Prophix®

Security and compliance

How to navigate cloud vendors on the market today

So, you're choosing a Cloud Software-as-a-Service provider...

What exactly do you need to know?

Security and Compliance are key elements to evaluate when choosing a vendor. Peace of mind regarding the security and protection of your data is essential, which is why we would like to demystify the evaluation process and explain what to look for when comparing and evaluating vendors.

This document intends to help you learn more about cloud security and compliance, Prophix security standards, and assess what is important when comparing security features with other vendors.

Here's what to look for:

1. The frequency of audits

It's important to ask how frequently a vendor performs its security audits. A cloud SaaS company has the option of doing yearly audits or more frequent audits. The average cloud vendor opts to do their audits yearly, meaning it may take up to a year to discover whether an unfavorable event has occurred and its effect on your data.

Prophix completes security audits every six months.

2. The compliance standards met

It's easy to be intimidated by the sheer volume of acronyms in the Security and Compliance space. One of the most common acronyms you may come across is Security Operations Center (SOC) and Trust Service Principles (TSPs).

A Security Operations Center's (SOC's) responsibility is continuously monitoring and analyzing an organization's security posture. SOC reports give assurance over control environments as they relate to the retrieval, storage, processing, and transfer of data.

There are multiple reports that prove an organization is in good standing. Namely, SOC 1 and SOC 2 compliances, and it's vital that both Type 1 and Type 2 Reports are complete for these SOCs.

Step 1

Type 1 Report - Demonstrates a company's internal controls are properly designed to meet relevant Trust Principles. This report **does not** confirm efficacy of controls over a period.

Step 2

Type 2 Report - Further demonstrates that your controls operate effectively over a period.

Did you know?
To claim compliance with SOC, vendors only need to have a SOC 1 Type 1 Report completed, not the full SOC compliance that includes a Type 2 Report. It is important to ask a vendor whether their SOC compliance includes a Type 2 Report. Only then, are you assured that the controls have been tested over a period of time.

Now let's talk about differences between SOC 1 and SOC 2 compliance...

SOC 1

A SOC 1 report gives assurance that your financial information is being handled safely and securely. Typically, when a vendor says they are SOC 1 compliant, the implication is that they have completed both Type 1 and Type 2 reports. The international version of the SOC 1 report is commonly referred to as ISAE 3402.

Prophix is ISAE 3402 compliant, which is the same as having SOC 1 compliance.

SOC 2

This report gives assurance over control environments as they relate to the retrieval, storage, processing, and transfer of data.

Here is where Trust Service Principles (TSPs) come into play.

SOC 2 reports evaluate an organization's compliance against five criteria, commonly called Trust Service Principles (TSPs).

Trust Service Principles

- **Security** – Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems.
- **Availability** – Information and systems are available for operation and use.
- **Processing Integrity** – System processing is complete, valid, accurate, timely, and authorized.
- **Confidentiality** – Information designated as confidential is protected.
- **Privacy** – Personal information is collected, used, retained, disclosed, and disposed.

Did you know?
It is important to ask a vendor what Trust Service Principals are being met for SOC 2 Type 2 Report. To claim compliance with SOC 2 Type 2 Report, vendors only need to meet at least one of the five TSPs. Make sure to ask vendors if they have met all five TSPs as part of their SOC 2 compliance.

Reminder!

1. SOC Type 1 Report: Snapshot look at controls at a 'point in time.'
2. SOC Type 2 Report: Observing how controls perform during a 'period in time.'

Prophix is SOC 2 compliant on all five Trust Service Principles and completes these audits every six months.

3. The value of HITRUST Risk-based, 2-Year (r2) certification

Achieving HITRUST certification helps build trust with customers, partners, and regulators. HITRUST certification shows that data protection is a priority and helps meet compliance requirements for certain regulations, such as HIPAA and HITRUST CSF.

HITRUST Risk-based, 2-year Certification now goes beyond fulfilling the healthcare industry's compliance and risk management needs. This rigorous certification process evaluates an organization's information security policies, procedures, and controls against industry standards and best practices.

The certification provided by the HITRUST Risk-based, 2-year Validated Assessment indicates that adopting an extremely proactive, expanded practices approach to safeguarding data and mitigating information risks. This assessment is widely acknowledged as a top-tier validation demonstrating an enterprise's ability to effectively manage risk by surpassing the cybersecurity standards set by the industry.

Prophix has invested in obtaining HITRUST Risk-based, 2-Year Certification.

4. What frameworks is the vendor certified in?

To claim they are secure, an organization must adhere to a framework that dictates how the organization should manage their data. You can think of this as a standard, or a set of practices to follow. This framework is built around an Information Security Management System (ISMS).

What is ISMS? An ISMS is a systematic approach to managing sensitive company information so that it remains secure and encompasses people, processes, and systems by applying a risk management process.

ISO 27001 is a globally recognized framework that indicates a secure organization (i.e., being 'certified' against this framework).

Did you know?
There are different ISMS frameworks that a vendor can use. It is also possible to not have a framework at all. It is important to ask a vendor whether they use an ISMS framework or not. If a vendor does not use an ISMS framework, it indicates they may not have the appropriate security in place.

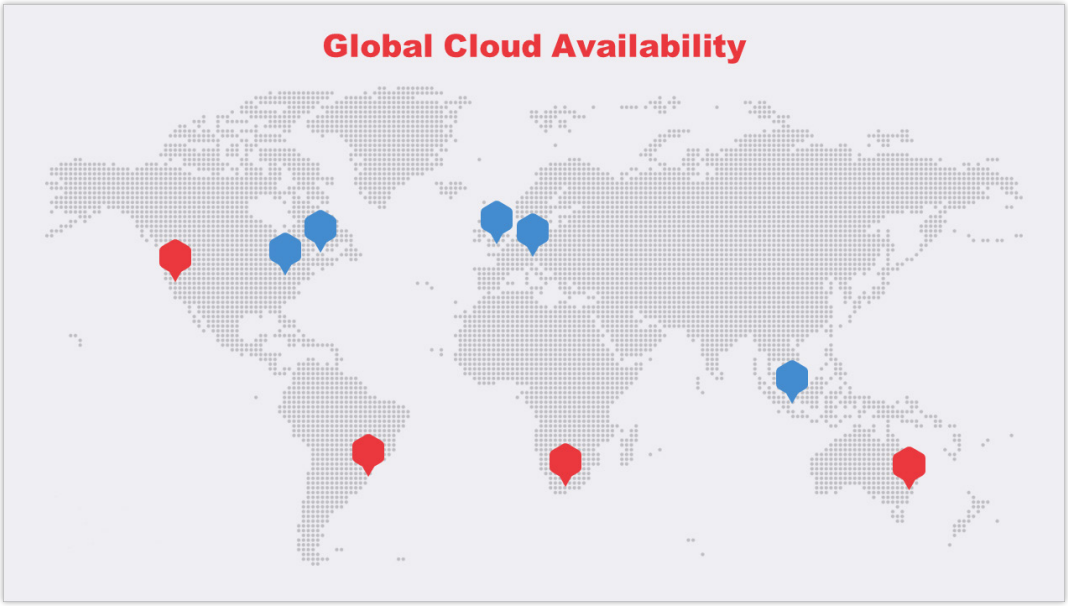
Prophix is ISO 27001 certified, so all appropriate security is in place. This certification extends to our customers, meaning that our customers' environments are also ISO certified.

5. Who is providing the underlying cloud technology?

There are a handful of well-known providers of cloud infrastructure that underpin the technology of cloud software vendors. They include AWS, Azure, and Google. If a software vendor does not use one of the above-mentioned providers, it is worthwhile asking who is providing their underlying cloud technology. It is also important to know their backup strategy, where their data is located, and their platform uptime.

Where will your data reside? To stay compliant with information privacy and protection acts, data centers and servers may need to reside in the same country as your organization. Ask the vendor where your data will reside.

Prophix data centers are located globally.



2022 Gartner Cloud Infrastructure and Platform Services (CIPS) Magic Quadrant

Prophix delivers uptime availability levels of at least 99.5%, consistent performance, and a high-security posture for our customers.

Prophix uses AWS technology, which has been recognized by Gartner as a leader in Cloud Infrastructure and has data centers around the world.

Figure 1: Magic Quadrant for Cloud Infrastructure and Platform Services

6. How have they streamlined end-user authentication (i.e., the login process)?

SSO, SAML, MFA – what do all these acronyms mean, and what do they have in common? They all relate to how streamlined and secure the login process will be for your end-users.

Likely, you are already using single sign-on (SSO) at your organization. An SSO set-up minimizes the number of times you need to enter sets of credentials by using a single ID (ex., your work email) to access multiple systems.

Multi-factor authentication adds additional security to the login process by requiring two or more pieces of evidence that prove your identity before logging in.

Security Assertion Markup Language (SAML) is the proverbial glue that ensure SSO can be integrated with existing systems at your organization that already use SSO.

If you'd like to minimize the time it takes for your team to enter a system and start working within it, then SSO and MFA should matter to you. SSO allows your users to manage a single login rather than several separate logins and credentials for each of your systems (i.e., usernames and passwords).

Did you know?
It's important to ask whether the SSO supported by the vendor abides by the SAML standard. Without meeting the SAML standard, you may need to investigate whether the product will integrate correctly with your existing IT environment.

For more information, please visit https://trust.prophix.com/

Sample Questionnaire

Below is a security questionnaire prepopulated with responses reflecting how Prophix would respond to the corresponding questions.

Are you ISAE 3402 compliant, meaning you have both SOC 1 Type 1 and Type 2?

- [x] Yes, have both SOC 1 Type 1 and SOC 1 Type 2
- [ ] No, have only Type 1
- [ ] No, have no SOC 1 compliance at all

Are you SOC 2 compliant?

- [x] Yes, have both SOC 2 Type 1 and SOC 2 Type 2; I complete my audits every 6 months
- [ ] Yes, have both SOC 2 Type 1 and SOC 2 Type 2; I complete my audits once a year
- [ ] No, only have Type 1
- [ ] No, have no SOC 2 compliance at all

If you are SOC 2 compliant (with Type 1 and Type 2), are you currently certified for all five Trust Service Principles (TSPs)?

- [x] Yes
- [ ] No

Check which of the five you fulfill today.

- [x] Security
- [x] Availability
- [x] Confidentiality
- [x] Privacy
- [x] Processing Integrity

If some are in production, please choose which apply:

- [x] N/A, I have all five attestations
- [ ] Security
- [ ] Availability
- [ ] Confidentiality
- [ ] Privacy
- [ ] Processing Integrity

If any are missing, please indicate why:

N/A – Prophix meets all five TSPs.

Are you HITRUST Risk-based, 2-year (r2) certified?

- [x] Yes
- [ ] No, but we are in the process of obtaining certification
- [ ] No, we are not HITRUST Risk-based, 2-year (r2) certified

A: Prophix has obtained HITRUST Risk-based, 2-year (r2) Certification

Are you ISO 27001 certified?

- [x] Yes
- [ ] No, we use another framework
- [ ] No, we don't use a framework

If you use another framework, which other framework do you use, if any?

N/A – We built our software as a net-new service offering NIST standards, ISO 27001:2013 standard, and ISO 27,017 standard. From there, we built out a dedicated framework in customer environments, specifically a multi-tenant environment.

If you are providing a cloud platform, what underlying technology is hosting your cloud instances?

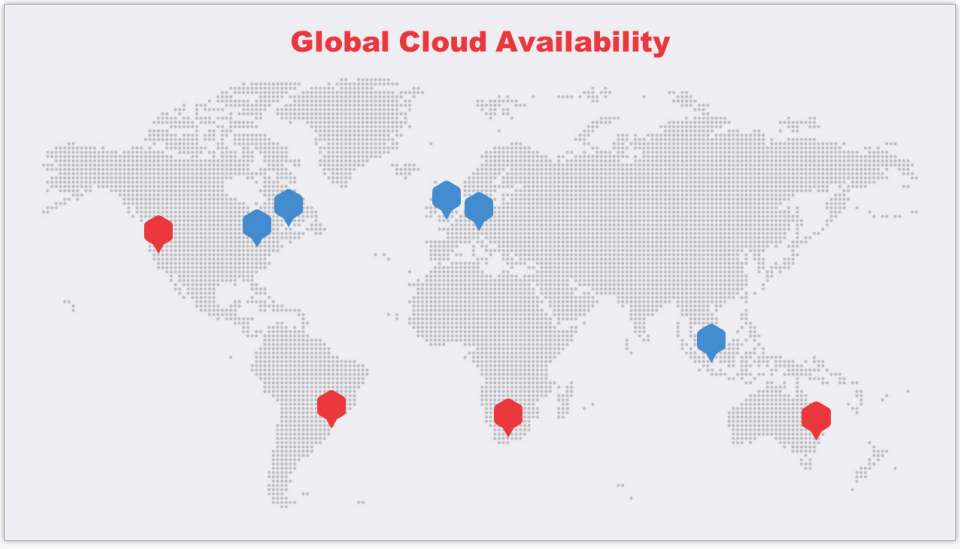
- [x] AWS
- [ ] Azure
- [ ] Google Cloud
- [ ] Other

If you use 'other', what is it?

N/A

Where are the data centers located?

Our data centers are located globally.



What is the published uptime of the vendor's cloud platform?

A: Prophix delivers uptime availability levels of at least 99.5%.

Do you support single sign-on (SSO)?

- [x] Yes
- [ ] No

If so, what SSO vendors do you support?

A: Prophix supports Okta, ADFS, and Azure AD, or any SAML 2.0 compliant Identity Provider (IdP).

Are those vendors compliant with Security Assertion Markup Language (SAML) 2.0?

- [x] Yes
- [ ] No

Do you support Multi-Factor Authentication (MFA)?

- [x] Yes
- [ ] No

If so, what SSO vendors do you support?

A: Prophix supports the market leader DUO, in stand-alone mode or your current MFA provider when utilized with your in-house SAML 2.0 IdP.

*Please note if you need a blank questionnaire to do your vendor analysis, talk to your Prophix sales rep.

Prophix®

350 Burnhamthorpe Rd. West,
Suite 1000, Mississauga,
Ontario, Canada L5B 3J1
Tel: +1-905-279-8711
Toll-free: +1-800-387-5915
info@prophix.com

v 2023.04.28