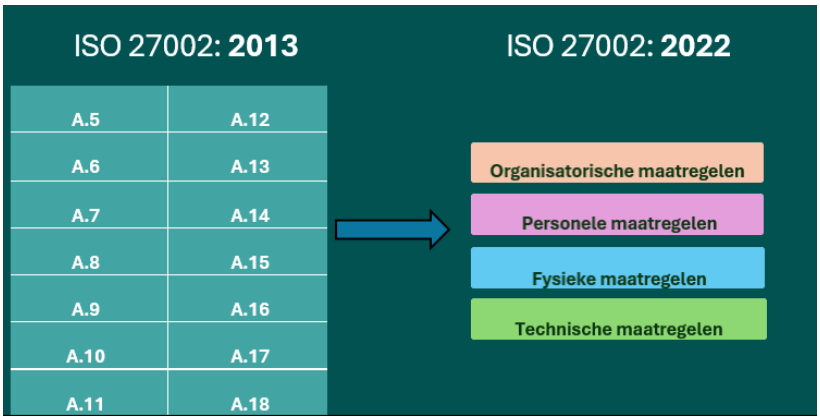
BIJLAGE 1. Duiding bij de Vragenlijst

De basis van informatiebeveiliging

Eigen vragenlijsten uitvinden heeft weinig zin en leidt tot inconsistenties, daarom is de VTC er voorstander van om vragenlijsten te baseren op basis van de **ISO27001/27002** (waarbij we uitdrukkelijk stellen dat vooralsnog geen formele certificatie vereist wordt).

De verhouding tussen deze twee internationale standaarden wordt uitgedrukt d.m.v. onderstaande figuur:

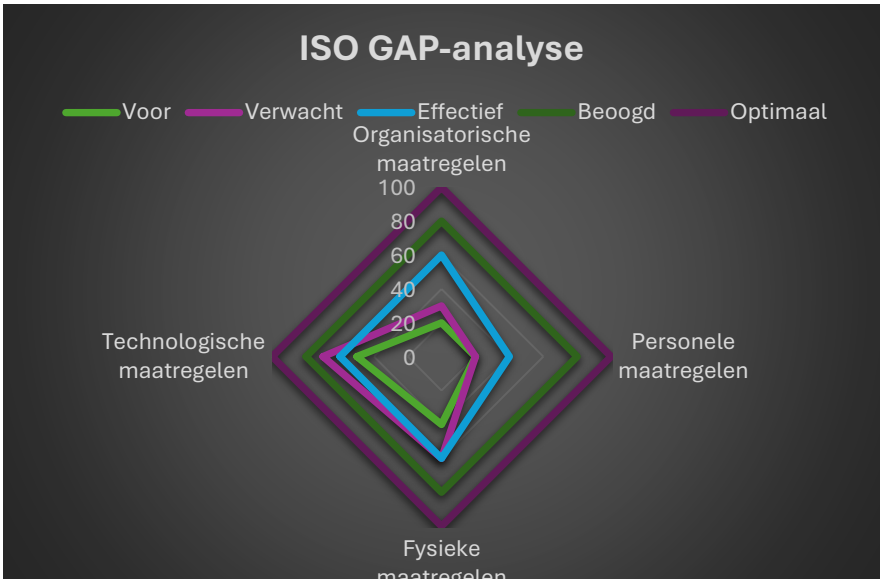
In deze standaarden wordt gekeken naar de verschillende dimensies van informatiebeveiliging. We tonen eerst de ISO27001:2013 omdat deze een eenvoudig overzicht geeft en vervolgens de structuur van de nieuwere ISO27001:2022 omdat deze herverdeelde in 4 duidelijke categorieën:



Context en Meten is weten

De lijst van organisatorische, persoons-, fysieke en technische maatregelen domweg kopiëren leidt geenszins tot de juiste maatregelen. De verwerkingsverantwoordelijke en de verwerker moeten deze per verwerking steeds in "context" van de verwerking en haar risicoprofiel interpreteren. Niettemin geven we hierna een vragenlijst weer die men als handvest kan gebruiken (maar dus dient te interpreteren per verwerking en bv. in geval van cloudservices dient te evalueren rekening houdende met bestaande VTC-adviezen). Dus bv. niet (met referentie aan advies VTC/A/2022/02) "Beschermt u data in motion?". Maar wel, en in geval van gegevens met evt. zware negatieve impact, past u "TLS en sterke authenticatie toe?".

Eens de leverancier de vragenlijst heeft ingevuld, kan overgaan worden tot "weging" tussen het "vereiste niveau" en het "niveau dat de leverancier effectief kan leveren". Dit moet dan bv. het volgende type diagram kunnen leveren en duiden of er onaanvaardbare gebreken, belangrijke gebreken of beperkte of geen gebreken zijn voor wat de geplande of bestaande leverancier-verwerker betreft.



Te beschouwen dimensies

Vaak wordt deze lijst van maatregelen als een "platte lijst" doorlopen wat niet correct is. De verwerking is immers gebaseerd op meerdere diensten/producten. We onderscheiden minstens de volgende niveaus die meegenomen moeten worden bij de evaluatie van een leverancier-verwerker:

- de **applicatie op zich**: heeft deze de nodige beveiliging op niveau van de gewone **gebruikers**?
- de **beheersapplicatie** die uw eigen beheerders krijgen: werden de nodige beveiligingsmaatregelen toegepast?
- de **applicatie-of platformlaag** die de dienstenleverancier u biedt: werden de nodige beveiligingsmaatregelen toegepast?
- de **infrastructuur** (bv. cloud) die uw leverancier gebruikt: werden de nodige beveiligingsmaatregelen toegepast?
- de **ontwikkel- en deploymentsystemen** die uw leverancier gebruikt: bieden deze de nodige beveiliging?
- de **beheerssystemen** die uw **leverancier** gebruikt: bieden deze de nodige zekerheden?
- de **security(monitoring) systemen** die het geheel moeten beschermen: voldoen deze?