

---

# API Gateway and Management Design Training Course: Policy, Security and Platform Operations

18 – 22 April 2027  
Manama





## API Gateway and Management Design Training Course: Policy, Security and Platform Operations

Ref: 290\_20347 Date: 18 – 22 April 2027 Location: Manama Fees: 4300 GBP

### Programme Summary

API gateway and management is the subject of this one-week training course for enterprise architects, platform and integration leaders and heads of digital delivery, ending in an API gateway and management design for one API estate. Gateways and policies are often built team by team, with unclear ownership. The approach moves from roles and placement, through risk and traffic diagnosis, to policy and operating design, and then to a worked design. Mars Training Centre UK delivers this programme in API gateway and management.

### The Business Case

When many teams publish interfaces without common policies, security gaps, outages from uncontrolled traffic and duplicated effort appear late and cost more to correct. Leaders who decide where the gateway sits, who owns each interface and which policies apply can reduce exposure and protect shared services.

- API Security Exposure: Reduces as risk review and consistent authentication and validation policies apply to every interface.
- Service Availability: Improves as rate limits, quotas and capacity checks protect shared back-end services.
- Delivery Cycle Time: Falls as published standards, a catalogue and a developer portal replace repeated onboarding work.

### Principles and Evidence Base

- OWASP API Security Top 10: Its list of API-specific risks structures the threat review in Session 2 and the policy set in Session 3.
- Little's Law: This queueing relationship between concurrency, arrival rate and response time underpins the capacity and rate limit work in Sessions 2 and 3.
- Conway's Law: Its link between organisation structure and system design guides the ownership and review arrangements in Session 4.

### Intended Participants

- Enterprise architects who decide how interfaces are exposed, secured and reused.
- Platform leaders who run shared gateway and integration services for many teams.
- Integration leaders who manage partner and internal interface consumers.
- Heads of digital delivery who sponsor interface standards across product teams.

The programme serves banking, telecommunications, government services and logistics organisations.



## Learning Outcomes

1. Participants will be able to differentiate the roles of a gateway and a management platform and justify a placement option.
2. Participants will be able to diagnose security weaknesses in an API estate against a recognised risk list.
3. Participants will be able to evaluate traffic profiles and set rate limit and quota tiers.
4. Participants will be able to construct authentication, validation and versioning policies for a set of interfaces.
5. Participants will be able to prioritise monitoring measures and service level objectives for platform operations.
6. Participants will be able to justify an ownership and governance model to a platform sponsor and a security lead.

## Programme Structure

### Day 1: API Gateway and Management Roles and Placement

What does a gateway do, what does a management platform add, and where should each sit?

- API Estate Inventory and Consumer Map
- Gateway and Management Platform Role Matrix
- Gateway Placement Options Comparison
- Ownership and Funding Model Sketch
- Case Review of Two Sector Platforms

### Day 2: Risk and Traffic Diagnosis

Where is the estate exposed, and how much traffic must it carry?

- OWASP API Security Top 10 Risk Walkthrough
- API Threat Model Worksheet
- Consumer Authentication Gap Review
- Traffic Profile and Peak Load Estimate
- Little's Law Capacity Check

### Day 3: Policy Design

Which policies should every interface carry, and which vary by consumer?

- Authentication and Authorisation Pattern Set
- Rate Limit and Quota Tiers
- Request Validation and Error Handling Rules
- Versioning and Deprecation Policy
- Developer Portal Content Plan



## Day 4: Platform Operations and Governance

How is the platform run, measured and kept under review?

- Service Level Objective Sheet
- Logging, Metrics and Alert Design
- Release and Change Control Flow
- Team Ownership Map Using Conway's Law
- API Catalogue Review Board Terms

## Day 5: Applying API Gateway and Management to One API Estate

Is the design ready for the platform sponsor and the security lead to approve?

- Applying the Session 1 Role Matrix to the Chosen Estate
- Testing the Session 2 Risk Findings Against Sample Interfaces
- Checking Session 3 Policies Against Consumer Needs
- Applying the Session 4 Ownership Map to Open Issues
- Completing the API Gateway and Management Design

## Methodology

The programme is built around structured exercises on an anonymised API estate. Participants map interfaces, review risks, set traffic tiers and draft policies in small teams, then defend their design before a simulated architecture board. No programming is required.

- Suggested activity: Rating ten sample interfaces against the OWASP list and ranking fixes.
- Suggested activity: Setting quota tiers for three consumer groups from a traffic profile.
- Suggested activity: Drafting a deprecation notice policy for a partner-facing interface.

## Capstone Output

Each participant completes an API gateway and management design for one API estate. It contains a role and placement decision, a risk register, a policy set with rate limit tiers, a service level objective sheet, an ownership map and a catalogue review process. It is used to brief the platform sponsor and security lead and to plan the first delivery stage.

## Frequently Asked Questions

### Is API gateway and management suitable for architects without hands-on tool experience?

Yes. API gateway and management is set at managerial level and assumes responsibility for interface or platform decisions, not experience of a particular gateway product or coding.



## **Which models does API gateway and management rest on?**

API gateway and management rests on the OWASP API Security Top 10 for risk, Little's Law for capacity and Conway's Law for ownership design.

## **How is the design from API gateway and management used at work?**

You use the design from API gateway and management to brief your sponsor, set common interface policies and plan the first stage of platform delivery.

## **How does API gateway and management differ from a vendor tool course?**

API gateway and management centres on placement, policy, ownership and measures that apply to any product, while a vendor tool course centres on configuring one product.