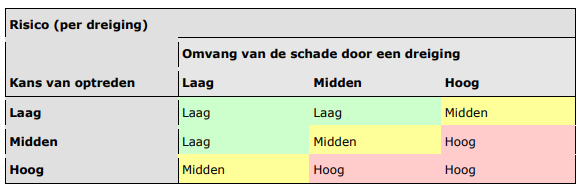
**Risicoanalyse/Beveiligingsanalyse (Met arjen overleggen)**

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)

Kwalifirecing risicos******

Het eindresultaat van deze 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, of aanvullende maatregelen nodig zijn en om vast te stellen of er mogelijk nog een restrisico bestaat. (Bron: Edhub, Grip op Secure Software, 4.3, alinea 16)

Het resultaat van de risicoanalyse moet aangeven:

* Welke beveiligingseisen relevant zijn voor de software, uit te splitsen naar het inrichten van preventieve, detectieve, correctieve en repressieve beveiligingsmaatregelen.
* Welke defecten en fouten leiden tot welke beveiligingsrisico’s.
* Waar in de levenscyclus beveiligingseisen moeten worden getest en of getoetst op defecten en fouten
* Welke artefacten moeten worden getest en getoetst.
* Welke testhulpmiddelen en testtechnieken moeten worden gebruikt.
* Welke restrisico’s blijven openstaan.  
  (Bron: Edhub, Grip op Secure Software, 4.3, Een-na-laatste Alinea)

**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

***Inschatting van dreigingen via STRIDE***

*\*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)*

*\*Een Hulpmiddel met daarin gedetailleerde uitleg over de maatregelen (uitgebracht 2015):* [*https://tiny.cc/SecureWebDevInJava*](https://tiny.cc/SecureWebDevInJava) *Hierbij te aanraden hoofdstukken + koppen die van belang kunnen zijn in het product:*

1. *Webapplication Security Basics*
   * *HTTP Security Considerations*
   * *Anti Patterns and Weaknesses*
   * *Security Controls and Positive Patters*
   * *Input Validation*
2. *Authentication and Session-Management*
   * *Registration of users*
     1. *Preventing Automated Registration*
   * *Secure Cookie Properties*
   * *Credential Security*
     1. *forget password workflow (optioneel. Waarschijnlijk niet nodig bij de eindopdracht)*
   * *Username Harvesting*
   * *Brute Force Attacks*
   * *Remember Me Feature – its unsave*
   * *Summary*
3. *Acces Control (Beoordelen of dit nodig is)*
4. *Cross-site Scripting Defense*
   * *Content Spoofing*
   * *Defending Against Xss*
   * *Resources Against:*
     1. *Output Encoding*
     2. *HTML Sanitization*
     3. *JavaScript Librarys*
   * *Summary*
5. *Cross-site Request Forgery and Clickjacking (Beoordelen of dit nodig is)*
6. *Protecting Sentsitive Data – alle tussenkoppen*
7. *SQL Injection + Other Injection Attacks*
   * *What is SQL Injection*
   * *Other SQL Injection Examples*
   * *Defense in Depth*
   * *Input Validation and Type Security*
   * *Reducing the Impact of SQL injection*
8. *Safe File Upload + File I/O*
   * *Antipatterns and Designflaws*
   * *File Upload Sequrity*
   * *Patterns of Attack*
   * *Summary*
   * *Resources (beoordelen of het bruikbaar/nodig is)*
9. *Logging, Error Handling and Intrafusion Detection*
   * *Logging Basics: What to log*
   * *Logging Frameworks for sequrity*
   * *Safe Error Handling*
   * *App Layer infusion detection*
   * *Summary*
10. *Not chapter 10. Chapter A: Resources*
    * *Secure Coding Librarys*

*Hier kom je er gauw achter dat Security een vak op zich is. Al met al beoordelen welke mogelijkheden haalbaar zijn voor het project; en hebben we daarbij keurige een “Handleiding” in hoe we dit moeten doen.\**

***Kwalificering van de risico’s:***