

Trust in Practice: Evaluating Third-Party Software in Large Organisational Procurement

About

This study investigates how large organizations evaluate and manage trust when procuring third-party software. Drawing from literature reviews and nine semi-structured interviews with professionals, the research identifies key trust factors and maps how they are applied throughout the procurement lifecycle. The goal is to provide practical insights for improving procurement strategies and for software vendors seeking to build trust.

Problem

As businesses increasingly depend on external software for core operations, the risk of supply chain attacks and data breaches has grown significantly. While trust in a software vendor is critical, there is limited understanding of how large organizations practically assess and maintain this trust beyond formal checklists. This study addresses the gap between prescribed procurement models and the real-world, dynamic processes companies use to manage vendor risk.

Study Outcome

- Organizations employ a layered trust strategy, combining formal mechanisms like ISO/SOC certifications and legal contracts with relational ones such as vendor transparency and past performance.
- Trust is not a one-time check but an ongoing process that is monitored and re-evaluated throughout the vendor relationship, especially at contract renewal or after security incidents.
- Procurement processes are often flexible, adapting based on the software's risk level, cost, and the data it handles; high-risk tools undergo stricter scrutiny.
- Legal and geopolitical factors, particularly concerning data residency and regulations like GDPR and the U.S. CLOUD Act, are major considerations in vendor selection.
- The study found that organizations balance formal requirements with practical needs, sometimes compromising on certain criteria when no ideal alternative vendor exists.

Keywords

Trust • Third-party software • Procurement • Compliance management • Organisational cybersecurity • Risk assessment • Vendor management