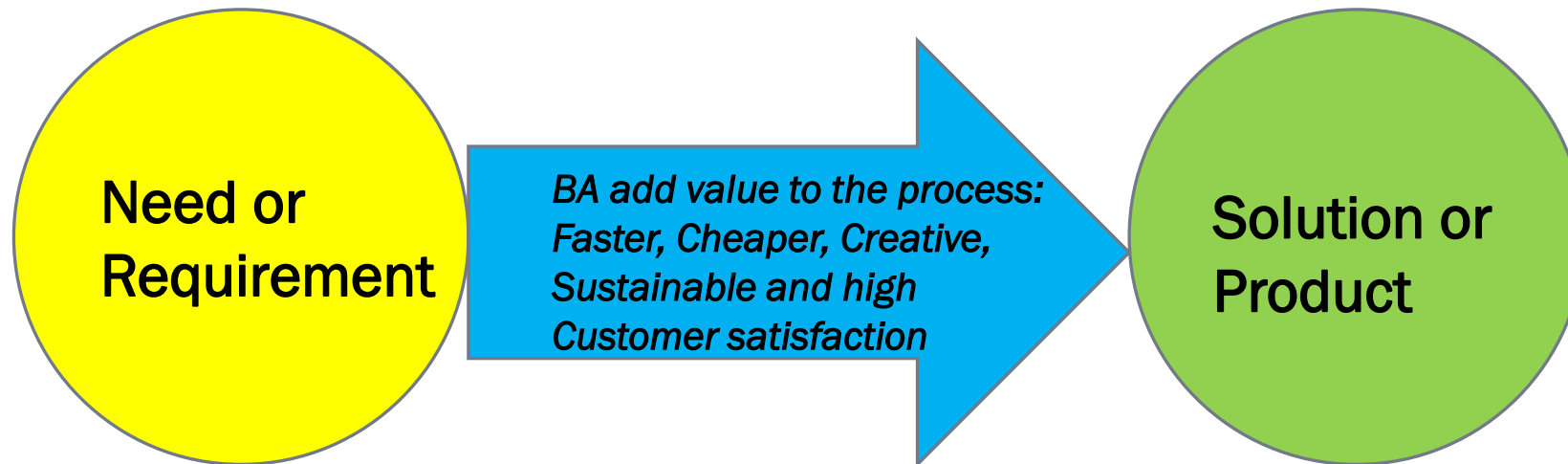


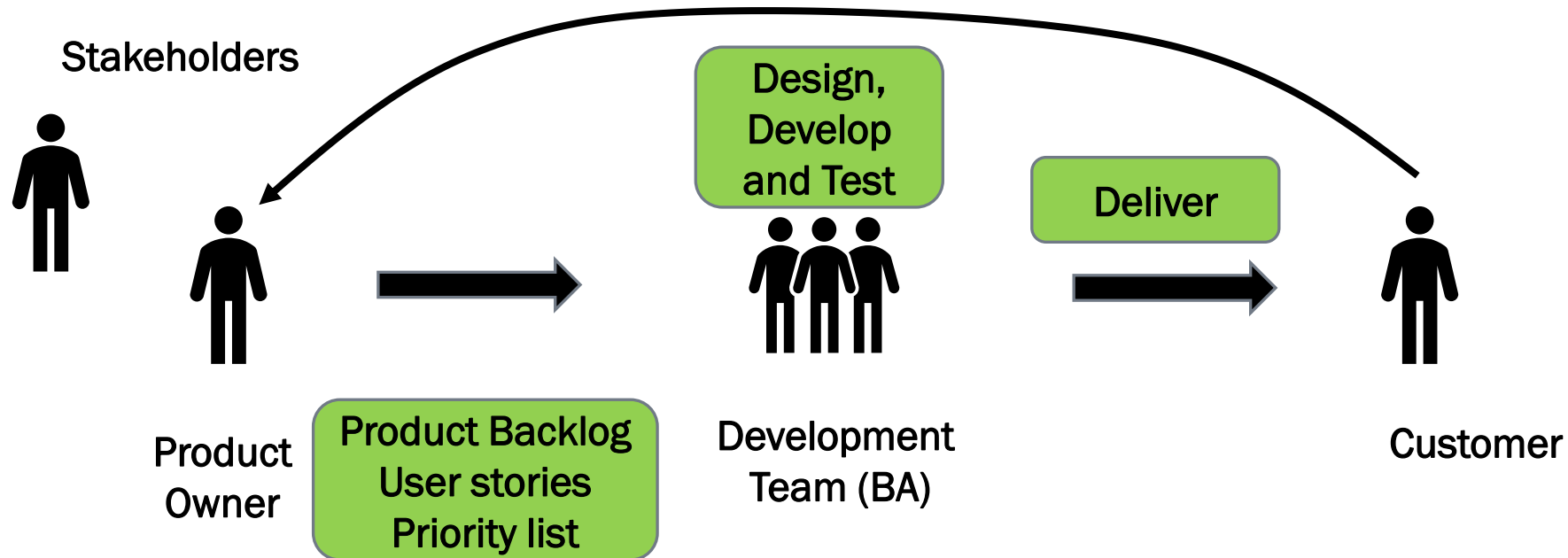
Business Analyst



Business Analyst (BA)



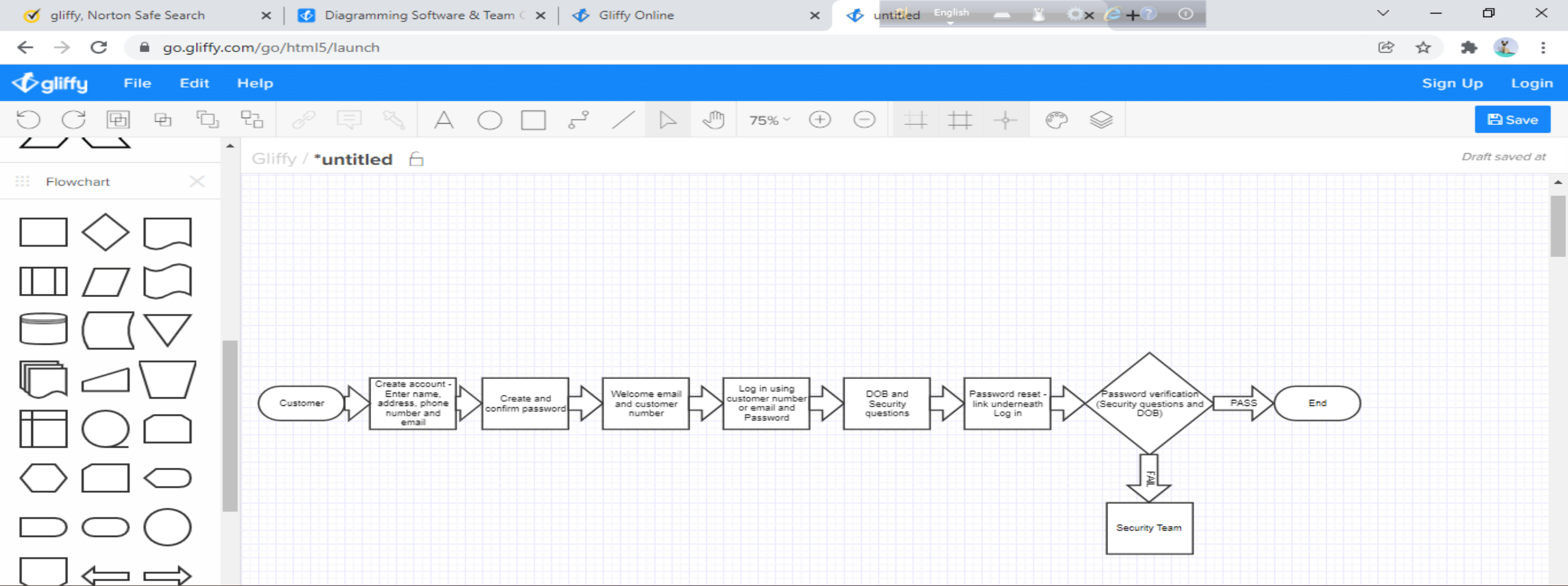
Product or solution development



Case A: Two factor authentication at Medisafe software

Problem : Medisafe is a web based health insurance provider targeted 18-30yrs

- 1. A new Customer Relation Management (CRM) Platform is required due to legislative change which requires security and privacy of customer information**
- 2. Two factor authentication when a user logs in: (a) Every 12hrs or (b) Every time the user logs in**
- 3. Within 8wks**



Current state

Product owner and stakeholders

1. Carlos Sainz (Head Legal Council) : 2FA (two factor authentication) and 8wks – Stakeholder
2. Fiona De Silva (National Security Manager) : Investigate multiple failed login, Unable to answer security questions. Real time reporting of failure. Stakeholder
3. Akash Singh (CRM Product owner) : Project plan, Risk (8wks), MVP, basic 2FA and basic compliance. Product owner
4. Melissa Rao (Head of customer and experience) : Focus session with existing customer group (cohort). Stakeholder
5. Beth Egan (Solution architect communication infrastructure) : additional communication to customer. Stakeholder

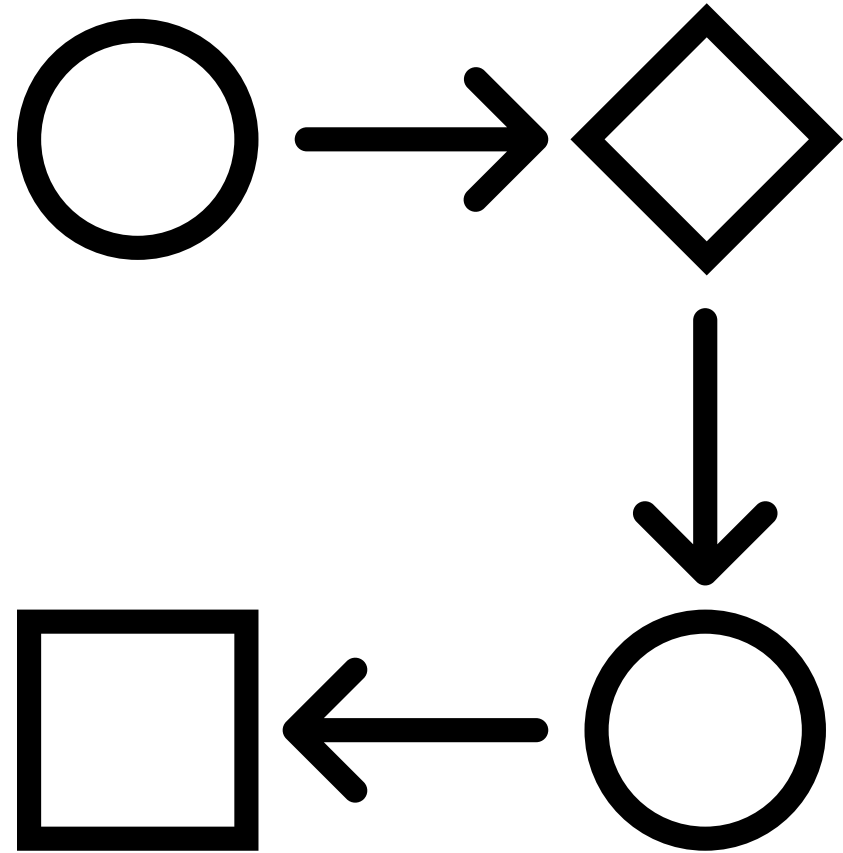
Actor Register

Case A	Two factor authentication at Medisafe Australia		
	Actor Types: Primary, Secondary, Supporting	Role: name of role/system, not the name of a person	Responsibility: Short description of what they do or how they fit into this project.
	Actor type	Actor 'name'	Responsibility
Case A	Primary	New Customer Relation Management (CRM) Platform	Ensure 2FA (Factor Authentication)
Case A	Primary	Head Legal Council	Ensure 2FA is completed in 8wks
Case A	Primary	CRM Product owner	Project Plan, Risk Mgt, MVP, Basic 2FA and achieve base level compliance
Case A	Secondary	National Security Manager	Investigate failure, real-time reporting
Case A	Secondary	Head of Customer and Experience	Focus session with existing customer cohort
Case A	Supporting	Solution architect communication infrastructure	Set up any additional communication to customer

Requirement details and priority rating

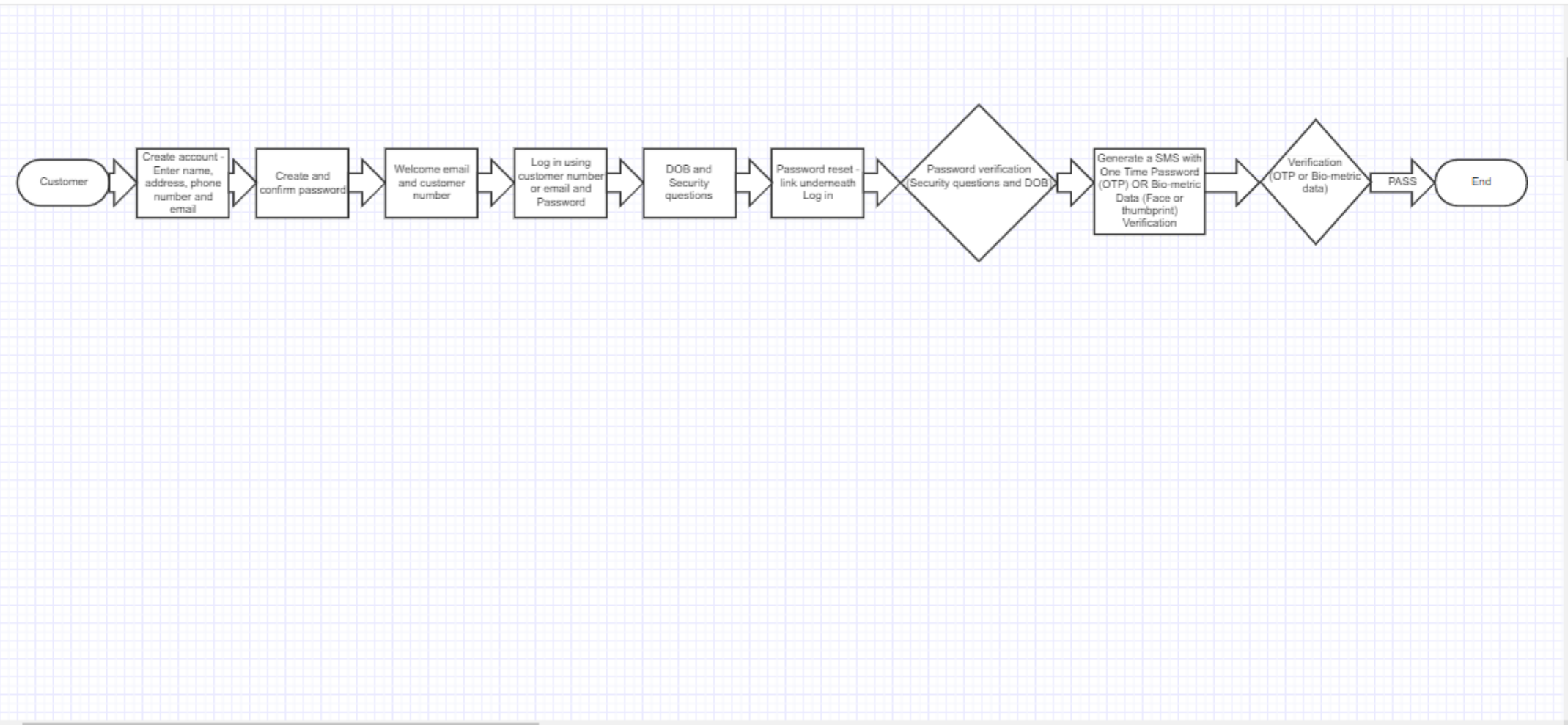
ID	MoSCoW Rating	Requirement Details	Owner/Source
1	Must	Two factor authentication (2FA) every 12 hrs or every time a customer log out and want to log back in	Carlos Sainz (Legal Counsel)
2	Must	Complete the task in 8 wks	Carlos Sainz (Legal Counsel)
3	Must	Compliant with new legislation which requires security and privacy of customer information.	Carlos Sainz (Legal Counsel)
4	Should	Pick the suspicious activity	Fiona DeSilva (National Security Manager)
5	Should	Customers prefer to receive an SMS that pre-populates into the authentication window	Melissa Rao (Head of customer and experience)
6	Should	Additional step for 2FA doesn't make customer logging into their account harder	Melissa Rao (Head of customer and experience)
7	Could	Use of biometric data like their face or thumbprint for customer logging into their account	Melissa Rao (Head of customer and experience)
8	Should	Customer uses a clickable link in the welcome email to verify their identity.	Akash Singh (Store owner)
9	Would	Customer enters login and click next, an email is generated with the link and embedded token. When the customer clicks the link, they are redirected back to the original login page with their login details already pre-populated.	Beth Egan (Solution architect)

Future state process map



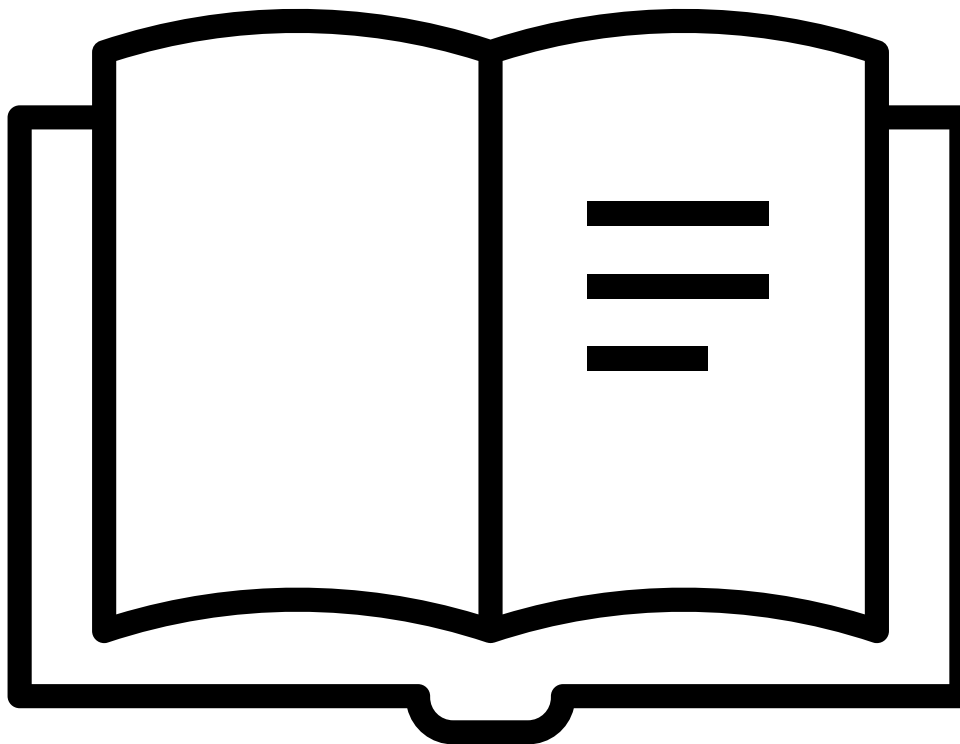
Flowchart

Gliffy / *untitled Draft saved at



More Shapes

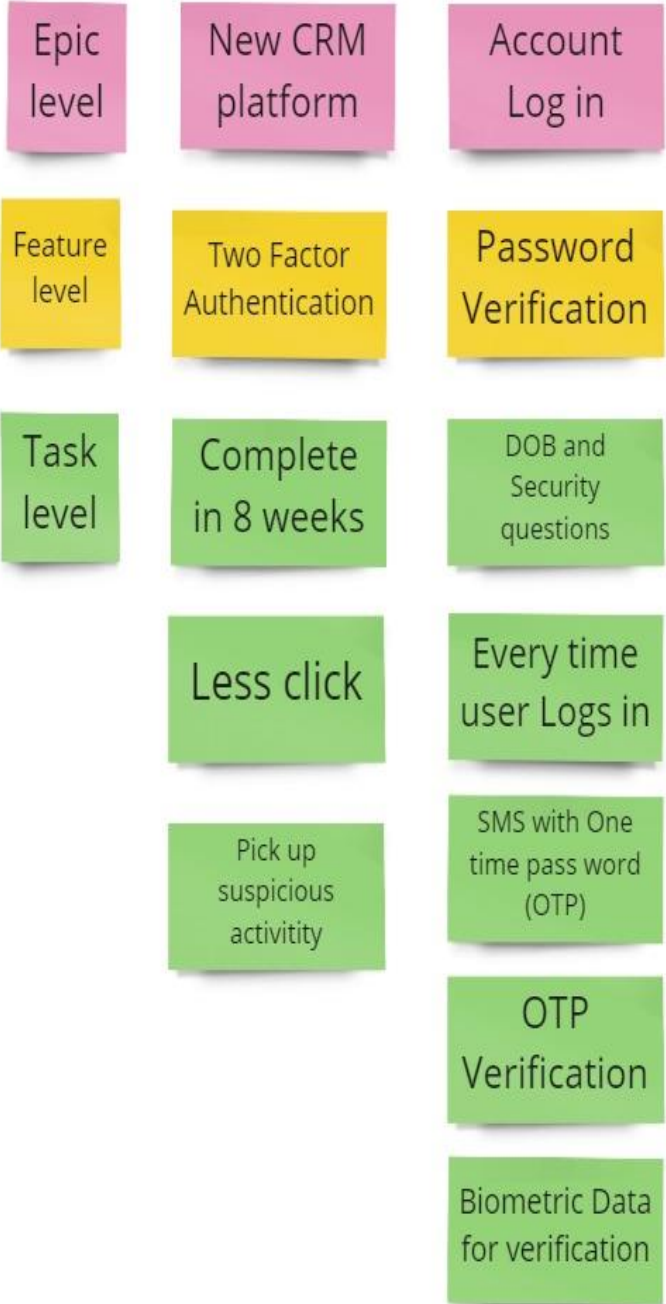
User Story



REQUIREMENT INFORMATION		RELATIONSHIP TRACEABILITY	
ID	Requirement Details	Owner/Source	User Story
1	Two factor authentication (2FA) every 12 hrs or every time a customer log out and want to log back in	Carlos Sainz (Legal Counsel)	As a Legal counsel, I want 2FA completed in 8 wks so that CRM is compliant with new legislation.
2	Complete the task in 8 wks	Carlos Sainz (Legal Counsel)	
3	Compliant with new legislation which requires security and privacy of customer information.	Carlos Sainz (Legal Counsel)	
4	Pick the suspicious activity	Fiona DeSilva (National Security Manager)	As a Security manager, I want the CRM picks the suspicious activity, so that contact center can verify the customer.
5	Customer prefer to receive an SMS that pre-poulates into the authentication window	Melissa Rao (Head of customer and experience)	As a Head of customer, I want that customer receives a SMS that pre-populates into the system authentication window, so that system becomes less click and more fluid.

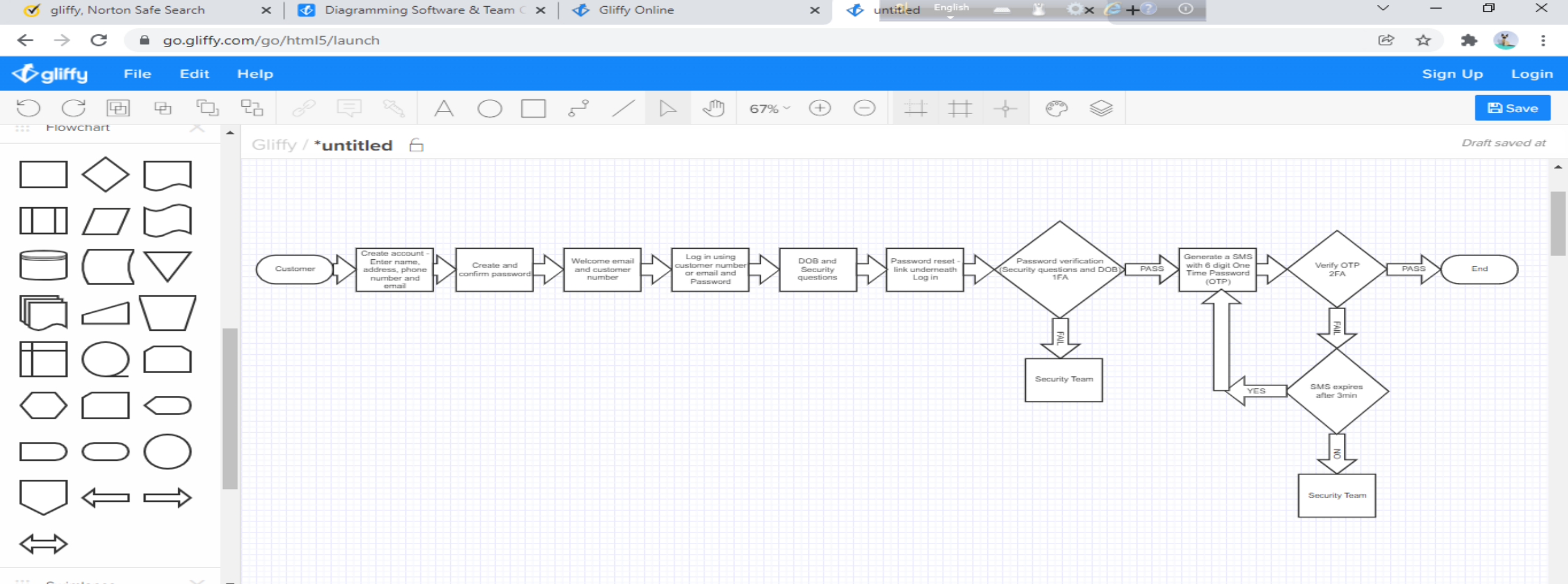
REQUIREMENT INFORMATION		RELATIONSHIP TRACEABILITY	
ID	Requirement Details	Owner/Source	User Story
6	Additional step for 2FA doesn't make customer logging into their account harder	Melissa Rao (Head of customer and experience)	As a Head of customer, I want that additional step for 2FA doesn't make customer logging into their account harder, so that system becomes less click and more fluid.
7	Use of biometric data like their face or thumbprint for customer logging into their account	Melissa Rao (Head of customer and experience)	As a Head of customer, I want the use of biometric data like their face or thumbprint for customer logging into their account, so that system becomes less click and more fluid.
8	Customer uses a clickable link in the welcome email to verify their identity.	Akash Singh (Store owner)	As a store owner, I want the customer uses a clickable link in the welcome email to verify their identity, so that CRM is as straightforward as possible.
9	Customer enters login and click next, an email is generated with the link and embeded token. When the customer clicks the link, they are redirected back to the original login page with their login details already pre-populated.	Beth Egan (Solution architect)	As a Solution architect, I want the customer enters login and click next and an email is generated with the link and embedded token, so that it makes customer login process easy.

User story map



REQUIREMENT INFORMATION		RISK REGISTER			
ID	Requirement Details	Risk Details	Impact	Likelihood	Risk Category
1	Two factor authentication (2FA) every 12 hrs or every time a customer log out and want to log back in	The solutions may not be implemented in time to be compliant with government legislation	Major	Possible	Legal/Regulatory
2	Complete the task in 8 wks				
3	Compliant with new legislation which requires security and privacy of customer information.				
4	Pick the suspicious activity	No staff at the customer service to response	Major	Unlikely	Performance
5	Customer prefer to receive an SMS that pre-poulates into the authentication window	The organisations SMS system may not be capable of sending a high volume of messages	Major	Unlikely	Operational

ID	Requirement Details	Risk Details	Impact	Likelihood	Risk Category
6	Additional step for 2FA doesn't make customer logging into their account harder	Unnecessary requirements may be added to the scope of work	Moderate	Unlikely	Operational
7	Use of biometric data like their face or thumbprint for customer logging into their account	Unnecessary requirements may be added to the scope of work	Major	Possible	Operational
8	Customer uses a clickable link in the welcome email to verify their identity.	Unnecessary requirements may be added to the scope of work	Moderate	Unlikely	Operational
9	Customer enters login and click next, an email is generated with the link and embeded token. When the customer clicks the link, they are redirected back to the original login page with their login details already pre-populated.	Unnecessary requirements may be added to the scope of work	Moderate	Unlikely	Operational



Updated future
process map

Thank you

