Ako testovať limity pracovníkov banky pri zásahoch do klientskych údajov

**Príklad**

Klient nahlásil, že zamestnanec pobočky upravil kontaktné údaje na účte bez súhlasu. Prišiel s tým, že operácia prebehla rýchlo, bez viditeľného auditu. Po preštudovaní záznamov sa zistilo, že pracovník mal nadlimitované práva (možnosť upravovať údaje) a systém nezaznamenal detailné kroky (kto, kedy, aké polia), čo skomplikovalo vyšetrenie a spätnú opravu. Takéto medzery vedú k reputačnému riziku, porušeniu regulácií a sťažnosti klienta.

# Ako otestovať

1. **Príprava a modelovanie scenárov**

* Zmapuj všetky role a úrovne prístupov (viewer, editor, supervisor, admin).
* Definuj limity (ktoré polia sa môžu meniť, kto potrebuje autorizáciu, pri akých hodnotách sa vyžaduje eskalácia).
* Vytvor testovacie účty naprieč rolami a automatizované testovacie dáta.

1. **Funkčné testy prístupov a oprávnení**

* Over, že užívateľ bez práva na editáciu nemôže meniť citlivé polia (IBAN, adresa, telefón).
* Testuj kombinácie rolí (napr. pracovník pobočky + dočasné oprávnenie).
* Skúšaj opravy na rôznych typoch účtov (fyzická osoba, firemný účet, joint account).

1. **Testy limitov a eskalácií**

* Simuluj situácie, kde zmena nad limit (napr. zmena limitu transakcií, zmena záznamov vo viac ako 3 poliach) vyžaduje supervisor podpis/OTP — over, že systém blokuje alebo žiada eskaláciu.
* Otestuj časové limity (dočasné práva udelené na určitý čas) — over automatické zrušenie práv po uplynutí.

1. **Auditné a loggingové testy**

* Over, že každá zmena sa loguje: kto, identifikátor pracoviska, timestamp, predchádzajúca a nová hodnota (differences), dôvod zmeny.
* Skontroluj integritu logov pri rôznych zlyhaniach (prerušenie spojenia, rollback transakcie).
* Testuj vyhľadávanie a filtrovateľnosť auditných záznamov (dátum, používateľ, typ zmeny).

1. **Bezpečnostné testy a zneužiteľné scenáre (negative testing)**

* Pokusy o obchádzanie pravidiel (manipulácia request parametrov, API s vyššími právami).
* Testy súbežných zmien: dvaja pracovníci upravujú rovnaký záznam — over riešenie konfliktu (locking, optimistic concurrency).
* Over, že zmeny cez interné nástroje (backoffice) aj cez API majú rovnaké validácie a audity.

1. **Testovanie procesov podpory a revízie**

* Over, či existuje workflow pre revert zmeny (kto môže vrátiť zmenu, ako sa identifikuje legitímny revert).
* Simuluj sťažnosť klienta a krok po kroku sleduj, či podpora dokáže z histórie rekonštruovať zmeny.
* Testuj notifikácie (interné upozornenia pri citlivej zmene) a SLA pre riešenie.

1. **Testovanie súladu s pravidlami a GDPR / reguláciami**

* Over, či sú splnené požiadavky na záznamy prístupov a možnosti poskytnutia logov klientovi/regulatorovi.
* Testuj anonymizáciu/export auditov pre právne požiadavky.

1. **Automatizácia a reportovanie**

* Automatizuj opakované kontroly práv a základné scenáre (CI testy pri nasadení).
* Vytvor report pre manažment: počet zásahov pracovníkov, percento eskalácií, príčiny reverzov.

**Krátke checklisty (rýchle kontroly)**

* Každá zmena má autora, čas, IP/identifikátor pracoviska.
* Zmeny citlivých polí vyžadujú dodatočné overenie/eskaláciu.
* Dočasné práva majú automatické vypršanie.
* API a UI majú rovnaké pravidlá.
* Logy sú nezmeniteľné (write-once / append-only) a archivované podľa pravidiel.

**#testing #qa #banking #security #accesscontrol #audit #GDPR #bankingIT**