Governance Studio
by Adapted Media Pty Ltd

OPENAI CODEX ADDS AMAZON BEDROCK RUNTIME AS A BUILT-IN PROVIDER

OPERATIONAL SIGNAL

DOMAIN: CAP — Capability I **CONFIDENCE LEVEL:** HIGH
INSTITUTIONAL DIMENSIONS: Authority I Attribution I Visibility I Escalation I Continuity

Signal ID	Platform	Source	Audience	Signal Date
SIG-CAP-025	OpenAI Codex	Link	Technology I Security	2026-08-18

CAPABILITY SHIFT

OpenAI Codex now supports Amazon Bedrock Runtime as a built-in provider. The release note confirms support for AWS profiles, AWS regions and GPT-5.6 routing when Bedrock Runtime is selected. This gives Codex CLI and TUI users another provider path for model execution without requiring a custom provider integration.

ORGANISATIONAL CONSEQUENCE

Provider choice can now be expressed through Codex configuration that references an AWS profile and region. Teams using the option should know who can select or change that provider, which AWS identity and region are used, and how provider-specific usage is observed. The release note does not establish new AWS permission defaults, data-residency guarantees or logging behaviour.

WHAT TO WATCH

- Codex configuration selecting Amazon Bedrock Runtime and the AWS profile or region attached to it
- Changes in provider selection across shared repositories or managed developer environments
- Operational records that distinguish Bedrock-routed sessions from other Codex provider paths

WHY THIS MATTERS NOW

A built-in Bedrock Runtime option makes AWS-backed provider selection part of ordinary Codex configuration rather than a separate custom integration path.

WHAT TO REVIEW

- Who can set or override the Codex provider in managed developer environments
- Which AWS profiles and regions are approved for Bedrock Runtime use
- How Bedrock-routed Codex usage is identified for monitoring, support and cost review
- Whether existing Codex guidance covers multi-provider configuration

GOVERNANCE CONTEXT

The material shift is configurability: teams can choose an AWS-backed execution provider directly in Codex. Clear authority over provider settings and visibility into which path handled a session become important when multiple runtime options are available.

Scope Boundary: This artefact translates observed platform capability changes into operational considerations. It does not constitute policy, legal advice, or enforcement guidance.