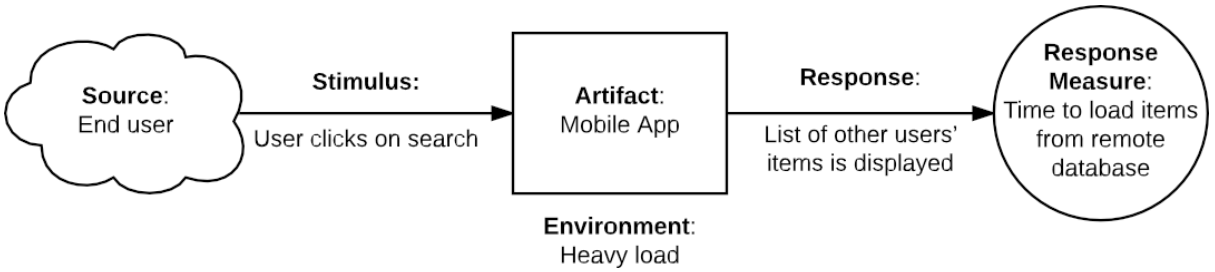
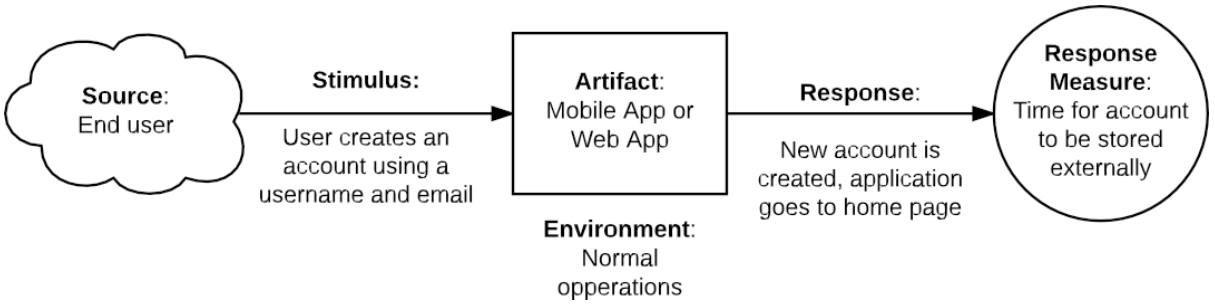
1



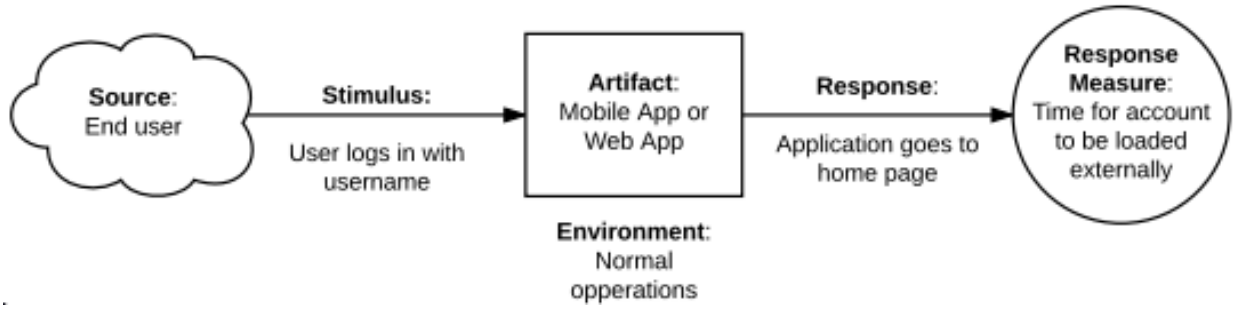
It can be marked as a **risk**. The system takes more time to complete the task than specified in the ASR requirements.

2



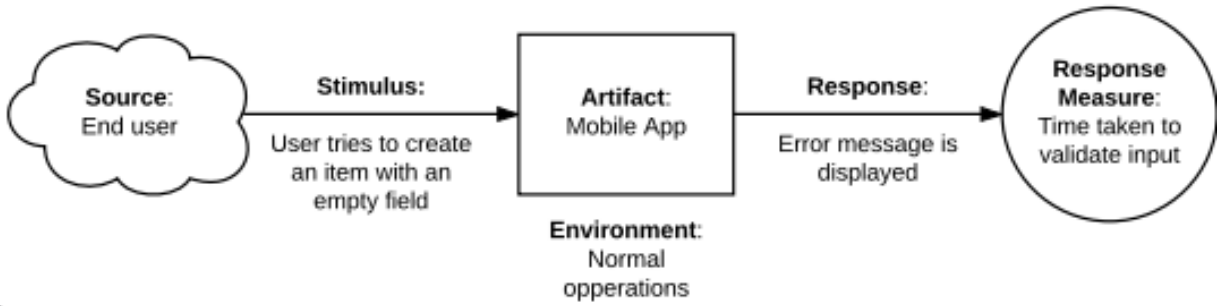
This scenario can be identified as a **risk**. It seems like the application does not require the creation and use of a password. Login is only by username and email, which is quite dangerous. Email verification is also not provided.

3



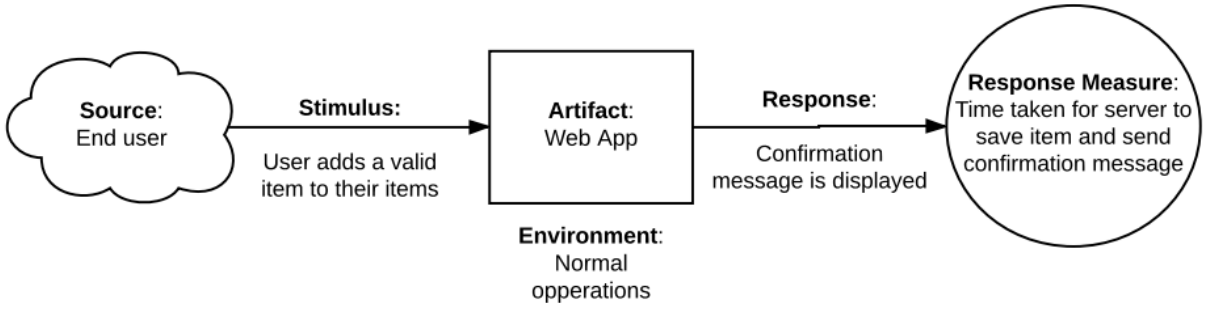
This scenario can be identified as a **trade-off**. You do not have to use a password, a username is enough to log in to your account. This speeds up account login, but significantly degrades the security of the application.

4



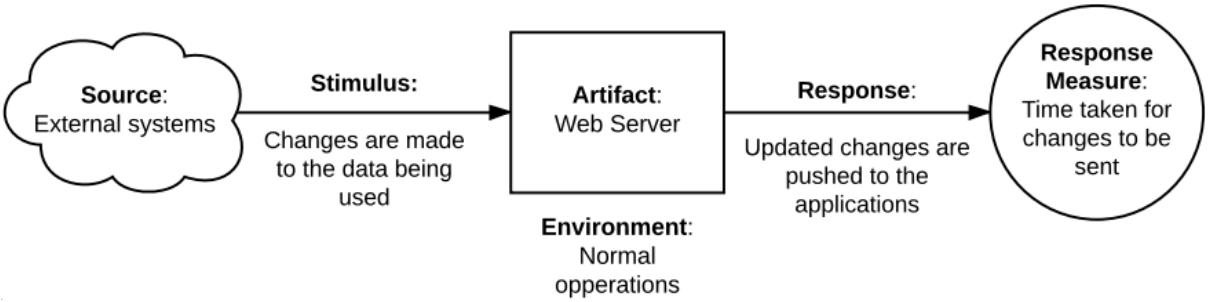
This is a **non-risk** scenario. All fields are validated and empty values aren't allowed.

5



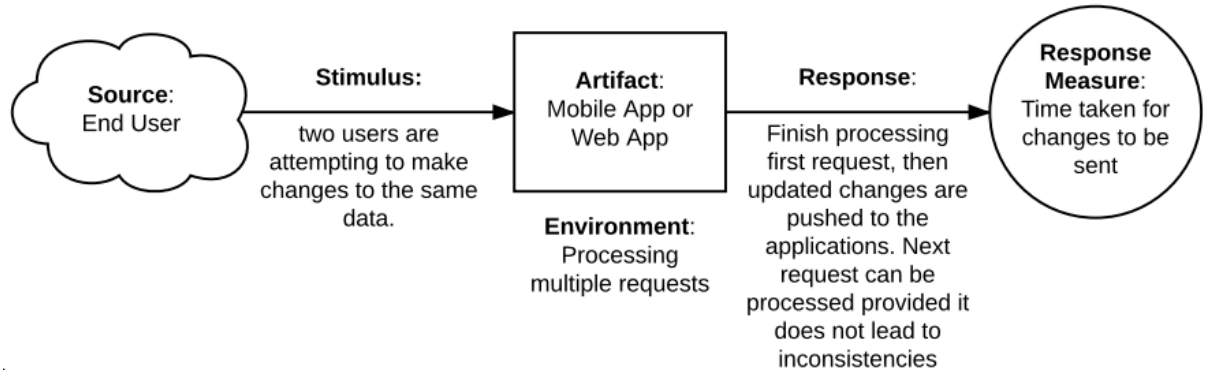
This is a **non-risk** scenario. User adds a valid item and the system works as expected.

6



This scenario presents a **sensitivity point**. There is no notification system for changes in the data used, so the user can work with outdated information and not notice it.

7



This is a non-risk scenario. In such cases, conflicts could arise during the implementation of the changes, but we solve this problem by rejecting the conflicting requests.