Managing third-party risk: A 15-point checklist

Plenty can be done proactively to protect your organization from third-party risk. Here are 15 examples, starting with things that can be done externally.

1. Conduct due diligence on potential third-party vendors.
2. Ask for documentation on how well the third party has secured its services or products.
3. Inventory and keep track of each third-party vendor and software supplier.
4. Implement an automated third-party-risk management platform.
5. Continuously monitor your third-party vendors and suppliers.
6. Implement a zero-trust or limited-privilege network access policy.
7. Incorporate DevSecOps into your software development life cycle (SDLC).
8. Segment your networks.
9. Mandate strong multi-factor authentication (MFA) for all staff accounts.
10. Make plans for when and if you suddenly must move to a new supplier or vendor.
11. Categorize your vendors by the inherent risk each carries.
12. Consider reducing the number of "critical" vendors you work with.
13. Restrict the access of third-party programs.
14. Understand the shared-responsibility agreements you have with each of your SaaS and cloud providers.
15. Last but not least, get the principal stakeholders on board.