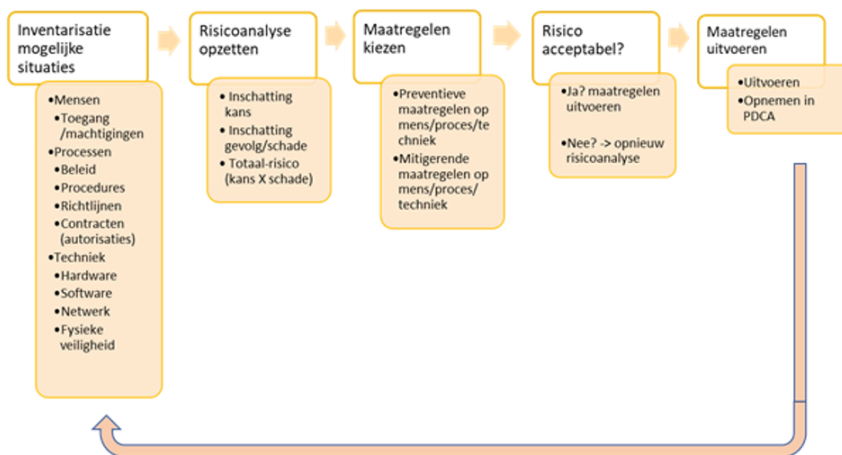




Balans

Een belangrijke stap bij informatieveiligheid, is het kijken waar in jouw organisatie de grootste risico's voorkomen. En daarbij vervolgens de maatregelen kiezen die passen bij die risico's. Dit samen heet risicomanagement. We nemen je hieronder mee in een eenvoudige uitleg van de stappen die je daarbij doorloopt. Deze stappen doorloop je als bestuurder niet allemaal zelf, maar je geeft er wel opdracht toe en controleert of de uitvoering ervan en de PDCA cyclus plaatsvindt. Omdat jij als bestuurder eindverantwoordelijke bent, heb je een belangrijke rol in het bespreken waar de grootste risico's in jouw organisatie voorkomen en besluiten of de balans tussen mate van risico, mate van impact en uitvoerbaarheid van de maatregelen aanvaardbaar is.

Schema met stappen binnen risicomanagement:



Je inventariseert eerst de mogelijke situaties in je organisatie. Denk daarbij aan elementen horend bij mensen, processen en techniek. Vervolgens maak je een risicoanalyse. Dat wil zeggen dat je inschat wat de kans is van een incident en wat de schade en impact is van een dergelijk incident. Dit leidt vervolgens tot een risicomatrix. Hieronder een vereenvoudigd voorbeeld van een risicomatrix:

		Impact				
		niet merkbaar	klein	gemiddeld	groot	desastreus
Kans	dagelijks	gemiddeld	hoog	hoog	kritiek	kritiek
	wekelijks	gemiddeld	gemiddeld	hoog	kritiek	kritiek
	maandelijks	laag	gemiddeld	hoog	hoog	kritiek
	jaarlijks	laag	gemiddeld	gemiddeld	hoog	hoog
	> jaarlijks	laag	laag	gemiddeld	gemiddeld	hoog

Bron: NCSC

Na de risicoanalyse is er zicht op de belangrijkste risico's voor jouw organisatie. Op basis daarvan kies je maatregelen die daarbij passen. Dit zijn zowel preventieve als mitigerende maatregelen. Bekijk de set van maatregelen in zijn geheel. Is het geheel werkbaar en het risico dat je loopt aanvaardbaar?

Het gaat daarbij dus om de balans tussen het geheel aan mate van risico, mate van impact en uitvoerbaarheid van maatregelen. Als het antwoord ja is, dan ga je over tot uitvoering en neem je de maatregelen op in de PDCA cyclus voor informatieveiligheid. Dit hele proces is een cyclus en gaat dus onverminderd door om bij te blijven bij de snelle ontwikkelingen in de wereld van de cybersecurity.