Security Questionnaire

Simple Vendor Assessment v1.0, Ericius Security Company, CC-BY-SA-4.

When engaging with a vendor that will store, receive, or process your sensitive information, purchasing software as a service (SaaS), or selecting a cloud service to integrate with your operations, you should briefly stop to consider how risky that service is—and how security will help manage or defend the new tool. Below is a brief security questionnaire you can use to start or guide the security discussion with potential vendors:

1 VENDOR INFO

1.1 COST AND VALUE

Question	Answer
Vendor Name	The name of the vendor and the name of the service as applicable
Cost	How much does the service costs in your preferred period (monthly, quarterly, yearly, or three-year)? It may benefit you to note if the service is an operational expenditure (normal for SaaS, etc; May be deductible as business expense) or capital expenditure (for example hardware, one-time licenses, etc)
Term of Agreement	How long the contract lasts for; Is it month to month? Or are you locking into a three-year term? This is often also a chance to discuss opportunities for discounts for committing to longer terms or pre-paying for an entire year.
Billing period	How often are you billed? For example, many SaaS companies will encourage you to sign up for a year long term and then will either bill you up front or monthly. Many managed service providers will establish three-year terms with monthly or quarterly billing. Billing is important for you to understand, as well as its impact on your capital or operational expenditures and—accordingly—taxes.
Cancellation Notice Due	When do you owe written notification if you intend to cancel? Important to track to avoid unwanted automatic renewals
What does your service do?	What is the intended use case for the service?
What value do you provide? Why should we purchase your services?	What is the value proposition of the service? Why is it useful to you? How does it help you accomplish your mission or reduce costs/friction?

1.2 REGULATIONS

Question	Answer
What compliance standards are you required to meet? (for example, GDPR, HIPAA, SOX…)	Vendors should understand what their compliance requirements are and should demonstrate that they are meeting their requirements well. Vendors housing data or with customers in the European Union should have a publicly available statement on GDPR compliance, health care related services such as electronic health record providers should meet HIPAA standards, publicly traded companies should be compliant with Sarbanes-Oxley, vendors handling part of payment processing must meet Payment Card Industry standards, etc
What security certifications do you maintain (for example, ISO, HITRUST, ITIL, SOC 2 Type II, etc)	Security certifications should match the location of the service provider and the value proposition. They are not, of themselves, indicative of good cyber defense and risk management practices but do demonstrate a foundation of effort. SaaS providers will likely attempt to meet one or more ISO standards and/or SOC 2 Type II. Providers with HIPAA obligations likely will seek out HITRUST certifications, etc. It may be worth your time to compare the certifications that your vendor asserts and those of their competitors. You can generally find the purpose behind a given certification by researching online, particularly with certifying authorities. This can also be used as an opportunity to discuss what training oriented certifications the vendor's team maintains. For example, you may want a SaaS company leveraging AWS and processing your critical information to have trained AWS Solutions Architects.

2 SECURITY AND RISK CONTROLS

2.1 ACCESS MANAGEMENT

Question	Answer
Do you support Single Sign-on (SSO/SAML)?	Single sign-on allows you to unify and centrally manage authentication via your preferred provider. If the vendor supports your provider (e.g. M365, Google, Okta, etc), then you likely can set and control standards for access and authentication regardless of the controls native to the vendor. In other words, if your users must log in using your M365 tenant, they will have to

	comply with *your* MFA standards which you have already set and manage. SSO is also a huge quality of life upgrade for most users, will speed up authentication, and limit the number of potential credentials to expose.
Do you support multi-factor authentication (MFA)?	MFA is frequently comprised of something you know and something you have. Because it relies on something you have (e.g., a one-time passcode generator, etc), accounts protected by MFA are substantially more difficult to phish, brute force, guess credentials, or otherwise breach via credential abuse. Vendors *should* provide an MFA option, though many still do not. If vendors provide MFA, there are a variety of quality options which should be available: 1. Hardware keys are better than… 2. One-time passcodes (via an app) are better than… 3. Push notifications are better than… 4. SMS (text) notifications are better than… 5. Nothing In the quality order proposed above, #1 is strongest and least flexible for users and #5 is weakest and most flexible.
Can we see or control which of our users haven't applied MFA or who sign-in without SSO?	Vendors should give you control over your users and should also present a view of who complies with your access standards. For example, you should be able to both see and limit access to a user who logs in directly with their email if you have required that all users log in with SSO.
What passwords standards can we set for our users?	Vendors should allow you to increase the length and complexity standards for your users' passwords, especially if they do not provide SSO or MFA. In some cases, vendors may already require strong passwords and will not allow you to decrease nor increase the strength of those standards. This may be adequate to your needs.
How do you manage identities across domains? What API integrations do you support?	The best vendors will integrate with other identity providers so that you do not have to build a second version of your user directory in their system. Ideally this system will also let you secure access and automate access granting and revocation via API calls, provide a system for cross-domain identity management (SCIM), or similar.
How do you manage your developers', engineers', or administrators' access to our accounts?	Vendors' developers and engineers generally shouldn't have access to your private information or accounts except in specific situations such as fixing a bug or account access problem with you. Ideally, vendors log all access of their employees

	to your accounts and your data and require some form of two-person integrity when accessing customer's information.
How do you prevent unauthorized access to our accounts or account take over attacks?	Vendors should have security features in place beyond simple authentication controls such as rate limiting log-in attempts, automatically locking accounts that fail authentication prompts multiple times, fraud detection, and conditional access controls.
What conditional access controls do you provide?	Vendors ideally will provide conditional access tools to extend your control over authentication methods. Conditional access controls allow you and the vendor to identify unusual authentication activities and to add additional challenges such as captchas or a verification email and will create alerts for you when users access their accounts from unusual locations (for example, when a user from Dallas suddenly logs in from Moscow)
How do you help us manage roles? How can we control the scope of each role?	Vendors should allow you control over your users and what permissions or privileges they have based on *roles*—not just privileges attached to a username. In addition to roles, better vendors will allow you to define a scope against which users or groups can exercise their roles. For example, a help desk administrator may have a role for "password manager" which allows him to reset passwords with a scope limited to "generic user email accounts."
What access controls or auditing do you have in place for your administrators or engineers?	Like the access controls vendors should provide for your users, vendors should strictly control their administrators. When administrators use elevated privileges and especially when administrators access your data, vendors should log that activity so they can trace or audit administrators' behavior.
Do you require MFA for remote access for all your employees, regardless of privilege level?	Vendors should not allow remote access to their *infrastructure* without additional controls beyond usernames and passwords. Vendors may determine that some remote connections do not present a risk which merits MFA and other controls, in which case they should be prepared to make a compelling argument since they are neglecting to rigorously control entry into their trust boundary.
How do you separate users, tenants, and/or administrator access levels?	Beyond roles and scopes, there should be clear logical and physical boundaries between your data and the data of other organizations. Your administrators should not be able to access any data outside of your tenant.

	Controls may include API security features, cryptography and key control, (micro-)segmentation, zero trust, etc

2.2 DATA

Question	Answer
Who owns our data when it is stored on your systems? Us or you?	Vendors will likely either assert 1) that you own your data but that they are allowed to use it for their business purposes (somewhat common) or 2) they own data housed on their systems (somewhat rare). This question is intended to help you gauge how vendors use and monetize your data as well as understand ownership of intellectual property housed on others' systems. Remember that even if vendors "own" data housed on their systems you may still be considered the owner *and liable* in case of a breach of the vendor's systems, especially in cases involving regulated data such as electronic protected health information (ePHI). Vendors might provide access to your data to third parties—ostensibly to accomplish legitimate business functions—or may use contractors and partnered organizations to engineer their systems and provide their services, which may further increase your exposure or allow for spread of your data.
How and where is our data stored?	Vendors should have a better answer than "In AWS" or "In Azure," though many vendors will stop with this response. Vendors should understand and be able to provide the general location within their systems or their cloud service providers' systems in which your data is housed both by region and by platform (e.g., "AWS S3 in Frankfurt", etc). In addition, vendors should readily be able to describe how that data is stored and protected.
Do we have any say in where our data is stored? (e.g. Country or Region)	The best vendors will allow you some say on where your data is stored, though it will likely be limited to locations they already support. Knowing which region your data is stored in and choosing the correct one from options allows you to maintain your compliance obligations. For example, if you are collecting Personally Identifiable Information (PII) under the General Data Protection Regulation (GDPR), you will

	probably want to select a data center in the European Union.
How is our data protected? Do you implement full disk encryption? Download restrictions?	Your data should generally be protected and encrypted at rest, if only to separate that data from other organizations' tenants with your vendors. Full disk encryption (FDE) may or may not be relevant, depending on how the vendor builds their infrastructure and the control their infrastructure provides them over storage (e.g., do they use their own hardware or are they limited to the features of infrastructure- or platform-as-a-service). Ideally vendors will provide download restrictions by user, roles, access conditions, etc. For example, you may want a data base provider to disable copy-paste within their application and to forbid downloads by business analysts so that you can control/prevent data creep.
How is our data kept separate from other customers' data?	Under no circumstances should other customers be able to access your data, so vendors should not only manage cryptographic keys maturely but also lock down their APIs, apply cloud access security brokers, etc. If the vendor requires you directly share data with them from your cloud service provider, requests that you federate/trust your active directories with theirs, or similar it is generally a sign of poor engineering and build-time controls. Further, vendors may fail to truly separate your data if they replicate their production data into their test environment. It is not abnormal for a SaaS company to fail to evaluate and securely engineer their test and development environments, even while using real world data within that low-trust environment.
How long is our data retained for while we do business with you? Afterwards?	Vendors should have clear policies on data retention both while you are a customer and after. Preferably a vendor will *wipe* your data after you terminate your relationship with them so that you do not maintain a risk after losing influence over/value from a relationship.
Do YOU have access to our data? What do YOU use our data for?	Most vendors will have some access to your data in order to deliver support or deliver their services to you. Vendors should be able to clearly delineate who has access to what data and why. Vendors who process your data should be able to describe the risk of processing activities (ROPA) or data processing impact assessment (DPIA) in

	general terms. They are unlikely to provide you with copies of internal risk assessments. Some vendors will use your data to develop new services instead of generating simulated data. This may increase your exposure without increasing the value you gain. Further, vendors may fail to truly separate your data if they replicate their production data into their test environment. It is not abnormal for a SaaS company to fail to evaluate and securely engineer their test and development environments, even while using real world data within that low-trust environment.

2.3 IT OPERATIONS

Question	Answer
Do you keep an inventory of your assets according to how important they are?	Vendors who do not fully enumerate/identify their assets and evaluate the criticality of their assets cannot hope to defend their environments nor your data. Vendors are unlikely to share their asset inventory with you, but inventory should include devices, software and cloud services, networks, data, and users. Just like for your organization, you cannot hope to manage what you do not know you have. You cannot defend nor secure an asset that you're unaware you own. The functions of protect, detect, respond, and recover all depend on the previous functions as pre-requisites[1], so a vendor who does not identify their assets cannot claim to manage their IT and cybersecurity risks.
How often are your systems patched? (e.g., how often are critical and high security patches managed)	Vendors who patch generally indicate that they are attempting to manage their inventory, identify problems, and protect their environment. Patching is an indicator of fundamentals and basic proficiency, *especially for vendors building their own infrastructure.* If you are purchasing a SaaS product and it *is not* highly available (99.99%+), always up to date, and always at the latest version, you are probably purchasing from an immature provider.

[1] Sounil Yu, *Cyber Defense Matrix* (Morrisville: JupiterOne, 2022), 12

Do you rely on any systems or software that are past end-of-life?	If a vendor relies on a system that is past end-of-life (EOL), they may be providing for a niche or anachronistic need (for example, supporting a legacy database still vital to many customers). Vendors using such systems should be able to describe their process for establishing mitigating defenses in depth. Vendors without a clear value proposition for EOL systems are likely hiding technical debt and operating without much true margin—which makes them a risk for sudden business failure. Or they are failing to track, manage, update, and defend their systems
How do you backup your systems?	Vendors should have backup and/or failover processes in case of emergencies above and beyond data breach. Vendors backup and emergency plans should also be tested or practiced.
How large is your: **- Cybersecurity Staff** **- IT Staff** **- Development Team** **- Engineering Team** **- Security Operations Center**	Teams solve problems, not heroes. Organizations who run on excessively small teams are in technical debt and will be disrupted by personnel turnover. Excessively small teams burn out team members and do not provide margin (neither time nor money) for emergencies. Organizations who use the same staff for any combination of IT, development, and security either 1) have a legendarily rare, ultra-mature DevSecOps staff or 2) do not recognize the specialization and the unique skillsets required to execute each function professionally.
How does management support cybersecurity efforts and personnel?	If management does not support security efforts or security staff, then the organization's security efforts will fail. Vendors should describe how they treat security as a significant stakeholder for design, development, and operations discussions and how risk management and build-time controls are considered at the ground-floor of every new initiative. Vendors are unlikely to admit where they are failing to support the disciplined initiative of their security team.

2.4 SECURITY OPERATIONS

Question	Answer
Have you ever been breached? What happened? How did you identify it?	Hopefully the vendor has never been breached and will never be breached. However, breaches occur and not all of them are deal breakers.

	You will likely receive a very brief summary of the response process if a vendor has publicly disclosed a breach in the past, but vendors will likely not provide you with all the fine details. Vendors who have been breached should be able to describe a mature process of quickly identifying the incident via automation and dedicated security analysts. When breach is identified and triaged, they should have scrambled resources to contain and eradicate it, assess root causes, and harden their system against repeat compromise. In addition to the thoroughness of the actual response, it's important that vendors communicate truthfully and thoroughly with customers whose data or accounts were impacted. Vendors who have been breached but did not communicate impact truthfully to their customers post breach or who did not execute incident response quickly and maturely may not be a good match for your organization.
What happens if you are breached? Do you have an incident response plan?	Vendors should have an incident response team to identify incidents, notify an incident response team, triage the incident, assess root causes, contain the incident, eradicate the attackers' presence, and recover from the incident. Vendors' description of their plan should probably be more detailed than the paragraph of common knowledge immediately above this one. Vendors likely will not share a copy of their security plan but should be able to describe some of the resources (people, software, etc) allocated to the problem and how they use runbooks, checklists, plans, and/or procedures to respond to incidents. Probably most importantly, vendors should have an incident response team identified in advance. Mature vendors will conduct routine rehearsals of their incident response plans.
If you are breached, how and when will you communicate it to us?	Vendors should know and communicate clear criteria for informing you of a breach. Many will not inform you if it does not impact your data. If your accounts or data are compromised, vendors should already have notification timelines in their service level agreements or master services agreements. If a vendor is not prepared to answer this question and doesn't point you to an accompanying SLA or MSA, they may be unprepared to notify you or work with you during a security incident.

	This is also an opportunity to learn about how you might be compensated in response to a breach, if at all. In conversation and follow-up questions, you should seek to learn who determines fault or assigns fault due to a breach. Determine if you as the customer can be assigned fault and—if so—when and what are the consequences?
What level of cybersecurity insurance coverage do you carry?	Cybersecurity insurance is a table stakes requirement for vendors, especially for cloud services. It is a vital part of recovering from a breach quickly and affordably, as well as covering some of your risk which you inherit by working with the vendor.
How do you monitor the health, availability, and security of your services?	Vendors should proactively monitor the up-time of their systems and ensure they function properly. They should have people allocated to understanding and monitoring whether the systems function normally and identifying bad actors in abnormal activity. This likely manifests itself as a Network Operations Center or Development and Operations team responsible with monitoring system health alerts. That team should interoperate with the Security Operations Center or Information Security Team. Both divisions should have monitoring and automated alerting.
How do you monitor for threats and cybersecurity incidents?	Related to the question above, the vendor should have a security team with analysts who monitor systems for security alerts. Alerting should rely on logging and monitoring across the environment and all types of assets and should be synthesized in a Security Incident Event Management system or similar. Ideally the vendor will have a dedicated team of security analysts responding to alerts and automated tools assisting with response and triage. Analysts should be equipped with threat intelligence which allows them to match the techniques of current threat actors with the behavior of the vendor's systems.
Do you have a 24x7 On-call Incident Response Team?	Vendors should have a dedicated on-call incident response team (IRT). Better vendors will have an internal team assigned to emergencies and will be prepared to call an external team for assistance. They will almost certainly not tell you the identity of that external IRT. It is common for companies to source their external IRT from their insurance providers' requirements or recommendations.
Are you able to aid us in the event of an incident or investigation?	Audit and security logs created by the vendor would help you investigate any incident you

	detect and wish to examine—especially if it directly relates to your data housed by the vendor. Vendors may not scramble an IRT to assist you with the investigation, but they should be generally willing to assist your investigations with their security analysts and/or with access to logs.
What have you done to protect your company from ransomware (or to recover from it)?	Ransomware is a common cybersecurity concern which most if not all companies have discussed or planned for. Given the likelihood of this security scenario, you can expect a vendor to have some level of plan for it. Plans should cover at least identifying the presence and activation of ransomware, blocking it, containing its spread/isolating infected machines, and recovering from tested backups. Plans should also cover interacting with attackers, paying ransoms (or not), and the potential for secondary breaches (though it would be fair for a secondary breach to trigger a second incident response playbook and not be directly managed by the ransomware playbook). As with Incident Response plans, do not expect vendors to provide a copy of their ransomware playbook. Do expect them to have a ready answer that is thorough.
When did you last conduct a vulnerability assessment, risk assessment, or penetration test with an external assessor?	Vendors should routinely identify, assess, and manage risks within their own organizations. In general, mature organizations should be working with third-party assessors once every one to three years, either to conduct a risk assessment, a penetration test, or other audit. Ideally the vendor already publishes the results of such assessments, but it would not be abnormal for a vendor to keep results private. Mature vendors will understand their compliance obligations and will immediately be able to explain what their last audit was, why they purchased it, and how well they performed/what they have remediated as a result.

3 REFERENCES

1. Yu, Sounil. *Cyber Defense Matrix*. Morrisville: JupiterOne, 2022
2. “Resources.” Github. Ericius Security, 2023. https://github.com/ericiussecurity/Resources
3. “7 SaaS security risks that every business should address.” Vendr.com. Vendr, 2022. https://www.vendr.com/blog/saas-security