GUIDEWIRE

Guidewire Cloud: Fast Facts

How do I know Guidewire Cloud is compliant?

Choosing a SaaS vendor that has demonstrated compliance with recognized standards is a key to protecting your financial, organizational, and customer information.

Guidewire Software has demonstrated that all applications hosted via Guidewire Cloud™ comply with standards set by the AICPA and PCI SSC. We can provide the following on request:

- SOC 1 (Type 1 and Type 2 reports)
- SOC 2 (Type 1 and Type 2 reports)
- PCI ROC (Attestation of Compliance)

What Are Compliance Standards?

In general, there are three steps to compliance:

1. A governing body must write a standard.
2. Organizations (like Guidewire Software) build services that follow that standard.
3. Somebody (typically a third-party auditor) evaluates the specific services and produces a report validating that those services meet the standard.

Let's take a closer look at each of the reports that Guidewire offers for its applications that are hosted via Guidewire Cloud.

System and Organization Controls (SOC) 1: Financial Reporting

This report is based on the American Institute of Certified Public Accountants (AICPA) Statement of Standards for Attestation Engagements (SSAE) 18, section AT-C 320. This standard focuses on financial reporting. In the United States, a SOC 1 report is frequently required by publicly traded companies that must comply with the Sarbanes-Oxley Act.

> "Celent believes that the evaluation of insurance core systems and solutions must go beyond features and functions. Other critical criteria include strong controls for financial reporting, security, availability, confidentiality, and privacy. Successful completion of SOC 1 and SOC 2 audits provides an important level of assurance for those areas."
>
> — Donald Light
> Director, North America P&C Practice
> Celent

System and Organization Controls (SOC) 2: Trust and Security

This report is also based on the AICPA SSAE 18 standard. It focuses on sections AT-C 105 and AT-C 205, which outline the AICPA Trust Services Criteria (TSC). In fact, there are five such criteria: Security, Availability, Processing Integrity, Confidentiality, and Privacy. Although only the Security criterion is required for a SOC 2 report, Guidewire's SOC 2 reports show that all cloud-hosted applications meet four of these criteria: Security, Availability, Processing Integrity, and Confidentiality.

Payment Card Industry (PCI) Report of Compliance (ROC): Protecting Customers' Payment Card Information

The PCI Security Standards Council (SSC) created the Data Security Standard (DSS) to improve the security of cardholder information and to facilitate global consistency in data security standards. It consists of 12 requirements and the testing procedures to ensure that these requirements are met.

In terms of validating that a cloud service is compliant with the PCI DSS, vendors can complete a PCI Self-Assessment Questionnaire (SAQ) or hire a third-party Qualified Security Assessor (QSA) to produce a ROC. Guidewire can provide a PCI ROC for all applications that are hosted via Guidewire Cloud.

To further demonstrate our commitment to PCI security, we have registered with Visa as a Third Party Agent (TPA.)

REPORT TYPES

Both SOC 1 and SOC 2 reports can be produced as either Type 1 or Type 2 reports.

Type 1 reports: These evaluate an organization's controls at a single point in time (i.e., does the organization have the right controls in place to meet the standard?).

Type 2 reports: These include the Type 1 report and evaluate the effectiveness of the controls (i.e., did the organization's controls work?) over a period of time that is typically 6–18 months.

"More and more insurers are moving to the cloud and entrusting the security of their data to a cloud service provider. Guidewire has actively implemented controls and managed them in our cloud environments. To ensure that we have appropriate controls implemented and that they are working effectively, Guidewire has undergone independent audits of these environments. The audits, which are becoming a table stakes requirement for cloud services providers, provide assurance that the information environment is secure."

— Kirk Sanford

Chief information Security Officer (CISO)

Guidewire

Cloud-Hosted Application	SOC 1 Types 1 & 2	SOC 2 Types 1 & 2	PCI ROC	ISO 27001
InsuranceSuite via Guidewire Cloud	Jan-19	Jan-19	Jan-19	2020
InsuranceNow	Jan-19	Jan-19	Jan-19	
Underwriting Management	N/A*	Jan-19	N/A**	
Predictive Analytics	N/A*	Jan-19	N/A**	
Live	N/A*	Jan-19	N/A**	
Live Analytics	N/A*	Jan-19	N/A**	
Guidewire Digital	N/A*	Jan-19	N/A**	
DataHub and InfoCenter	N/A*	Jan-19	N/A**	
Cyence	N/A*		N/A**	Nov-18
Digital Small Business (DSB)	N/A*		Jan-19	

The Last Word

We know that the security and integrity of your organization's data are top concerns. That is why we've built a world-class organization that will continue to demonstrate that we comply with the industry's highest standards.

* *These applications do not affect financial reporting, so SOC 1 is a non-applicable (N/A) standard.*

** *These applications do not handle payment card information, so PCI DSS is a non-applicable (N/A) standard.*

About Guidewire Software

Guidewire delivers the industry platform that Property and Casualty (P&C) insurers rely upon to adapt and succeed in a time of accelerating change. We provide the software, services, and partner ecosystem to enable our customers to run, differentiate, and grow their business. We are privileged to serve more than 350 companies in 32 countries. For more information, please visit www.guidewire.com and follow us on twitter: @Guidewire_PandC.