



OpSource Compliance Solutions

Ensuring Compliant Delivery of Web Applications

Companies face a myriad of challenges and issues regarding the compliant delivery of web applications. Enterprises of all sizes must ensure supplier, operational and regulatory (such as Sarbanes-Oxley and HIPAA) compliance in order to drive down risk. These requirements are complex and should be managed strategically.

Customers delivering applications through the OpSource On-Demand environment can take advantage of OpSource's certifications to help them comply with their own internal controls and regulatory requirements.

The three critical certifications maintained by OpSource are:

PCI DSS Service Provider Certification

SAS 70 Type I and Type II

Salesforce.com AppExchange Certification

PCI DSS Service Provider Certification

PCI DSS (Payment Card Industry Data Security Standard) is a prescriptive data security standard that applies to any electronic application that is storing, processing, or transmitting credit/debit card data. The standard is maintained by the PCI Security Standards Council, and includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. These requirements are designed around six major principles:

- Build and Maintain a Secure Network
- Protect Cardholder Data
- Maintain a Vulnerability Management Program
- Implement Strong Access Control Measures
- Regularly Monitor and Test Networks
- Maintain an Information Security Policy

All of the major credit/debit card companies require that any application that stores, transmits, or processes credit card information meet this standard and most require that any service provider used by the application meet these standards as well.

OpSource maintains a PCI-certified environment to help our customers address this requirement. By running their application inside our PCI compliant environment, OpSource On-Demand customers meet the majority of the overall requirements associated with the standard, particularly the requirements associated with Build and Maintain a Secure Network, Implement Strong Access Control Measures, and Regularly Monitor and Test Networks sections. This allows our customers to concentrate their compliance efforts on the application-specific portions of the standard, speeding the time-to-market associated with deploying

applications that involve accepting, storing, or transmitting credit and debit cardholder information. In fact, OpSource On-Demand customers have full responsibility for only 2 of the 12 PCI DSS requirement areas!

PCI DSS Requirement	OpSource Fulfilled	Customer Fulfilled
1) Install and maintain a firewall configuration to protect cardholder data	*	
2) Do not use vendor-supplied defaults for system passwords and other security parameters	*	
3) Protect stored cardholder data		*
4) Encrypt transmission of cardholder data sent across open, public networks	*	*
5) Use and regularly update anti-virus software	*	
6) Develop and maintain secure systems and applications	*	*
7) Restrict access to cardholder data by business need-to-know		*
8) Assign a unique ID to each person with computer access	*	*
9) Restrict physical access to cardholder data	*	
10) Track and monitor all access to network resources and cardholder data	*	
11) Regularly test security systems and processes	*	
12) Maintain a policy that addresses information security-Connected Entities and Contracts	*	*

OpSource's PCI-certified environment is audited yearly by TrustWave and meets all of the requirements associated with Service Provider Level 3 certification.

SAS 70 Type I and Type II

SAS 70 is an auditing standard developed by the American Institute of Certified Public Accountants (AICPA) to evaluate the internal controls of a service provider. The Type I audit evaluates the service provider's documented internal procedures and processes to ensure that they are sufficient to achieve the service provider's control objectives. The Type II audit conducts a series of tests to ensure that the service provider is actually following those documented procedures and processes.

OpSource maintains both SAS 70 Type I and Type II attestations in conjunction with our auditor SAS 70 Solutions. In the context of OpSource, these SAS 70 audits assure OpSource On-Demand customers that OpSource is living up to the commitments it made. An in-depth series of documented controls covering the entire operational spectrum of the OpSource organization was designed:

- Data Center security procedures, processes, and systems
- Data Center environmental (HVAC, power, etc.) procedures, processes, and systems
- Information and data security procedures, processes, and systems, including the network, firewalls, servers, and applications
- System backup procedures, processes, and systems

You Build It. We Deliver It.

SAS 70 Type I and Type II continued

- Customer care, monitoring, and troubleshooting procedures, processes, and systems
- Operational and HR policies, including change control processes, background checks, confidentiality agreements, and employee termination procedures

SAS 70 is designed to allow customers' auditors to "plug in" to the audits already performed on OpSource as part of the SAS 70 process. OpSource customers with auditing needs related to Sarbanes-Oxley, Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley, or other legal or professional requirements can leverage the detailed OpSource SAS 70 audit to provide their auditors an in-depth understanding of OpSource's processes and controls. This helps OpSource On-Demand customers ensure compliance with their own internal controls and regulatory requirements.

HIPAA, Sarbanes-Oxley and Other Regulations

Although the PCI standards were developed specifically for credit and debit cardholder data, the service provider requirements map closely to the security needs associated with any sensitive information. Customers with applications subject to other regulatory requirements such as Health Insurance Portability and Accountability Act (HIPAA) and Sarbanes-Oxley (SOX) can take advantage of our PCI-certified environment to address the security needs associated with these types of applications.

OpSource has implemented the processes and procedures to act as a "business associate" of a HIPAA-covered entity under HIPAA regulations. We recommend that applications that are storing or transmitting protected health information be placed in our PCI

environment to ensure the strongest protections available to protect the integrity and confidentiality of that data. Similarly, we recommend the PCI standards as a good security outline for any applications working with highly confidential or sensitive data.

Salesforce.com AppExchange Certification

OpSource maintains a Salesforce.com AppExchange Service Provider certification. To obtain this certification, OpSource undergoes an extensive audit on a yearly basis that evaluates the security profile provided by our OpSource On-Demand environment, including our operational processes, access controls, HR policies, and security incident response procedures. In addition, the Op-Source On-Demand environment undergoes an extensive network penetration test. The extensive scope of the audit makes the AppExchange Service Provider certification a rare achievement, currently held by only one other service provider.

Because Salesforce has already done an in-depth evaluation of the OpSource On-Demand environment, our customers looking to make their application available on AppExchange go through a shorter, reduced scope audit of their own application. This expedited review process speeds time-to-market and ensures our customers the opportunity to offer their application to the AppExchange community as quickly as possible. By leveraging OpSource On-Demand's world-class Web application delivery platform and its years of experience in working with salesforce.com as a certified partner, customers can accelerate the Salesforce certification and on-boarding process by 33 percent, enabling them to more quickly bring innovative SaaS solutions to market via the AppExchange.

About OpSource

OpSource™ delivers Web applications and software as a service for on-demand companies, with hundreds of applications, millions of users and billions of transactions supported daily. OpSource On-Demand, the leading platform for Web application delivery, is defining how Web-based software is delivered. By choosing OpSource as their Web application delivery partner, companies are freed from investing in and managing the complex and costly infrastructure and services necessary to deliver applications over the Web. They can instead focus their resources on developing, marketing and selling their applications and services. OpSource On-Demand is suitable for companies at any stage of growth, with any type of on-demand application. OpSource is the only company to offer Success-Based PricingSM, a unit-based pricing model that allows businesses to begin with a modest minimum commitment and scale expenses as revenues increase.

Headquartered in Santa Clara, CA, OpSource has Web application delivery centers in Virginia, London and Bangalore. For more information about OpSource, visit www.opsources.net.



OpSource[™]
The SaaS Delivery Experts

Corporate Headquarters
5201 Great America Parkway
Suite 120
Santa Clara, CA 95054
1-800-664-9973 (USA)
+44 207 043 1240 (UK)
sales@opsources.net
www.opsources.net