

No. 103

CYBERSECURITY

Identity and Access Management Basics

Who can access what, and how to keep it that way

oJAYo.com

oJAYo

FREE SAMPLE · ojayo.com

SECTRAININGNOW SERIES · NO. 103

Identity and Access Management Basics

Who can access what, and how to keep it that way

oJAYo
Published by oJAYo.com

FREE SAMPLE · ojayo.com

Identity and Access Management Basics
Who can access what, and how to keep it that way

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. Product and company names mentioned in this book are trademarks of their respective owners. All other product names are trademarks of their respective owners. oJAYo.com is not affiliated with, sponsored by or endorsed by any vendor named in this book.

The information in this book is provided for general education. AI products, features, plans, prices and policies change frequently; always confirm details in the vendor's current documentation. Screens marked “Illustration” are simplified drawings, not captures of real 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 What IAM is 4
2 Why IAM matters 6
3 Identities and accounts 7
4 The four steps of access 9
5 Directories and identity providers 11
6 IAM and zero trust 12

PART II · AUTHENTICATION

7 Authentication factors 14
8 Passwords done right 15
9 Multi-factor authentication 17
10 Passkeys and passwordless 19
11 Single sign-on and federation 20
12 Account recovery 21
13 Biometrics 22

PART III · AUTHORIZATION

14 Least privilege 25
15 Role-based access control 26
16 Other authorization models 28
17 Segregation of duties 30
18 Privileged access 31
19 Common IAM mistakes 32

PART IV · LIFECYCLE AND GOVERNANCE

20 Joiners, movers and leavers 34
21 Access requests and approvals 36
22 Access reviews 37

FREE SAMPLE · ojayo.com

23 Non-human identities 39
24 Customer identity 40
25 Monitoring identity 41
26 Architecture and tools 42
27 An IAM roadmap 44
28 A worked example 45
Checklists 46
Glossary 47
Further reading 48

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.

Identity and access management (IAM) is the discipline of making sure the right people and systems have the right access to the right resources, at the right time, for the right reasons, and no more. It sounds administrative, but it sits at the heart of security: most breaches involve a stolen, misused or over-privileged identity.

This book explains IAM from the ground up for beginners. It covers what identities are, how authentication and authorization work, how access is granted and removed over time, and how organizations govern access to stay secure and pass audits.

What this book covers

- Identities, accounts and the four steps of access.
- Authentication: passwords, MFA, passkeys and single sign-on.
- Authorization: roles, attributes, policies and least privilege.
- The identity lifecycle: joiners, movers and leavers.
- Governance: access reviews, segregation of duties and audits.
- Privileged and non-human identities, monitoring and a roadmap.

Who this book is for

- **IT staff and help-desk teams** who manage accounts.
- **Security beginners** and students.
- **Managers and application owners** who approve access.

FREE SAMPLE · ojayo.com

How the book is organized

- **Part I — Foundations** (Chapters 1–6): what IAM is, why it matters, identities and accounts, the four steps of access, directories, and zero trust.
- **Part II — Authentication** (Chapters 7–13): factors, passwords, MFA, passkeys, single sign-on, account recovery, and biometrics.
- **Part III — Authorization** (Chapters 14–19): least privilege, roles, other models, segregation of duties, privileged access, and common mistakes.
- **Part IV — Lifecycle and governance** (Chapters 20–28): joiners, movers and leavers; requests and approvals; access reviews; non-human identities; customer identity; monitoring; architecture and tools; a roadmap; and a worked example.
- **Reference**: checklists, glossary and further reading.

Callouts

TIP
Practical advice you can use straight away.

IN PRACTICE
How an idea looks in a real organization.

WATCH OUT
Common mistakes and risks.

KEY IDEA
The one thing to remember from a section.

A note on screens

Screens are **simplified illustrations**, not captures of real products. Names are fictional.

FREE SAMPLE · ojayo.com

PART I

Foundations

These chapters explain what IAM is, why it matters so much for security, what identities are and how access decisions are made.

FREE SAMPLE · ojayo.com

CHAPTER 1

What IAM is

IAM controls who can do what.

A simple definition

IAM is the combination of **processes**, **policies** and **technology** that manages digital identities and controls their access to systems and data.

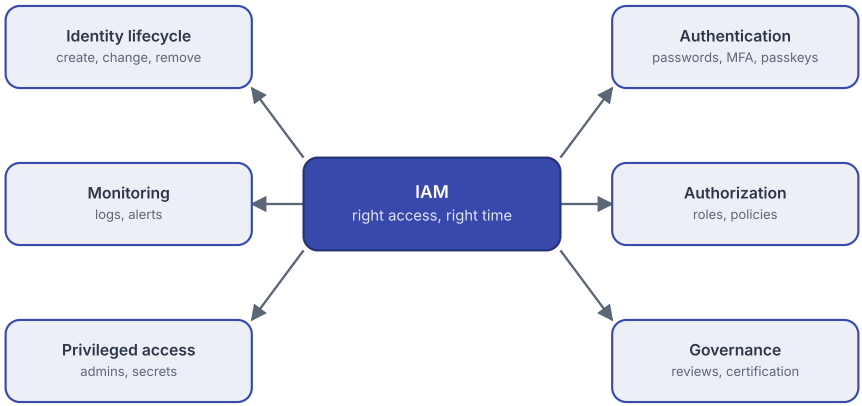


Figure 1.1 The building blocks of IAM

Everyday examples

- A new employee receives an email account and access to the systems their job needs.
- You sign in to an app with your work account and approve a prompt on your phone.
- A manager confirms each quarter that their team still needs access to the finance system.

FREE SAMPLE · ojayo.com

- A leaver's accounts are disabled on their last day.

Who is involved

IAM is not only an IT job. HR provides the source of truth about people, managers approve access, application owners define roles, and security sets policies.

KEY IDEA

IAM answers three questions: who are you, what can you access, and should you still have it?

FREE SAMPLE · ojayo.com

CHAPTER 2

Why IAM matters

Identity is the target of most modern attacks.

Attackers log in

Attackers rarely "hack in" through clever code. More often they **log in** with stolen passwords, tokens or reset tricks. Verizon's 2026 Data Breach Investigations Report found a human element in 62% of breaches, and Google's cloud research found identity compromise behind most cloud and SaaS compromises it investigated.

Excess access multiplies damage

When an account has more access than it needs, a single compromise exposes far more. Good IAM limits the **blast radius**.

Compliance

Regulations and standards such as GDPR, SOX, HIPAA, PCI DSS, ISO 27001 and SOC 2 all require controlled, reviewed access.

Productivity

Done well, IAM also makes life easier: one sign-in, fast access on day one and self-service requests.

FREE SAMPLE · ojayo.com

CHAPTER 3

Identities and accounts

Many kinds of identity need managing.

Identity type	Examples
Workforce	employees, contractors
Customer	app and website users
Partner	suppliers, guests
Non-human	service accounts, API keys, bots
AI agents	assistants acting for people

Figure 3.1 Kinds of digital identity

Identity versus account

An **identity** represents a person or thing. An **account** is that identity's presence in a particular system. One person may have dozens of accounts across applications.

Attributes

Identities carry **attributes**: name, department, job title, manager, location, employment status. These drive access decisions and automation.

Non-human identities

Service accounts, API keys and bots often outnumber people and frequently hold powerful access. AI agents acting for people are a fast-growing new category.

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
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 (you a…
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

Identity and Access Management Basics

Enjoyed it? The full book has 53 pages and 28 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.