

Pre-Conference Workshops - 06th AUGUST 2026

Workshop 1 (Build)

A deep dive into Agentic AI Lifecycle with labs

Presenters

Mr. Suresh Kannappan
Mr. Shyam Soundar



Amazon Web Services India Pvt Ltd

Description

Agentic AI is transforming how organizations design, deploy, and govern intelligent systems capable of autonomous decision-making and task execution. This hands-on workshop provides participants with a comprehensive understanding of the Agentic AI lifecycle, from architecture and development to deployment and governance.

The workshop will cover key Agentic AI concepts and AWS services, including Amazon Bedrock Agents, Amazon Bedrock AgentCore, Amazon Kiro, and related AWS capabilities that enable organizations to build, orchestrate, secure, and scale AI agents effectively. Participants will gain practical experience through guided labs, demonstrations, and real-world use cases that illustrate how Agentic AI solutions can be developed and managed in enterprise environments.

High level Agenda

TIME	SESSION
09:30 AM – 10:00 AM	Introduction, Workshop Context, and Opening Remarks
10:00 AM – 11:15 AM	Session 1 (Presentation) – Introduction to AWS AI Services, Amazon Bedrock, Amazon Bedrock AgentCore and Amazon Kiro
11:15 AM – 11:30 AM	Networking Break
11:30 AM – 01:00 PM	Session 2 (Hands-on): Deep Dive into Amazon Bedrock AgentCore
01:00 PM – 02:00 PM	Lunch Break
02:00 PM – 03:30 PM	Session 3 (Hands-on): Building AI Agents with Amazon Kiro
03:30 PM – 03:45 PM	Tea / Networking Break
03:45 PM – 04:45 PM	Session 4 (Discussion): Questions, Clarifications and Reflections
04:40 PM – 05:00 PM	Closure Comments and Wrap-up

Workshop 2 (Assure)

AI Guardrails Lab with adversarial benchmarks and validation

Presenters

Dr. Tejasvi Addagada
Mr. Praveen Kumar Raju B
Mr. Uday K



Zytra

Description

As organizations increasingly adopt Generative AI and Agentic AI solutions, ensuring that these systems are secure, trustworthy, compliant, and resilient against adversarial threats has become a critical business requirement. AI systems are susceptible to risks such as prompt injection attacks, jailbreak attempts, data leakage, hallucinations, model misuse, and regulatory non-compliance, making effective AI guardrails essential for safe deployment.

This hands-on workshop provides participants with practical knowledge and experience in designing, implementing, testing, and validating AI guardrails for enterprise AI systems. Attendees will learn how to identify vulnerabilities, conduct adversarial testing, evaluate guardrail effectiveness, and establish governance and assurance frameworks aligned with industry best practices and regulatory expectations.

The session will also introduce participants to the Zytra AI Governance Portal and demonstrate how organizations can operationalize AI governance, risk management, assurance, and compliance across the AI lifecycle. Through demonstrations, case studies, and hands-on exercises, participants will gain exposure to real-world AI safety challenges and validation methodologies, including AI red teaming and adversarial benchmarking approaches.

High level Agenda

TIME	SESSION
09:30 AM – 10:00 AM	Introduction, Workshop Context, and Opening Remarks
10:00 AM – 11:15 AM	Session 1: Introduction to AI, AI Risks, and Effective Use of AI Guardrails
11:15 AM – 11:30 AM	Tea / Networking Break
11:30 AM – 01:00 PM	Session 2: Introduction to Zytra AI Governance Portal and Application Walkthrough
01:00 PM – 02:00 PM	Lunch Break
02:00 PM – 03:30 PM	Hands-on Lab Session – Part 1 (AI Guardrails Implementation and Validation)
03:30 PM – 03:45 PM	Tea / Networking Break
03:45 PM – 04:30 PM	Hands-on Lab Session – Part 2 (Evaluation Framework Setup and Benchmark Configuration)
04:30 PM – 05:00 PM	Q&A, and Closing Remarks

Workshop 3 (Trust)

Implementing DPDPA and Consent Management Hands-on

Presenter

Mr. Aayush Jain



PROTAXOLOGY

TAX | INFOSEC | RISK

India’s Digital Personal Data Protection Act (DPDPA) shifts the focus from privacy compliance theory to implementation. This hands-on workshop is designed for practitioners looking to translate DPDPA requirements into practical organizational controls, operating models, and implementation roadmaps covering practical aspects such as data fiduciary obligations, data principal rights handling, privacy governance structures, control design and compliance readiness.

A dedicated focus area will be consent management, including:

- Designing consent notices and purpose specifications
- Consent capture, withdrawal, and preference management processes
- Consent recordkeeping and auditability requirements
- Integrating consent management platforms into business and technology processes
- Practical challenges in operationalizing consent across digital channels and ecosystems

Through implementation scenarios, walkthroughs, use cases, and interactive exercises, participants will work through practical approaches, templates, and considerations for building a DPDPA compliance program and operationalizing consent management in real-world environments.

High level Agenda

TIME	SESSION
09:30 AM – 10:00 AM	Introduction, Workshop Context, and Opening Remarks
10:00 AM – 11:15 AM	Session 1 (Presentation) — DPDPA: The Implementation Landscape
11:15 AM – 12:15 PM	Session 2 (Use Cases) — Data Fiduciary Obligations & Data Principal Rights in Practice
12:15 PM – 12:45 PM	Session 3 (Group Discussion) — Privacy Governance & Compliance Programme Structure
12:45 PM – 01:30 PM	Lunch Break
01:30 PM – 02:30 PM	Session 4 (Hands-on and AI Assisted) — Consent Deep-Dive: Designing Notices & Purpose Specifications
02:30 PM – 03:30 PM	Session 5 (Hands-on and AI Assisted) — Consent Capture, Withdrawal & Preference Management
03:30 PM – 03:40 PM	Tea / Networking Break
03:40 PM – 04:40 PM	Session 6 (Hands-on and AI Assisted) — Consent Recordkeeping, Auditability & Platform Integration
04:40 PM – 05:00 PM	Wrap-Up, Q&A & Handout Pack

Click here to explore detailed information about the workshops

