

# Compliance as Code: Common Misconceptions

Compliance as code is transforming how organizations manage security and regulatory requirements... but confusion about what it is and how it works can hold teams back. Let's clear up the most common myths.



## #1. It's Too Complex — Just a Science Project

**The Truth:** Compliance as code works behind the scenes to superpower your existing tools and bridge the gap between compliance and DevSecOps teams. It integrates seamlessly into workflows you already use.

## #2. AI Is Making Compliance as Code Obsolete

**The Truth:** They're complementary, not competitive. AI excels at speed and being "generally right," but cybersecurity demands more precision. To keep attackers from being right even once, train your AI models on highly precise data and use them alongside compliance as code.

## #3. OSCAL Is Federal-Only

**The Truth:** NIST OSCAL is a powerful, vendor-neutral open standard that works with any framework and any tool. Whether you're managing SOC 2, ISO 27001, PCI DSS, or custom requirements, OSCAL provides a universal language for compliance data.

## #4. It's Either AI, Compliance as Code, OR Framework Mapping

**The Truth:** They're better together. Leading organizations layer all three: AI agents analyze OSCAL-formatted data while cross-framework mappings (like the CRI Profile) eliminate duplicate work across standards. The result is efficiency beyond automation — work simply disappears.

## #5. Compliance as Code Only Handles Technical Controls

**The Truth:** Every policy, procedure, and governance requirement can be expressed in OSCAL. This is where an integrated solution truly shines: analyzing governance data, identifying gaps with AI, and streamlining administrative controls monitoring.

Learn more

