DevOpsSchool

Course curriculum · November 2026

LEVEL 04 OF 04 · ADVANCED

AWS Security Identity Compliance Advanced Training

Govern security across AWS Organizations with guardrails, data perimeters, compliance automation and incident playbooks.

LIVE ONLINE **Max 8-10 hours**	CORPORATE (DAY-WISE) **5 days · Days 1-5**	SELF-PACED VIDEO **1-year LMS access**
BATCH SIZE **Max 10 learners**	NEXT BATCHES **1st of every month · weekends: first Saturday**	CERTIFICATE **Verifiable certificate of completion**

Foundation	Essential	Intermediate	Advanced
1 day · Included	2 days · Included	3 days · Included	5 days · This curriculum

INSIDE THIS CURRICULUM

What you will achieve	Outcomes and level focus
Who should attend	Audience and prerequisites
Agenda	46 topics · Foundation to Advanced
Hands-on labs	4 labs
Formats and fees	Live, 1:1, self-paced, corporate
Trainer and reviews	Rajesh Kumar
Enrolment	Batches, payment, contacts

WHY DEVOPSSCHOOL

- Rated 4.6 on Google
- 1,500+ verifiable certificates issued in the public registry
- Trainer Rajesh Kumar: 20 years in industry
- Small batches: max 10 learners, every session recorded

Course page: www.devopsschool.com/courses/aws/aws-security-identity-compliance-advance-training.html
Talk to us: WhatsApp +91 99057 40781 · +1 (469) 756-6329 · contact@DevOpsSchool.com · reply within 1 hour

OUTCOMES

What you will achieve

By the end of the AWS Security Identity Compliance course path, you will be able to:

1

Control identity and access

Design least-privilege IAM, federation and cross-account access that scales across accounts.

2

Protect data and detect threats

Encrypt data with KMS, manage secrets and detect and respond to threats with AWS security services.

3

Automate compliance and governance

Enforce organisation-wide guardrails and produce continuous compliance evidence.

WHAT THE ADVANCED LEVEL ADDS

Organisation guardrails, data perimeters and compliance automation

Hands-on: Secure multi-account landing zone. Apply SCPs, a data perimeter and delegated security services across an organisation and produce an automated compliance report.

WHO SHOULD ATTEND

- Experienced AWS Security Identity Compliance practitioners responsible for quality, security and scale.
- Senior engineers, architects and leads who design and troubleshoot AWS Security Identity Compliance solutions.
- Teams making AWS Security Identity Compliance an organisation-wide standard.

BEFORE YOU START

- The Intermediate level, or equivalent hands-on experience.
- You can already: Detect, investigate and respond to threats with GuardDuty, Security Hub, Inspector, Macie, WAF and automation.
- Basic computer skills and a laptop with a stable internet connection for the live sessions and labs.
- This curriculum includes every earlier level, so it is complete on its own.

AGENDA · FOUNDATION TO ADVANCED

AWS Security Identity Compliance Advanced Training agenda

46 topics. Each level builds on the one before it, so this curriculum lists every earlier level in full. Days are for corporate (day-wise) delivery; live online batches cover the same agenda in max 8-10 hours.

DAY 1 — Foundation: Shared responsibility, IAM basics and account security

Included from Foundation

1. Shared responsibility model: security of the cloud versus security in the cloud by service type
2. AWS security services landscape: identity, detection, infrastructure protection, data protection and compliance
3. Root user protection: MFA, removing access keys, alternate contacts and account recovery
4. IAM fundamentals: users, groups, roles, access keys and console sign-in
5. IAM policy structure: Effect, Action, Resource, Condition and reading JSON policies
6. Managed policies: AWS managed versus customer managed policies and least privilege from the start
7. Network security basics: security groups versus network ACLs and private subnets
8. Encryption concepts: encryption at rest and in transit, keys and certificates
9. Logging basics: AWS CloudTrail event history and creating a trail
10. Compliance programs: AWS Artifact reports, SOC, ISO 27001, PCI DSS and HIPAA eligibility
11. Security checks: AWS Trusted Advisor and the IAM credential report

DAY 2 — Essential: Advanced IAM, federation, encryption and secrets

Included from Essential

12. Policy evaluation logic: explicit deny, identity-based, resource-based and session policies
13. Roles and STS: AssumeRole, trust policies, temporary credentials and cross-account access
14. Permissions boundaries: delegating IAM administration safely
15. IAM Identity Center: permission sets, multi-account access and an external identity provider
16. IAM Access Analyzer: external access findings, unused access and policy validation
17. AWS KMS: AWS managed versus customer managed keys, key policies, grants and envelope encryption
18. Secrets management: Secrets Manager rotation and Systems Manager Parameter Store SecureString
19. S3 data protection: Block Public Access, bucket policies, SSE-S3 versus SSE-KMS and Object Lock
20. Certificates: AWS Certificate Manager public and private certificates and renewal
21. VPC protection: VPC endpoints with endpoint policies and VPC Flow Logs
22. Configuration compliance: AWS Config managed rules and remediation
23. Application identity: Amazon Cognito user pools and identity pools

DAY 3 — Intermediate: Threat detection, protection services and incident response

Included from Intermediate

24. Amazon GuardDuty: threat findings, protection plans for S3, EKS and malware, and suppression rules
25. AWS Security Hub: security standards such as CIS AWS Foundations and AWS Foundational Security Best Practices
26. Amazon Inspector: vulnerability scanning for EC2, ECR images and Lambda functions
27. Amazon Macie: sensitive data discovery in S3 and findings handling
28. Amazon Detective: investigating findings with behaviour graphs
29. Edge protection: AWS WAF rules and managed rule groups, AWS Shield Standard and Advanced
30. Network protection: AWS Network Firewall and DNS Firewall

31. Automated response: EventBridge rules with Lambda or Systems Manager Automation runbooks
32. Secure operations: Session Manager without SSH keys and Patch Manager baselines
33. Centralised logging: organization trails, a log archive account and CloudWatch Logs retention
34. Troubleshooting access: policy simulator, CloudTrail lookups and access-denied error messages

DAYS 4-5 **Advanced: Organisation guardrails, data perimeters and compliance automation** — **New at this level**

35. Organization guardrails: service control policies and resource control policies
36. Landing zone security: AWS Control Tower controls, security and log archive accounts
37. Data perimeter: identity, resource and network perimeter conditions and VPC endpoint policies
38. Attribute-based access control: tagging strategies and session tags
39. Advanced key management: multi-Region keys, CloudHSM, imported key material and key rotation
40. Compliance automation: AWS Config conformance packs and AWS Audit Manager frameworks
41. Amazon Security Lake: centralising security data in OCSF and subscriber access
42. Incident response: playbooks, isolation, forensic snapshots and post-incident review
43. Delegated administration: running security services across all accounts and Regions
44. Security pillar review: Well-Architected Security pillar and tracking remediation
45. Regulatory mapping: mapping controls to PCI DSS, HIPAA, ISO 27001 and GDPR requirements
46. Capstone: secure multi-account landing zone with automated compliance reporting

PRACTICE

Hands-on labs

You build these yourself during the course, guided by the trainer.

FOUNDATION **Secure a new AWS account**
Harden the root user, create admin and developer groups with least-privilege policies, enable CloudTrail and review the credential report.

ESSENTIAL **Least-privilege cross-account access**
Set up Identity Center with permission sets, a cross-account role, KMS-encrypted S3 data and rotating secrets for an app.

INTERMEDIATE **Detect and respond to an attack**
Enable GuardDuty, Security Hub and Inspector, simulate suspicious activity and auto-remediate a finding with EventBridge and Lambda.

ADVANCED **Secure multi-account landing zone**
Apply SCPs, a data perimeter and delegated security services across an organisation and produce an automated compliance report.

HOW YOU CAN LEARN

Formats and fees

The same agenda in four formats. Fees are in Indian rupees as of November 2026; the course page shows them in your currency.

FORMAT	DURATION	WHAT YOU GET	FEE
Live & interactive (online)	Max 8-10 hours	Instructor-led public batch of max 10 learners with demos, labs, Q&A and assignment review. Weekday batches start on the 1st of every month, weekend batches on the first Saturday of every month.	**INR 34,999**
1:1 live training (online)	Max 8-10 hours, one-to-one	The same agenda, taught one-to-one by the trainer. Starts immediately, without waiting for the next batch; sessions planned around your working hours, at your pace.	**INR 99,999**
Self-paced video	1-year LMS access	All four AWS Security Identity Compliance levels, plus 20+ more courses and 50+ tools, at your own pace.	**INR 833/month** billed yearly at INR 9,996
Corporate (day-wise)	5 days for this level	A private batch for your team, on demand. Foundation 1 day, Essential 2, Intermediate 3, Advanced 5 (cumulative).	**Quote on request**

ASSESSMENT AND CERTIFICATE

Your progress is checked through hands-on labs and assignments at every level. On completion you receive a DevOpsSchool certificate of completion with a unique credential ID that anyone can verify at devopsschool.com/certificates.

INCLUDED WITH EVERY LIVE BATCH

- Every live session is recorded and stays in your LMS for a year.
- Can't attend your batch? Move to next month's batch.
- Free demo class before you pay.
- Free 10-15 minute call with an advisor or the trainer to check the course fits you.

YOUR TRAINER

Learn from Rajesh Kumar

Principal Architect, trainer and mentor in DevOps, SRE, DevSecOps and platform engineering, with 20 years across 8+ software MNCs, including Staff DevOps/SRE Engineer for a leading Japanese mobile-payment platform and Principal DevOps Architect and Manager in Europe.

Profile: www.rajeshkumar.xyz · Videos: youtube.com/@TheDevOpsSchool

20 years in industry	**200+** corporate trainings
10,000+ engineers mentored	**70+** organisations coached

REVIEWS

What learners say

Rated 4.6 on Google · more reviews at devopsschool.com/testimonials and in our video testimonials.

> “Rajesh is very good trainer. Rajesh was able to resolve our queries and question effectively. We really liked the hands-on examples covered during this training program.”
>
> Indrayani, India

> “Very well organized training, helped a lot to understand the AWS concept and detailed related to various tools. Very helpful”
>
> Sumit Kulkarni, Software Engineer

START YOUR AWS SECURITY IDENTITY COMPLIANCE TRAINING

Join the next batch

Weekday batches start on the 1st of every month and weekend batches on the first Saturday of every month, with max 10 learners each. 1:1 training can start immediately; corporate batches run on demand. We reply within 1 hour.

Pay by UPI, credit and debit cards, net banking or PayPal. Before you pay, read our refund policy. All levels of this course: www.devopsschool.com/courses/aws/

ENROL OR RESERVE A SEAT
AWS Security Identity Compliance Advanced Training

WHATSAPP · INDIA
+91 99057 40781

WHATSAPP · USA
+1 (469) 756-6329

EMAIL
contact@DevOpsSchool.com