Vendor Management

To Reduce Cyber Risk

Vendors connected to your network have access to confidential information and pose a threat to your security. Do you have the right management functions in place to ensure vendors aren't putting your company at risk?

5 Questions You Should Ask:

Do you monitor the usage of third parties?

Monitor third party accounts to see how and when they're being used, for what purpose, and whether vendors truly need access.

Do you consider cybersecurity requirements and risks when building relationships with suppliers and third parties?

Onboarding a vendor requires multi-department involvement to develop a complete view of potential risks. This includes drawing up contracts that state security levels and requirements that third parties must meet, and potential risks and repercusions if they can't meet them.

Do you conduct a Security Impact Analysis when bringing in new technologies?

Test new software and technologies before introduction to your company to mitigate the chance of risk. Assess new systems in a developmental testing environment before fully connecting them to your company's ecosystem.

Do you require notification of vulnerability-inducing product defects throughout the life-cycle of delivered products?

Clearly state in each contract that vendors who identify a problem or vulnerability must notify of problem and solution within a certain time period (24-72 hours). Foster good relationships with vendors, who will then be more likely to notify you if a problem occurs.

Do you require approval from account managers before granting access to third parties?

Assign one point of contact responsible for knowing who has access to company information and ensuring access is appropriately scoped. A sunset date is needed for each account to restrict information access after vendors' contracts end.