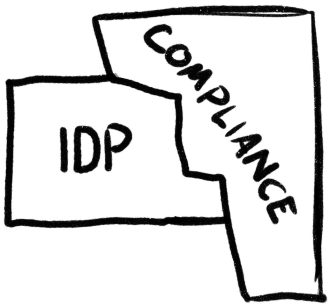
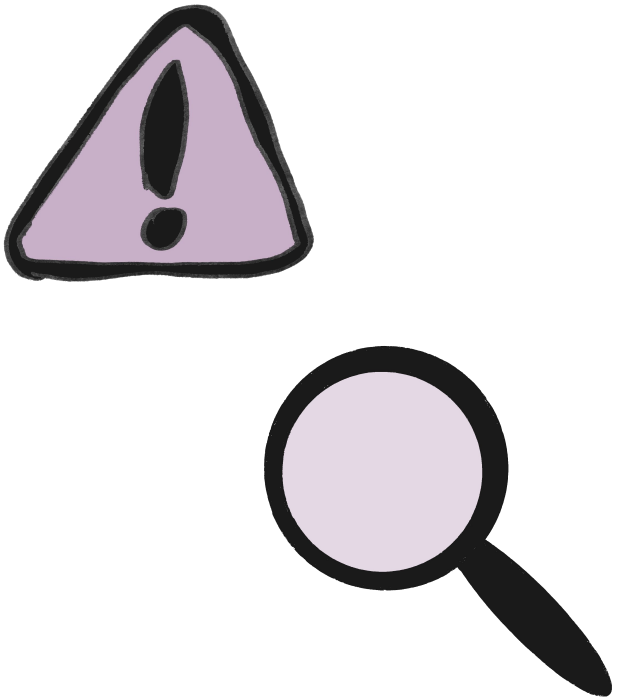
Pragmatic Guide to Compliance and Platform







Pragmatic approach

Design for compliance

Work with what's already there

Apply platform thinking to compliance



Jessica Andersson

Cloud Architect
CNCF Ambassador

@solidtubez.com

TRICE

Rise of the Internal Developer Platform

Glue together the sprawl of tools and systems

Encourage and enforce best practices

Speed up provisioning and CI/CD

Provide abstractions over complex infrastructure



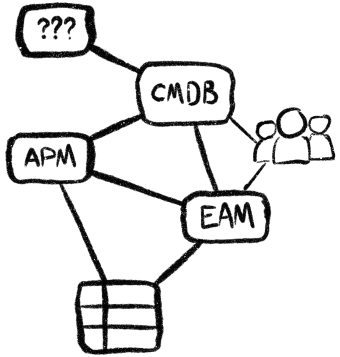
Reduce cognitive load for developers



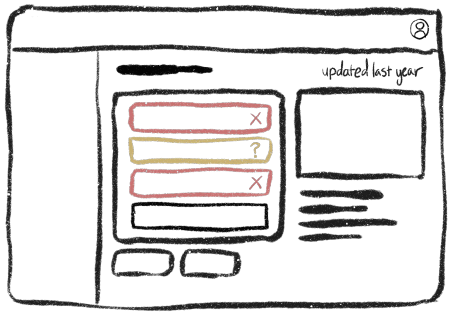
Why platform needs to care about compliance



Existing compliance workflows



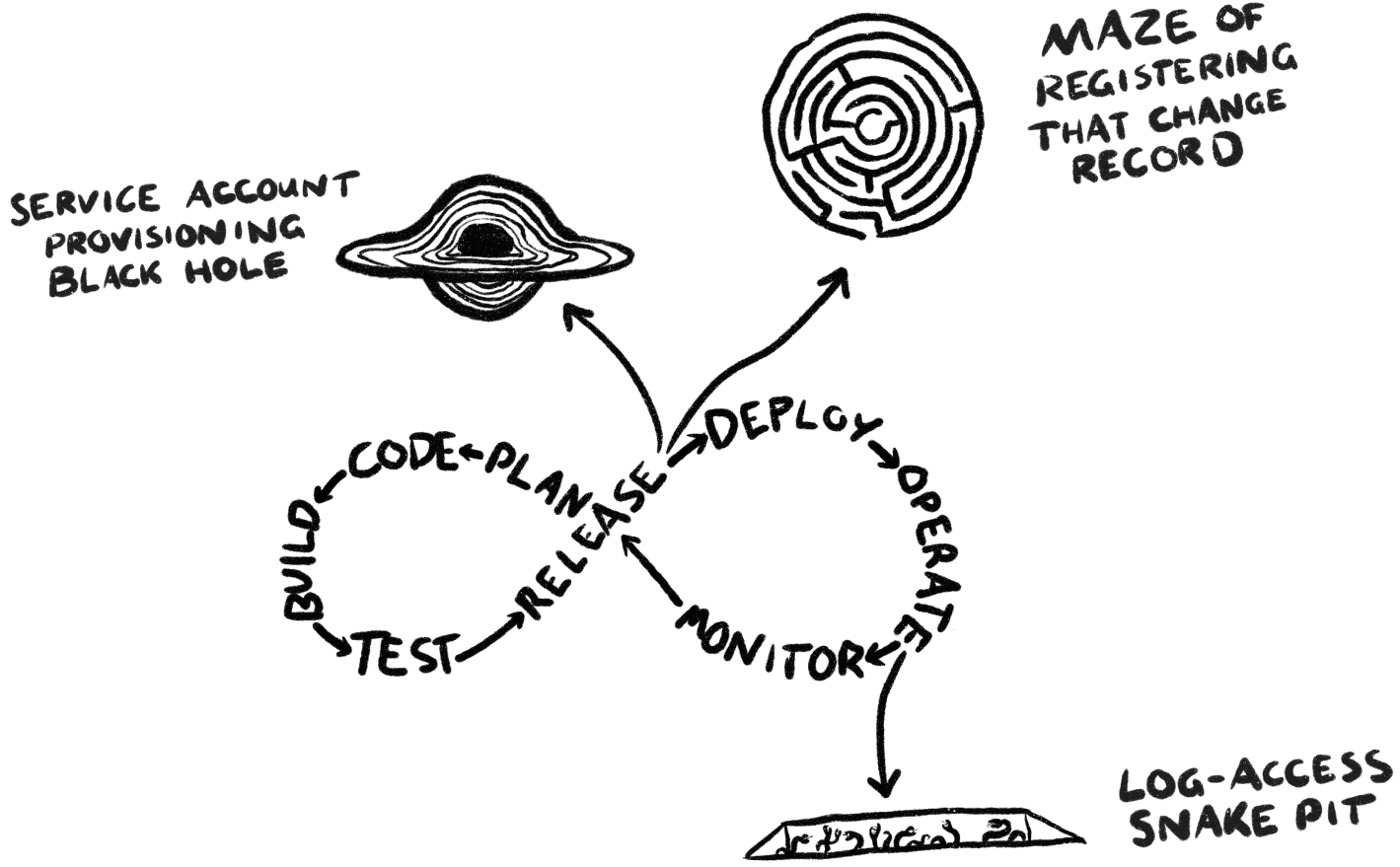
Combination of purpose made systems and workflow tools.



Data quality suffers as development processes evolve.



Despite frustrations, replacement efforts routinely fail.


SERVICE ACCOUNT PROVISIONING BLACK HOLE
MAZE OF REGISTERING THAT CHANGE RECORD
PLAN
CODE
BUILD
TEST
RELEASE
DEPLOY
OPERATE
MONITOR
LOG-ACCESS SNAKE PIT

A pragmatic approach



Integrate with existing ways of working

Build trust over time

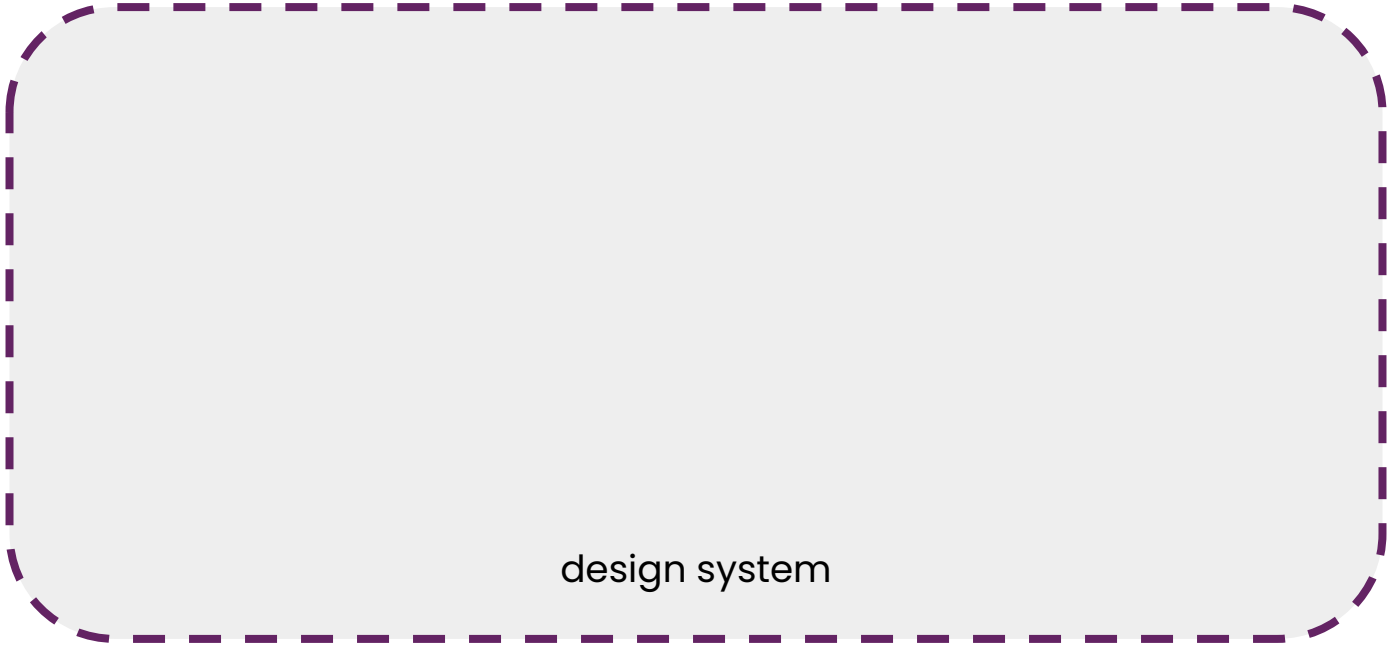


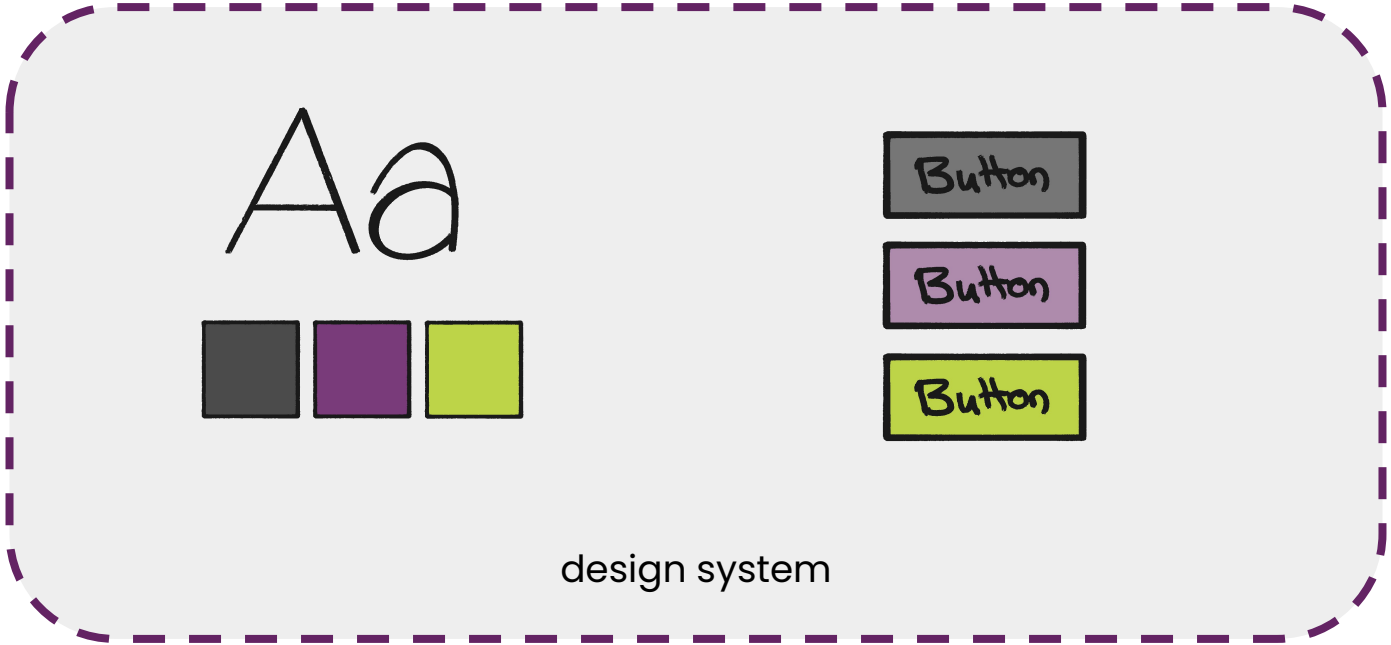


Don’t get distracted by silver bullets

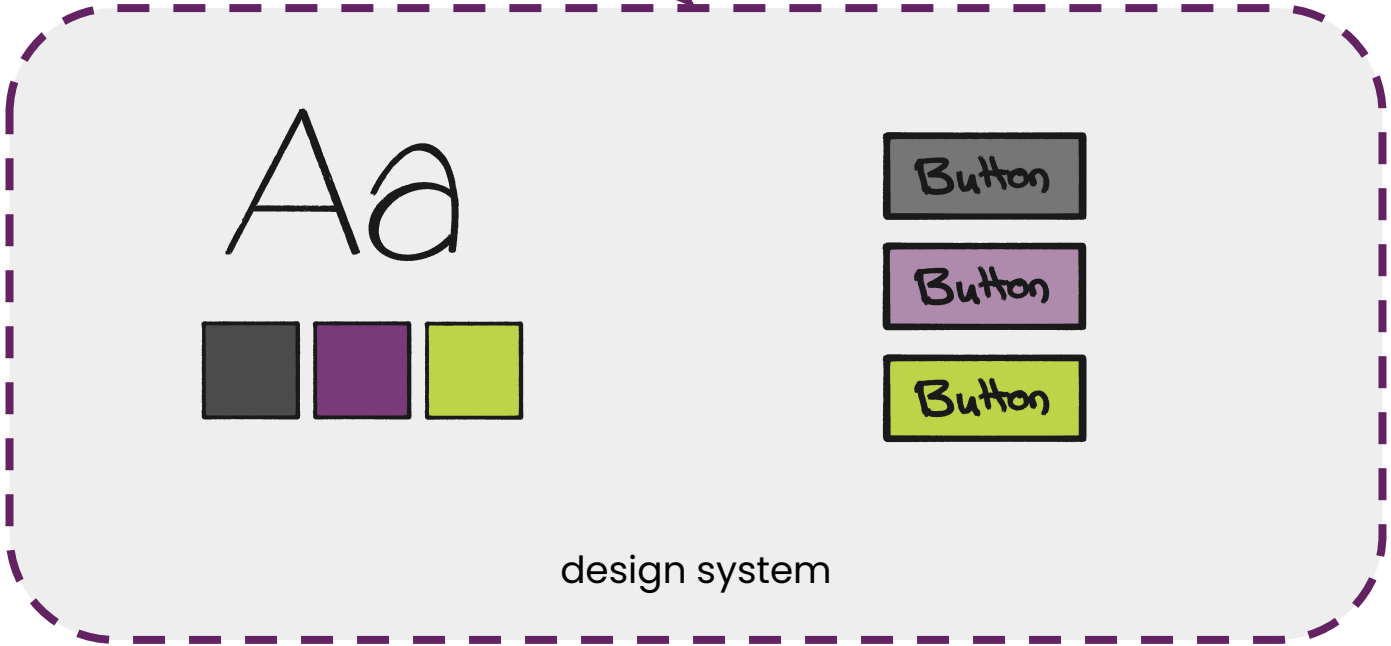
examples



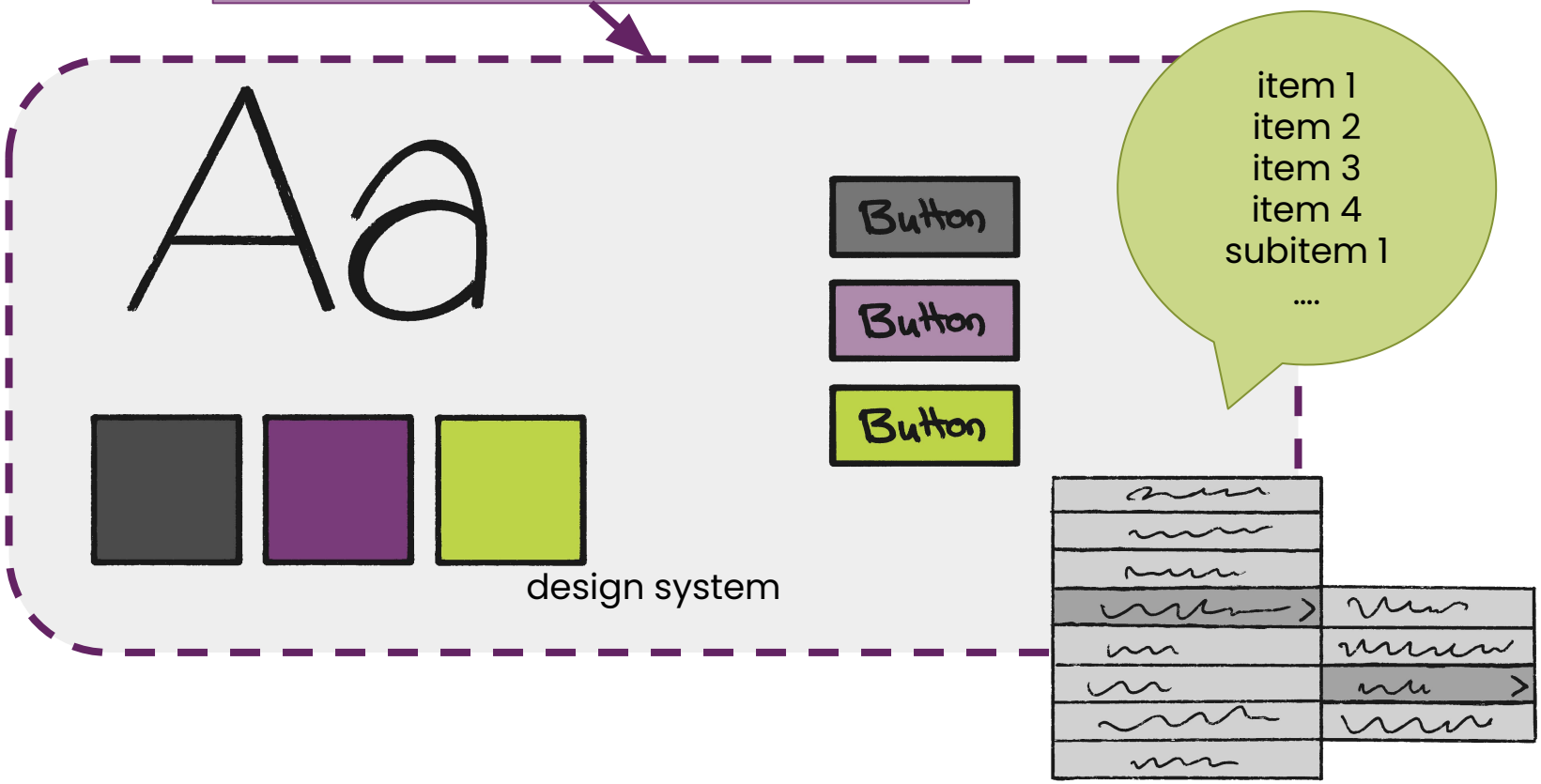

design system


Aa
Button
Button
Button
design system

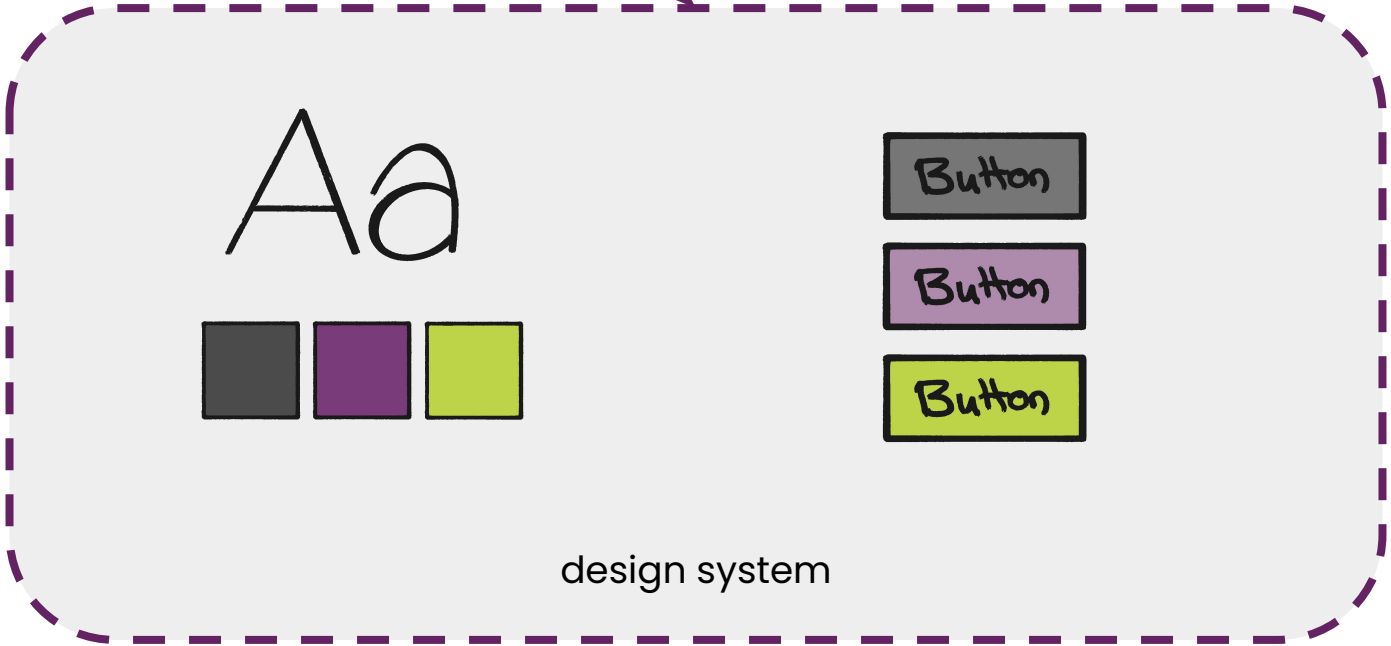
European Accessibility Act



European Accessibility Act



European Accessibility Act



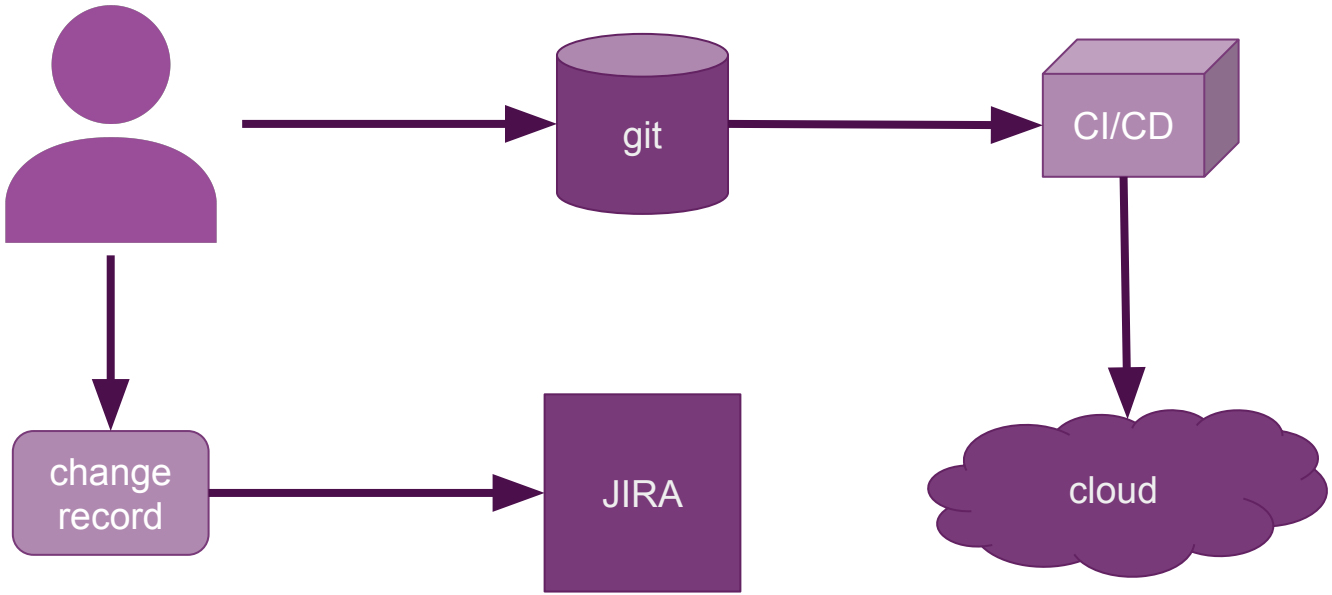
Digital Operational Resilience Act (DORA)

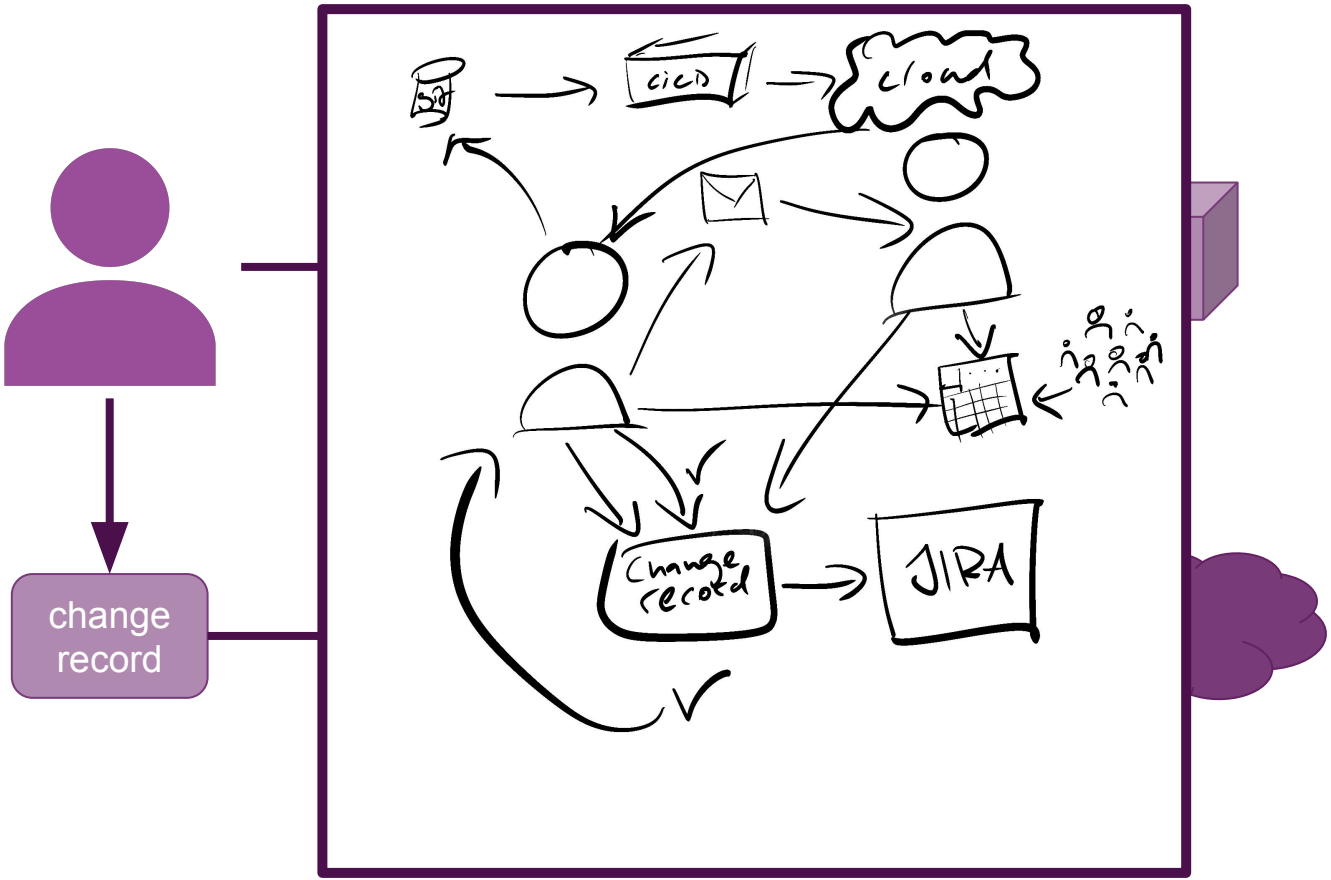
ICT Risk Management

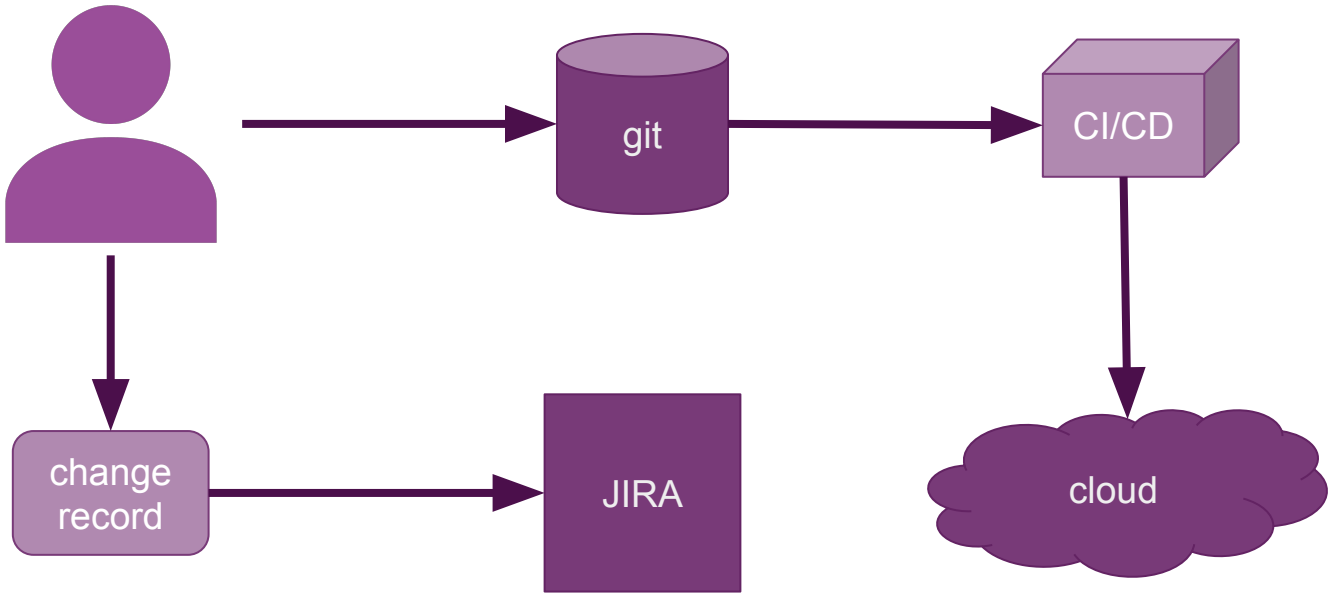
*"in order to ensure that **all changes to ICT systems are recorded**, tested, assessed, approved, implemented and verified in a controlled manner"* - Article 9.4(e)

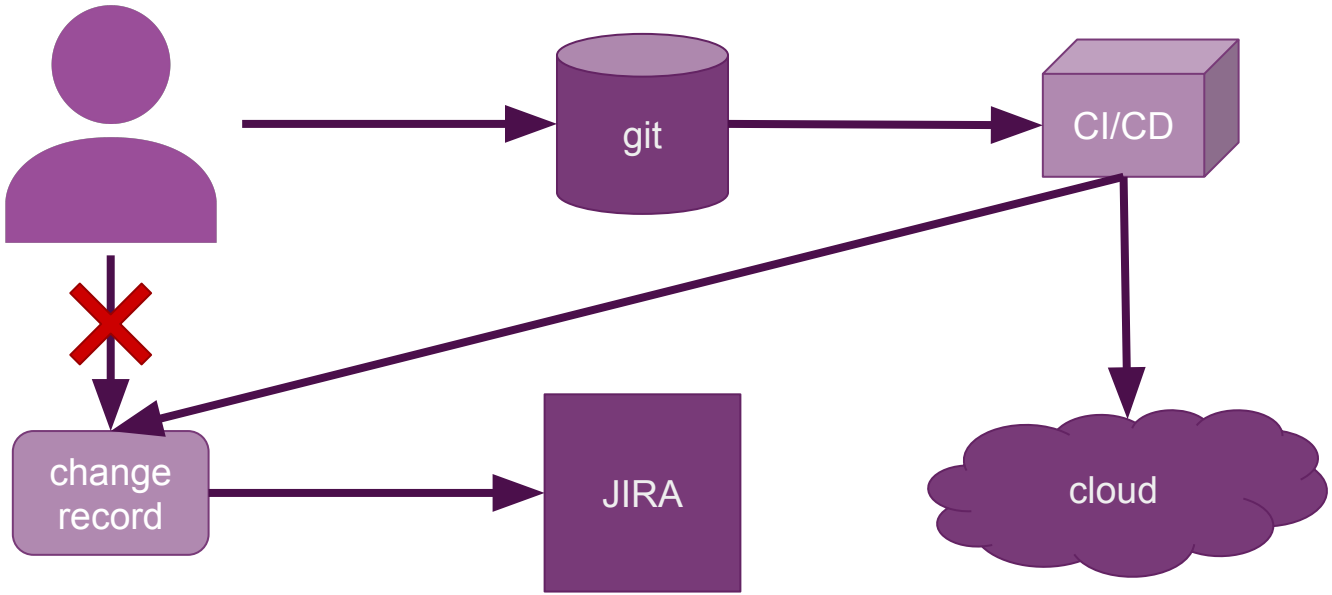
"ICT change management, including changes to software, hardware, firmware components, systems or security parameters,"

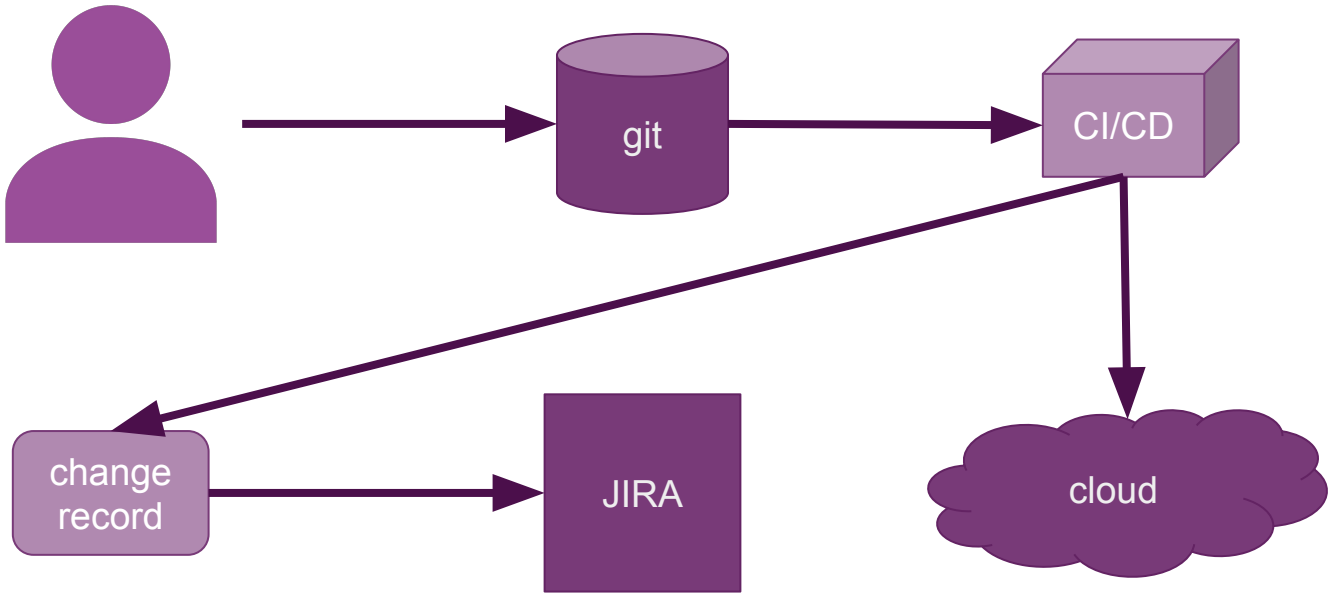



git
CI/CD
change
record
JIRA
cloud


change record
cicd
cloud
change record
JIRA


git
CI/CD
change
record
JIRA
cloud


git
CI/CD
change
record
JIRA
cloud

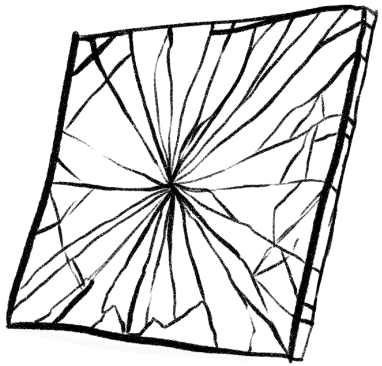

git
CI/CD
change
record
JIRA
cloud

traceability

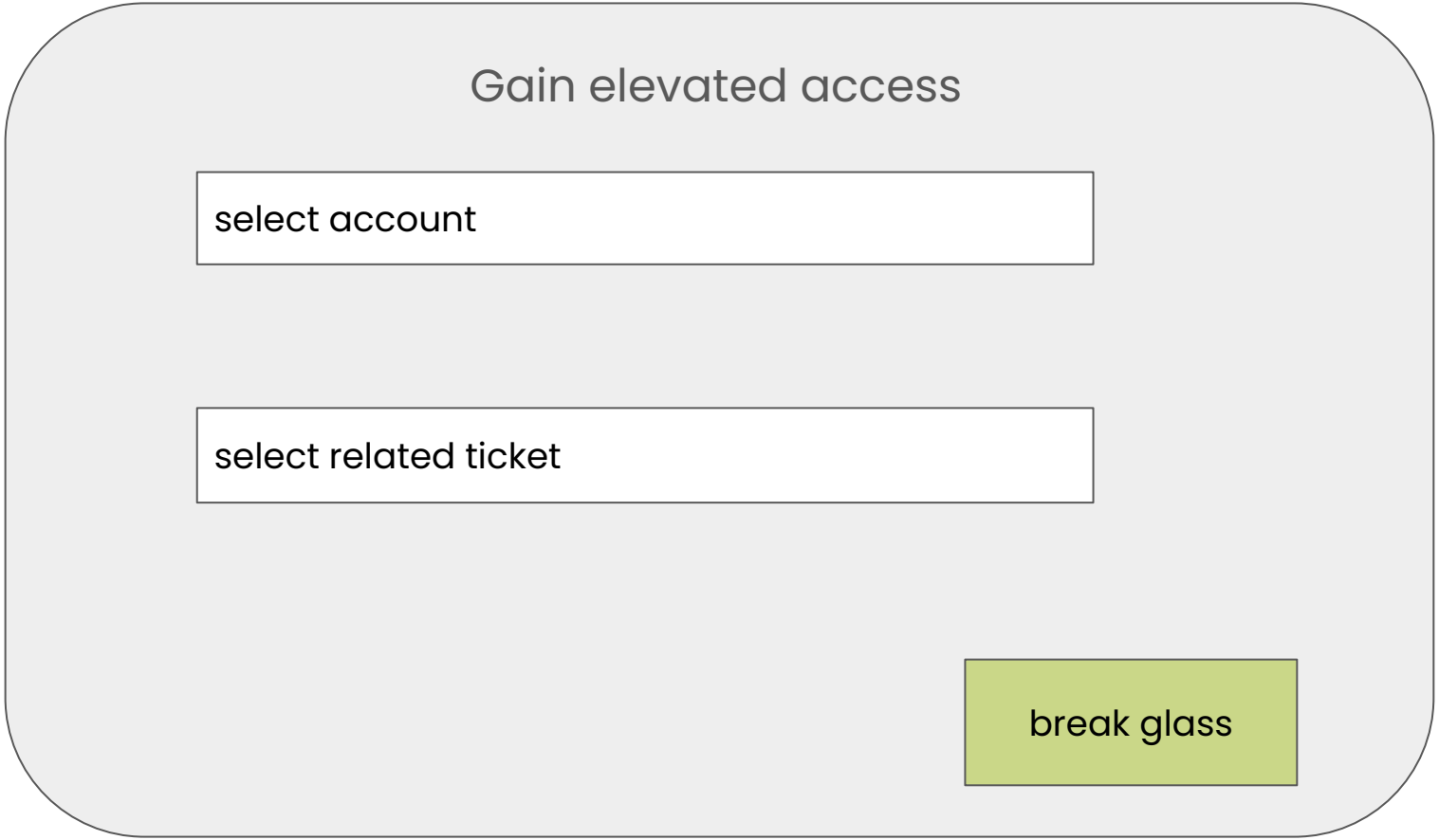


break glass

view,
read

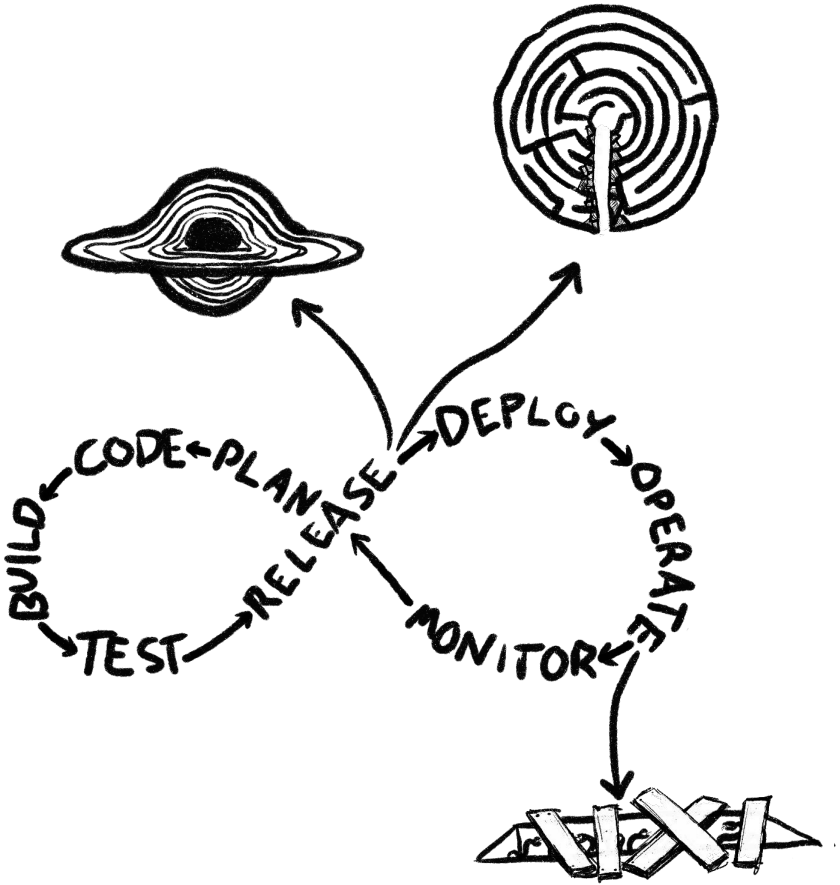


change,
read
sensitive
data


Gain elevated access
select account
select related ticket
break glass

<user_id> gained elevated access to <account_id> for <issue_id>
<user_id> on <account_id> read <row> in <database_id>
<user_id> on <account_id> read <secret_id>
<user_id> on <account_id> increased disk on <database_instance_id>




PLAN
CODE
BUILD
TEST
RELEASE
DEPLOY
OPERATE
MONITOR