Lien Solutions

A security framework for building financial services solutions



In today's digital environment, trust is one of the most valuable assets a financial institution can have.

Protecting sensitive information, maintaining operational resilience, and supporting regulatory obligations require partnerships built on strong security foundations.

Security is embedded throughout the design, delivery, and operation of iLien. The platform operates within Wolters Kluwer's enterprise security framework and applies controls designed to protect sensitive information, support operational resilience, and help customers address evolving regulatory and compliance expectations.

The security challenges financial institutions face

Financial institutions operate in an environment of constantly evolving cyber and operational risks. Threat actors continue to leverage increasingly sophisticated techniques, while regulatory expectations and customer demands continue to grow.

Organizations today must be prepared to address challenges such as:

- Ransomware and cyber extortion
- Business email compromise and fraud
- Unauthorized access and credential compromise
- Third-party and supply chain vulnerabilities
- Operational disruptions affecting critical services
- AI-enabled attacks and advanced social engineering tactics

As these risks evolve, organizations need technology partners that demonstrate transparency, accountability, and operational resilience.

What to expect from a trusted security partner

When evaluating technology and information-service providers, financial institutions should look for partners that demonstrate a mature and comprehensive approach to security.

Key areas of focus include:

- User-access and identity controls
- Privacy and data governance for the entire information lifecycle
- Secure software development practices
- Vulnerability management and testing
- Incident response and customer communication processes
- Security awareness training
- Monitoring and threat detection processes
- Technology asset management
- Security governance and oversight
- Business continuity and disaster recovery capabilities
- Third-party risk management

Our security approach

Protecting customer information and supporting business continuity require more than any single control or technology. Our approach brings together people, processes, and technology to help manage risk, support resilience, and maintain the security of the services our customers depend on.

Protecting information



We apply information classification and data handling practices to help ensure information receives protection appropriate to its sensitivity and business value.

Our program supports:

- Protection of confidential and restricted information
- Access based on demonstrated business need
- Encryption and secure transmission methods
- Secure data handling, retention, and disposal practices

Securing access



Within iLien we use layered identity and access management controls designed to help ensure access is granted appropriately and reviewed regularly.

Key controls include:

- Unique user identities
- Multifactor authentication
- Role-based access controls
- Separation of responsibilities to reduce risk and prevent misuse

Building security into our solutions



Security is integrated throughout the software development lifecycle. By embedding security and quality practices into our product development processes, we strive to identify and address risks early.

This includes:

- Secure software development practices aligned with industry-recognized security standards
- Automated security testing and code scanning to identify vulnerabilities early
- Security assessment and penetration testing both conducted internally and by an independent third party
- Ongoing security training for development teams
- Formal code review and software design standards
- Processes for identifying, prioritizing, and remediating vulnerabilities
- Governance over third-party and open-source software components
- Controlled development and deployment processes that reduce operational and security risk

Protecting the environment



Operational environments are designed with multiple layers of protection to help safeguard systems and support reliable service delivery.

These protections include:

- Network security controls
- Firewall technologies
- Secure remote access capabilities
- Ongoing identification and remediation of security weaknesses
- Independent testing of security controls
- Timely application of security updates and patches
- Security monitoring capabilities

Responsible AI innovation

We believe AI based innovation must be accompanied by strong governance, transparency, and accountability.

Our **responsible AI approach** helps ensure AI-enabled capabilities are developed and deployed within established security and privacy frameworks. Through the **Wolters Kluwer Enterprise AI Platform (FAB)**, we support innovation while maintaining a focus on trust and risk management.

Our AI governance framework emphasizes:

- Security and privacy protections
- Human oversight and accountability
- Controlled access and authorization
- Governance and risk management
- Ongoing monitoring and validation



AI capabilities operate within established security controls and authorized use parameters.

Prepared to respond

Strong security is not only about prevention. It also requires the ability to identify, respond to, and recover from unexpected events. Our resilience programs are designed to help minimize disruption and support continuity when it matters most.

Monitoring and incident response



Our security teams monitor critical systems and evaluate potential security events to help support timely investigation, containment, mitigation, and recovery activities.

Business continuity and recovery



Our disaster recovery and business continuity programs help support critical operations through:

- Recovery planning
- Data backup and replication capabilities
- Continuity testing
- Ongoing program improvement activities

Managing risk across our ecosystem

Security extends beyond organizational boundaries. As business ecosystems become increasingly interconnected, understanding and managing third-party risk remains an important part of maintaining resilience and trust.

Our Supply Chain Risk Management Program includes:

- Vendor due diligence
- Risk-based assessments
- Ongoing oversight
- Security and continuity expectations for third parties



These activities help support the security, reliability, and resilience of the services we provide.

Security is everyone's responsibility

Technology alone cannot create a secure environment. Effective security depends on a culture in which individuals understand their role in protecting information and supporting operational resilience.

We reinforce this culture through:

- Confidentiality and security policies
- Workforce training and awareness programs
- Background screening, where applicable
- Controlled facility access and physical security safeguards

Partnering with our customers

Trust is built through transparency, communication, and collaboration. We work with customers to support their security reviews, due diligence activities, and risk management requirements throughout the relationship lifecycle.

To help customers make informed decisions, we may provide:

- Security questionnaire responses
- Assurance documentation
- Privacy resources
- Trust center materials
- Customer support and guidance

Our objective is to foster confidence through openness, responsiveness, and ongoing partnership.

Our commitment

Protecting customer trust is fundamental to everything we do. Our commitment to helping safeguard information, strengthen resilience, support compliance, and enable innovation helps create a secure foundation for our customers' success.

As the threat landscape continues to evolve, we remain focused on advancing our security capabilities while maintaining the transparency, reliability, and accountability our customers expect.



Contact us today to schedule a demo and see how Lien Solutions can simplify integration, reduce operational effort, and enable more flexible, AI-driven workflows.