### Projekt constraints i relation til projektledelse

I relation til projektledelse er det vigtigt at indtænke de fire forskellige projekt constraints:

* Kvalitet (Quality)
* Tid (Time)
* Økonomi (Economy)
* Mål (Goals)

idet alle fire aspekter influerer hinanden. Derfor bør der være nogle overvejelser og forventnings-afstemninger med key stakeholder forud for projektets start – hvad vægtes højest? Hvad er fastlåst?

Og hvad er målet?

I vores projekt er det tidsmæssige aspekt fastlåst, idet projektperioden ikke er til forhandling. Det er noget, der kan komme til at have indflydelse på kvaliteten af det færdige system. Hvis ikke alle kravsspecifikationer er opfyldt til projektets deadline, er målet ikke nået. Derfor kan det være nødvendigt at slække på kvaliteten, for at nå målet.

Hvad angår økonomistyringen, er det ikke noget, vi som projektgruppe har nogen indflydelse på og vi tænker derfor ikke særlig meget over det. Key stakeholder har stillet lokaler og personale til rådighed gennem hele processen, og kravspecifikationerne er låst (kravsspecifikationerne i casen skal være opfyldt). Vores egne timer skal ikke finansieres, og tæller derfor ikke som en del af det økonomiske regnskab.

Projektgruppens ambitioner for det færdige produkt er at levere et system af høj kvalitet. Vi er opmærksomme på, at tiden kan volde os problemer, og tænker derfor meget i genbrug af kode, komponenter og gode designpatterns. Afgrænsninger ift. projektet er også indtænkt som en faktor, der kan give mere tid til vores tilvalg, og derved være med til at højne kvaliteten af det færdige produkt.

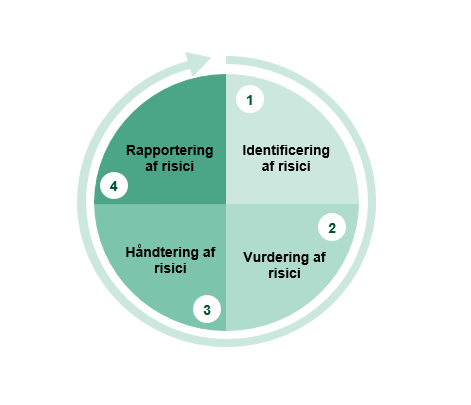
### Organisatoriske aspekter i relation til IT-projekter.

I relation til IT-projekter i en organisation er der flere centrale punkter at tage højde for. I det

følgende vil vi tage udgangspunkt i risikostyring og forandringsledelse.

* **Risikostyring**

Risikostyring i en virksomhed består af 4 søjler.



Billede 1: Risikostyrings 4 søjler[[1]](#footnote-1).

Først identificeres eventuelle risici. Dernæst vurderes de fundne risici ud fra sandsynlighed og konsekvens. Så håndteres de fundne risici ved at finde de bedst mulige strategier, til effektivt at håndtere disse risici og reducere risikoen for at de sker. Herfra undersøges der løbende, om de fundne risicis konsekvens eller sandsynlighed ændrer sig – hvis dette er tilfældet, revurderes ricisiens og dens håndtering.

At identificere risici og rangere disse efter deres konsekvens og sandsynlighed, kan gøres som matematisk formel:

Dette visualiseres ofte i en matrix, baseret på udregningen af formel ”Risikoa”:

Et billede, der indeholder tekst, skærmbillede, linje/række, Font/skrifttype

Automatisk genereret beskrivelse

Billede 2: Risiko map der inddeler fundne risici i fire risikogrupper ud fra deres konsekvens og sandsynlighed

I relation til vores system er der flere forskellige risici, som skal tages i betrækning. Følgende er fundet:

|  |  |  |  |
| --- | --- | --- | --- |
| Risiko | Sandsynlighed (1 – 10) | Konsekvens (1 – 10) | Risiko(a) |
| Brand | 2 | 8 |  |
| Tyveri | 3 | 8 |  |
| Brugerfejl | 5 | 3 |  |
| Uautoriseret adgang | 4 | 5 |  |
| Vandskade | 1 | 8 |  |

*Her opgøres sandsynlighed fra 1 til 10, hvor 10 er det mest sandsynlige. Ligeledes inddeles konsekvens fra 1 til 10, hvor 10 har størst konsekvens.*

Ud fra overstående identificeres to risici med en høj risikoværdi. Det er hhv. Tyveri (risikoværdi på 24) og Uautoriseret adgang (risikoværdi på 20). For at imødegå disse kan flere værktøjer tages i brug.

I forhold til tyveri kan systemet designes til at sænke konsekvensen ved ofte at tage backup, som gemmes på en anden lokation. Derved sænkes konsekvensen.

I forhold til uautoriseret adgang til systemet menes der, at en person, der ikke er tilknyttet skolen, kan få adgang til systemet og booking af lokaler. Dette kan imødegås på flere måder. Vi har blandt andet designet systemet til, at man skal have en aktiv e-mail tilhørende institutionen for at kunne booke et lokale. Derudover kunne man også indtænke, at der bliver sendt en bekræftelsesmail til mailadressen, der anvendes til bookingen. Herved tages der højde for, at en brugers e-mail kan misbruges af en anden person. Det udelukker ikke sandsynligheden for at det sker, men ejeren af den misbrugtes e-mail bliver gjort opmærksom på det, og kan handle på det.

1. Kilde: https://oes.dk/it-og-oekonomistyring/risikostyring/ [↑](#footnote-ref-1)