oradian

Improve your financial institution's **security** with Oradian

Your financial institution's security is Oradian's priority. Security is designed into the design and architecture of our cloud-based core banking system, Instafin. Oradian's security governance enables financial institution to operate continuously and comply with local regulations, while maintaining the lowest possible security risk.

Oradian provides you with the maximum level of security across key parts of your financial institution's operating environment: secure **data storage**, a protected **network** and a secure community cloud-based **core banking system**.

1. Secure storage of your data

Oradian hosts Instafin in data centres that are geographically dispersed throughout Europe. These data centres are protected by a multi-layered security model that is compliant with key industry standards such as ISO/IEC 27001. This model includes perimeter security, video surveillance, security personnel, sophisticated access controls system and protection from external and environmental threats.

Oradian takes care of the security of your data, your network architecture, your applications and your security operations.

What is ISO 27001?

The ISO/IEC 27001 family of standards helps organisations keep their information secure.

ISO/IEC 27001 is the best-known standard in the family providing requirements for an information security management system (ISMS) that ensures information security is continuously aligend with business and regulatory requirements.

Oradian uses a community cloud model that ensures that only authorised customers are onboarded to our platform. A multi-tenancy design ensures that each of Oradian's customers runs in its own secured and isolated environment.

2. Providing you with a secure network and infrastructure – at your head office and at all of your branches

Instafin is built on a robust and scalable network infrastructure that maximises data availability and security. Data is stored behind a firewall that controls and monitors access to data. Network access controls limit connectivity to only authorised users and devices. Network segmentation and demilitarised zones (DMZ) also mitigate the risk of unauthorised access to data.

Intelligent distributed denial of service (DDoS) protection engines protect Instafin, ensuring that your core banking system is resistant to denial-of-service attacks, is always up and running, and that the stored data is continuously available.

Your secure network and infrastructure (continued)

Instafin aligns with secure configuration standards for operating systems and system components that are based on the leading industry standards, including those from the Center for Internet Security, the National Institute of Standards Technology and SysAdmin Audit Network Security.

These standards ensure that the security settings and parameters are implemented on all Instafin's components to prevent any misuse of the Instafin platform. The configuration of infrastructure components is periodically audited to assure continuous compliance to best practices.

3. Delivering a secure cloud-based core banking system

Instafin incorporates information security throughout the Software-Development Life Cycle (SDLC) from requirements definition, design and analysis to development and testing.

Source code reviews conducted by senior developers is a standard best practice in Oradian's development cycle that ensures no coding vulnerabilities are introduced.

An additional level of security is provided by the separation of development, testing and production environments and prohibited usage of production data on testing environments through obfuscation and anonymisation techniques.

Some of the Instafin's application security controls include: authentication, password security, authorisation and access control, session management, input validation, logging and proper error handling.

We conduct penetration tests of Instafin on a periodic basis to check the effectiveness of the security controls implemented. Our penetration tests validate that Instafin's application security is at a maximum level.

A member of the Cloud Security Alliance

Oradian is a member of the Cloud Security Alliance, the world's leading organisation dedicated to promoting best practices for secure cloud computing.

Continuous testing, assessment and improvement

Period vulnerability assessments are conducted to keep up with security trends and remediate all newly discovered vulnerabilities.

Network and infrastructure penetration testing is conducted by a qualified third party. This enables Oradian information technology and security professionals to understand the behaviour of malicious attackers and configure our system to be resistant to attacks.

Ensuring business continuity

Oradian supports your financial institution's business continuity by protecting against and handling major disruptions like cyber attacks, floods and supply failures. Oradian uses three data centres to ensure business continuity.

- The primary data centre is used for running the service
- The secondary data centre is used for disaster recovery that is a mirror of Instafin on primary data centre
- The third data centre is used for storage of encrypted data backups

Oradian tests backups and performs disaster recovery test regularly.

cloud CSA security alliance®