Blackbaud Hosting Services™
Compliance for the Hosted Customer

Compliance Challenges

Blackbaud customers both small and large find being compliant with regulations an often daunting task. These regulations exist to govern security, privacy, and breach disclosures. Managing them, and then designing and implementing appropriate controls to address them, requires significant resources, both in terms of personnel and capital expenses. This is why many organizations trust Blackbaud to enforce strong compliance controls related to their data, including PCI DSS, AICPA SSAE-16 (also known as SOC 1, formerly SAS-70) and AICPA SOC 2.

PCI DSS

It is neither easy nor inexpensive to become PCI DSS compliant. This certification is aimed at reducing the risk of payment card transactions by requiring merchants and service providers to follow key security standards in networking, systems, and application development. Blackbaud's Research Delivery Operations is proud to have received its report on compliance for all applications in the hosting environment every year for the past five years.

Blackbaud Hosting Services achieved this gold standard by building strong networks, protecting cardholder data, and maintaining a robust vulnerability management program. We've also implemented strong access control measures; we regularly monitor and test our networks and maintain a strict information security policy.

SOC 2/SOC 1 (SSAE-16)

Blackbaud has also achieved a Service Organization Control (SOC) 2 Type II report. The SOC 2 report was developed for service organizations whose customers expect evaluation on the most stringent of operational best practices and trust principles. For select applications, we also undergo SOC 1 audits, designed to give our customers assurance of the integrity of financial statements, and providing one more reason to entrust their valuable data to Blackbaud.