

## **Definitiestudie**

Met een haalbaarheidsstudie en systeemanalyse probeert men antwoorden te vinden op de volgende vragen: (waarom, hoe en wat het informatiesysteem gaat doen) (Edhub, Informatiesystemen, 12.1, alinea 2). Het doel van de definitiestudie is dan ook om te kijken of het te maken informatiesysteem er redelijkerwijs kan komen.

De haalbaarheidsstudie is het startpunt voor een project dat daadwerkelijk het systeem gaat maken. Tijdens de start van een project om een nieuw informatiesysteem te creëren is het verstandig om ook te kijken naar de mogelijke risico's ervan. Risicomanagement maakt dan ook deel uit van de haalbaarheidsstudie. Immers, met veel risico's komt de haalbaarheid in het geding (Edhub, Informatiesystemen, 12.1, alinea 3).

## **Haalbaarheidsstudie**

De haalbaarheidsstudie heeft als eerste stap het onderzoeken of er wel een informatiesysteem gemaakt moet worden als oplossing voor het gesignaleerde probleem.

Het toetsen op de haalbaarheid gebeurt drievoudig, waarbij gekeken wordt of het informatiesysteem:

- Technisch haalbaar is;
- Economisch haalbaar is;
- Operationeel en organiek haalbaar is (Edhub, Informatiesystemen, 12.2, alinea 2).

### ***Technische Haalbaarheid:***

*\*uitwerking haalbaarheidsstudie hieronder\**

*Technisch haalbaar betekent dat de technieken die gebruikt gaan worden bestaan of kunnen worden gemaakt. \*In de Eindopdracht.pdf staan de (meeste) technische eisen. De nieuwere eisen worden duidelijk na het gesprek met Arjen Wiersma.\**

- *Mogelijkheid uploaden van mp3-bestand.*
- *Mogelijkheid andere type audiobestanden te uploaden: eg: .wav .wave . ogg.*
- *Mogelijkheid omzetten van .xxx naar mp3-bestand.*
- *Mogelijkheid omzetten van .xxx naar mp3-bestand.*
- *Mogelijkheid omzetten van .xxx naar mp3-bestand.*

*Per technisch aspect aangeven wel/niet haalbaar bijv: "Haalbaar want: er bestaat een Spring Booth Library voor het behalen van (de ontwikkeling voor) deze functionaliteit."*

### ***Economische Haalbaarheid:***

*\*uitwerking haalbaarheidsstudie hieronder\**

Economisch haalbaar betekent dat de opbrengsten van een informatiesysteem meer zijn dan de kosten en de inspanning. De opbrengsten van zo'n informatiesysteem zijn echter niet alleen financieel. De baten kunnen ook op menselijk of ecologisch vlak liggen. Het is vaak lastiger om deze

baten goed zichtbaar te maken in de haalbaarheidsstudie. ([Edhub, Informatiesyste-men, 12.2, alinea 5](#)).

### **Operationele en organiek haalbaarheid:**

*\*uitwerking haalbaarheidsstudie hieronder\**

### **Systeemanalyse**

In de systeemanalyse probeert men de business requirements van het te maken systeem helder te krijgen. ([Edhub, Informatiesyste-men, 12.3, alinea 1](#)).

### **Functionele requirements:**

*\*uitwerking systeemanalyse hieronder\**

### **Niet-functionele requirements:**

*\* uitwerking systeemanalyse hieronder \**

### **Risicoanalyse**

De risicoanalyse heeft tot doel per project zwakheden in de beveiliging of de opzet van de software te vinden en te onderkennen.

### **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> Hierbij te aanraden hoofdstukken + koppen om door te nemen:

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*
      - a. *Preventing Automated Registration*
    - *Secure Cookie Properties*
    - *Credential Security*
      - a. *forget password workflow (optioneel. Waarschijnlijk niet nodig bij de eindopdracht)*
    - *Username Harvesting*
    - *Brute Force Attacks*
    - *Remember Me Feature – its unsave*
    - *Summary*
  3. *Access Control (Beoordelen of dit nodig is)*
  4. *Cross-site Scripting Defense*
    - *Content Spoofing*
    - *Defending Against Xss*
    - *Resources Against:*
      - a. *Output Encoding*
      - b. *HTML Sanitization*
      - c. *JavaScript Libraries*
    - *Summary*
  5. *Cross-site Request Forgery and Clickjacking (Beoordelen of dit nodig is)*
  6. *Protecting Sensitive 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 Security*
    - *Patterns of Attack*
    - *Summary*
    - *Resources (beoordelen of het bruikbaar/nodig is)*
  9. *Logging, Error Handling and Intrusion Detection*
    - *Logging Basics: What to log*
    - *Logging Frameworks for security*
    - *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:**

Risico (per dreiging)			
Kans van optreden	Omvang van de schade door een dreiging		
	Laag	Midden	Hoog
Laag	Laag	Laag	Midden
Midden	Laag	Midden	Hoog
Hoog	Midden	Hoog	Hoog