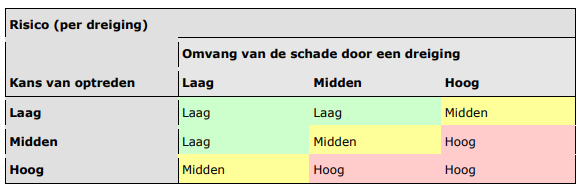
**Risicoanalyse/Beveiligingsanalyse**

De risicoanalyse heeft tot doel per project zwakheden in de beveiliging of opzet van de software te vinden en te onderkennen. (Bron: Edhub, Grip op Secure Software, 4.3, alinea 1)

Het eindresultaat van de risicoanalyse is een lijst met dreigingen die relevant worden geacht voor de IT-middelen binnen de scope en inzicht in de ernst van deze dreigingen. Deze lijst is het uitgangspunt voor het bepalen welke standaard beveiligingseisen + maatregelen toepasselijk zijn, en of er mogelijk nog een restrisico bestaat. (Bron: Edhub, Grip op Secure Software, 4.3, alinea 16)

Kwalificering risico’s******

**Rest-risico’s:**

Indien er sprake is van een restrisico dient dit te worden gemeld aan de opdrachtgever, die schriftelijk het restrisico moet accepteren namens het betreffende bedrijfsonderdeel.  
(Bron: Edhub, Grip op Secure Software, 4.3, alinea 16)

Deze schriftelijke ondertekening is te vinden in: Restrisicos\_Ondertekening.pdf

**Einde Risico-analyse**

***\*Spiekblaadje: voorkomt…***

*\*uitwerking risicoanalyse hieronder\**

*De naam STRIDE is een afkorting van de namen van zes categorieën aan dreigingen, namelijk:*

* *Spoofing (misbruik van de gebruikersidentiteit, namelijk zich als een ander voordoen);*
* *Tampering (schending van de Integriteit);*
* *Repudiation (weerlegbaarheid);*
* *Information disclosure (schending van de privacy of het lekken van data);*
* *Denial of Service (DoS) (onbeschikbaarheid);*
* *Elevation of privilege (misbruik van bevoegdheden)*