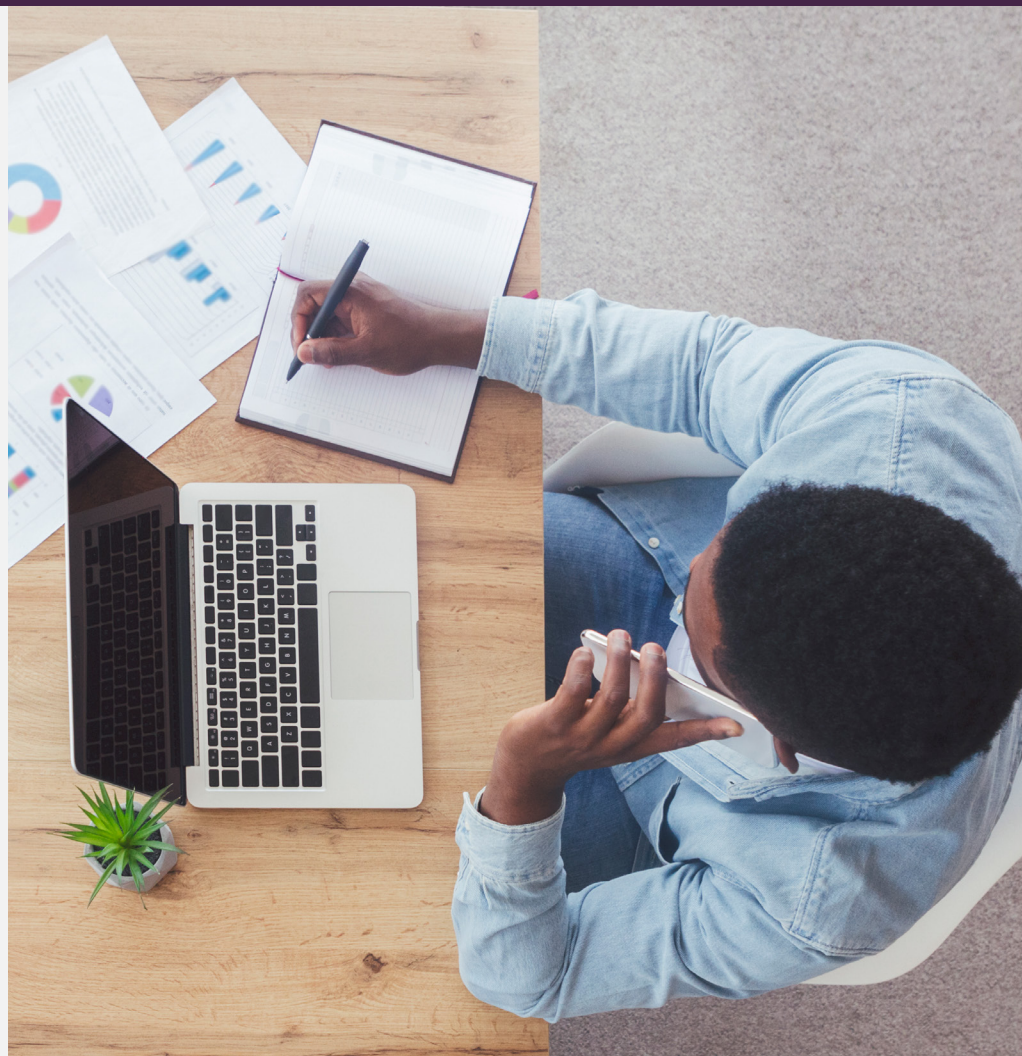
FiscalNote

4 Security Questions You Really Need to Ask Your Issues Management Software Provider

You have enough on your plate, don't add security compliance to the list.

There's a lot of smoke and mirrors when it comes to security. Many vendors will use jargon about SSO, encryption, and proactive threat monitoring to give the impression they're ticking all the boxes, but you can't afford to mess around when it comes to data security.

Asking these simple questions will help you make sure you're trusting the safest, most secure vendor with your sensitive information.



Are you SOC 2, Type II compliant, and can you send me your report?

There are two types of audit's that measure an organization's overall security: SOC 1 and SOC 2. These are two completely different reports with different standards, with SOC 1 focused mainly on internal controls for financial reporting. Organizations with only SOC 1 compliance have yet to complete the full test audit, and have simply filled out forms that relate to their internal financial reporting.

For a SOC 2 report to be granted, a third party auditor will perform tests of operating processes to validate that all necessary security controls are in place and operating effectively. SOC 2 is safer, more secure, and provides stricter safeguards for sensitive client information than SOC 1.

Oftentimes, a provider might only offer SOC 1 compliance but try to skirt around the issue by sending lots of confusing, detailed security documents in the hopes that you won't notice or ask the question. In order to ensure your data is in the best hands, don't just ask if they meet the requirements, ask to see a copy of the report as well.

Do you have an onsite security team?

Software security is complicated. If your vendor doesn't have a dedicated team on staff with expertise in this field, chances are they aren't taking the risk posed to you, seriously so, how can you be sure that your data is safe? Responding to a potential threat like a hack, breach, or leak is going to be haphazard at best if no one at the organization "owns" the job. Security teams are crucial for protecting IT infrastructure, networks, data, and implementing security standards across the company.

Ask your vendor if they have an IT security team, or at least a Director of Security, to ensure their organization is staying on top of all the latest security best practices and ahead of any potential issue that could impact their you and your data.

Do you offer SAML and not just SSO?

Not all SSO is equal. If your vendor doesn't offer SAML authentication on their platform, your information could be at risk. Security Assertion Markup Language, or SAML, is a system that issues more secure authentication when logging onto a software platform. It allows users to use single sign-on (SSO) in conjunction with GSuite or Active Directory to ensure another layer of security that prevents unauthorized log-ins, lowers the risk of a breach or hack, and ensures the utmost privacy of the user.

Without SAML, for example, previous employees can use old log-in credentials to access sensitive information. Equally, if you're using SAML, as soon as someone leaves the company, deactivating their email will log them out of all software at the company they had access to.

Do you have Fair Processing?

Personal information that is collected from organizations must be fairly and lawfully processed. This means having legitimate grounds for collecting data and not using it in any way that may have unjustified adverse effects on the individual or organization.

You want to ensure that all vendors you work with take the protection of your data seriously and apply appropriate measures to prevent misuse or unauthorized access. Ask your provider if they are compliant with the General Data Protection Regulation (GDPR) and Fair Processing compliance before providing them with your confidential information.