DevOps Institute

DevSecOps Practitioner (DSOP)^{SM} v1.0

Examination Requirements

DevSecOps Practitioner (DSOP)^{SM} Certification

DevSecOps Practitioner is a certification that is accredited by DevOps Institute. The purpose of this certification and its associated course is to impart, test and validate knowledge, comprehension, and application of advanced DevSecOps practices, methods, and tools. The DevSecOps Practitioner certification is tailored for anyone who desires more depth when bringing DevSecOps to their organization. Each section covers practical maturity guides, and then discusses how people, process and technology can be combined to improve outcomes. The certification prepares individuals to have deep technical discussions about creating and securing DevOps pipelines.

Eligibility for Examination

The following prerequisite must be met before sitting for the DevSecOps Practitioner certification exam:

- It is highly recommended that Candidates have successfully completed and earned the DevSecOps Foundation certification from DevOps Institute.
- Although there are no formal training prerequisites for the exam, DevOps Institute highly recommends that candidates complete at least 24 contact hours of formal, approved DevSecOps Practitioner training delivered by an accredited Education Partner of DevOps Institute in order to prepare for the exam.

Examination Administration

The DevSecOps Practitioner examination is accredited, managed, and administered under the strict protocols and standards of DevOps Institute.

Level of Difficulty

The DevSecOps Practitioner certification uses the Bloom Taxonomy of Educational Objectives in the construction of both the learning content and the examination.

- The DevSecOps Practitioner exam contains Bloom 1 questions that test learners' ***knowledge*** of advanced DevSecOps terms and concepts
- The DevSecOps Practitioner exam contains Bloom 2 questions that test learners' ***comprehension*** of advanced DevSecOps terms and concepts.

- The exam also contains Bloom 3 questions that test learners' ***application*** of advanced DevSecOps concepts in various contexts.

Format of the Examination

Candidates must achieve a passing score to gain the DevSecOps Practitioner Certification.

Exam Type	40 multiple choice questions
Duration	90 minutes
Prerequisites	The DevSecOps Foundation certification from DevOps Institute is highly recommended to sit for the DevSecOps Practitioner exam. It is also recommended that candidates complete the DevSecOps Practitioner course from an accredited DevOps Institute Education Partner
Supervised	No
Open Book	Yes
Passing Score	65%
Delivery	Web-based
Badge	DevSecOps Practitioner Certified

Exam Topic Areas and Question Weighting

The DevSecOps Practitioner exam requires knowledge of the topic areas specified below:

Topic Area	Description	Max Questions
Module 1	DevSecOps Advanced Basics	4
Module 2	Applied Metrics	5
Module 3	Architecture	5
Module 4	Infrastructure	6
Module 5	Pipeline	5
Module 6	Observing Outcomes	6
Module 7	Experimentation	6
Module 8	Next Steps	4

Concept and Terminology List

The candidate is expected to understand and comprehend the following DevSecOps concepts and vocabulary at a Blooms Level 1 (Knowledge), 2 (Comprehension) and 3 (Application).

- Agile
- Architecture
- Architecture Maturity
- Architecture Tradeoff Analysis Method (ATAM)
- Audits
- Bleeding Edge
- Biodesign
- CALMS Model
- CASE Tools
- Chaos Engineering
- CICD Pipeline
- Container Security
- Continuous Delivery (CD)
- Continuous Integration (CI)
- Continuous Monitoring
- Continuous Security
- Cloud Architects
- Cloud-Native
- Conway's Law
- Continuous Delivery Architect
- Core Agile Concepts
- Culture
- Cultural Pillars
- Cutting Edge
- DevSecOps
- Dynamic Analysis
- Event-Driven Architecture
- Expanded Risk
- Harvard Architecture
- Idempotent
- Infrastructure
- Kanban Board
- Key Metrics
- Kubernetes
- LEAN
- Lift and Shift
- Log
- Logging
- Maturity Levels
- Mean to Recover (MTTR)
- Merged Architecture
- Microservices
- Model
- Monoliths
- Metrics
- Observability
- Open Source
- Ops
- Priority
- Process
- Qualitative vs. Quantitative Analysis
- Quantum Computing
- RACI
- Release
- Release Management
- Retrospective
- Resilience
- Risks
- Safety Culture
- Scaled Agile Framework (SAFE)
- Scrum Master
- Security as Code
- Security Scans
- Simple Risk

- Source Control
- Static Code Analysis
- Strangler Pattern
- SWIFT Hacking
- Telemetry
- The Third Way Applications
- The Three Ways
- The Unicorn Project
- Threat
- Tracing
- UI/UX Scales
- User
- Value Stream
- Von Neuman Architecture
- Velocity
- Vulnerability
- Vulnerability Scans
- Westrum (Organization Types)
- Work in Progress Principles (WIP)
- Workflows