NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Doel: het bepalen van het inherente cyber risico (ICR). Dit als input voor de CSA.
De vragen en aanpak zijn gebaseerd op het FFIEC-raamwerk (zie https://www.ffiec.gov/cyberassessmenttool.htm).

	Categorie:	Vraag:	Risico-inschatting:			Uw inschatting: 1 (Hoog), 2 (Midden) of 3 (Laag)
Vraagnr			1 = Hoog	2 = Midden	3 = Laag	
1	**Algemeen**	Is uw organisatie aangewezen als Aanbieder van een Essentiele Dienst (AED) of als Andere Aangewezen Vitale Aanbieder (AAVA)? Zie voetnoot a) voor nadere toelichting.	Organisatie is AED of AAVA	Wel vitale aanbieder, maar niet als zodanig aangemerkt door de vakdepartementen	Nee	1
2		Werkt uw organisatie samen met organisaties die een rol hebben in de vitale processen van de Nederlandse vitale infrastructuur?	Er is samenwerking w.o. binnen processen van de vitale infrastructuur	Er is samenwerking , echter niet binnen de processen die onderdeel zijn van de vitale infrastructuur	Geen samenwerking met organisaties die een rol hebben in de processen van de vitale infrastructuur	2
3	**Organisatie karakteristieken**	Is binnen uw organisatie sprake van een re(her)organisatie?	Grootschalig - forse impact - directie wisselingen	Beperkte - met gemiddelde impact	Geen	3
4		Overweegt uw organisatie een overname of is uw organisatie zelf een (mogelijke) kandidaat voor overname?	Ja, besluitvorming in gevorderd stadium of integratie loopt momenteel	Verkenning is uitgevoerd	Geen	3
5		Is uw organisatie afhankelijk van internationale handel?	Internationaal actief (buiten de EU)	Alleen actief in de EU	Nee, alleen actief in NL	2
6		Wat is het aantal vaste werknemers in FTE's (inclusief ICT) en externen/inhuur binnen uw organisatie?	> MKB	MKB (<250 werknemers)	ZZP en KB (Klein Bedrijf - < 50 werknemers)	2
7		In welke mate is uw bedrijfsvoering afhankelijk van ICT?	Uitval van ICT heeft direct klantenimpact	uw organisatie kan een paar dagen functioneren zonder klantenimpact	uw organisatie kan zonder ICT functioneren, weinig impact voor klanten of de dienstverlening	2
8		Wat is binnen uw organisatie het verloop onder de vaste ICT-werknemers?	> 10% van het ICT-personeel per jaar wordt vervangen	5 - 10% van het ICT-personeel per jaar wordt vervangen	5% van het ICT-personeel per jaar vervangen	2
9		Welke percentage van de ICT-infrastructuur van uw organisatie wordt maandelijks geraakt door wijzigingen?	> 20%	10-20%	0 -10%	1
10		Wordt de afhankelijkheid van ICT-voorziening voor uw organisatie groter bijv. als gevolg van verdergaande digitalisering / automatisering?	Ja - diverse trajecten lopen momenteel	op termijn verdergaande digitalisering	Nee	1
11	**Technologie & derde partijen**	Maakt uw organisatie gebruik van onbeveiligde externe verbindingen voor het uitwisselen van data zoals het gebruik van FTP (file transfer protocol) en e-mail?	1 of meer onbeveiligde verbindingen	NVT	Geen onbeveiligde verbindingen	3
12		Zijn er intern draaiende kritische applicaties/technologieën (incl. spreadsheets en databases, etc.)?	Meer dan de helft interne applicaties / technologieën	Beperkt (minder dan de helft) aantal interne applicaties / technologieën	Geen interne applicaties/technologieën	2
13		Wordt binnen uw organisatie gebruik gemaakt van hardware en/of software, die End of Life / Out of Support is.?	Meer dan 10% van de totale populatie hardware/software is End-of-Life/End-of-Support	Minder dan 10% van de totale populatie hardware/software is End-of-Life/End-of-Support	Geen verouderde systemen	2
14		Hebben derde partijen toegang tot de interne systemen van uw organisatie?	1 of meer derde partijen met toegang tot interne systemen	NVT	Geen derde partijen, individuen met toegang tot interne systemen	3
15		Zijn er derde partijen die bedrijf kritische informatie van uw organisatie bewaren en/of verwerken?	1 of meer partijen die kritische activiteiten ondersteunen	NVT	Geen derde partijen die kritische activiteiten ondersteunen	3
16	**Online aangeboden producten of diensten**	Kunnen de door uw organisatie aangeboden producten of diensten online betaald worden?	Online betalingen	Online betalingen via PrePay (zoals iDeal /PayPal) en/of After Pay (zoals Credit Card)	Geen online betalingen	2
17		Biedt uw organisatie financiële producten of diensten aan zoals verzekeringspolissen, hypotheken, sparen ...?	Diverse diensten (>= 3)	Beperkt aantal (<3) financiële producten of diensten	Geen financiële diensten	2
18		Accepteert uw organisatie bitcoins of andere innovatieve betaalproducten (crypto?	Meerdere innovatieve betaalproducten	Bitcoin of ander innovatief betaalproduct	Geen gebruik van innovatieve betaalproducten	2
19		Is uw organisatie actief op het gebied van online gegevensverwerking? Denk onder meer aan verwerking van gegevens m.b.t. intellectueel eigendom, gegevens m.b.t. videobewaking van gevangenissen, banken, bedrijven, etc.	Verwerking van beeldmateriaal door derde partijen buiten uw organisatie	Verwerking van beeldmateriaal binnen uw organisatie	Geen online verwerking van beeldmateriaal	2
20		Kunnen vanuit uw organisatie onderdelen van de vitale infrastructuur (PLC/SCADA systemen) op afstand/online worden bediend/onderhouden? Denk aan pompen/kleppen van een drinkwaterzuiveringsinstallatie, gasmengstations, sluizen/gemalen, etc	Er wordt gebruik gemaakt van remote beheer tools welke toegankelijk zijn via internet (2-weg informatie uitwisseling: ontvangen / verzenden)	Er wordt gebruik gemaakt van remote beheer tools welke beperkt toegankelijk zijn via internet (alleen voor het ontvangen van info)	Geen online remote beheer/onderhoud	2
21	**Externe cyberdreigingen**	Is uw organisatie (inherent) doelwit van cyberaanvallen (uw organisatie wordt bijvoorbeeld genoemd in hackersfora)?	Specifiek geschreven malware bestaat	Organisatie wordt genoemd op hackersfora	Geen (geslaagde) pogingen tot cyberaanvallen	2
22		Heeft uw organisatie last van (DDoS) aanvallen op haar eigen infrastructuur of die van haar partners?	Enkele (DDoS)-aanvallen per maand	Een beperkt aantal aanvallen per jaar	Nee	1
23		Heeft uw organisatie datalekken gehad als gevolg van cyberaanvallen of social engineering of verlies van assets?	Datalekken met bijzondere persoonsgegevens	Datalekken met algemene persoonsgegevens	Nee	1
24		Heeft uw organisatie last (te maken gehad met) van APT (Advanced Persistent Threats) binnen haar eigen infrastructuur?	APT hebben geleid tot een groot verlies van bedrijfsgevoelige gegevens	APT hebben geleid tot een beperkt verlies van bedrijfsgevoelige gegevens	Nee	3
					Totaal inherent cyber risk	**49**

Risicoscore	Hoog risico

	maximum score	72
	minimum score	24
	L-risico indien totaal >	52
	M-risico indien totaal tussen	43 - 52
	H-risico indien totaal <	43
	H-risico indien aangewezen als vitale aanbieder (vraag 1 = H en/of vraag 2 = H)	

Voetnoot a)
Hier vindt u meer informatie over vitale aanbieders: https://nctv.nl/Wbni/vitale-aanbieders.aspx. De meeste vitale aanbieders worden in of op grond van het Besluit beveiliging netwerk- en informatiesystemen (Bbni) aangewezen als aanbieder van een essentiële dienst (AED) of als aanbieder van een andere dienst waarvan de continuïteit van vitaal belang is voor de Nederlandse samenleving ('andere aangewezen vitale aanbieder', AAVA).