Compliance Roadblocks to DevOps

DevOps的合规障碍

Most regulators and auditors are lawyers and accountants—or they

think like them. They don’t necessarily understand Agile development,

Infrastructure as Code, or Continuous Delivery. The accelerated

pace of Agile and DevOps raises a number of concerns for

them.

大多数监管者和审计师都是律师和会计师，或者像他们一样思考。他们不一定理解敏捷开发，基础设施即代码，或持续交付。加速的敏捷和DevOps步伐引起了他们的担忧。

They want evidence that managers are directly involved in decisions

about what changes are made and when these changes are implemented.

They want to know that compliance and legal reviews are

consistently done as part of change management. They want evidence

of security testing before changes go in. They are used to

looking at written policies and procedures and specifications and

checklists and Change Advisory Board (CAB) meeting minutes and

other documents to prove all of this, not code and system logs.

他们希望有证据表明经理们对进行了哪些变更以及何时实施这些变更直接参与了决策。他们想知道合规和法律审查始终作为变更管理实施的一部分。他们想要证据在变更之前进行了安全测试。他们习惯了查看书面政策、程序和规范，以及检查表和变更咨询委员会（CAB）会议纪要以及证明所有这些的其他文档，而不是代码和系统日志。

Regulators and auditors like Waterfall delivery and ITIL, with

approval gates built in and paper audit trails. They look to industry

best practices and standards for guidance. But there are no standards

for Continuous Delivery, and DevOps has not been around

long enough for best practices to be codified yet. Finally, auditors

depend on the walls built up between development and operations

to ensure separation of duties—the same walls that DevOps tries to

tear down.

监管者和审计人员喜欢瀑布交付和ITIL，内置了审批门槛以及和文件审计跟踪。他们向业界最佳实践和标准寻求指导。但是没有持续交付的标准，DevOps的出现时间还不够长，还没有编纂出所谓的最佳实践。最后，审计员依赖于开发和运营之间的墙来确保职责分离，而这正是DevOps所试图拆毁的墙。