

No. 02

SAP GRC

Access Control Field Guide

SAP GRC Access Control and segregation of duties, explained for beginners

oJAYo.com

oJAYo

FREE SAMPLE · ojayo.com

SECTRAININGNOW SERIES · NO. 02

Access Control Field Guide

SAP GRC Access Control and segregation of duties, explained for beginners

oJAYo
Published by oJAYo.com

FREE SAMPLE · ojayo.com

Access Control Field Guide
SAP GRC Access Control and segregation of duties, explained for beginners

First edition, 2026. Copyright © 2026 oJAYo. Published by oJAYo.com. All rights reserved. No part of this book may be reproduced or shared without written permission, except for brief quotations in reviews.

This book is an independent publication. SAP, SAP S/4HANA, SAP Fiori, SAP Gateway, SAP BTP, SAP Build Work Zone and other SAP products mentioned are trademarks or registered trademarks of SAP SE in Germany and other countries. All other product names are trademarks of their respective owners. oJAYo.com is not affiliated with, sponsored by or endorsed by SAP SE or any other vendor named in this book.

The information in this book is provided for education. Product features change between releases; always confirm details in the official documentation for your release before changing a production system. Screens marked “Illustration” are simplified drawings, not captures of real SAP software. Company and person names in examples are fictional.

[ISBN: add if registered]

FREE SAMPLE · ojayo.com

CONTENTS

How to use this book 1

PART I · FOUNDATIONS

1 Why access risk matters 4
2 SAP Access Control at a glance 8
3 Rule sets explained 13

PART II · DAILY OPERATIONS

4 Access risk analysis 19
5 Remediation and mitigating controls 23
6 Access request management 27
7 Emergency access management 31
8 Business role management 36
9 Periodic reviews 40

PART III · RUNNING A GRC PROGRAM

10 Get clean, stay clean, prove clean 45
11 Audit evidence and common findings 48
12 What's next — and a readiness checklist 52

Glossary 55
Further reading 58

FREE SAMPLE · ojayo.com

BEFORE YOU BEGIN

How to use this book

What this book covers, who it is for, and how to use it.

Every company that runs SAP has the same quiet problem: over time, people collect access. They change jobs, cover for colleagues, join projects and keep permissions “just in case.” Sooner or later, someone can do two things that should never sit in the same hands — such as creating a supplier and paying that supplier. Auditors call this a **segregation of duties** (SoD) conflict, and finding and controlling such conflicts is the core job of **SAP Access Control**, part of SAP's governance, risk and compliance (GRC) portfolio.

This book is a beginner's field guide to SAP Access Control. It explains the ideas first — risks, functions, rule sets, mitigation — and then walks through the daily work: analyzing risk, handling access requests, managing emergency access, designing roles, running reviews and preparing evidence for auditors.

Who this book is for

- **People starting in SAP security or GRC** who need a clear map before they open the system.
- **Business process owners and approvers** who receive GRC requests and want to understand what they are approving.
- **Internal auditors and controls teams** who rely on GRC reports and want to know how they are produced.

How the book is organized

- **Part I — Foundations** (Chapters 1–3): why access risk matters, SAP Access Control at a glance, and how rule sets work.

FREE SAMPLE · ojayo.com

- **Part II — Daily operations** (Chapters 4–9): risk analysis, remediation and mitigation, access requests, emergency access, role management and periodic reviews.
- **Part III — Running a GRC program** (Chapters 10–12): getting clean and staying clean, audit evidence, and what is changing in SAP's GRC roadmap.

A glossary and reading list are at the back.

Conventions

TIP

Practical advice you can apply straight away.

IN SAP

Product-specific details and transactions.

WATCH OUT

Common mistakes and risks.

Transactions and technical names appear in a monospaced font, such as `PFCG` or `GRAC_SPM`. Diagrams are original. Screens marked **Illustration** are simplified drawings, not captures of SAP software, and all values in them are examples. People and companies in examples are fictional.

A NOTE ON VERSIONS

Most of this book describes SAP Access Control 12.0, the version most customers run today, and the concepts that carry over to SAP's newer offerings. Menus, apps and options differ between releases and support packages. Always confirm details in SAP's documentation for your system.

FREE SAMPLE · ojayo.com

PART I

Foundations

Why access risk matters, what SAP Access Control does, and how a rule set turns business risks into something a system can check.

FREE SAMPLE · ojayo.com

CHAPTER 1

Why access risk matters

Before learning the tool, it helps to understand the problem it solves — and why auditors care so much about it.

Most business fraud does not involve hackers. It involves trusted people with too much access, and processes that let one person complete a sensitive task from start to finish without anyone else noticing. Access governance exists to make that difficult.

Segregation of duties in one picture

The classic example comes from purchasing and payables. If one person can **create a supplier** and also **pay that supplier**, they could invent a supplier with their own bank account, send it an invoice, and pay it. Each step looks normal on its own.

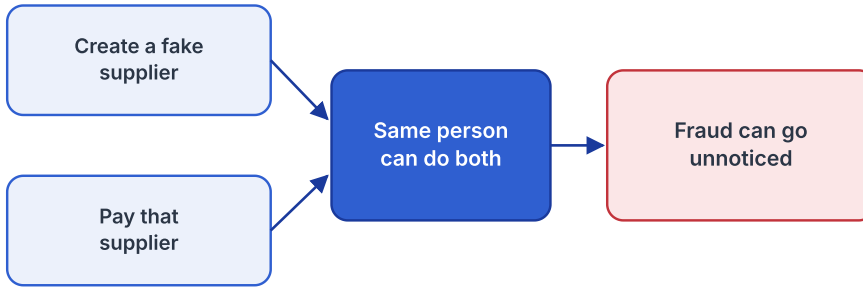


Figure 1.1 The idea behind segregation of duties. Each task is legitimate; the risk comes from combining them in one person.

FREE SAMPLE · ojayo.com

Segregation of duties (SoD) means splitting such steps between different people, so that completing the sensitive process needs at least two of them. The same thinking applies across the business:

- creating a purchase order and approving it;
- posting a journal entry and approving it;
- maintaining employee pay data and running payroll;
- creating users and assigning roles to them.

Critical access

Some access is risky even on its own, without any combination. Examples include changing system settings in production, opening and closing accounting periods, maintaining bank details for payments, or administering users. These are usually called **critical access** (or sensitive access). They should be held by few people, for clear reasons, and monitored.

Why auditors care

For companies listed in the United States, the **Sarbanes–Oxley Act** (SOX) requires management to maintain internal controls over financial reporting, and external auditors to test them. Similar expectations exist in many other countries and industries. Because SAP systems often run the processes that produce financial results, auditors routinely test:

- **who can do what** in SAP (access controls);
- whether SoD conflicts exist, and if they do, whether **mitigating controls** cover them;
- whether **new access** is approved before it is granted;
- whether **access is reviewed** regularly; and
- whether **privileged or emergency access** is controlled and logged.

These are often grouped as **IT general controls** for access. Weak access controls are among the most common audit findings in SAP environments.

FREE SAMPLE · ojayo.com

Why manual control does not scale

A small company can track access in a spreadsheet. A large SAP landscape cannot:

- There may be thousands of users and roles, and tens of thousands of transactions and authorization values.
- A single role can contain hundreds of authorizations; a user can hold dozens of roles.
- Whether a user can *really* perform a function depends not just on transaction codes, but on authorization objects and field values.
- Access changes every day as people join, move and leave.

This is the problem SAP Access Control automates: it holds a **rule set** describing risky combinations, compares it with the real authorizations in your systems, and builds checks into the processes that change access.

Preventive and detective controls

Access governance uses both kinds of control:

- **Preventive** controls stop a risk from being introduced: for example, analyzing every access request for SoD conflicts *before* approval.
- **Detective** controls find risks that already exist or activity that already happened: for example, a quarterly SoD report or a review of emergency access logs.

Good programs use both. Preventive checks keep new problems out; detective checks catch what slipped through and prove to auditors that controls work.

> **TIP**
> When you explain GRC to a business manager, avoid jargon. Say: *"We are making sure no single person can complete a sensitive process alone, and that when someone needs extra access, it is approved, time-limited and checked."*

FREE SAMPLE · ojayo.com

KEY TAKEAWAYS

- **Segregation of duties** splits sensitive processes so that no one person can complete them alone.
- **Critical access** is risky on its own and must be limited and monitored.
- Auditors test access approvals, SoD, mitigating controls, reviews and privileged access.
- Large SAP landscapes need **automation**: a rule set compared with real authorizations, plus checks built into access processes.
- Combine **preventive** and **detective** controls.

FREE SAMPLE · ojayo.com

CHAPTER 2

SAP Access Control at a glance

SAP Access Control is a suite of connected capabilities. This chapter maps them, explains where they came from, and shows how the system connects to your SAP landscape.

SAP Access Control (often still called “GRC Access Control” or simply “GRC”) brings together the main access-governance processes in one application. SAP describes it in terms of five capabilities.

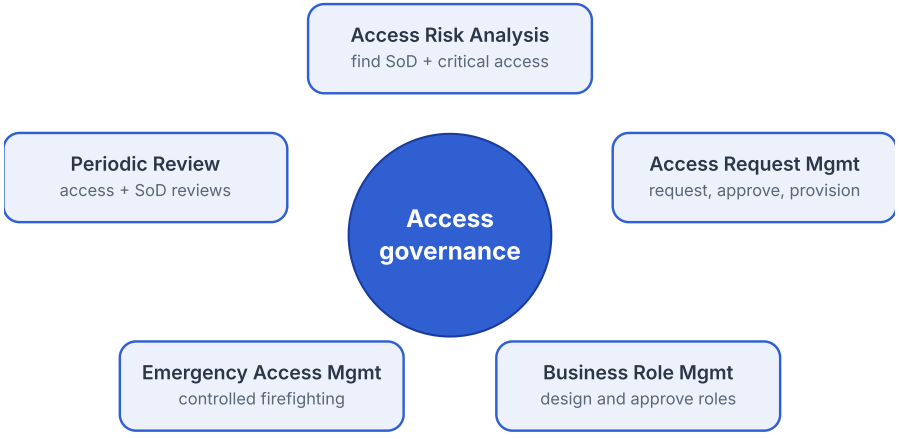


Figure 2.1 The five capabilities of SAP Access Control around the shared goal of access governance.

FREE SAMPLE · ojayo.com

The oJAYo library

170 plain-language PDF books · $49 each · free sample of every book at ojayo.com

SAP SECURITY · 67 BOOKS

SAP Role Design Handbook
Access Control Field Guide (you are reading this)
Signavio Process Governance
ABAC in Practice
Auditing SAP Systems
Securing SAP BTP
Securing SAP Fiori
SAP User Training Playbook
SAP Basis Essentials
SAP HANA Security
SAP Authorization Troubleshooting
HR and Payroll Security
Finance and Procurement Authorizations
BW and BusinessObjects Security
SAP Network and Web Security
SAP Security Interview Guide
SAP Cloud ALM Security
SAP Data Services Security
SAP Architecture Explained
SAP SD Security
SAP CRM Security
SAP SRM Security
SAP Ariba Security
SailPoint for SAP
SAP PP Security
SAP QM Security
PI/PO and Integration Suite Security
SAPUI5 Security
Testing in SAP Cloud ALM with Jira
SAP SLT Security
SAP PS Security
SAP Plant Maintenance Security
SAP EWM Security
SAP Digital Manufacturing Security
SAP SuccessFactors Security
Security in SAP Activate
SAP Concur Security
SAP Fieldglass Security
SAP Analytics Cloud Security
SAP Datasphere and Business Data Cloud Security
SAP Build and Work Zone Security
Joule and SAP Business AI Security
SAP MDG Security
SAP TM Security
SAP IBP Security
SAP GTS Security
SAP Sales, Service and Commerce Cloud Security
SAP S/4HANA Cloud Public Edition Security
SAP Business One and ByDesign Security
SAP Identity Management Migration
SAP Security Patching
Threat Detection and SIEM for SAP
Data Privacy (GDPR) for SAP
RISE with SAP Security
Ransomware and Incident Response for SAP
Compliance Mapping for SAP
Third-Party and Support Access for SAP
SAP Process Control and Risk Management
SAP Cloud Identity Access Governance
SAP Cloud Identity Services
SAP System Hardening
SAP Certificates and Encryption
SAP Penetration Testing
SAP Security Roadmap
Secure Development on SAP BTP
SAP Data Custodian and Data Sovereignty
Threat Intelligence for SAP

CYBERSECURITY · 64 BOOKS

Zero Trust Networks
Productivity at Work
ABAP Custom Code Security
S/4HANA Conversion Role Redesign
Getting Started with Canva AI
Getting Started with Character.AI
Getting Started with DeepL
Getting Started with Perplexity
Prompt Engineering
Cybersecurity Basics
Python for Beginners
JavaScript for Beginners
DevOps and Platform Engineering
AI-Powered Cyber Attacks
Securing AI Agents and Shadow AI
Ransomware
Phishing and Social Engineering
Deepfakes and Identity Fraud
Post-Quantum Cryptography
Software Supply Chain Security and DevSecOps
OT and Industrial Security
Sovereign Cloud and Data Sovereignty
Geopolitical Cyber Risk
Cloud Security and Identity Protection
Identity and Access Management Basics
Privileged Access Management
Passwordless and Passkeys
Identity Threat Detection and Response
SSO and Federation
AWS Security Fundamentals
Microsoft Azure and Entra ID Security
Google Cloud Security
Kubernetes and Container Security

FREE SAMPLE · ojayo.com

The oJAYo library (continued)

170 plain-language PDF books · $49 each · free sample of every book at ojayo.com

Cloud Security Posture Management
Serverless Security
OWASP Top 10 for Web Applications
API Security
Secure Coding Practices
Threat Modeling
Mobile App Security
SOC Fundamentals
Incident Response Planning
Digital Forensics
Threat Hunting
EDR and XDR
Malware Analysis Basics
Ethical Hacking for Beginners
Red Teaming and Purple Teaming
Bug Bounty Hunting
CTF for Beginners
Data Loss Prevention
Encryption Basics
Privacy Engineering and Privacy by Design
Data Classification and Governance
NIST CSF 2.0
ISO 27001
SOC 2 for Startups
PCI DSS 4.0
HIPAA Security for Healthcare
Third-Party and Vendor Risk Management
Email Security: DMARC, SPF and DKIM
IoT and Smart Device Security
Cyber Insurance
Security Awareness Training Programs

AI · 11 BOOKS

Working with Claude
Working with ChatGPT
Getting Started with Google Gemini
Getting Started with DeepSeek
Getting Started with Grok
Getting Started with Microsoft Copilot
Agentic AI Explained
MCP: The Model Context Protocol
Vibe Coding
AI Coding Tools
AI Detection

CERTIFICATION GUIDES · 28 BOOKS

CompTIA Security+ Study Guide
ISC2 CC Study Guide
ISC2 CISSP Study Guide
ISACA CISM Study Guide
ISACA CISA Study Guide
ISACA CRISC Study Guide
ISC2 CCSP Study Guide
CompTIA CySA+ Study Guide
CompTIA PenTest+ Study Guide
EC-Council CEH Study Guide
OffSec OSCP+ Study Guide
CompTIA SecurityX Study Guide
GIAC GSEC Study Guide
AWS Certified Security - Specialty Study Guide
Microsoft Security Certifications Study Guide
CompTIA SecAI+ Study Guide
ISACA AAISM Study Guide
ISACA AAIA Study Guide
ISACA AAIR Study Guide
IAPP AIGP Study Guide
ISO/IEC 42001 Lead Implementer and Lead Auditor…
AWS Certified AI Practitioner Study Guide
AWS Certified Machine Learning Engineer - Associ…
AWS Certified Generative AI Developer - Profession…
Microsoft AI-901 Study Guide
Microsoft AI-103 Study Guide
Google Cloud Generative AI Leader Study Guide
Google Cloud Professional Machine Learning Engin…

BUNDLES · 18 PACKS, SAVE UP TO $145

SAP Security Starter Pack (5 books, $149)
SAP GRC and Audit Pack (5 books, $129)
S/4HANA Migration Security Pack (4 books, $109)
SAP Cloud Security Pack (5 books, $129)
SAP Threat Defense Pack (5 books, $129)
Cybersecurity Starter Pack (5 books, $129)
Identity and Access Pack (5 books, $129)
Cloud Security Pack (6 books, $149)
SOC and Incident Response Pack (5 books, $129)
Application Security Pack (5 books, $129)
Security Compliance Pack (5 books, $129)
Ethical Hacking Pack (5 books, $129)
AI at Work Pack (5 books, $129)
AI Developer Pack (5 books, $129)
AI Security and Governance Pack (5 books, $129)
CISSP + Security+ Exam Pack (2 books, $79)
ISACA Exam Pack (3 books, $99)
AI Certification Pack (4 books, $109)

END OF FREE SAMPLE

Access Control Field Guide

Enjoyed it? The full book has 63 pages and 12 chapters.
Instant PDF download, $49.

Get the full book

ojayo.com · Created by the oJAYo expert team

This sample may be shared freely. The full book is licensed to one reader.