Enterprise Software Platforms

Case Studie

s67-3

2021

Inhoud

[1. Eerste meeting 3](#_Toc65058613)

[1.1 Vragen om de case duidelijker te krijgen 3](#_Toc65058614)

[1.2 Resultaten van de brainstorming 3](#_Toc65058615)

[1.3 Vereiste kennisvragen 3](#_Toc65058616)

[2. Approach 4](#_Toc65058617)

[3. Results 5](#_Toc65058618)

[3.1 Findings group 1 (Joost van Herwaarden & Sjoerd Halmans) 5](#_Toc65058619)

[Vraag 1 - Welke bekende frameworks zijn er geschikt voor Enterprise Software? 5](#_Toc65058620)

[Vraag 2 - Kan dit veilig in de Cloud? 6](#_Toc65058621)

[Vraag 3 - Op welke manier kunnen we de veiligheid van data van de bank waarborgen? 6](#_Toc65058622)

[Vraag 4 - Welke team organisatie omgevingen zijn gangbaar voor een groot team met veel processen? 8](#_Toc65058623)

[3.2 Findings group 2 (Nicky Janse & Tom van Kaathoven) 9](#_Toc65058624)

[Vraag 1 - Welke bekende frameworks zijn er geschikt voor Enterprise Software? 9](#_Toc65058625)

[Vraag 2 - Kan dit veilig in de Cloud? 10](#_Toc65058626)

[Vraag 3 - Op welke manier kunnen we de veiligheid van data van de bank waarborgen? 10](#_Toc65058627)

[Vraag 4 - Welke team organisatie omgevingen zijn gangbaar voor een groot team met veel processen? 11](#_Toc65058628)

[3.3 Findings group 3 (Mario & Wiebe) 12](#_Toc65058629)

[Vraag 1 - Welke bekende frameworks zijn er geschikt voor Enterprise Software? 12](#_Toc65058630)

[Vraag 2 - Kan dit veilig in de Cloud? 13](#_Toc65058631)

[Vraag 3 - Op welke manier kunnen we de veiligheid van data van de bank waarborgen? 13](#_Toc65058632)

[Vraag 4 - Welke team organisatie omgevingen zijn gangbaar voor een groot team met veel processen? 14](#_Toc65058633)

[4. Conclusions 15](#_Toc65058634)

[Vraag 1 - Welke bekende frameworks zijn er geschikt voor Enterprise Software? 15](#_Toc65058635)

[Vraag 2 - Kan dit veilig in de Cloud? 16](#_Toc65058636)

[Vraag 3 - Op welke manier kunnen we de veiligheid van data van de bank waarborgen? 17](#_Toc65058637)

[Vraag 4 - Welke team organisatie omgevingen zijn gangbaar voor een groot team met veel processen? 18](#_Toc65058638)

# The case

Author: Leon Schrijvers

Date: December 18, 2019

“*A large Dutch banking organisation is struggling in the digital era. In order to compete with rising, modern and agile FinTech companies, the organisation is investing into digital transformation. As a part of this endeavour, the organisation wants to extend their application portfolio with new applications that enable customers to perform extensive self-service tasks.*

*During this project, it became clear that extending the legacy backend services was much harder than estimated. The majority of the critical services are written in COBOL and most of the COBOL engineers are already retired.*

*The board of directors faces a complete failure of the digital transformation project and discovered a huge risk regarding the continuity of the organisation! (Side note: Why this issue wasn't addressed earlier is still under investigation...)*

*Based on an advice from the IT department, the board has decided that the organisation must migrate its backend services to a new Enterprise Software Platform. Because of the scale and the importance of this operation, the organisation has decided to partner with an external software agency. This agency has the know-how and necessary track record in similar projects.*

*As part of this agency, your task is to select a suitable Enterprise Software Platform for this banking organisation. You need to think about what 'suitable' means in this case: what characteristics of a platform are important in an enterprise context, and what is important to the organisation and its end customers? Make a complete context discovery e.g.: banking is a regulated sector with huge impact (see recent economic crises). You should also think of the development environment suitable for a large team and processes to support the project.*

*Because your advice will be the foundation of the organisations STRATEGY-2025, the board of directors expects a well-motivated report. The report will help to reassure shareholders that the project will be executed without risks, delays and with accordance with law and public interests.*

*The report should contain an advice on what you think is the most context-fitting enterprise software platform, including supporting frameworks and/or libraries. Because the board of directors can be hard to convince and will be reviewed by auditors, the report should follow a structured approach. You should explain clearly what steps you took during the selection process. Your explanation must be accompanied by a motivation aligned with the project’s context.”*

# 1. Eerste meeting

## 1.1 Vragen om de case duidelijker te krijgen

Als groep hebben we de case besproken en hieruit is gebleken dat we toch nog meerdere onduidelijkheden hebben over de case welke we wel relevant vinden. De vragen die hier gezamenlijk uit zijn gekomen zijn als volgt:

1. Welke (kritische) services zijn er?
2. Waar wordt de (gevoelige) data opgeslagen?
3. Staat er momenteel iets qua CI/CD?
4. Hoe houdt het huidige project rekening met security en het voorkomen van een data lek?
5. Hoe ziet de huidige DevOps omgeving eruit?
6. Er wordt aangegeven dat de COBOL-expertise het bedrijf uit is. In welke talen heeft het team wel veel kennis?
7. Wat is de werkwijze van de ontwikkelaars binnen de bank? (waterval, scrum)
8. Word er ook gebruik gemaakt van externe partijen? (Auth0 etc.)

## 1.2 Resultaten van de brainstorming

Eigenlijk zijn we tot de conclusie gekomen dat we nog te weinig technische kennis in huis hebben en de case te onduidelijk is om al grote aanbevelingen te doen vooraf. Ook is het nog niet helemaal duidelijk welke platformen precies beschikbaar zijn. Vooraf dachten we aan Azure, AWS en Google Cloud.

Mogelijke oplossingen zijn dus nog wat lastig te bepalen. Wel hebben we kort dingen besproken zoals een backend in Spring Boot.

## 1.3 Vereiste kennisvragen

Op basis van de brainstormsessie hebben we wat vragen opgesteld om kennis te vergaren zodat we een betere aanbeveling kunnen doen en om inzicht te krijgen in de verschillende mogelijkheden. Deze vragen zijn als volgt:

1. Welke bekende frameworks zijn er geschikt voor Enterprise Software?
2. Kan dit veilig in de Cloud (en zo ja, hoe veel van het project wel en niet)?
3. Op welke manier kunnen we de veiligheid van data van de bank waarborgen?
4. Welke team organisatie omgevingen zijn gangbaar voor een groot team met veel processen?

# 2. Approach

We hebben als tweetallen alle kennisvragen beantwoord. Deze zijn te vinden in hoofdstuk 3 en beantwoord volgens het DOT Framework (*http://ictresearchmethods.nl/The\_DOT\_Framework*[1]). Vervolgens zijn we weer bij elkaar gekomen om de bevindingen te bespreken en te sparren wat we vinden. De uiteindelijke conclusie welke we willen gebruiken als aanbeveling is te vinden in hoofdstuk 4.

# 3. Results

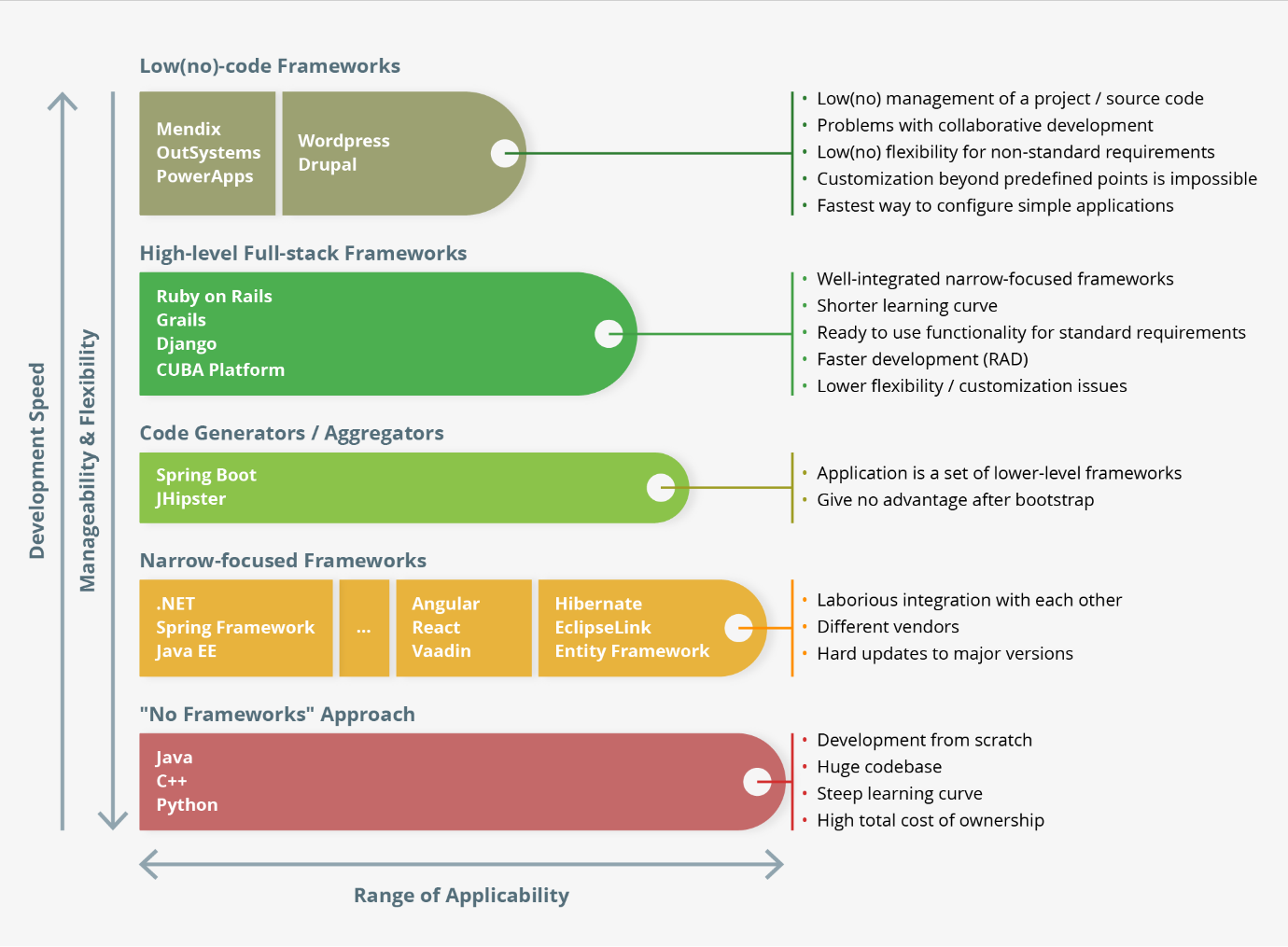
## 3.1 Findings group 1 (Joost van Herwaarden & Sjoerd Halmans)

### Vraag 1 - Welke bekende frameworks zijn er geschikt voor Enterprise Software?

Om te beantwoorden welke veel gebruikte frameworks beschikbaar zijn voor Enterprise software hebben we volgens het DOT framework de community research module toegepast.

Online zijn we verschillende frameworks tegengekomen met verschillende classificaties. Zo heb je bijvoorbeeld Low-code frameworks, high level full-stack frameworks, code generators en narrow-focused frameworks *(Stukalov, z.d.)*.

Hieronder in afbeelding 3.1.1 is een afbeelding te vinden waarin eigenlijk deze vraag grotendeels is beantwoord.

  
Afbeelding 3.1.1

Zoals we kunnen zien staan hier verschillende talen en frameworks vermeld met daarbij ook de voor en nadelen. Dit zijn dan wat ons betreft ook de verschillende frameworks die we mee gaan nemen in onze overweging.

### Vraag 2 - Kan dit veilig in de Cloud?

Om deze vraag te kunnen beantwoorden hebben we wederom de community research methode toegepast. Hieruit concluderen we dat dit inderdaad mogelijk en veilig is in deze tijd. Zelfs met gevoelige data waar de bank mee werkt. *“The public clouds have been safe places to store mission-critical and sensitive data for some time, but it takes a pandemic to push most enterprises over the tipping point” (Linthicum, 2020).*

Ook volgens een Cyber Security rapport van PwC is het mogelijk zelfs de veiligste plek om data op te slaan. Dit geven ze aan in hun PDF rapport *“the cloud may be the safest place for storing sensitive data”. (pwc-cloud-safest-place-storing-sensitive-data, 2015)*

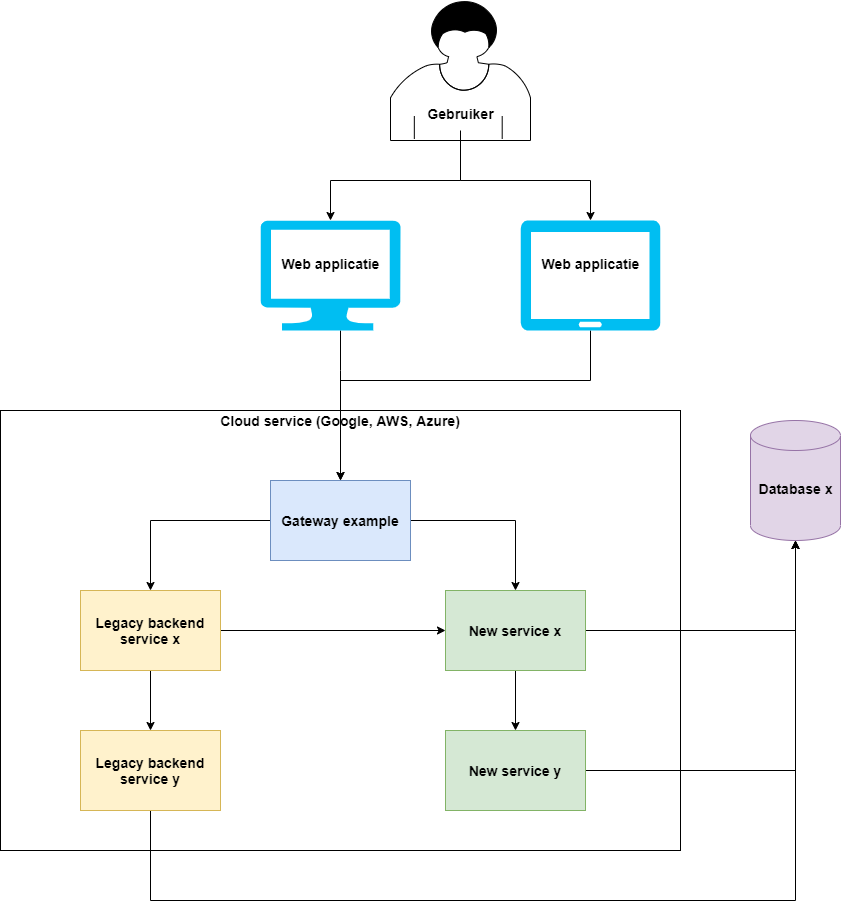
### Vraag 3 - Op welke manier kunnen we de veiligheid van data van de bank waarborgen?

Om te bepalen hoe data veilig opgeslagen kan worden in de Cloud gaan we wederom aan de slag met een community research. Hierin onderzoeken we of data veilig is in de Cloud ervan uitgaande dat dit niet gehackt kan worden.

Dit lijkt niet het geval te zijn. Het is namelijk zo dat partij waar je de data host verzocht kan worden door de overheid om deze data te delen. Omdat deze derde partij in beheer is van de data ligt de keuze ook bij de derde partij zelfs als de bank het hier niet mee eens is. Alleen dit al zou een overweging kunnen zijn voor de bank om de data in-house te houden zodat de keuze om data te delen met de overheid ook zelf gemaakt kan worden per case. *“Even if data isn’t stolen or published, it can still be viewed. Governments can legally request information stored in the cloud, and it’s up to the cloud services provider to deny access.” (Bozicevic, 2018).*

Mocht dit voor de bank niet relevant zijn in de keuze dan is Cyber Security ook nog een grote rol die mee kan spelen in de overweging. Het voordeel van een Cloud storage is dat deze security al geregeld is. Toch is het verstandig om back-ups te maken van belangrijke data en deze exporteren naar een sandbox omgeving om de data te beschermen tegen bijvoorbeeld ransomware.

Daarnaast hebben we ook nog de IT architecture sketching methode toegepast. Op deze manier willen we met de vergaarde kennis uit onze community research een ontwerp bedenken waarbij we veiligheid vooropstellen.

  
Afbeelding 3.1.3

Zoals we hier zien is dit een heel globaal plaatje waarbij we vanuit een toplevel view naar de applicatie kijken. Zo zou in de nieuwe architectuur het er zo uit te komen zien dat de oude COBOL-services welke in gebruik blijven in de Cloud omgeving terecht komen. Daarnaast komen ook de nieuwe services in deze omgeving tevoorschijn om de wensen van de consument mogelijk te maken. Deze maken onderling verbinding waar nodig en verbinden met een database buiten de Cloud.

Dit ontwerp is gemaakt met de aanname dat de bank zelf verantwoordelijk wil zijn om data te delen met de overheid. Mocht de bank hier geen mening over hebben dan kan de database eventueel ook binnen de Cloud gehangen worden.

### Vraag 4 - Welke team organisatie omgevingen zijn gangbaar voor een groot team met veel processen?

Om deze vraag te beantwoorden moeten we kijken naar wat het uiteindelijke doel is van de organisatie en wat de schaal van het product is (dit kunnen we doen met behulp van het DOT framework en de available product analysis methode). In ons geval hebben we te maken met een grootschalige refractor van een bestaand systeem, dit zal veel tijd kosten en er zal een goede planning gemaakt moeten worden om ervoor te zorgen dat elke developer in het team ook daadwerkelijk weet wat hij/zij moeten doen en wat hun doelen zijn.

Voor deze stelling zijn er een paar kandidaten om uit te kiezen, systemen zoals Jira en Taiga nemen hier in de leiding. Door hun focus op grote projecten en de mogelijkheid om veel verschillende systemen te koppelen aan een project (denk github repositories) is het mogelijk om een heel groot project te plannen en dit in verschillende sprints op te delen en taken uit te delen aan de verschillende developers in het project.

Een platform als trello zou geen goede kandidaat zijn in dit geval, hoewel het simpel op te zetten is, kan het snel zijn dat je de bomen door het bos niet meer ziet. Ook is het moeilijk om te zien welke taken jij moet verzorgen in het project als je met een grote groep developers aan de slag gaat.

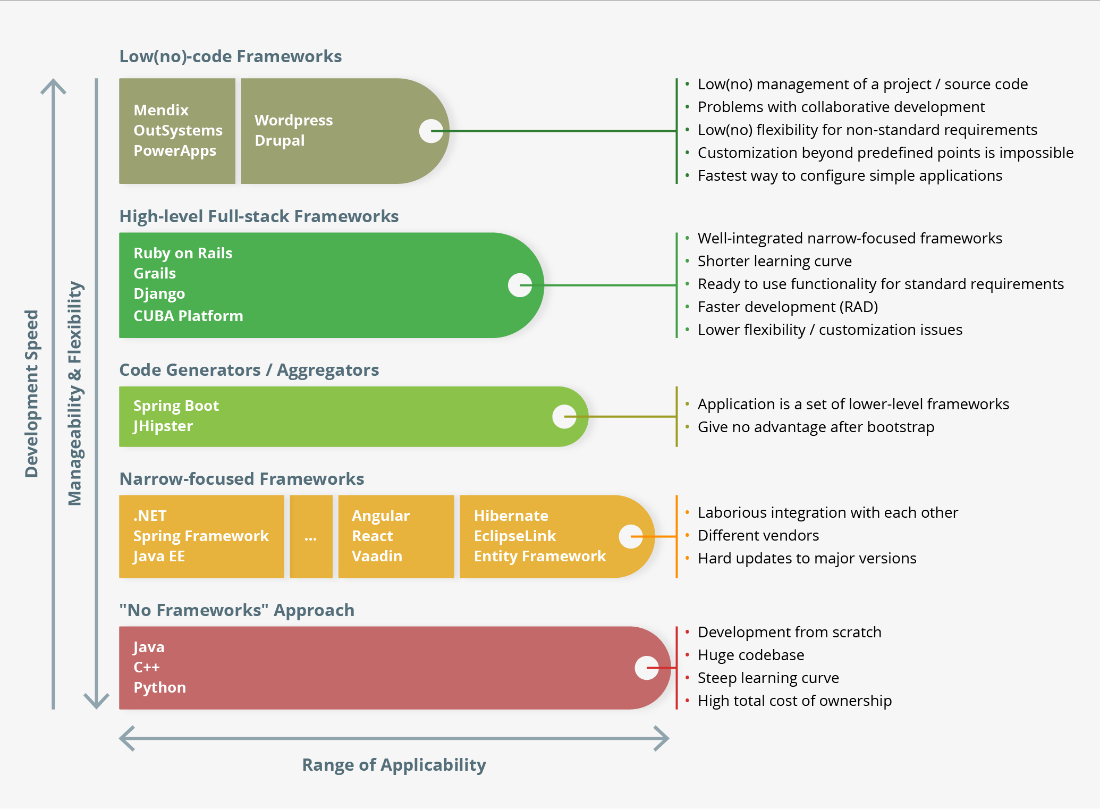
## 3.2 Findings group 2 (Nicky Janse & Tom van Kaathoven)

Om de onderstaande vragen te kunnen beantwoorden is er gebruik gemaakt van het DOT Framework. Bij elke vraag worden er een aantal onderzoeksmethoden benoemd welke gebruikt zijn om de vraag te beantwoorden.

### Vraag 1 - Welke bekende frameworks zijn er geschikt voor Enterprise Software?

#### Community research/Design pattern research

Welk(e) framework(s) geschikt is/zijn voor een project is afhankelijk van meerdere factoren; de range van toepasbaarheid; de onderhoudbaarheid en flexibiliteit; en de snelheid van ontwikkeling. De onderstaande afbeelding geeft een erg duidelijk overzicht van verschillende frameworks en de voor- en nadelen hiervan. Het kiezen van het juiste framework of de juiste frameworks is een afweging tussen deze verschillende factoren.



#### Problem analysis

De bankorganisatie huidige systeem is geschreven in COBOL, dit is een oudere ontwikkel taal. De ontwikkelaars die COBOL kennen zijn schaars op de markt. Omdat dit schaars is betekend dat de ontwikkeling in COBOL achterloopt op andere technieken die gebruikt kunnen worden.

Het probleem wat de bankorganisatie heeft luidt als volgt:

“Het huidige systeem is ontwikkeld in een oudere taal wat innovatie en ontwikkeling remt.”

### Vraag 2 - Kan dit veilig in de Cloud?

#### Community research

Omdat we in dit geval te maken hebben met een banking systeem is veiligheid van erg groot belang. Steeds meer bedrijven maken de overstap op het gebruikt van Cloud oplossingen.

Het volgende is geciteerd uit een artikel over Cloud database security.

“*Here are some interesting facts that we’ve recently uncovered about cloud database security in the* [*Oracle and KPMG Cloud Threat Report 2019*](https://www.oracle.com/cloud/cloud-threat-report/?source=:ow:o:bl:gts:SecurityThreatBlog&intcmp=:ow:o:bl:gts:SecurityThreatBlog)*:*

* *73 percent of respondents feel the public cloud is more secure than what they can deliver in their own data center and are moving to the cloud.*
* *71 percent of organizations indicated that a majority of this cloud data is sensitive—up from 50% last year.*
* *30% cited the inability of existing network security controls to provide visibility into cloud-resident server workloads as a cloud security challenge.*
* *92% of organizations are concerned about employees following cloud policies designed to protect this data.*”

Tiao, S. (2019, 25 feb). Cloud Database Security—What Is There to Know? Geraadpleegd op 23-02-2021 van:  
[*https://blogs.oracle.com/database/cloud-database-security*](https://blogs.oracle.com/database/cloud-database-security)

Uit het genoemde onderzoek blijkt dat het gebruik van Cloud oplossingen steeds meer voorkomend is en dat het vertrouwen in de veiligheid van deze systemen ook meegroeit.

Echter zijn er nog wel risico's aan verbonden. Zo is er in het nieuws bijvoorbeeld geregeld een bericht is van data lekken waarbij gevoelige data van honderden of zelfs duizenden personen op straat zijn komen te liggen. Dit is natuurlijk een risico dat je als banking systeem niet mag nemen.

### Vraag 3 - Op welke manier kunnen we de veiligheid van data van de bank waarborgen?

#### Community research

Om data te waarborgen voor de bankorganisatie zijn er een paar veiligheid punten waar op gelet moet worden.

Afhankelijk van waar de data wordt opgeslagen kunnen 3de partijen mogelijk machtiging hebben tot het inzien van hen data.

Afhankelijk van structuur en gebruik van code van 3de partijen zou er mogelijk ook een data lek kunnen ontstaan bij de 3de partij. Keuze in eigen code gebruiken of oplossingen van 3de partijen zouden in overweging genomen moeten worden.

Om data te waarborgen staan hieronder 6 tips die toegepast kunnen worden

1. Hou de data traceerbaar  
Weet welke weg je data heeft afgelegd en waar de verschillende stromen oorspronkelijk vandaan komen.  
  
2. Behoud inzicht en creëer transparantie  
Goede en heldere definities zijn noodzakelijk. Zeker wanneer informatie tussen verschillende afdelingen, bedrijven of productieketens gedeeld worden.

3. Begrijp de data  
Dwing jezelf om goed te begrijpen waar je naar kijkt en waar je het over hebt. Doorvragen en de diepte in gaan kosten tijd.

4. Behoud grip en controle  
Zorg dat je op de hoogte gesteld wordt wanneer er dingen in de datastroom veranderen zodat je de impact ervan kunt bepalen.

5. Ben bewust van aannames en onzekerheden  
Modellen of afgeleiden indicatoren vragen vaak om aannames en het inbouwen van een (correctie)factor. Dit houdt systemen werkbaar, maar wees je bewust van de gedane aannames en de onzekerheid die het eventueel met zich mee kan brengen. Zeker wanneer modellen ‘gestapeld’ worden kunnen fouten exponentiële gevolgen hebben.

6. Verifieer en stuur bij  
Met behulp van een data audit moet je bovenstaande elementen periodiek toetsen en nalopen. Zeker in een veranderlijke, complexe omgeving als die van de agrofood sector.

### Vraag 4 - Welke team organisatie omgevingen zijn gangbaar voor een groot team met veel processen?

#### Community research/ available product

Om een team goed te kunnen begeleiden in het ontwikkelen van software zijn er op de markt een aantal systemen/producten mogelijk. Afhankelijk van de ontwikkelomgeving kan er een toepassende tool gebruikt worden. Zo kan DevOps via een pipeline deployment en testen uitvoeren binnen de Azure omgeving. Github is een andere kandidaat die mogelijk gebruikt kan worden. Github heeft verschillende tools die een team ondersteunen in het ontwikkelen. Ook zijn er producten geschreven die op basis van Github werken.

Er zijn meerdere kandidaten op de markt met eigen hun voordelen en nadelen. De keuze zou het beste gemaakt kunnen worden op basis van de ontwikkelomgeving.

Simpele team management tools zijn af te raden voor softwareontwikkeling. Afspraken zouden wel bijgehouden kunnen worden qua business in deze simpele tools. Trello is een goede tool om een team aan te sturen maar het mist de benodigdheden die ontwikkelaars nodig hebben. Ook kan Trello snel te groot worden en hiermee ook onoverzichtelijk.

Als de bankorganisatie al een team management tool gebruikt die voor hen werkt wordt er niet aangeraden om over te stappen naar een andere tool.

## 3.3 Findings group 3 (Mario & Wiebe)

Om antwoord te geven op de onderstaande vragen, hebben wij gebruik gemaakt van het DOT-Framework. Bij elke vraag staan de toegepaste onderzoeksmethodes vermeld.

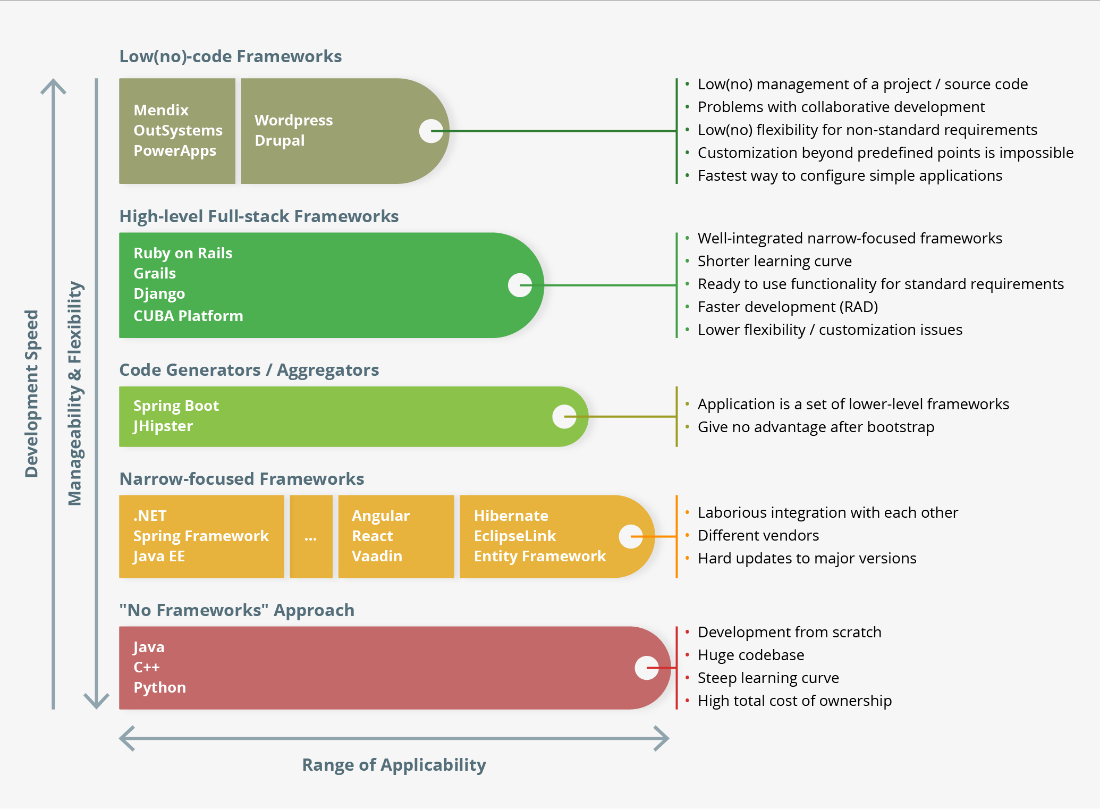
### Vraag 1 - Welke bekende frameworks zijn er geschikt voor Enterprise Software?

Om te ontdekken welke frameworks er gebruikt kunnen worden voor de usecase is het van belang dat er onderzoek wordt gedaan naar de verschillende mogelijkheden. Uit dit onderzoek komen de voor en nadelen aanbod voor desbetreffende framework. Op basis van dit resultaat kunnen wij een wel overwogen beslissingen maken over welke technologieën wij gaan toepassen op deze usecase.

De onderzoeksmethode die toegepast is, is community research, uit het onderzoekstrategie library. Er is voor deze methode gekozen omdat wij niet de eerste zijn die deze vraag hebben. Hierdoor kunnen we de kennis van andere gebruiken om zo onze keuze te onderbouwen.

Uit onderzoek is er gebleken dat het kiezen van een framework kan worden gedaan op basis van de benodigde criteria. Om een framework te kiezen die goed bij het project past bekijk je of de toepasbaarheid, onder houdbaarheid, flexibiliteit, ontwikkelsnelheid. Toepasbaar zijn voor het project wat je wilt maken. Door het maken van deze afweging komen één of meerdere frameworks naar voren die gebruikt kunnen worden.

Om de zoektocht voor het geschrikte framework makkelijker te maken kan er gebruik worden gemaakt van de onderstaande afbeelding.



### Vraag 2 - Kan dit veilig in de Cloud?

#### Literature Study:

Cloud opslag is een steeds meer voorkomend middel van dataopslag. Dit komt door de gemakkelijkheid die het met zich meebrengt. Het kan vanuit meerdere apparaten beheerd worden wat zorgt voor efficiëntie. Toch ontstaan er twijfels bij bedrijven of het veilig genoeg is. Dit erg van toepassing bij deze case aangezien een bank beschikt over gevoelige data van klanten.

##### Waarom heeft men twijfels over de cloud?

Het grootste probleem waar men tegenaan loopt, is het feit dat de data niet meer in hun handen is. Het wordt niet meer opgeslagen op de HDD van je PC. In plaats daarvan staat het opgeslagen in een datacentra ver weg van huis. En het is aan de Cloudprovider om de data te beveiligen.

Quote van Jérôme Segura, Senior Security Researcher at Malwarebytes.: “Whether data is being sent automatically (think apps that sync to the cloud) or driven by users uploading photos to social media, the end result is that it’s all there somewhere being logged and stored,”

En die ‘somewhere’ is niet direct in controle van de bank.

##### Voordelen van de CLoud:

De data die wordt opgeslagen in de Cloud is veel veiliger dan degene op je HDD. Cloud servers zijn zwaarbewaakte gebouwen. Daarnaast is alle data encrypted wat hacken erg moeizaam maakt. Terwijl een Malware infectie op de PC al je persoonlijke data ineen keer blootstelt.

##### Conclusie:

De data van de bank is relatief veilig in de Cloud. Hiernaast zijn de bestanden ook makkelijker bereikbaar en uitstekend te onderhouden.

### Vraag 3 - Op welke manier kunnen we de veiligheid van data van de bank waarborgen?

Voor het opslaan van gevoelige data is het van belang dat de data goed beveiligd wordt, maar hoe doe je dat?

Om hierachter te komen is er gebruik gemaakt van de volgende twee onderzoeksmethodes, community research en literature studies. Er is gekozen voor deze methodes omdat er online veel informatie te vinden is over dit probleem. Hierdoor kan je leren van je medemens en met deze informatie zelf een implementatie maken.

Na het lezen van een expertinterview over het beveiligen van gevoelige data zijn er een aantal punten naar voren gekomen.

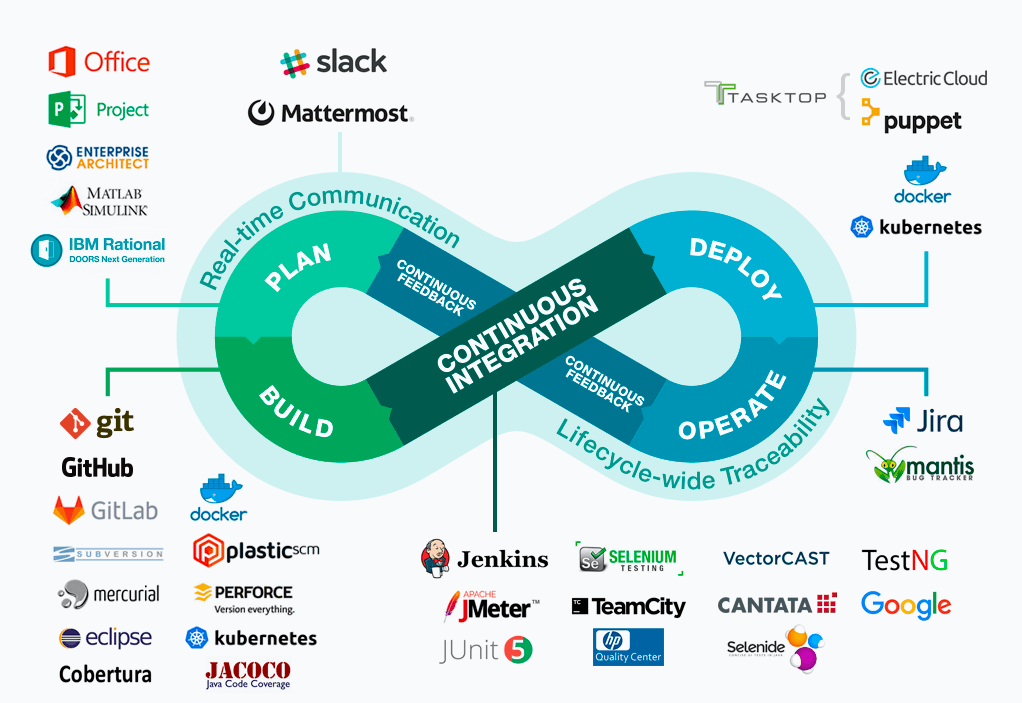
* Zorg voor data classification. Hiermee wordt duidelijk aangegeven welk gevaar bepaalde data met zich meebrengt wanneer dit lekt. De niveaus zijn restricted, confidential or private en public. Restricted heeft een hoog risico en kan daardoor alleen opgevraagd worden op een “need-to-know basis”. Confidential or pricate heeft een gemiddelde risico en kan alleen intern worden opgevraagd of door het bedrijf waar van het is. Als laatst is er public data en hierbij is er geen tot weinig risico.
* Encryptie. Encrypt gevoelige data.
* Cloud. Wees slim met cloud gebruik. Het is vergelijkbaar met het opslaan van data op een computer van een vriend. Wanneer het daar staat heb jij niet meer de controle. Zorg er daarom ook voor dat je het encrypt. Lees ook de voorwaarden goed door, deze vertellen je wat er gebeurt wanneer een cloud provider je data verliest.
* Mensen. Je programma kan goed geprogrammeerd zijn maar een mens kan altijd een fout maken. Daarom is het van belang dat je je personeel goed voorlicht.
* Endpoint security. Een endpoint levert de meeste data op en wordt daardoor ook vaak gebruikt voor een aanval. Vaak worden bij deze aanvallen gedaan op basis van een bekende exploit in de huidige softwareversie. Om dit op te lossen is het van belang om je software up-to-date te houden.

In andere online blogpost wordt er weer aandacht besteed aan de encryptie van je data. Ook wordt er aangeraden om een role-based control op te zetten. Hierdoor is de data alleen beschikbaar voor de personen die daar recht op hebben.

Als laatst wordt er gesproken over een back-up en recovery plan voor wanneer het fout gaat. Door regelmatig een backup te doen kan de schade aanzienlijk kleiner zijn wanneer een aanval toch lukt.

### Vraag 4 - Welke team organisatie omgevingen zijn gangbaar voor een groot team met veel processen?

#### Community Research:

Om een antwoord te geven op deze vraag is er gebruik gemaakt van de ‘Community Research’ strategie. 

Zoals te zien in het bovenstaande plaatje zijn er erg veel opties voor het correct inrichten van de Devops omgeving. Allen hebben voor- en nadelen. Deze kunnen het best bepaald worden met oog op de momentele ontwikkelomgeving.

Voor deze case is het slim om vooral te kijken naar programma’s die vooral enterprised zijn ingericht (Taiga > Trello). Het is ook mogelijk dat de bank al gebruik maakt van een planning tool zoals Taiga. Wanneer deze prima werkt binnen het team is het natuurlijk overbodig om een verandering hierin te maken.

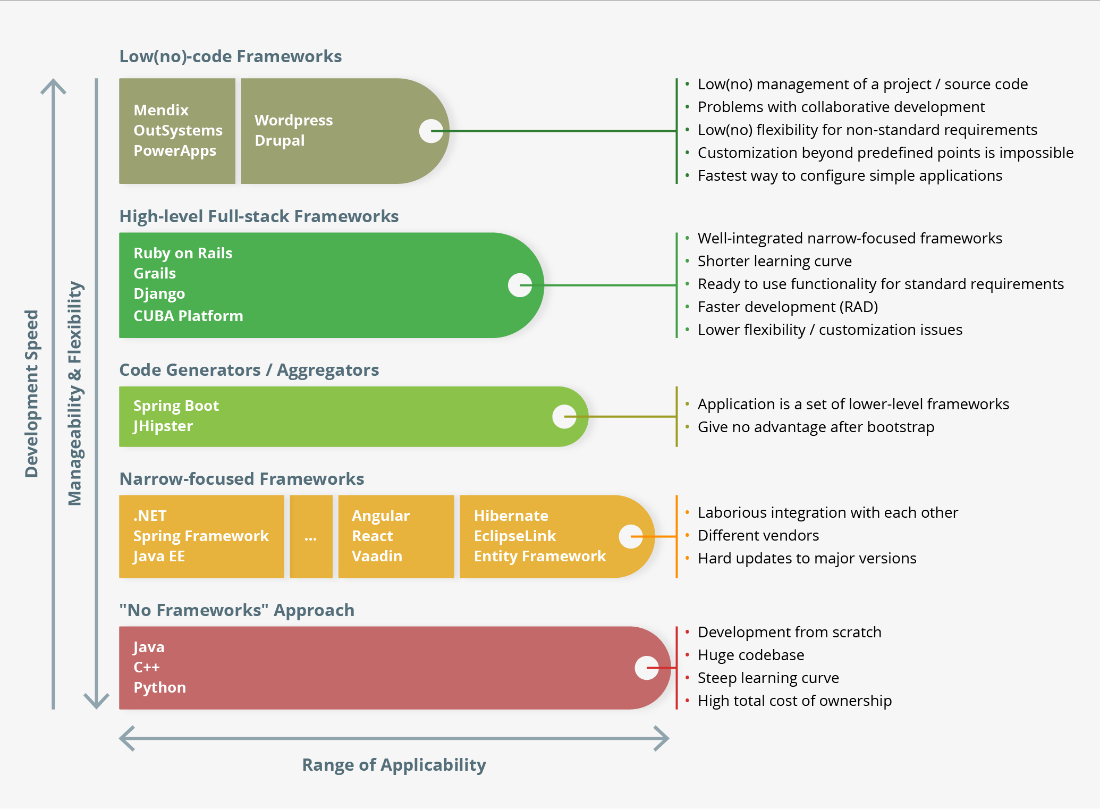
# 4. Conclusions

### Vraag 1 - Welke bekende frameworks zijn er geschikt voor Enterprise Software?

Bij deze vraag hebben we ondervonden dat alle groepjes het grotendeels met elkaar eens zijn. Ook zijn we als elk duo bij hetzelfde plaatje terecht gekomen via Canvas of via een online artikel. Dit heeft elk groepje gedaan door de Community Research methode toe te passen.

Uit onderzoek is er gebleken dat het kiezen van een framework kan worden gedaan op basis van de benodigde criteria. Om een framework te kiezen dat goed bij het project past bekijk je of de toepasbaarheid, onder houdbaarheid, flexibiliteit, ontwikkelsnelheid samen gaan met het project dat je wilt maken. Door het maken van deze afweging komen één of meerdere frameworks naar voren die gebruikt kunnen worden.

De onderstaande afbeelding geeft een erg duidelijk overzicht van verschillende frameworks en de voor- en nadelen hiervan. Het kiezen van het juiste framework of de juiste frameworks is een afweging tussen deze verschillende factoren.



### Vraag 2 - Kan dit veilig in de Cloud?

Cloud opslag is een steeds meer voorkomend middel van dataopslag. Dit komt door de gemakkelijkheid die het met zich meebrengt. Het kan vanuit meerdere apparaten beheerd worden wat zorgt voor efficiëntie. Toch ontstaan er twijfels bij bedrijven of het veilig genoeg is.

Omdat we in dit geval te maken hebben met een banking systeem is veiligheid van erg groot belang. Steeds meer bedrijven maken de overstap op het gebruikt van Cloud oplossingen.

Het volgende is geciteerd uit een artikel over Cloud database security.

“*Here are some interesting facts that we’ve recently uncovered about cloud database security in the* [*Oracle and KPMG Cloud Threat Report 2019*](https://www.oracle.com/cloud/cloud-threat-report/?source=:ow:o:bl:gts:SecurityThreatBlog&intcmp=:ow:o:bl:gts:SecurityThreatBlog)*:*

* *73 percent of respondents feel the public cloud is more secure than what they can deliver in their own data center and are moving to the cloud.*
* *71 percent of organizations indicated that a majority of this cloud data is sensitive—up from 50% last year.*
* *30% cited the inability of existing network security controls to provide visibility into cloud-resident server workloads as a cloud security challenge.*
* *92% of organizations are concerned about employees following cloud policies designed to protect this data.*”

Tiao, S. (2019, 25 feb). Cloud Database Security—What Is There to Know? Geraadpleegd op 23-02-2021 van:  
[*https://blogs.oracle.com/database/cloud-database-security*](https://blogs.oracle.com/database/cloud-database-security)

Uit het genoemde onderzoek blijkt dat het gebruik van Cloud oplossingen steeds meer voorkomend is en dat het vertrouwen in de veiligheid van deze systemen ook meegroeit.

Ook volgens een Cyber Security rapport van PwC is het mogelijk zelfs de veiligste plek om data op te slaan. Dit geven ze aan in hun PDF rapport *“the cloud may be the safest place for storing sensitive data”. (pwc-cloud-safest-place-storing-sensitive-data, 2015).*

Voor de security is dus veel te zeggen. Een groot probleem hiervan is echter dat overheidsinstanties data kunnen opvragen en de keuze om dit te accepteren ligt bij de partij waar de data staat.

Ons advies als groep is dus dat de logica zonder problemen op de Cloud gehost zou kunnen worden. Bij data is de vraag niet zo zeer of dit door hackers gekraakt kan worden maar meer of de keuze om data af te staan aan de overheid behouden wil blijven of dat het geen probleem is als een derde partij hierover kan beslissen.

### Vraag 3 - Op welke manier kunnen we de veiligheid van data van de bank waarborgen?

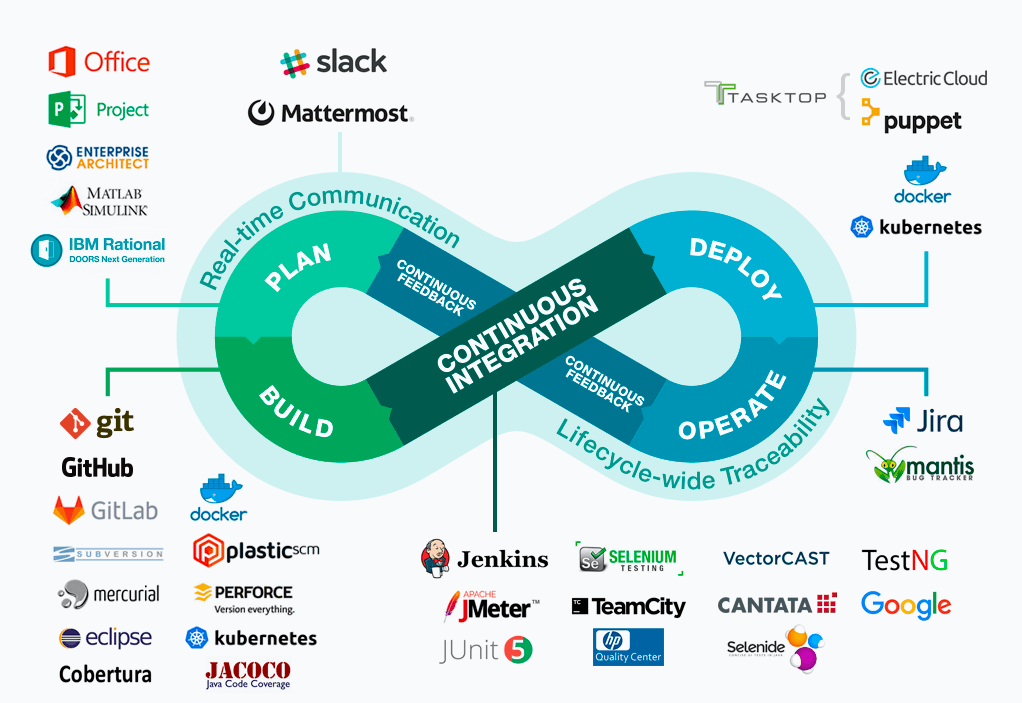
Als eerste dient de afweging gemaakt te worden om (ook) de data in de Cloud te hosten of om dit zelf te doen op een server. Hierbij is als eerste een belangrijke afweging of het een probleem zou zijn dat de overheid in handen komt van deze data. Zie hiervoor ook de conclusie van de tweede vraag. Alleen dit al zou een overweging kunnen zijn voor de bank om de data in-house te houden zodat de keuze om data te delen met de overheid ook zelf gemaakt kan worden per case. *“Even if data isn’t stolen or published, it can still be viewed. Governments can legally request information stored in the cloud, and it’s up to the cloud services provider to deny access.” (Bozicevic, 2018).*

Vervolgens dienen de technische verschillen ook in kaart gebracht te worden. Hierbij kijken we dus meer vanuit het oogpunt van een hacker. Op basis van onze bevindingen hebben we volgende drie punten die van hoog belang zijn:

* Encryptie. Encrypt gevoelige data.
* Mensen. Je programma kan goed geprogrammeerd zijn maar een mens kan altijd een fout maken. Daarom is het van belang dat je je personeel goed voorlicht.
* User-roles. Zorg ervoor dat niet elke gebruiker administrator rechten heeft. Indien mogelijk zou het handig zijn om rechten per individu in te stellen. Als hier de resources niet voor zijn maak dan enkele voorgeschreven rollen op basis van de functie van de medewerker.

Door bovenstaande 3 punten goed toe te passen is een bedrijf al een heel eind op weg naar het volledig beveiligen van data.

### Vraag 4 - Welke team organisatie omgevingen zijn gangbaar voor een groot team met veel processen?



Zoals te zien in het bovenstaande plaatje zijn er erg veel opties voor het correct inrichten van de DevOps omgeving. Allen hebben voor- en nadelen. Deze kunnen het best bepaald worden met oog op de momentele ontwikkelomgeving.

Zo kan DevOps via een pipeline deployment en testen uitvoeren binnen de Azure omgeving. Github is een andere kandidaat die mogelijk gebruikt kan worden. Github heeft verschillende tools die een team ondersteunen in het ontwikkelen. Ook zijn er producten geschreven die op basis van Github werken.

Simpele team management tools zoals Trello zijn af te raden voor softwareontwikkeling. Afspraken zouden wel bijgehouden kunnen worden qua business in deze simpele tools. Trello is een goede tool om een team aan te sturen maar het mist de benodigdheden die ontwikkelaars nodig hebben. Ook kan Trello snel te groot worden en hiermee ook onoverzichtelijk.

Als de bankorganisatie al een team management tool gebruikt die voor hen werkt wordt er niet aangeraden om over te stappen naar een andere tool.

# Bronnen

-Stukalov. (z.d.). *Classification of Development Frameworks for Enterprise Applications*. CUBA.Platform. Geraadpleegd op 23 februari 2021, van https://www.cuba-platform.com/blog/classification-of-development-frameworks-for-enterprise-applications/

-Stukalov. (z.d.). *Classification of Development Frameworks for Enterprise Applications*. CUBA.Platform. Geraadpleegd op 23 februari 2021, van https://www.cuba-platform.com/blog/classification-of-development-frameworks-for-enterprise-applications/

-*pwc-cloud-safest-place-storing-sensitive-data*. (2015). PwC (organisatie). https://www.pwc.nl/nl/assets/documents/pwc-cloud-safest-place-storing-sensitive-data.pdf

-Bozicevic, V. (2018, 28 juni). *Is Data Safe in the Cloud?* GlobalDots. <https://www.globaldots.com/blog/data-safe-cloud#:%7E:text=Cloud%20security%20is%20tight%2C%20but,it%20can%20still%20be%20viewed>

*-An Expert Guide to Securing Sensitive Data: 34 Experts Reveal the Biggest Mistakes Companies Make with Data Security*. (2021, 17 februari). Digital Guardian. <https://digitalguardian.com/blog/expert-guide-securing-sensitive-data-34-experts-reveal-biggest-mistakes-companies-make-data>

-Hope, D. (2020, 22 november). *Factors Behind Data Storage Security: Is Your Business Vulnerable?* SmartData Collective. <https://www.smartdatacollective.com/factors-behind-data-storage-security-is-business-vulnerable/>

-Zamora, W. (2018, 26 juli). *Should you store your data in the cloud?* Malwarebytes Labs. https://blog.malwarebytes.com/101/2016/04/should-you-store-your-data-in-the-cloud/