EXIN DEVOPS PROFESSIONAL — TABLE OF CONTENTS

The "EXIN DevOps Professional" 2-day course is designed to provide participants with a comprehensive understanding of DevOps principles and practices. The course covers topics such as DevOps adoption, the three ways of DevOps (flow, feedback, and continuous learning), information security, and change management. It aims to equip candidates with the knowledge and skills required to drive value in their organizations through effective DevOps implementation.

Day 1: Foundations and The First Way: Flow

1. DevOps Adoption

- 1.1 Basic Concepts of DevOps

- 1.1.1 Describe basic DevOps concepts such as continuous delivery, Agile infrastructure, kata, work in progress (WIP), technical debt, and lead time.

- 1.2 Principles of the Three Ways

- 1.2.1 Distinguish the principles of flow, feedback, and continuous learning and experimentation.

- 1.2.2 Explain the difference between system of records (SoR) and system of engagement (SoE) in relation to DevOps.

- 1.3 Organization

- 1.3.1 Explain how various DevOps roles collaborate to add business value.

- 1.3.2 Contrast I-shape, T-shape, and E-shape personas in DevOps contexts.

- 1.3.3 Integrate Operations into Development's daily workflow.

2. The First Way: Flow

- 2.1 Deployment Pipeline

- 2.1.1 Utilize techniques like infrastructure as code and containers to address deployment pipeline challenges.

- 2.1.2 Choose optimal solutions to enhance the value stream.

- 2.1.3 Evaluate a shared version control repository for thoroughness.

- 2.1.4 Tailor the definition of done (DoD) to align with DevOps principles.

- 2.1.5 Automate environment setup and configuration through appropriate tooling.

- 2.2 Automated Testing

- 2.2.1 Differentiate between non-ideal and ideal testing pyramids.

- 2.2.2 Select and apply test-driven development appropriately within a flow.

- 2.3 Continuous Integration

- 2.3.1 Determine the best branching strategy.

- 2.3.2 Assess technical debt's impact on flow and strategies for elimination.

- 2.4 Low-risk Releases

- 2.4.1 Evaluate release and deployment patterns to enable low-risk releases.

- 2.4.2 Choose suitable architectural archetypes for risk reduction.

Day 2: The Second and Third Ways, Security, and Change Management

3. The Second Way: Feedback

- 3.1 Telemetry

- 3.1.1 Discuss how telemetry optimizes the value stream.

- 3.1.2 Outline the components of a monitoring framework.

- 3.1.3 Highlight the benefits of self-service telemetry access.

- 3.2 Feedback

- 3.2.1 Resolve deployment issues using fix-forward and roll-back strategies.
- 3.2.2 Adapt launching guidance checklists to a DevOps framework.
- 3.2.3 Conduct safety checks with launch readiness and hand-off reviews.
- 3.2.4 Utilize UX design as a feedback mechanism.
- 3.3 Hypothesis-driven Development and A/B-testing
- 3.3.1 Integrate A/B testing in releases and feature tests.
- 3.3.2 Employ hypothesis-driven development for expected delivery outcomes.
- 3.4 Review and Coordination
- 3.4.1 Assess the efficacy of pull-request processes.
- 3.4.2 Explain review techniques like pair programming and tool-assisted reviews.
- 3.4.3 Select the appropriate review method for specific scenarios.

4. The Third Way: Continual Learning and Experimentation

- 4.1 Learning
- 4.1.1 Identify various Simian Army monkey types to enhance learning.
- 4.1.2 Facilitate blameless postmortem meetings.
- 4.1.3 Discuss how production failure injections foster resilience.
- 4.1.4 Plan and execute game days effectively.
- 4.2 Discoveries
- 4.2.1 Leverage codified non-functional requirements (NFRs) for Operations design.
- 4.2.2 Incorporate reusable operations user stories in development.
- 4.2.3 Identify objects for storage in the shared source code repository.
- 4.2.4 Transform local discoveries into organization-wide improvements.

5. Information Security and Change Management

- 5.1 Information Security
- 5.1.1 Integrate preventive security controls into DevOps processes.
- 5.1.2 Embed security practices in the deployment pipeline.

- 5.1.3 Utilize telemetry to bolster security measures.
- 5.2 Change Management
- 5.2.1 Ensure security maintenance during organizational changes.
- 5.2.2 Sustain compliance continuity throughout change processes.