

# Google Faces New Compliance Challenges, ET CISO

---

**ET**  
CISO [ciso.economictimes.indiatimes.com/news/indias-first-antitrust-settlement-google-faces-new-compliance-challenges/121552505](https://ciso.economictimes.indiatimes.com/news/indias-first-antitrust-settlement-google-faces-new-compliance-challenges/121552505)

ET CISO

June 1, 2025

**By Gauri Chhabra,**

The Competition Commission of India (CCI) issued its first-ever settlement order—just over a year after introducing the Settlement Regulations, 2024. This marks a pivotal moment for antitrust enforcement in India, opening a new pathway for resolution in abuse of dominance and vertical restraint cases. While the order introduces procedural clarity and faster dispute resolution, it also brings to the fore critical questions around regulatory compliance, digital competition, and associated technology and cybersecurity risks.

The Settlement Regulations, effective from March 6, 2024, allow parties to settle after the Director General's (DG) investigation report is submitted but before the CCI issues a final order. Settling parties can receive up to a 15% reduction in penalty, with the CCI expected to dispose of such applications within 180 days. This framework promises to reduce litigation timelines, particularly in complex digital markets, while preserving the deterrence function of competition law.



The first order under this framework involved Google, accused of tying practices with smart TV original equipment manufacturers (SOEMs). The allegation centered on compelling SOEMs to pre-install the entire suite of Google apps—including YouTube and the Play Store—across all device categories (not just smart TVs), while also restricting dealings with rival operating systems and app stores. In response, Google agreed to unbundle these services, offer standalone licenses, and remove exclusivity clauses—steps aimed at restoring competitive neutrality.

This order holds Google’s dominant position in both the smart TV OS market and the Android app store market in India, raising the bar for its future compliance obligations. The CCI’s finding that the Play Store is an “essential facility” underscores an emerging

duty to deal for dominant digital platforms—an area likely to see increased scrutiny under India’s evolving antitrust doctrine.

### **Technology and cyber risk dimensions**

The case also illustrates how antitrust and technology governance are converging, particularly in platform markets where control over software ecosystems can create systemic dependencies. Whilst unbundling is a welcome step, it requires robust implementation, including technical reengineering, contractual oversight, and possibly API access audits — each posing its own cyber risk.

From a procedural standpoint, the CCI’s approach reflects commendable regulatory discipline. The commission engaged with stakeholder feedback, reviewed remedies in detail, and issued a reasoned order despite limited institutional capacity. However, without a grandfathering clause, it remains unclear how legacy cases will transition to this new framework. Moreover, the timeline for DG investigations now becomes more critical—delays at this stage could undermine the efficiency gains intended by the settlement mechanism.

Another legal grey area is the potential for follow-on claims, where third parties may seek damages based on conduct acknowledged in settlement applications. While settlements aim to avoid prolonged litigation, they may open parallel avenues for civil liability, especially if competition harm is explicitly identified.

As SOEMs begin to explore alternatives, the security implications of new software ecosystems become salient. The Android ecosystem’s scale provided certain cybersecurity baselines. In contrast, fragmentation or rapid onboarding of new app store providers may inadvertently introduce vulnerabilities, data privacy concerns, or misaligned security protocols.

Furthermore, the order obligates Google to notify SOEMs of their new rights. These communications and subsequent configurations—especially if handled through online dashboards or cloud-based license management—could become targets for cyberattacks or data breaches if not adequately secured. Any compromise could expose sensitive licensing data, business models, or integration pathways.

For regulators and firms alike, this highlights the need to integrate cyber resilience into antitrust remedy design. The efficacy of structural or behavioral remedies in tech markets increasingly depends not only on legal clarity but also on digital security, interoperability, and auditable data flows.

The CCI’s first settlement order marks an evolution in India’s antitrust enforcement—from purely punitive models to more negotiated, market-corrective approaches. Yet, for such settlements to work in tech-heavy sectors, regulators must consider not just competition effects but also compliance architecture, digital operational risks, and ecosystem-level cyber vulnerabilities.

As more digital market cases opt for the settlement route, India's antitrust landscape will need to mature beyond procedural templates to account for the deeper technological and security implications of platform regulation.

**The author is Partner – Competition Law, Trilegal & Team.**

***Disclaimer:*** *The views expressed are solely of the author and ETCISO does not necessarily subscribe to it. ETCISO shall not be responsible for any damage caused to any person/organization directly or indirectly.*