Nr	Categorie	Risico	Verwachte periode van optreden	A
1	Verantwoordelijkheid	Gebrek aan sturing op informatiebeveiliging vanuit [redacted]		
2	Verantwoordelijkheid	[redacted]hun verantwoordelijkheid voor informatiebeveiliging niet.		
3	Verantwoordelijkheid	Onvoldoende aandacht voor beveiliging binnen projecten.		
4	Verantwoordelijkheid	Medewerkers handelen onvoldoende naar hetgeen van hen verwacht wordt.		
5	Continuïteit en betrouwbaarheid van systemen	Onvoldoende aandacht voor beveiliging bij softwareontwikkeling.		
6	Continuïteit en betrouwbaarheid van systemen	Toegang tot informatie wordt geblokkeerd.		
7	Continuïteit en betrouwbaarheid van systemen	Netwerkdiensten raken overbelast.		
8	Continuïteit en betrouwbaarheid van systemen	Aanvallen via systemen die niet in eigen beheer zijn.		
9	Continuïteit en betrouwbaarheid van systemen	Uitval van systemen door hardwarefouten.		
10	Continuïteit en betrouwbaarheid van systemen	Uitval van systemen door configuratiefouten.		
11	Continuïteit en betrouwbaarheid van systemen	Uitval van systemen door softwarefouten.		
12	Continuïteit en betrouwbaarheid van systemen	Fouten als gevolg van wijzigingen in andere systemen.		
13	Menselijk handelen	Gebruikersfouten.		
14	Menselijk handelen	Systemen worden niet gebruikt waarvoor ze bedoeld zijn.		
15	Menselijk handelen	Wegnemen van bedrijfsmiddelen.		
16	Menselijk handelen	Beleid wordt niet gevolgd door ontbreken van sancties.		
17	Menselijk handelen	Toelaten van externen in het pand of op het netwerk.		
18	Menselijk handelen	Verlies van mobiele apparatuur en opslagmedia.		
19	Menselijk handelen	Misbruik van andermans identiteit.		
20	Menselijk handelen	Misbruik van speciale bevoegdheden.		

21	Menselijk handelen	Onterecht hebben van rechten.		
22	Toegang tot informatie	Slecht wachtwoordgebruik.		
23	Toegang tot informatie	Onbeheerd achterlaten van werkplekken.		
24	Toegang tot informatie	Onduidelijkheid over classificatie en bevoegdheden.		
25	Toegang tot informatie	Informatie op systemen bij reparatie of verwijdering.		
26	Toegang tot informatie	Misbruik van kwetsbaarheden in applicaties of hardware.		
27	Toegang tot informatie	Misbruik van zwakheden in netwerkbeveiliging.		
28	Toegang tot informatie	Onvoldoende aandacht voor beveiliging bij uitbesteding van werkzaamheden.		
29	Toegang tot informatie	Informatie buiten de beschermde omgeving.		
30	Toegang tot informatie	Afluisterapparatuur.		
31	Uitwisselen en bewaren van informatie	Onveilig versturen van gevoelige informatie.		
32	Uitwisselen en bewaren van informatie	Versturen van gevoelige informatie naar onjuiste persoon.		
33	Uitwisselen en bewaren van informatie	Informatieverlies door verlopen van houdbaarheid van opslagwijze.		
34	Uitwisselen en bewaren van informatie	Foutieve informatie.		
35	Uitwisselen en bewaren van informatie	Misbruik van cryptografische sleutels en/of gebruik van zwakke algoritmen.		
36	Wet- en regelgeving	Wetgeving over informatie in de cloud.		
37	Wet- en regelgeving	Buitenlandse wetgeving bij het bezoeken van een land.		
38	Wet- en regelgeving	Wetgeving over het gebruik van cryptografie.		
39	Incidentafhandeling	Incidenten worden niet tijdig opgepakt.		
40	Incidentafhandeling	Informatie voor het aanpakken van incidenten ontbreekt.		
41	Incidentafhandeling	Herhaling van incidenten		
42	Fysieke beveiliging	Ongeautoriseerde fysieke toegang.		
43	Fysieke beveiliging	Brand.		
44	Fysieke beveiliging	Explosie.		
45	Fysieke beveiliging	Overstroming en wateroverlast.		
46	Fysieke beveiliging	Verontreiniging van de omgeving.		
47	Fysieke beveiliging	Uitval van facilitaire middelen (gas, water, electra, airco).		
48	Fysieke beveiliging	Vandalisme.		

49	Bedrijfscontinuïteit	Niet beschikbaar zijn van diensten van derden.		
50	Bedrijfscontinuïteit	Software wordt niet meer ondersteund door de uitgever.		
51	Bedrijfscontinuïteit	Kwijtraken van belangrijke kennis bij niet beschikbaar zijn van medewerkers.		

Corona-keten IV								Risico			Mitigatie
B	C	D	E	F	G	H	I	Kans	Impact	Risico-score	Lopende / genomen maatregel(en)
								1	4	4	
								3	4	12	
								3	4	12	
								2	3	6	Awareness kan verbeterd worden
								3	4	12	Met name actiever op sturen richting softwareleveranciers
								1	3	3	Kans is vrij klein, maar de impact (niet kunnen werken) is groot
								1	3	3	Veel Saas applicaties waarop impact is
								1	4	4	
								1	3	3	
								1	2	2	
								1	2	2	
										0	Verdient nadere toelichting
								1	2	2	
								3	2	6	
								3	2	6	
								1	1	1	
								2	3	6	Op decentrale locaties is de kans op onbevoegd toegang door externen wat groter
								3	1	3	
								1	4	4	
								1	3	3	

								4	3	12	
								1	2	2	Kans is vrijwel nihil vanwege policies
								4	3	12	
								4	2	8	
								1	2	2	Gecertificeerd proces voor afvoer apparatuur
								2	4	8	
								2	4	8	
								1	4	4	Interpretatie: Databeveiliging
								2	3	6	
								1	3	3	
								1	4	4	Zorgmail
								3	3	9	
								1	2	2	
										0	Verdient nadere toelichting
								1	3	3	
								3	4	12	
										0	Verdient nadere toelichting
										0	Verdient nadere toelichting
								1	3	3	
								1	1	1	
								1	3	3	
								1	3	3	Decentraal wat grotere kans
								1	4	4	
								1	4	4	
								1	4	4	
								1	3	3	
								1	4	4	
								1	2	2	

								1	4	4	
								1	2	2	
								2	4	8	

Hulp nodig