# Segregation of Duties (SoD) vs Toxic Permissions Combinations (TPC)

Naiden Nedelchev © 2024

| | 1 DEFINITION | 2 OBJECTIVE | 3 FOCUS | 4 SCOPE | 5 PRIMARY CONCERN | 6 RISK MITIGATION | 7 EXAMPLES | 8 INSIGHTS |
|---|---|---|---|---|---|---|---|---|
| SEGREGATION OF DUTIES | SOD REFERS TO DIVIDING RESPONSIBILITIES AMONG INDIVIDUALS, TEAMS OR ENTITIES TO REDUCE THE RISK OF FRAUD OR ERROR. | PREVENT ERRORS, FRAUD, OR MISUSE BY ENSURING THAT NO SINGLE ACTOR HAS CONTROL OVER ALL CRITICAL ASPECTS OF A PROCESS. | DISTRIBUTION OF RISKY TASKS AND RESPONSIBILITIES ACROSS MULTIPLE ACTORS. | PROCESS AND ROLE-BASED. | WHO PERFORMS THE CRITICAL TASKS IN A PROCESS. | REDUCE RISK BY DIVIDING CRITICAL FUNCTIONS AMONG MULTIPLE ACTORS. | SEPARATING THE ROLES OF REQUESTOR, APPROVER AND OVERSEER IN CHANGE MANAGEMENT. | SOD OFTEN HELPS AVOID TOXIC PERMISSIONS BY ENSURING CRITICAL TASKS ARE SEPARATED AMONG USERS. |
| TOXIC PERMISSION COMBINATIONS | TPC REFERS TO ACCESS RIGHTS COMBINATIONS THAT CAN LEAD TO SECURITY RISK OR POLICY VIOLATION IF GRANTED TO A SINGLE USER. | IDENTIFY AND REMOVE EXCESSIVE, OVERLAPPING, OR CONFLICTING PERMISSIONS THAT COULD LEAD TO VIOLATIONS AND ASSETS MISUSE. | AVOIDANCE OF RISKY COMBINATIONS WHEN AUTHORIZING SYSTEM PERMISSIONS. | PERMISSIONS AND AUTHORIZATIONS-BASED. | WHAT PERMISSIONS A USER HAS AND ARE THEY VIOLATING THE LEAST PRIVILEGE AND NEED TO KNOW PRINCIPLES. | OPTIMIZE RISK FROM MULTIPLE VULNERABILITIES COVERAGE WITHIN A SINGLE USER IDENTITY. | A SYSTEM USER HAS MULTIPLE ACCOUNTS FOR A SAAS SERVICE, WITH ONE BEING AN ADMINISTRATOR. | TOXIC PERMISSIONS ARE A BYPRODUCT OF POOR SOD OR LACK OF COMPLIANT WITH SECURITY PRINCIPLES IAM ARCHITECTURE |