ORIGAMI RISK

Security

Protecting Your Data

Keeping your data secure is of paramount importance to Origami Risk. Our platform and business processes are designed to protect your organization's sensitive data.

Industry Compliance Standards

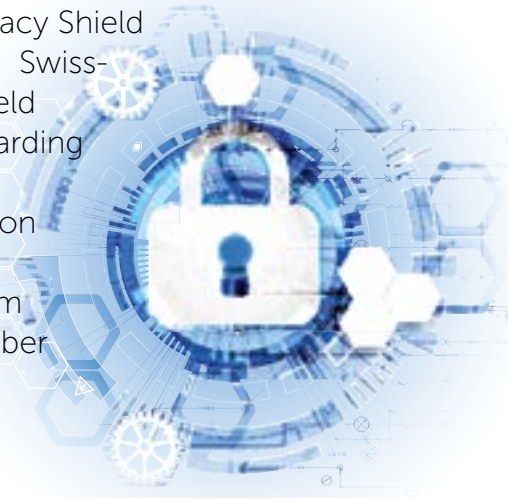
Origami Risk is audited and certified with a number of third-party standards.

SSAE 18: Origami Risk is SSAE 18 SOC 1 Type II and SOC 2 Type II certified. Compliance is assessed annually by a third-party auditing firm.

FISMA: Origami Risk is compliant with security controls based on NIST 800-53 Revision 4 and has received Federal Information Security Management Act (FISMA) Moderate System Authorization and Accreditation. The Origami Risk service has also received Authorization to Operate (ATO) by a federal authorizing agency.

HIPAA Security Rule: Compliance with NIST 800-53 allows Origami Risk, by way of existing security controls, to meet security requirements established by the HIPAA Security Rule in accordance with NIST SP800-66, "An Introductory Resource Guide for Implementing the HIPAA Security Rule".

Privacy Shield: Origami Risk complies with the EU-U.S. Privacy Shield Framework and Swiss-U.S. Privacy Shield Framework regarding the collection, use, and retention of personal information from European member countries and Switzerland.



Hosting Service

Origami Risk is hosted in a Virtual Private Cloud (VPC) within the Amazon Web Services (AWS) environment. This approach is ideal for clients because, in the ever-changing world of data security, Origami Risk is able to quickly adapt to changes and implement security features when they are needed.

AWS is certified to be compliant with SSAE18 SOC 1, 2 and 3, ISO 27001, HITECH, FISMA, and FedRAMP. In this secure environment, AWS provides Origami Risk with a blank canvas to build our application in the manner that best meets our clients' needs.

Data Encryption

All data is encrypted using Transport Layer Security (TLS) in transit; Transparent Data Encryption (TDE) at rest [for SQL Server]; and AES-256 for block storage, file system, and full Virtual Machine encryption.

Origami Risk enforces strict secure HTTPS encryption for all browser sessions. Data transfers are encrypted with PGP encryption and are transmitted using secure file transfer protocols.

Mirror Site & Separate Backup Facility

All databases are mirrored in real time to a separate database server located in a separate Amazon Availability Zone.

Data is backed up to Amazon S3 storage. Amazon S3 is redundantly stored across facilities and devices, providing 99.999999999% durability. As of 2013, Amazon S3 was storing more than two trillion distinct objects.

ORIGAMI RISK

Security

Independent Annual Penetration Tests

Origami Risk uses independent auditors to perform annual penetration tests. These tests simulate real-world attacks attempting to break into the Origami Risk system.

In addition to independent, third-party audits, Origami Risk conducts vulnerability assessments and monitoring on an ongoing basis to continually test and improve security measures.

Annual Board-Level Security Review

Origami Risk maintains a Security Steering Committee made up of several members of the Origami Risk Board, IT Operations, Development, and Customer Service. This committee conducts reviews of the Origami Risk security policies, processes, and procedures on an annual basis.

These reviews are augmented with continuous oversight by the Steering Committee, a security incident reporting system, and vigilant attention to the ever-changing security landscape by Origami Risk security personnel.

Code Review

Origami Risk uses a variety of tools to verify that code is secure. Dynamic site scans are used to identify cross-site scripting vulnerabilities and other common security issues.

Intrusion Detection

Origami Risk utilizes multiple levels of security within the Amazon Web Services (AWS) environment. AWS provides IDS and network analyzers which are monitored continually by AWS engineers.

Origami Risk also deploys and continually monitors its own Host and Network IDS/IPS solutions to provide maximum visibility to the security of the environment. Physical access to AWS data centers is also strictly controlled by state-of-the-art intrusion detection systems.

Firewalls

Origami Risk's infrastructure is behind multiple firewalls, starting with a Web Application Firewall (WAF) that controls the ingress and egress of all traffic. Additionally, the WAF inspects traffic at Layer 7 to protect against common attacks such as cross-site scripting and SQL injections. The WAF also provides protection against MITM attacks, IP Spoofing, port scanning, and packet sniffing. Within the Origami Risk AWS environment, both internal network and host-based firewalls are utilized to control traffic flow between functional areas.