Sample Software Development Cascade

Simple Salt
make security easy

Repo: branch → Branch → Trunk

developer: Branch clone — Dev, Unit Test / SAST → New code

Pull, Merge

Developer 2: Pair review

CI/CD: Lib/art gov → build; Release build; Approve

Library and artifact governance for software supply chain management

Test Env: App → Autotest DAST → Funct Test; build

UAT env: App → Integ. testing Cust. Accept → Vuln scan Pen Test

Assurance
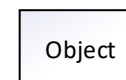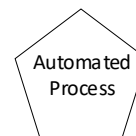
Sometimes performed on prod

Prod: App

Maturity Levels:
1: yeehaw!
2: controlled code and methodical testing
3: automated build and testing
4: Rigorous testing
5: integrated governance

Automated Process | Object | Manual Process | Sometimes Required

Created by Dylan Evans; shamelessly replicated from a May 2018 presentation by Alex Bauerts, co-pres MN OWASP