Notities Security Essentials week 4

### De vier lagen

1. Mensen
2. Bedrijfsprocessen
3. Applicatie/data/info
4. Infrastructuur

De bedrijfsprocessen dragen bij aan de missie, visie, strategie en doelstellingen van een organisatie daarnaast moet een organisatie zich ook houden aan de wet en regelgeving.

### Assets en informatie

* Iedere Asset heeft afhankelijkheden met andere Assets. Al die afhankelijkheden zorgen er voor dat informatie ontstaat en bewerkt, verstuurd, opgeslagen of verwijderd wordt.
* Dit ontstaan, versturen, opslaan, wijzigen of verwijderen gebeurt binnen de bedrijfsprocessen. En dat is ook de plek waar het fout kan gaan, binnen de bedrijfsprocessen en bij de betrokken Assets.
* Als je al die afhankelijkheden analyseert, dan kom je vanzelf bij alle informatie die je wilt beveiligen en die zet je in de Informatie- en datalaag.

### Wat is een bedrijfsproces

Een bedrijfsproces kan worden gedefinieerd als een flow of aaneensluiting van verschillende activiteiten welke bedrijfsdoelstellingen ondersteunen en welke wordt gefaciliteerd door data en of andere middelen

* Primair proces
* Ondersteunend proces

### Standaarden

Een standaard is een afspraak, informatie of een proces. Als computersystemen gegevens uitwisselen dan moeten zij die afspraken of processen hanteren doen ze dit niet? Kunnen er fouten ontstaan, het systeem kan worden misbruikt of wordt verkeerde dat overgenomen. Voorbeelden van standaarden zijn:

* COBIT
* ISO 27000 series
* NIST
* NEN 7510

**COBIT** staat voor **Control Objectives for Information and Related Technology** en is een raamwerk voor managers voor het beheer van informatie technology . Het is ontworp als een hulp middel om de kloof te overbruggen tussen technische problemen, risico's en controle vereisten

**ISO 27005**

* Norm voor risicomanagement
* H8 – Information security risk assessment
  + Risk management is een belangrijk proces uit de ISO 27001
* H8.2.2 – Assets identificeren etc.
  + Alles dat waarde heeft voor een organisatie
  + Vastleggen op voldoende niveau
  + Vindt de Asset Eigenaar!

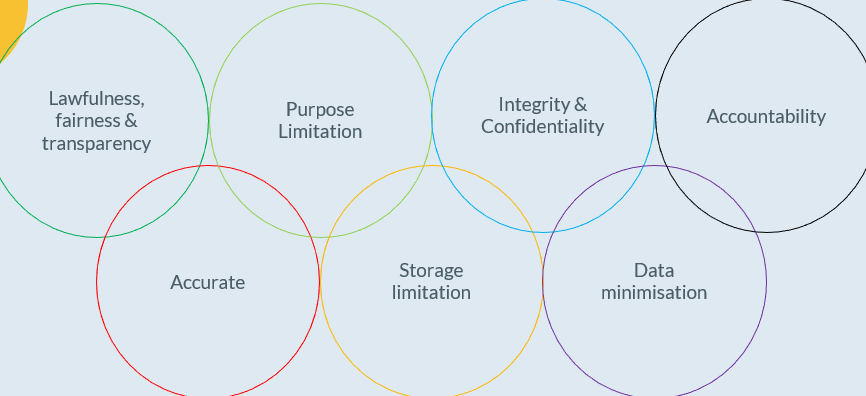
### Certificering

Met een certificaat wordt er aangetoond dat een organisatie efficiënt en veilig werkt dat de werkzaamheden en de werkprocessen beheerst worden en dat duurzaamheid nastreeft.

* Certificeren om vertrouwen tussen organisaties te vergroten
* Certificering belangrijk bij informatiebeveiliging
* ISO-certificeringen zijn mogelijk
* Professionals kunnen zich ook certificeren
  + CISM
  + CISA
  + CISSP
  + Etc.

## Wet en regel geving

‘De Algemene Verordening Gegevensbescherming (AVG)’ en in het buitenland ‘General Data Protection Regulation (GDPR)’. Elk bedrijf binnen europa dient zich hieraan te houden maar ook bedrijven vanuit het buitenland die met europese bedrijven samenwerken dienen zich aan de AVG te houden .Binnen de AVG staan 7 beginselen centraal. Door deze beginselen zorgt de AVG ervoor dat de privacyrechten van mensen (data subjects) worden uitgebreid en versterkt. Organisaties die gegevens verwerken moeten daarom duidelijk aangeven wat er met de data gedaan gaat worden. Dit wordt tegenwoordig veel gedaan om niet alleen de mensen in te lichten waar hun gegevens naar toe gaan, maar ook om een boete te voorkomen. Denk bijvoorbeeld aan websites die om cookies vragen.



### De AP

* Autoriteit Persoonsgegevens (AP)
* Toezichthouder op de naleving van de wettelijke regels voor bescherming van persoonsgegevens.
* Als de AP een overtreding constateert, kan er een boete opgelegd worden tot 20 miljoen euro of 4% van de wereldwijde jaaromzet van de organisatie.

### De Wet computercriminaliteit

Wat is computercriminaliteit?

* Computercriminaliteit is op twee manieren te definiëren:
* 1: Misdrijven waarbij computers of netwerken een rol spelen. (Breed)
* 2: Misdrijven die niet zonder tussenkomst of gebruik van computers of netwerken gepleegd kunnen worden.
* Meer hierover in het semester over cybercrime. Maar je moet wel op de hoogte zijn dat deze wet bestaat.