in een onderzoek (Aberle & Henkel, 2017) waaruit opgemaakt kan worden dan een verkorte versie van een volwassenheidsmodel gebruikt kan worden voor het vaststellen van een volwassenheidsniveau.

Externe validiteit

Voor de generaliseerbaarheid van dit onderzoek is het noodzakelijk om verschillende mkb-bedrijven te onderzoeken. Zoals in de inleiding aangegeven is er sprake van een onjuiste risicoperceptie bij circa 60% van de mkb-bedrijven. Dit kan in het onderzoek eveneens de resultaten beïnvloeden. Met deze beperking is rekening gehouden door een lijst met risico's aan te leveren en bij de keuze van respondenten rekening te houden met de achtergrond en functie van de respondent. Een andere beperking in de externe validiteit is dat door middel van *convenience sampling* met name connecties uit de kring van de onderzoeker zijn bevraagd. Mogelijk worden op deze manier mkb-bedrijven bevraagd die een hogere mate van risicoperceptie hebben en daarmee bepaalde risico's uitsluiten.

Betrouwbaarheid

Ten aanzien van de betrouwbaarheid van het onderzoek is gekozen om de enquêtevragen op te nemen in de bijlage. Eveneens zijn waar mogelijk de diagrammen afkomstig uit SPSS opgenomen in de bijlagen.

Ethische aspecten

Aangezien mkb-bedrijven in dit onderzoek informatie geven over de staat van hun digitale weerbaarheidsniveau worden gegevens geanonimiseerd waardoor resultaten niet herleidbaar zijn naar welk mkb-bedrijf welk digitaal weerbaarheidsniveau heeft.

4. Resultaten

Het empirische deel van het onderzoek heeft als doel invulling te geven aan welke risico's voor de bedrijfsvoering bestaan bij een bepaald niveau van genomen weerbaarheidsmaatregelen, procesvolwassenheid en mate van digitalisering. Het uiteindelijke doel is om de risico's in te vullen in het raamwerk. Allereest wordt er een validatie uitgevoerd van het conceptuele model waarbij de op basis van overeenkomende deelgebieden samengenomen variabelen (mate van procesvolwassenheid en mate van digitalisering) wordt gevalideerd op basis van de data. Vervolgens wordt bepaald welke risicofactoren bestaan op basis van de variabelen. Tot slot wordt het nieuwe model voorgesteld.

4.1. Validatie conceptueel model

Voorgesteld vanuit de overeenkomsten in deelgebieden is het samennemen van de variabelen mate van procesvolwassenheid en mate van digitalisering. Om te valideren of deze overeenkomst eveneens blijkt uit de data is er een analyse uitgevoerd op basis van Cronbach's alpha (Saunders et al., 2016) en Spearman's rho (Wohlin et al., 2012). In Tabel 6 zijn de waardes voor Cronbach's alpha per samengenomen variabelen opgenomen. Een waarde voor Cronbach's alpha groter dan 0.7 geeft aan dat de vragen hetzelfde construct meten (Saunders et al., 2016).Tabel 6 - Cronbach's alpha

Tabel 6 - Cronbach's alpha

Variabelen:	**Cronbach's alpha:**
Procesvolwassenheid en digitalisering	0.453
Procesvolwassenheid en digitale weerbaarheidsmaatregelen	0.741
Digitalisering en digitale weerbaarheidsmaatregelen	0.563

Op basis van Cronbach's alpha groter dan 0.7 kan worden aangenomen dat de variabelen mate van procesvolwassenheid en mate van genomen digitale weerbaarheidsmaatregelen hetzelfde construct

meten. Het eerder in het conceptueel model voorgestelde verband tussen mate van procesvolwassenheid en mate van digitalisering heeft een lagere samenhang (.453).

Eveneens kan op basis van Spearman's rho een verband worden aangetoond. De correlatiecoëfficiënt wordt weergegeven op een schaal van -1 (perfecte negatieve correlatie) tot 1 (perfecte positieve correlatie) (Saunders et al., 2016). In Tabel 7 worden de correlaties en bijbehorende significantieniveaus weergegeven. Een significantieniveau groter dan 0.05 wordt beschouwd als niet statistisch significant (Saunders et al., 2016).

Tabel 7 - Spearman's rho

Variabelen	**Spearman's rho**	**Significantie**
Procesvolwassenheid en digitalisering	0.316	0.030
Procesvolwassenheid en digitale weerbaarheidsmaatregelen	0.628	0.007
Digitalisering en digitale weerbaarheidsmaatregelen	0.390	0.007

Op basis van een correlatiecoëfficiënt kan worden geconcludeerd dat er een statistisch significante sterk positieve correlatie bestaat tussen mate van procesvolwassenheid en mate van genomen digitale weerbaarheidsmaatregelen (r = .628, p = 0.007). En dergelijk sterk positief verband lijkt niet te bestaan tussen procesvolwassenheid en digitalisering (r = .316, p = 0.030) en digitalisering en digitale weerbaarheidsmaatregelen (r = .390, p = 0.007).

Op basis van zowel de waarden voor Cronbach's alpha als Spearman's rho voor de mate van procesvolwassenheid en de mate van genomen digitale weerbaarheidsmaatregelen welke een samenhang suggereren is een nieuwe variabele opgesteld waarbij de mate van procesvolwassenheid en de mate van genomen digitale weerbaarheidsmaatregelen samen zijn genomen. Deze variabele is opgesteld door middel van een Principal Component Analysis (Prokop, 2011), waarbij met de nieuwe variabele in totaal 79.468% van de variantie in mate van procesvolwassenheid en mate van digitalisering kan worden verklaard. Het streven naar een zo hoog mogelijke waarde in de verklarende variantie is gewenst (Larose, 2006), daarbij leidt het toevoegen van een aanvullende factor weliswaar tot een verklarende variantie van 100%, maar niet tot een samenvoeging van de mate van procesvolwassenheid en de mate van genomen digitale weerbaarheidsmaatregelen in één nieuwe variabele. De verklarende waarde van 79.468% van de nieuwe variabele wordt dus geaccepteerd.

4.2. Bepalen correlaties

Na validatie van het conceptueel model en het voorstellen van een nieuwe variabele waarmee de mate van procesvolwassenheid en mate van genomen digitale weerbaarheidsmaatregelen worden samengenomen in één factor zijn vervolgens de verbanden tussen deze nieuwe variabele, de dertien risico's (Cebula & Young, 2010) en mate van digitalisering onderzocht. Met behulp van Spearman's rank correlation coëfficiënt zijn coëfficiënten uitgerekend op basis van de dertien risico's en de variabelen. Onderstaand wordt per risico uitgewerkt in welke mate de variabelen met het genoemde risico correleren en met welke mate van significantie. Hierbij is gekeken naar correlatiecoëfficiënten met een significantieniveau van < .05 en < .001. Een significantieniveau > .05 wordt immers

beschouwd als niet statistisch significant (Saunders et al., 2016). De coëfficiënten zijn in tabelvorm opgenomen in bijlage 7.5.

Risico 1 - Acties van personen: Perongeluk

De risicoklasse Acties van personen: Perongeluk heeft een statistisch significant gemiddeld negatieve relatie met de mate van procesvolwassenheid en genomen digitale weerbaarheidsmaatregelen (r = -.342, p = .017). Er bestaat geen statistisch significante relatie met de mate van digitalisering.

Risico 2 – Acties van personen: Opzettelijk

De risicoklasse Acties van personen: Opzettelijk heeft een statistisch significant gemiddeld negatieve relatie met de mate van digitalisering (r = -.346, p = .017). Er bestaat geen statistisch significante relatie met de mate van procesvolwassenheid en genomen digitale weerbaarheidsmaatregelen.

Risico 3 – Acties van personen: Inaction

De risicoklasse Acties van personen: Inaction heeft een statistisch significant gemiddeld negatieve relatie met de mate van digitalisering (r = -.451, p = .001). Eveneens bestaat er een statistisch significant zwak negatieve relatie met de mate van procesvolwassenheid en mate van genomen digitale weerbaarheidsmaatregelen (r = -.307, p = .036).

Risico 4 – Falen van systemen en technologie: Hardware

De risicoklasse Falen van systemen en technologie: Hardware heeft een statistisch significant gemiddeld negatieve relatie met de mate van digitalisering (r = -.397, p = .006). Er bestaat geen statistisch significante relatie met de mate van procesvolwassenheid en genomen digitale weerbaarheidsmaatregelen.

Risico 5 – Falen van systemen en technologie: Software

De risicoklasse Falen van systemen en technologie: Software heeft een statistisch significant gemiddeld negatieve relatie met de mate van procesvolwassenheid en genomen digitale weerbaarheidsmaatregelen (r = -.451, p = .001). Eveneens bestaat er een statistisch significant gemiddeld negatieve relatie met de mate van digitalisering en mate van genomen digitale weerbaarheidsmaatregelen (r = -.384, p = .008).

Risico 6 – Falen van systemen en technologie: Systemen

De risicoklasse Falen van systemen en technologie: Systemen heeft geen statistisch significante relaties met de mate van digitalisering en de mate van procesvolwassenheid en genomen digitale weerbaarheidsmaatregelen.

Risico 7 – Falen van interne processen: Procesontwerp of uitvoer

De risicoklasse Falen van interne processen: Procesontwerp of uitvoer heeft een statistisch significant gemiddeld negatieve relatie met de mate van digitalisering (r = -.424, p = .003). Eveneens bestaat er een statistisch significant gemiddeld negatieve relatie met de mate van procesvolwassenheid en mate van genomen digitale weerbaarheidsmaatregelen (r = -.411, p = .004).

Risico 8 – Falen van interne processen: Procescontrols

De risicoklasse Falen van interne processen: Procescontrols heeft een statistisch significant zwak negatieve relatie met de mate van digitalisering (r = -.335, p = .021). Eveneens bestaat er een

statistisch significant zwak negatieve relatie met de mate van procesvolwassenheid en mate van genomen digitale weerbaarheidsmaatregelen (r = -.322, p = .027).

Risico 9 – Falen van interne processen: Ondersteunende processen

De risicoklasse Falen van interne processen: Ondersteunende processen heeft een statistisch significant gemiddeld negatieve relatie met de mate van digitalisering (r = -.387, p = .007). Eveneens bestaat er een statistisch significant gemiddeld negatieve relatie met de mate van procesvolwassenheid en mate van genomen digitale weerbaarheidsmaatregelen (r = -.387, p = .007).

Risico 10 – Externe gebeurtenissen: Rampen

De risicoklasse Externe gebeurtenissen: Rampen heeft een statistisch significant gemiddeld negatieve relatie met de mate van digitalisering (r = -.474, p = .001). Eveneens bestaat er een statistisch significant gemiddeld negatieve relatie met de mate van procesvolwassenheid en mate van genomen digitale weerbaarheidsmaatregelen (r = -.351, p = .016).

Risico 11 – Externe gebeurtenissen: Juridische problemen

De risicoklasse Externe gebeurtenissen: Juridische problemen heeft een statistisch significant zwak negatieve relatie met de mate van procesvolwassenheid en genomen digitale weerbaarheidsmaatregelen (r = -.336, p = .021). Er bestaat geen statistisch significante relatie met de mate van digitalisering.

Risico 12 – Externe gebeurtenissen: Bedrijfsproblemen

De risicoklasse Externe gebeurtenissen: Bedrijfsproblemen heeft geen statistisch significante relaties met de mate van digitalisering en de mate van procesvolwassenheid en genomen digitale weerbaarheidsmaatregelen.

Risico 13 – Externe gebeurtenissen: Afhankelijkheid van diensten

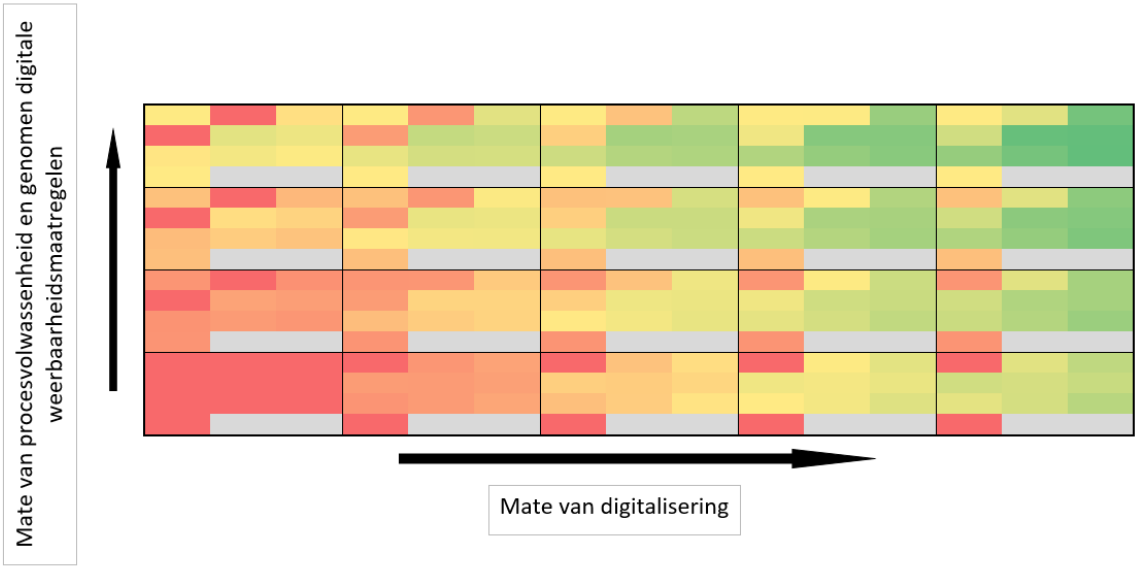
De risicoklasse Externe gebeurtenissen: Afhankelijkheid van diensten heeft geen statistisch significante relaties met de mate van digitalisering en de mate van procesvolwassenheid en genomen digitale weerbaarheidsmaatregelen.

4.3. Invulling conceptueel model

Met behulp van bovenstaande correlatiecoëfficiënten kunnen de 13 risico's worden teruggebracht naar 10 risico's welke verbanden vertonen met de mate van digitalisering en de mate van procesvolwassenheid en genomen digitale weerbaarheidsmaatregelen. Vervolgens kan het conceptueel model worden ingevuld met de 10 risico's en assen. Hierbij is gekozen om de correlatiecoëfficiënt de kleurgradatie van het risico te laten bepalen om op deze manier een overzicht te maken op welke manier de variabelen mate van digitalisering en mate van procesvolwassenheid en genomen digitale weerbaarheidsmaatregelen correleren met de 10 geïdentificeerde risico's.

Onderstaand in Figuur 6 is het model opgenomen. Op basis van de kleurgradaties kan worden waargenomen op welke manier een risico correleert met variabelen op de X en Y-as. De mapping in Tabel 8 kan worden gebruikt om een risico te koppelen aan een bepaalde kleur.

Figuur 6 - Model met risico's en coëfficiënten



Tabel 8 - Mapping risico's

Acties van personen: Per ongeluk	Acties van personen: Opzettelijk	Acties van personen: Inaction
Falen van systemen en technologie: Hardware	Falen van systemen en technologie: Software	Falen van interne processen: Procesontwerp of uitvoer
Falen van interne processen: Procescontrols	Falen van interne processen: Ondersteunende processen	Externe gebeurtenissen: Rampen
Externe gebeurtenissen: Juridische problemen		

5. Discussie, conclusies en aanbevelingen

5.1. Discussie

Het doel van dit onderzoek was om een raamwerk op te stellen waarmee wetenschappelijk onderbouwd de risico's voor de bedrijfsvoering van mkb-bedrijven inzichtelijk gemaakt kan worden. Vanuit het PVO Limburg bestond een vermoeden dat de risico's voor de bedrijfsvoering ook afhankelijk zijn van de mate van digitalisering binnen een bedrijf en de mate van volwassenheid van de procesinrichting naast de mate van genomen digitale weerbaarheidsmaatregelen. Een dergelijk vermoeden was niet te onderbouwen vanuit bestaande wetenschappelijke literatuur.

In dit onderzoek zijn in totaal 10 risico's geïdentificeerd welke correleren met de mate van procesvolwassenheid, de mate van digitalisering en de mate van genomen digitale weerbaarheidsmaatregelen. Eveneens is vastgesteld dat de mate van procesvolwassenheid en de mate van genomen digitale weerbaarheidsmaatregelen een sterke positieve correlatie ($r = .628$, $p = .007$) vertonen en daarom samengenomen kunnen worden. Een dergelijke samenhang zou kunnen worden verklaard vanuit de gebruikte modellen voor procesvolwassenheid (K. P. McCormack & W. C. Johnson, 2001) en genomen digitale weerbaarheidsmaatregelen (Spruit & Roeling, 2014) omdat de

onderdelen van procesvolwassenheid terugkomen in de focusgebieden van digitale weerbaarheid. Het gebruikte model voor digitalisering (Valdez-de-Leon, 2016) bevat deze focusgebieden niet.

Eveneens is gezien de correlatiecoëfficiënten duidelijk geworden dat risico's voor de bedrijfsvoering negatief correleren met procesvolwassenheid, genomen digitale weerbaarheidsmaatregelen en digitalisering. Echter correleert niet ieder risico op dezelfde manier met deze variabelen. Een dergelijk verschil tussen variabelen zou kunnen worden gebruikt om te bepalen waar het loont voor een mkb-bedrijf om volwassenheid op dat gebied te vergroten zodat het risico mogelijk wordt gereduceerd. Bijvoorbeeld voor het risico voor de bedrijfsvoering dat voortvloeit uit Rampen kan het lonen meer te investeren in digitalisering ($r = -.474$, $p = .001$), dan in procesvolwassenheid en genomen digitale weerbaarheidsmaatregelen ($r = -.351$, $p = .016$).

Voor het vaststellen van mate van procesvolwassenheid, mate van digitalisering en mate van genomen digitale weerbaarheidsmaatregelen zijn in dit onderzoek samenvattingen gemaakt van bestaande volwassenheidsmodellen. Dit is gedaan om uiteindelijk een reductie van het aantal vragen te bewerkstelligen (ruim 300 voor de drie modellen). Deze aanpak komt overeen met een eerder onderzoek (Aberle & Henkel, 2017), echter is niet getoetst in welke mate het samengevatte model overeenkomt met de oorspronkelijke modellen. Onduidelijk is welke invloed dit heeft gehad op het onderzoek.

Gezien het beperkte bewustzijn rondom cybercriminaliteit is er sprake van een onjuiste risicoperceptie mkb-bedrijven. Om hierin zoveel mogelijk te voorzien is gekozen een lijst met risico's op te nemen in tegenstelling tot een open vraag om risico's te benoemen. Een dergelijke aanpak wordt bijvoorbeeld ook gebruikt in de ISO 27005 standaard (ISO/IEC, 2018) waarbij bij een dergelijke aanpak gesproken wordt over een high-level risk assessment. Een verdere verdieping zou gemaakt kunnen worden door de 13 uitgevraagde risico's verder op te delen in de genoemde risico-elementen (Cebula & Young, 2010) of een gedetailleerd information security risk assessment uit te voeren (ISO/IEC, 2018).

Tot slot is dit onderzoek uitgevoerd met een N van 47 mkb-bedrijven. De resultaten zijn hiermee mogelijk beperkt te generaliseren voor geheel mkb in Nederland. De generaliseerbaarheid wordt mogelijk verder gereduceerd door de gebruikte methode van sampling (convenience en snowball) waarmee mogelijk bedrijven in een bepaalde sector/ met een bepaald niveau van volwassenheid zijn benaderd uit het eigen netwerk.

5.2. Conclusies

Uiteindelijk kan de hoofdvraag van dit onderzoek beantwoord worden:

Uit welke onderdelen bestaat een raamwerk waarmee een mkb-bedrijf inzichtelijk krijgt welke risico's het loopt voor zijn bedrijfsvoering, vanwege onvoldoende genomen digitale weerbaarheidsmaatregelen?

Risico's voor de bedrijfsvoering van mkb-bedrijven vertonen correlaties met de mate van procesvolwassenheid en genomen digitale weerbaarheidsmaatregelen en de mate van digitalisering. In totaal zijn 10 risico's geïdentificeerd welke individueel in meer of mindere mate correleren. De onderzochte risico's zijn samen te vatten in vier categorieën:

Acties van personen

De categorie acties van personen beschrijft de risico's welke voortvloeien uit problemen veroorzaakt door acties wel of niet uitgevoerd door personen in bepaalde situaties. Geïdentificeerde risico's zijn: Per ongeluk, Opzettelijk en Inaction.

Falen van systemen en technologie

De categorie falen van systemen en technologie beschrijft de risico's welke voortvloeien uit problemen met abnormaal of onverwacht functioneren van technologische middelen. Geïdentificeerde risico's zijn: Hardware en Software.

Falen van interne processen

De categorie falen van interne processen beschrijft risico's welke voortvloeien uit problematisch falen van interne processen om te doen wat van ze verwacht wordt of nodig is. Geïdentificeerde risico's zijn: Procesontwerp of uitvoer, Procescontrols en Ondersteunende processen.

Externe gebeurtenissen

De categorie externe gebeurtenissen beschrijft risico's welke voortvloeien uit gebeurtenissen buiten bereik van de organisatie. Vaak kan de timing van dit soort gebeurtenissen niet worden voorspeld. Geïdentificeerde risico's zijn: Rampen en Juridische problemen.

5.1. Aanbevelingen voor de praktijk

Het ontwikkelde model kan worden gebruikt om op basis van de mate van digitalisering en de mate van procesvolwassenheid en genomen digitale weerbaarheidsmaatregelen te bepalen óf en in welke mate een risico van toepassing kan zijn voor een mkb-bedrijf. Na vaststellen van de volwassenheidsniveaus kan advies worden gegeven over een mogelijke investeringsrichting op het gebied van volwassenheidsniveaus om risico's te kunnen reduceren.

Door het PVO Limburg zou het model eveneens kunnen worden gebruikt. Om de volwassenheidsniveaus vast te kunnen stellen zou de huidige weerbaarheidsscan kunnen worden uitgebreid met de vragen afkomstig uit dit onderzoek. Vervolgens kan er een advies worden gegeven over welke risico's van toepassing zijn en op welke manier een verbetering van het volwassenheidsniveau leidt tot een mogelijk reductie van het risico.

5.2. Aanbevelingen voor verder onderzoek

Dit onderzoek heeft zich gericht op 13 risicocategorieën. Een verdere verdieping zou gemaakt kunnen worden door in plaats van deze risicocategorieën de genoemde risico-elementen (Cebula & Young, 2010) te gebruiken. Op die manier ontstaat een lijst van 57 elementen welke 13 cyberrisico categorieën invullen. Ook zou een gedetailleerd information security risk assessment uitgevoerd kunnen worden (ISO/IEC, 2018).Vervolgens zou op basis van correlatiecoëfficiënten een model kunnen worden ingevuld waarmee de invloed van procesvolwassenheid, digitalisering en genomen digitale weerbaarheidsmaatregelen inzichtelijk wordt gemaakt.

Eveneens kan als aanbeveling worden opgenomen het onderzoek uit te voeren met een grotere groep mkb-bedrijven om zo meer generaliseerbare resultaten te verkrijgen. Echter brengt dit ook de nodige beperkingen met zich mee. In dit onderzoek is door middel van *convenience sampling* en *snowball samping* een response ratio van circa 45% verkregen. Bij een eerste versie van de enquête zijn 5 van 33 enquêtes volledig ingevuld. Het lijkt dus lastig een mkb-bedrijf voldoende te motiveren om deel te nemen aan de enquête en deze volledig in te vullen. Bijvoorbeeld het afnemen van

enquêtes via telefoon of als gestructureerd interview kan tot een hogere response ratio leiden (Saunders et al., 2016).

5.3. Reflectie

Terugkijkend op de gehele afstudeerperiode ben ik best tevreden met het onderzoek dat ik de afgelopen twee jaar heb uitgevoerd. Bij de OU is dit afstuderen opgedeeld in twee delen, het voorbereiden afstuderen en het empirisch onderzoek. In het voorjaar van 2019 ben ik begonnen met het voorbereiden afstuderen en in het voorjaar van 2020 heb ik goedkeuring gekregen voor het literatuuronderzoek en het daarmee ontwikkelde conceptuele model om empirisch te gaan onderzoeken.

Het voorbereiden afstuderen begon met het vaststellen van de opdracht. In onze onderzoeksgroep hebben we gekozen voor een vaste verdeling. Mijn studiegenoten gingen een kwalitatief onderzoek uitvoeren en ik een kwantitatief onderzoek. Achteraf weet ik niet of een dergelijke keuze zo vroeg in het onderzoek verstandig is geweest. Sommige onderzoeksvragen lenen zich namelijk meer om kwalitatief onderzocht te worden, bijvoorbeeld de vragen om (exploratief) tot invulling van een conceptueel model te komen. Wellicht had een aanpak met hypothesestelling beter gepast bij een kwantitatief onderzoek, alleen had ik dan risico's moeten verkrijgen uit een kwalitatief onderzoek dat eerst uitgevoerd had moeten worden. Daar was gezien de afstudeerperiode geen tijd voor. Na het opstellen van de onderzoeksvragen was het literatuuronderzoek goed uit te voeren. De gehanteerde PRISMA-methodiek bood hiervoor voldoende houvast.

Uiteindelijk is het gelukt om in het voorjaar van 2020 het akkoord te krijgen voor het afstuderen en door te gaan met het empirisch onderzoek. Het daadwerkelijk verzamelen van data heeft nog aardig wat voeten in de aarde gehad. In mei 2020 is het eerste interview afgenomen met een MKB-bedrijf. De enquête bestond toen nog uit > 300 vragen. De tweede versie van het interview, met samengevatte volwassenheidsmodellen, is in juli verspreidt. Wellicht gezien vakanties en het niet direct aanschrijven van respondenten was de response helaas laag. Vervolgens is opnieuw een enquête uitgezet waarbij circa 130 respondenten persoonlijk zijn aangeschreven. Op deze manier is het uiteindelijk gelukt 61 ingevulde enquêtes te verkrijgen (waarvan 47 volledig ingevuld). Achteraf denk ik dat ik het verzamelen van de data te makkelijk heb ingeschat. Zelfs met het aanschrijven van respondenten is het gelukt 'slechts' een response van 50% te behalen. Zo had ik circa 600 bedrijven aan moeten schrijven om circa 300 respondenten te behalen voor mogelijke generaliseerbaarheid, waar je ook het liefst nog kiest uit willekeurige bedrijven gezien de steekproef. Ik denk dat het mkb zich lastiger laat bevragen, al helemaal in de huidige coronacrisis. Men heeft immers wel iets anders aan het hoofd dan het invullen van een enquête over risico's. Toch ben ik erg blij met de 61 reacties die ik heb mogen ontvangen.

Voor het analyseren van de data moest ik weer even terug in de studieboeken. Gelukkig heb ik de premaster aan de OU gevolgd en kon ik de kennis die ik daar heb opgedaan gebruiken om te bepalen op welke manier de data geanalyseerd kon worden. Ook kon ik de daar opgedane kennis voor wat betreft SPSS gebruiken in dit onderzoek. Uiteindelijk is het gelukt de data te analyseren middels non-parametrisch toetsen. Lastig hierbij vond ik wel het visualiseren van de correlaties in een model. Hier bestaat geen kant-en-klare aanpak voor, anders dan een correlatiematrix / heatmap. Met wat puzzelen is het toch gelukt een invulling te geven aan het model op basis van de correlatiecoëfficiënten.

Gedurende het gehele afstudeertraject heb ik veel gehad aan de samenwerking in groepsverband met mijn twee studiegenoten en de regelmatige begeleiding van Prof. dr. ir. Johan Versendaal. Door

samen te werken aan een afstudeeropdracht, ieder vanuit zijn eigen expertise en invalshoek gevoed door kennis uit de praktijk, was het mogelijk tot nieuwe inzichten te komen en elkaar verder te helpen. Uiteindelijk is het daarmee gelukt dit onderzoek uit te kunnen voeren.

6. Referenties

Aberle, D., & Henkel, J. (2017). The development of a questionnaire to measure business process maturity. *European Journal of Management Issues, 25*.

Agresti, A., & Finlay, B. (2009). *Statistical Methods for the Social Sciences*.

Alejandro, Mendes, Ayala, & Ghezzi. (2019). Servitization and Industry 4.0 convergence in the digital transformation ofproductfirms: A business model innovation perspective. *Technological Forecasting & Social Change, 141*.

Bailey, T., Del Miglio, A., & Richter, W. (2014). The Rising Strategic Risks of Cyberattacks. *McKinsey Quarterly, May*. Retrieved from http://www.mckinsey.com/insights/business_technology/the_rising_strategic_risks_of_cyberattacks

Barua, Konana, Whinston, & Yin. (2004). An Empirical Investigation of Net-Enabled Business Value. *MIS Quarterly, 28*(4).

Becker, J., Knackstedt, R., & Pöppelbuß, J. (2009). Developing Maturity Models for IT Management–A Procedure Model and its Application. *Business & Information Systems Engineering, 3*.

Bilge, K., Yildirim, S. O., & Baykal, N. (2016). A vulnerability-driven cyber security maturity model for measuring national critical infrastructure protection preparedness. *National critical infrastructure protection, 15*.

Blythe, J. M., & Coventry, L. (2018). Costly but effective: Comparing the factors that influence employee antimalware behaviours.

Böhme, R., Laube, S., & Riek, M. (2018). A Fundamental Approach to Cyber Risk Analysis. *CASUALTY ACTUARIAL SOCIETY, 12*(2).

Buecker, A., Borrett, M., Lorenz, C., & Powers, C. (2010). Introducing the IBM security framework and IBM security blueprint to realize business-driven security.

CBS. (2019). Meer 'kleine' mkb-bedrijven. Retrieved from https://www.cbs.nl/nl-nl/nieuws/2019/31/meer-kleine-mkb-bedrijven

CBS. (2020). Bedrijven: bedrijfstak.

Cebula, J. L., & Young, L. R. (2010). *A Taxonomy of Operational Cyber Security Risks*. Retrieved from

Chanchala, J., Kumar, U., & Tarey, K. (2015). A Review on Taxonomies of Attacks and Vulnerability in Computer and Network System. *International Journal of Advanced Research in Computer Science and Software Engineering*.

Donalds, C., Kweku-Muata, & Osei-Bryson. (2018). Toward a cybercrime classification ontology: A knowledge-based approach.

Dreher, & Dreher. (2011). Empowering Doctoral Candidates in Finding Relevant Concepts in a Literature Set. *International Journal of Doctoral Studies, 6*.

Edmondson, A. C., & McManus, S. E. (2007). METHODOLOGICAL FIT IN MANAGEMENT FIELD RESEARCH. *Academy of Management Review, 32*(4), 1155-1179.

Europese Commissie. (2015). Gebruikersgids bij de definitie van kmo's [Press release]

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cyber security investment. *Decision Support Systems, 86*.

Hevner, March, Park, & Ram. (2004). Design Science in Information Systems Research. *MIS Quarterly, 28*(1).

Humphrey, W. S. (1988). Characterizing the software process: a maturity framework.

ISO/IEC. (2018). NEN-ISO/IEC 27005. In.

Ivančić, Vukšić, Vesna, & Spremić. (2019). Mastering the Digital Transformation Process:Business Practices and Lessons Learned. *Technology Innovation Management Review, 9*(2).

Kaplan, S., & Garrick, B. J. (1981). On The Quantitative Definition of Risk. *Risk Analysis, 1*(1).

Larose, D. T. (2006). *Data Mining Methods and Models*.
Le, N. T., & Hoang, D. B. (2016). *Can maturity models support cyber security?* Paper presented at the 2016 IEEE 35th International Performance Computing and Communications Conference (IPCCC), Las Vegas, NV, USA.
Lee, J., Lee, D., & Kang, S. (2007). An Overview of the Business Process Maturity Model (BPMM).
Lindqvist, U., & Jonsson, E. (1997). *How to Systematically Classify Computer Security Intrusions.* Paper presented at the Proceedings. 1997 IEEE Symposium on Security and Privacy.
Lockamy, A., & McCormack, K. (2004). The development of a supply chain management process maturity model using the concepts of business process orientation. *Supply Chain Management: An International Journal, 9*(4).
McCormack, & Johnson. (2001). *Business Process Orientation: Gaining the e-Business Competitive Advantage*.
McCormack, K., Willems, J., Bergh, J. v. d., Deschoolmeesterand, D., Willaert, P., Sˇtemberger, M. I., . . . Vlahovic, N. (2009). A global investigation of key turning points in business process maturity. *Business Process Management Journal, 15*.
McCormack, K. P., & Johnson, W. C. (2001). *Business process orientation: gaining the e-business competitive advantage*: CRC Press LLC.
Miron, W., & Muita, K. (2014). Cybersecurity Capability Maturity Models for Providers of Critical Infrastructure. *Technology Innovation Management Review*.
Moher, Liberati, Tetzlaff, & Altman. (2009). PRISMA 2009 Flow Diagram.
National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity*

Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf:
NCSC. (2018). *Cybersecuritybeeld Nederland 2018*. Retrieved from
Platform Veilig Ondernemen Limburg, & Campus, B. S. S. (2018). *Cyberweerbaarheid in Limburg*. Retrieved from
Prokop, M. (2011). *Data dimensionality reduction methods for ordinal data*. Paper presented at the International Days of Statistics and Economics, Prague.
Rees, L. P., Deane, J. K., Rakes, T. R., & Baker, W. H. (2011). Decision support for Cybersecurity risk planning. *Decision Support Systems, 51*.
Renaud, K. (2016). How smaller businesses struggle with security advice.
Rijksdienst voor Ondernemend Nederland. (2004). Definitie van kleine en middelgrote ondernemingen.
ROC Friese Poort, Stichting Cyber Safety Noord Nederland, & Digital Trust Centrum. (2018). Scan Digitaal Veilig Ondernemen. In.
Roeling, M. (2010). *Towards an aligned organization on Information Security.* Utrecht University,
Röglinger, M., Pöppelbuß, J., & Becker, J. (2012). Maturity models in business process management. *Business Process Management Journal, 18*(2).
Saunders, M., Lewis, P., & Thornhill, A. (2016). *Research methods for business students*.
Schwer, Hitz, Wyss, Wirz, & Minonne. (2018). Digital Maturity Variables and their impact on the Enterprise Architecture Layers. *Problems and Perspectives in Management, 16*(4).
Spruit, M., & Roeling, M. (2014). *ISFAM: the Information Security Focus Area Maturity model*. Paper presented at the Twenty Second European Conference on Information Systems, Tel Aviv.
Tarhan, A., Turetken, O., & Reijers, H. A. (2016). Business process maturity models: Asystematic literature review. *Information and Software Technology, 75*.
Valdez-de-Leon. (2016). A Digital Maturity Model for Telecommunications Service Providers. *Technology Innovation Management Review, 6*(8).
Wangen, G., Hallstensen, C., & Snekkenes, E. (2017). A framework for estimating information security risk assessment method completeness. *International Journal Information Security*.
Weber, Curtis, & Gardiner. (2008). Business Process Maturity Model (BPMM).

Wilding, N. (2016). Cyber resilience: How importantis your reputation? How effectiveare your people?
Wohlin, C., Höst, M., & Regnell, B. (2012). *Experimentation in Software Engineering*.
Xu, J. (2014). *Managing Digital Enterprise: Ten Essential Topics*.

7. Bijlagen

7.1. Bijlage 1: Cyberrisico's (Cebula & Young, 2010)

Categorie	Subcategorie	Betekenis
Acties van personen	Per ongeluk	Een actie uitgevoerd zonder kwaad in de zin, bijvoorbeeld door een fout te begaan.
	Opzettelijk	Een actie uitgevoerd met kwaad in de zin, bijvoorbeeld fraude of vandalisme.
	Inaction	Het gebrek aan actie in een bepaalde situatie. Bijvoorbeeld door gebrek aan kennis of vaardigheden.
Falen van systemen en technologie	Hardware	Falen van fysieke apparatuur door bijvoorbeeld problemen met capaciteit, prestaties, gebrek aan onderhoud of veroudering.
	Software	Falen van programmatuur, applicaties en besturingssystemen door bijvoorbeeld incompatibiliteit, onjuiste beveiligingsinstellingen of gebrekkig testen.
	Systemen	Falen van systemen om niet te functioneren zoals verwacht door bijvoorbeeld ontwerpfouten, specificatiefouten, integratiefouten of complexiteit.
Falen van interne processen	Procesontwerp- of uitvoer	Falen van processen om niet te functioneren zoals verwacht door onjuist procesontwerp of onjuist uitvoeren van een juist procesontwerp. Bijvoorbeeld door onjuiste procesdocumentatie of onjuiste verdeling van rollen en verantwoordelijkheden.
	Proces controls	Falen van processen door onvoldoende controls op de uitvoer van een proces. Bijvoorbeeld door onjuist monitoren van een proces of vergeten het proces periodiek te beoordelen.
	Ondersteunende processen	Falen van ondersteunende processen om de passende middelen te leveren. Bijvoorbeeld

		door onvoldoende personeel, financiele middelen of training.
Externe gebeurtenissen	Rampen	Risico's door gebeurtenissen, bijvoorbeeld brand, overstroming of aardbeving.
	Juridische problemen	Risico's door juridische problemen, bijvoorbeeld nieuwe wetgeving die impact heeft op de organisatie of iemand die juridische stappen wil ondernemen tegen de organisatie.
	Bedrijfsproblemen	Risico's door veranderingen in de omgeving van de organisatie, bijvoorbeeld een leverancier die niet levert, de organisatie die geen producten kan leveren door marktcondities of gebrek aan financiele middelen door economische condities.
	Afhankelijkheid van diensten	Risico's door de afhankelijkheid van de organisatie op externen om te kunnen functioneren en het falen daarvan. Bijvoorbeeld stroomuitval, onderbreking van watertoevoer of gebrek aan brandstof voor een noodstroomaggregaat.

7.2. Volwassenheidsmodellen

7.2.1. Procesvolwassenheid (Aberle & Henkel, 2017; Lockamy & McCormack, 2004)

Niveau	*Karakteristieken*
Ad Hoc	Processen zijn niet gestructureerd. Processen worden niet gemeten.
Defined	Basisprocessen zijn vastgelegd. Functies binnen de organisatie bevatten een procesaspect.
Linked	Managers in de organisatie voeren procesbeheer uit met een strategisch doel. Samenwerking vindt plaats in de vorm van teams.
Integrated	Procesresultaten worden gemeten en beheert vanuit een tool. De processen produceren verwachte en voorspelbare resultaten.
Extended	Samenwerking vindt plaats op procesniveau tussen verschillende entiteiten (andere organisaties, leveranciers). Processen worden continue geoptimaliseerd.

7.2.2. Mate van digitalisering (Valdez-de-Leon, 2016)

Niveau	*Karakteristieken*
Initial	De organisatie wil graag meer digitaliseren en heeft een initiële digitale visie.
Enabling	De organisatie vormt de fundering voor digitalisering door bijvoorbeeld een digitale strategie vast te leggen, digitale kansen te verkennen en budget vrij te maken.
Integrating	De organisatie is bezig digitalisering in de gehele organisatie te integreren door bijvoorbeeld digitale initiatieven in de hele organisatie te implementeren, in deze initiatieven personen uit verschillende functies en afdelingen te betrekken en processen in de organisatie op één lijn te krijgen met digitale IT-infrastructuur.
Optimizing	De organisatie optimaliseert digitalisering door bijvoorbeeld nieuwe bedrijfsmodellen met digitale elementen in te zetten, digitale strategie te delen met aandeelhouders en real-time data te analyseren om de betrouwbaarheid van diensten te optimaliseren.
Pioneering	De organisatie is baanbrekend bezig met digitalisering, digitale diensten zorgen voor meer dan 10% van de omzet, de organisatie is gefocust op digitale innovatie en zet bijvoorbeeld technologieën als machine learning in om voorspellende analyses uit te voeren.

7.2.3. Mate van genomen weerbaarheidsmaatregelen (Roeling, 2010; Spruit & Roeling, 2014)

Niveau	*Karakteristieken*
Design	De organisatie is bezig met het ontwikkelen en ontwerpen van informatiebeveiliging, bijvoorbeeld door een informeel risicobeheerprogramma te hebben, beleid te ontwikkelen met behulp van informatie beschikbaar op het internet en gebruikersbeheer ad-hoc uit te voeren.
Implementation	De organisatie is bezig met het implementeren van informatiebeveiliging, bijvoorbeeld door een risicobeheerprogramma vast te stellen op strategisch niveau, toegangsbeheer tot belangrijke faciliteiten te limiteren tot een beperkt aantal personen en toegang tot applicaties en gebouwen vast te leggen.
Operational Effectiveness	De organisatie heeft informatiebeveiliging geïmplementeerd en informatiebeveiliging werkt zoals verwacht, bijvoorbeeld door risicobeheerprocessen te formaliseren, gebruikersbeheer periodiek (maand/jaar) uit te voeren en IT-architectuur te ontwerpen op basis van een standaard of raamwerk.
Monitoring	De organisatie monitort en controleert informatiebeveiliging, bijvoorbeeld door een risicobeheerprogramma op te stellen waarin klanten en leveranciers worden betrokken, gebruikersbeheer als continue proces te laten ondersteunen door een IT-systeem en de organisatie te laten voldoen aan of te certificeren voor een bepaalde standaard.

7.3. Enquête

1. Inleiding

Open Universiteit
www.ou.nl

Welkom bij de enquête over risico's voor de bedrijfsvoering van mkb-bedrijven voor het afstudeeronderzoek van Rob de Vries, student masteropleiding Business Process Management & IT aan de Open Universiteit.

Doel van dit onderzoek
In het project Cyberweerbaarheid in Limburg van het PVO Limburg en de Brightlands Smart Service Campus wil men deze ondernemers meer weerbaar maken tegen cybercriminaliteit. Onderdeel hiervan is het ontwikkelen van weerbaarheidsscans waarmee het bedrijfsproces en de daarbij ingezette IT-infrastructuur wordt doorgelicht om zo kritieke punten, risicofactoren en belangrijkste maatregelen die de ondernemer zou moeten (laten) nemen om meer weerbaar te worden tegen cybercriminaliteit.

Binnen het project is reeds een weerbaarheidsscan opgezet waarbij wordt gekeken naar vier onderdelen: een technische scan, een WiFi-scan, de digitale voetafdruk en een veilige website. Echter is tot op heden onduidelijk op welke manier de onderdelen van de scan vertaald kunnen worden naar risico's voor de bedrijfsvoering en op welke manier deze risico's aangepakt kunnen worden. Vanuit de praktijkervaring van het PVO Limburg bestaat een vermoeden dat de risico's voor de bedrijfsvoering ook afhankelijk zijn van de mate van digitalisering binnen een bedrijf en de mate van volwassenheid van de procesinrichting.

Dit onderzoek heeft als doel om een wetenschappelijk onderbouwd raamwerk te ontwikkelen waarmee de risico's voor de bedrijfsvoering door onvoldoende genomen digitale weerbaarheidsmaatregelen inzichtelijk gemaakt kunnen worden.

Instructie
Hierna volgen in totaal 10 vragen opgedeeld in de volgende categorieën:

- Algemene vragen over uw organisatie.
- Vragen over vaststellen mate van procesvolwassenheid van uw organisatie.
- Vragen over vaststellen mate van digitalisering van uw organisatie.
- Vragen over vaststellen mate van genomen digitale weerbaarheidsmaatregelen van uw organisatie.
- Vragen over vaststellen van toepassing zijnde risico's voor uw organisatie.

Voor de vragen over mate van procesvolwassenheid, digitale weerbaarheid en mate van digitalisering wordt gebruik gemaakt van een zogenaamd volwassenheidsmodel. Wilt u hierbij het niveau aangeven welke het meest voor uw organisatie van toepassing is?

Bij de vragen over risico's voor uw organisatie wordt gebruik gemaakt van een 5-punts Likertschaal. Wilt u hierbij aangeven in welke mate een genoemd risico een daadwerkelijk risico voor uw bedrijfsvoering is mocht dit voorkomen?

Tot slot kunt u eventuele opmerkingen achterlaten.

2. Controlevraag mkb-onderneming

Vraag: Kunt u aangeven welke definitie van mkb-bedrijven voor u het meest van toepassing is?

Antwoorden:

Vraag	**Antwoord A**	**Antwoord B**	**Antwoord C**	**Antwoord D**
Kunt u aangeven welke definitie van mkb-bedrijven voor u het meest van toepassing is?	Minder dan 10 werknemers en Jaaromzet hoogstens € 2 miljoen en / of Jaarbalans kleiner of gelijk aan € 2 miljoen	Minder dan 50 werknemers en Jaaromzet hoogstens € 10 miljoen en / of Jaarbalans kleiner of gelijk aan € 10 miljoen	Minder dan 250 werknemers en Jaaromzet hoogstens € 50 miljoen en / of Jaarbalans kleiner of gelijk aan € 43 miljoen	Geen van de bovenstaande

3. Vaststellen sector mkb-onderneming

Vraag: In welke sector is uw organisatie werkzaam?

Antwoorden:

Antwoord A	Antwoord B	Antwoord C	Antwoord D
Minder dan 10 werknemers en Jaaromzet hoogstens € 2 miljoen en / of Jaarbalans kleiner of gelijk aan € 2 miljoen	Minder dan 50 werknemers en Jaaromzet hoogstens € 10 miljoen en / of Jaarbalans kleiner of gelijk aan € 10 miljoen	Minder dan 250 werknemers en Jaaromzet hoogstens € 50 miljoen en / of Jaarbalans kleiner of gelijk aan € 43 miljoen	Geen van de bovenstaande

4. Mate van procesvolwassenheid

Inleiding:

De volgende vraag gaat over de mate van procesvolwassenheid in uw organisatie. De mate van procesvolwassenheid wordt gemeten in vijf niveau's. Kunt u aangeven welk niveau voor u het meest van toepassing is?

Vraag:

De mate van procesvolwassenheid in uw organisatie:

Antwoorden:

Antwoord A	Antwoord B	Antwoord C	Antwoord D	Antwoord E
Processen zijn niet gestructureerd. Processen worden niet gemeten.	Basisprocessen zijn vastgelegd. Functies binnen de organisatie bevatten een procesaspect.	Managers in de organisatie voeren procesbeheer uit met een strategisch doel. Samenwerking vindt plaats in de vorm van teams.	Procesresultaten worden gemeten en beheert vanuit een tool. De processen produceren verwachte en voorspelbare resultaten.	Samenwerking vindt plaats op procesniveau tussen verschillende entiteiten (andere organisaties, leveranciers). Processen worden continue geoptimaliseerd.

5. Mate van digitalisering

Inleiding:

De volgende vraag gaat over de mate van digitalisering in uw organisatie. De mate van digitalisering wordt gemeten in vijf niveau's. Kunt u aangeven welk niveau voor u het meest van toepassing is?

Vraag: De mate van digitalisering in uw organisatie:

Antwoorden:

Antwoord A	**Antwoord B**	**Antwoord C**	**Antwoord D**	**Antwoord E**
De organisatie wil graag meer digitaliseren en heeft een initiële digitale visie.	De organisatie vormt de fundering voor digitalisering door bijvoorbeeld een digitale strategie vast te leggen, digitale kansen te verkennen en budget vrij te maken.	De organisatie is bezig digitalisering in de gehele organisatie te integreren door bijvoorbeeld digitale initiatieven in de hele organisatie te implementeren, in deze initiatieven personen uit verschillende functies en afdelingen te betrekken en processen in de organisatie op één lijn te krijgen met digitale IT-infrastructuur.	De organisatie optimaliseert digitalisering door bijvoorbeeld nieuwe bedrijfsmodellen met digitale elementen in te zetten, digitale strategie te delen met aandeelhouders en real-time data te analyseren om de betrouwbaarheid van diensten te optimaliseren.	De organisatie is baanbrekend bezig met digitalisering, digitale diensten zorgen voor meer dan 10% van de omzet, de organisatie is gefocust op digitale innovatie en zet bijvoorbeeld technologieën als machine learning in om voorspellende analyses uit te voeren.

6. Mate van genomen digitale weerbaarheidsmaatregelen

Inleiding:

De volgende vraag gaat over de mate van genomen digitale weerbaarheidsmaatregelen. De mate van genomen digitale weerbaarheidsmaatregelen wordt gemeten in vier niveaus. Kunt u aangeven welk niveau voor u het meest van toepassing is?

Vraag: De mate van genomen digitale weerbaarheidsmaatregelen in uw organisatie:

Antwoorden:

Antwoord A	Antwoord B	Antwoord C	Antwoord D
De organisatie is bezig met het ontwikkelen en ontwerpen van informatiebeveiliging, bijvoorbeeld door een informeel risicobeheerprogramma te hebben, beleid te ontwikkelen met behulp van informatie beschikbaar op het internet en gebruikersbeheer ad-hoc uit te voeren.	De organisatie is bezig met het implementeren van informatiebeveiliging, bijvoorbeeld door een risicobeheerprogramma vast te stellen op strategisch niveau, toegangsbeheer tot belangrijke faciliteiten te limiteren tot een beperkt aantal personen en toegang tot applicaties en gebouwen vast te leggen.	De organisatie heeft informatiebeveiliging geïmplementeerd en informatiebeveiliging werkt zoals verwacht, bijvoorbeeld door risicobeheerprocessen te formaliseren, gebruikersbeheer periodiek (maand/jaar) uit te voeren en IT-architectuur te ontwerpen op basis van een standaard of raamwerk.	De organisatie monitort en controleert informatiebeveiliging, bijvoorbeeld door een risicobeheerprogramma op te stellen waarin klanten en leveranciers worden betrokken, gebruikersbeheer als continue proces te laten ondersteunen door een IT-systeem en de organisatie te laten voldoen aan of te certificeren voor een bepaalde standaard.

7. Risico's: acties van personen

Inleiding:

De volgende vraag gaat over de risico's welke te relateren zijn aan acties van personen. Kunt u aangeven in hoeverre een genoemd risico een daadwerkelijk risico voor uw bedrijfsvoering is mocht dit voorkomen?

Uitleg
De categorie acties van personen beschrijft de risico's welke voortvloeien uit problemen veroorzaakt door acties wel of niet uitgevoerd door personen in bepaalde situaties.

Per ongeluk: een actie uitgevoerd zonder kwaad in de zin, bijvoorbeeld door een fout te begaan.
Opzettelijk: een actie uitgevoerd met kwaad in de zin, bijvoorbeeld fraude of vandalisme.
Inaction: het gebrek aan actie in een bepaalde situatie. Bijvoorbeeld door gebrek aan kennis of vaardigheden.

Antwoorden:

	Geen	Een beetje	Redelijk	Erg	Extreem
Per ongeluk					
Opzettelijk					
Inaction					

8. Risico's: Falen van systemen en technologie

Inleiding:

De volgende vraag gaat over de risico's welke te relateren zijn aan falen van systemen en technologie. Kunt u aangeven in hoeverre een genoemd risico een daadwerkelijk risico voor uw bedrijfsvoering is mocht dit voorkomen?

Uitleg
De categorie falen van systemen en technologie beschrijft de risico's welke voortvloeien uit problemen met abonormaal of onverwacht functioneren van technologische middelen.

Hardware: falen van fysieke apparatuur door bijvoorbeeld problemen met capaciteit, prestaties, gebrek aan onderhoud of veroudering.
Software: falen van programmatuur, applicaties en besturingssystemen door bijvoorbeeld incompatibiliteit, onjuiste beveiligingsinstellingen of gebrekkig testen.
Systemen: falen van systemen om niet te functioneren zoals verwacht door bijvoorbeeld ontwerpfouten, specificatiefouten, integratiefouten of complexiteit.

Antwoorden:

	Geen	Een beetje	Redelijk	Erg	Extreem
Hardware					
Software					
Systemen					

9. Risico's: Falen van interne processen

Inleiding:

De volgende vraag gaat over de risico's welke te relateren zijn aan falen van interne processen. Kunt u aangeven in hoeverre een genoemd risico een daadwerkelijk risico voor uw bedrijfsvoering is mocht dit voorkomen?

Uitleg
De categorie falen van interne processen beschrijft risico's welke voortvloeien uit problematisch falen van interne processen om te doen wat van ze verwacht wordt of nodig is.

Procesontwerp of uitvoer: falen van processen om niet te functioneren zoals verwacht door onjuist procesontwerp of onjuist uitvoeren van een juist procesontwerp. Bijvoorbeeld door onjuiste procesdocumentatie of onjuiste verdeling van rollen en verantwoordelijkheden.
Procescontrols: falen van processen door onvoldoende controls op de uitvoer van een proces. Bijvoorbeeld door onjuist monitoren van een proces of vergeten het proces periodiek te beoordelen.
Ondersteunende processen: falen van ondersteunende processen om de passende middelen te leveren. Bijvoorbeeld door onvoldoende personeel, financiele middelen of training.

Antwoorden:

	Geen	Een beetje	Redelijk	Erg	Extreem
Procesontwerp of uitvoer					
Procescontrols					
Ondersteunende processen					

10. Risico's externe gebeurtenissen

Inleiding:

De volgende vraag gaat over de risico's welke te relateren zijn aan externe gebeurtenissen. Kunt u aangeven in hoeverre een genoemd risico een daadwerkelijk risico voor uw bedrijfsvoering is mocht dit voorkomen?

Uitleg

De categorie externe gebeurtenissen beschrijft risico's welke voortvloeien uit gebeurtenissen buiten bereik van de organisatie. Vaak kan de timing van dit soort gebeurtenissen niet worden voorspeld.

Rampen: risico's door gebeurtenissen, bijvoorbeeld brand, overstroming of aardbeving.
Juridische problemen: risico's door juridische problemen, bijvoorbeeld nieuwe wetgeving die impact heeft op de organisatie of iemand die juridische stappen wil ondernemen tegen de organisatie.
Bedrijfsproblemen: risico's door veranderingen in de omgeving van de organisatie, bijvoorbeeld een leverancier die niet levert, de organisatie die geen producten kan leveren door marktcondities of gebrek aan financiële middelen door economische condities.
Afhankelijkheid van diensten: risico's door de afhankelijkheid van de organisatie op externen om te kunnen functioneren en het falen daarvan. Bijvoorbeeld stroomuitval, onderbreking van watertoevoer of gebrek aan brandstof voor een noodstroomaggregaat.

Antwoorden:

	Geen	Een beetje	Redelijk	Erg	Extreem
Rampen					
Juridische problemen					
Bedrijfsproblemen					
Afhankelijkheid van diensten					

11. Afsluiting enquete

Dit is het einde van de enquête. Dank voor uw deelname!

Heeft u nog opmerkingen? Dan kunt u deze onderstaand achterlaten. Zou u dan zo vriendelijk willen zijn ook uw e-mailadres in te vullen? Zo kan er eventueel contact met u opgenomen worden.

7.4. Frequentietabellen resultaten

Procesvolwassenheid

PV_RECODE

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1,00	7	14,9	14,9	14,9
	2,00	16	34,0	34,0	48,9
	3,00	16	34,0	34,0	83,0
	4,00	7	14,9	14,9	97,9
	5,00	1	2,1	2,1	100,0
	Total	47	100,0	100,0	

Digitale weerbaarheid

DW_RECODE

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1,00	6	12,8	12,8	12,8
	2,00	12	25,5	25,5	38,3
	3,00	19	40,4	40,4	78,7
	4,00	10	21,3	21,3	100,0
	Total	47	100,0	100,0	

Digitalisering

DS_RECODE

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1,00	5	10,6	10,6	10,6
	2,00	22	46,8	46,8	57,4
	3,00	4	8,5	8,5	66,0
	4,00	9	19,1	19,1	85,1
	5,00	7	14,9	14,9	100,0
	Total	47	100,0	100,0	

Risico 1: Acties van personen – Perongeluk

RC1001_RECODE

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1,00	2	4,3	4,3	4,3
	2,00	16	34,0	34,0	38,3

	3,00	13	27,7	27,7	66,0
	4,00	14	29,8	29,8	95,7
	5,00	2	4,3	4,3	100,0
	Total	47	100,0	100,0	

Risico 2: Acties van personen – Opzettelijk

RC1002_RECODE

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1,00	4	8,5	8,5	8,5
	2,00	4	8,5	8,5	17,0
	3,00	12	25,5	25,5	42,6
	4,00	14	29,8	29,8	72,3
	5,00	13	27,7	27,7	100,0
	Total	47	100,0	100,0	

Risico 3: Acties van personen – Inaction

RC1003_RECODE

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1,00	8	17,0	17,0	17,0
	2,00	13	27,7	27,7	44,7
	3,00	20	42,6	42,6	87,2
	4,00	5	10,6	10,6	97,9
	5,00	1	2,1	2,1	100,0
	Total	47	100,0	100,0	

Risico 4: Falen van systemen en technologie – Hardware

RC2001_RECODE

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1,00	10	21,3	21,3	21,3
	2,00	17	36,2	36,2	57,4
	3,00	8	17,0	17,0	74,5
	4,00	10	21,3	21,3	95,7
	5,00	2	4,3	4,3	100,0
	Total	47	100,0	100,0	

Risico 5: Falen van systemen en technologie – Software

RC2002_RECODE

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1,00	3	6,4	6,4	6,4
	2,00	13	27,7	27,7	34,0
	3,00	9	19,1	19,1	53,2
	4,00	17	36,2	36,2	89,4
	5,00	5	10,6	10,6	100,0
	Total	47	100,0	100,0	

Risico 6: Falen van systemen en technologie – Systemen

RC2003_RECODE

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1,00	2	4,3	4,3	4,3
	2,00	13	27,7	27,7	31,9
	3,00	13	27,7	27,7	59,6
	4,00	16	34,0	34,0	93,6
	5,00	3	6,4	6,4	100,0
	Total	47	100,0	100,0	

Risico 7: Falen van interne processen – Procesontwerp of uitvoer

RC3001_RECODE

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1,00	2	4,3	4,3	4,3
	2,00	20	42,6	42,6	46,8
	3,00	15	31,9	31,9	78,7
	4,00	9	19,1	19,1	97,9
	5,00	1	2,1	2,1	100,0
	Total	47	100,0	100,0	

Risico 8: Falen van interne processen – Procesbesturing

RC3002_RECODE

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1,00	2	4,3	4,3	4,3
	2,00	15	31,9	31,9	36,2
	3,00	20	42,6	42,6	78,7
	4,00	9	19,1	19,1	97,9
	5,00	1	2,1	2,1	100,0
	Total	47	100,0	100,0	

Risico 9: Falen van interne processen – Ondersteunende processen

RC3003_RECODE

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1,00	4	8,5	8,5	8,5
	2,00	15	31,9	31,9	40,4
	3,00	20	42,6	42,6	83,0
	4,00	7	14,9	14,9	97,9
	5,00	1	2,1	2,1	100,0
	Total	47	100,0	100,0	

Risico 10: Externe gebeurtenissen – Rampen

RC4001_RECODE

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1,00	6	12,8	12,8	12,8
	2,00	15	31,9	31,9	44,7
	3,00	10	21,3	21,3	66,0
	4,00	14	29,8	29,8	95,7
	5,00	2	4,3	4,3	100,0
	Total	47	100,0	100,0	

Risico 11: Externe gebeurtenissen – Juridische problemen

RC4002_RECODE

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1,00	2	4,3	4,3	4,3
	2,00	14	29,8	29,8	34,0
	3,00	17	36,2	36,2	70,2
	4,00	12	25,5	25,5	95,7
	5,00	2	4,3	4,3	100,0
	Total	47	100,0	100,0	

Risico 12: Externe gebeurtenissen – Bedrijfsproblemen

RC4003_RECODE

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1,00	5	10,6	10,6	10,6
	2,00	12	25,5	25,5	36,2
	3,00	18	38,3	38,3	74,5
	4,00	12	25,5	25,5	100,0
	Total	47	100,0	100,0	

Risico 13: Externe gebeurtenissen – Afhankelijkheid van diensten

RC4004_RECODE

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2,00	8	17,0	17,0	17,0
	3,00	13	27,7	27,7	44,7
	4,00	23	48,9	48,9	93,6
	5,00	3	6,4	6,4	100,0
	Total	47	100,0	100,0	

7.5. Correlatietabel risico's

		Mate van digitalisering	Mate van procesvolwassenheid en genomen digitale weerbaarheidsmaatregelen
Risico 1 - Acties van personen: Perongeluk	Coëfficiënt	-.178	-.342*
	Significantie	.232	.019
Risico 2 – Acties van personen: Opzettelijk	Coëfficiënt	-.346*	-.156
	Significantie	.017	.294
Risico 3 – Acties van personen: Inaction	Coëfficiënt	-.451**	-.307*
	Significantie	.001	.036
Risico 4 – Falen van systemen en technologie: Hardware	Coëfficiënt	-.397**	-.253
	Significantie	.006	.086
Risico 5 – Falen van systemen en technologie: Software	Coëfficiënt	-.384**	-.451**
	Significantie	.008	.001
Risico 6 – Falen van systemen en technologie: Systemen	Coëfficiënt	-.134	-.271
	Significantie	.370	.065
Risico 7 – Falen van interne processen: Procesontwerp of uitvoer	Coëfficiënt	-.424**	-.411**
	Significantie	.003	.004
Risico 8 – Falen van interne processen: Procescontrols	Coëfficiënt	-.335*	-.322*
	Significantie	-.021	.027
Risico 9 – Falen van interne processen: Ondersteunende processen	Coëfficiënt	-.387**	-.387**
	Significantie	.007	.007
Risico 10 – Externe gebeurtenissen: Rampen	Coëfficiënt	-.474**	-.351*
	Significantie	.001	.016
Risico 11 – Externe gebeurtenissen: Juridische problemen	Coëfficiënt	-.184	-.336*
	Significantie	.217	.021

Risico 12 – Externe gebeurtenissen: Bedrijfsproblemen	Coëfficiënt	.017	-.011
	Significantie	.911	.941
Risico 13 – Externe gebeurtenissen: Afhankelijkheid van diensten	Coëfficiënt	.-112	-.165
	Significantie	.455	.269

* Correlatie is significant op 0.01 niveau

** Correlatie is significant op 0.05 niveau