Large Language Model API Integration Training Course: Architecture, Testing and Operations

26 – 30 July 2027
Cape town

Large Language Model API Integration Training Course: Architecture, Testing and Operations

Ref: 818_38303 **Date:** 26 – 30 July 2027 **Location:** Cape town **Fees:** 4800 GBP

Programme Summary

Large language model API integration is the subject of this one-week training course for technology leaders, solution architects and product owners, ending in an LLM integration design and operations plan for one application. Organisations are connecting language model services to customer, finance and service systems faster than they can test, secure and fund them. The programme moves from how these interfaces behave to data flow design, threat controls, testing, and the cost, monitoring and supplier arrangements that keep a live service dependable. Mars Training Centre UK delivers this programme on large language model API integration to mixed-organisation cohorts.

The Business Case

Banks, insurers, retailers and public bodies are adding language model services to products that handle customer records and decisions. Interface choices made early fix the cost, risk and reliability of the service for years. Leaders who can question designs, test plans and supplier terms avoid expensive rework and prevent data leaving the organisation by accident.

- Delivery Reliability: Improves when failure handling, rate limits and fallbacks are designed before launch.
- Security Exposure: Falls when input and output controls are mapped to known threat classes.
- Running Cost: Stays predictable when usage is metered, capped and reviewed against value.

Principles and Evidence Base

- OWASP Top 10 for LLM Applications: Lists risks such as prompt injection, insecure output handling and excessive agency, applied in Sessions 3 and 4 to threat and control mapping.
- ISO/IEC 42001: Defines an AI management system, applied in Sessions 1 and 5 to accountability and change control.
- ISO/IEC 27001: Defines information security management, applied in Session 2 to data classification and access limits.

Intended Participants

- Technology leaders who approve language model integrations and carry the delivery risk.
- Solution architects who design interfaces, data flows and fallbacks.
- Product owners who define what the service may and may not do.
- Security and vendor managers who set controls and supplier terms.

Typical settings include banking, insurance, retail and public services.

Learning Outcomes

1. Participants will be able to evaluate an interface design for data exposure and failure behaviour.
2. Participants will be able to construct a data flow map with classification and access limits.
3. Participants will be able to diagnose security weaknesses in prompts, outputs and tool access.
4. Participants will be able to design a test plan that measures answer quality and regression.
5. Participants will be able to prioritise cost and rate limit controls by usage pattern.
6. Participants will be able to justify an integration design and operations plan to a sponsor.

Programme Structure

Day 1: Large Language Model API Integration Foundations

What does a language model interface do, and where can it fail?

- Request and Response Anatomy Sheet
- Integration Pattern Catalogue
- Build, Buy or Configure Decision Grid
- Failure Mode Inventory
- ISO/IEC 42001 Accountability Map

Day 2: Data Flows and Interface Design

Which data may leave the organisation, and through which path?

- Data Classification Table
- Data Flow Diagram
- ISO/IEC 27001 Access Control Matrix
- Gateway Placement Review
- Retention and Logging Rules

Day 3: Prompt, Output and Threat Controls

How are misuse and manipulation of the service blocked?

- Prompt Injection Scenario Cards
- Output Handling Checklist
- OWASP Risk-to-Control Matrix
- Tool Permission Register
- Content Filter Design Sheet

Day 4: Testing, Cost and Operations

How is the service kept accurate, affordable and available?

- Answer Quality Test Set
- Regression Test Plan
- Rate Limit and Retry Policy
- Cost per Request Model
- Supplier Service Level Review

Day 5: LLM Integration Design and Operations Plan for One Application

Do the earlier tools join into a plan a sponsor can approve?

- Applying the Session 2 Data Flow Diagram
- Testing the Session 3 OWASP Risk-to-Control Matrix
- Checking the Session 4 Cost per Request Model
- Rehearsing the Design Review Challenge
- Completing the Integration Design and Operations Plan

Methodology

The programme uses case analysis built on prepared material for two applications, one a customer enquiry assistant in a bank and one a document summary service in a government agency. Participants review interface designs, test results and supplier terms, challenge each other's choices and defend their plan before peers acting as a design authority.

- Suggested activity: Tracing one customer record through a design and marking where it could leak.
- Suggested activity: Writing three prompt injection cases and deciding which control stops each.
- Suggested activity: Costing a month of usage and setting a cap with an alert threshold.

Capstone Output

Each participant completes an LLM integration design and operations plan for one application. It holds a data flow map, a threat and control matrix, a test plan, a cost and rate limit policy and a supplier review. At work it is used to brief a sponsor, to set conditions for a supplier and to guide the first release.

Frequently Asked Questions

Is a training course on large language model API integration suitable for leaders who do not write code?

Yes. Large language model API integration is taught through prepared designs and templates. The programme assumes responsibility for directing or approving a build, but no programming skills.

Which standards does large language model API integration rest on?

Large language model API integration rests on the OWASP Top 10 for LLM Applications for threats, ISO/IEC 42001 for AI management and ISO/IEC 27001 for information security.

How is the plan from large language model API integration used at work?

You use the integration design and operations plan to brief your sponsor, set supplier conditions, agree test and cost limits, and guide the first release.

How does large language model API integration differ from a programme on AI governance?

Large language model API integration concentrates on interfaces, data flows, testing and operations of one build, while an AI governance programme concentrates on policy, inventory and oversight across many systems.