



Security & Privacy For Financial Networks

“Traditional boundaries of risk are not applicable...extended enterprises must anticipate the potential risks related to every alliance they establish.”

Deloitte

ComplyChainSM is the premiere web-based service for empowering partners to collaboratively lower business and regulatory risks and costs in their joint information processes.

Recent Events Demand Compliance In Financial Service Networks

Financial service organizations depend on extensive networks of business partners to provide the services their customers expect. Recently, maintaining these networked collaborative services has become far more difficult. Cyber crime, malicious hacking, and overall service complexity continue to increase, as well as financial regulation and government scrutiny, e.g. the Gramm-Leach-Bliley Act, EU Directive 95/46/EC, The Patriot Act, and many others.

The Business Risk?

Financial organizations have rightly responded by producing partner agreements, service contracts and various certification schemes to regulate the security and privacy risks of their partners. But these efforts largely consist of terms and checklists that are enforceable by punitive measures after the fact, leaving unaddressed the core issues that threaten your business:

- Unauthorized disclosure of your clients' personal financial information jeopardizes GLBA compliance
- Lost or corrupted data affects quality of service, leading to loss of clients and revenue
- Invalid or unauthenticated transactions impact client records
- Operational impact from the unavailability of networked business partners' information systems
- Increasing costs to align information confidentiality, integrity and availability with networked partners

ComplyChain Manages Information Service Level Compliance

Extending and automating your oversight of Service Level Agreements (SLA) and other IT governance, information stewardship, and security and privacy service terms to protect shared information assets is called Information Service Level Compliance (ISLC). ComplyChain automates the ongoing negotiation and management of ISLC controls between partners in order to reduce the business and regulatory risks and that increase operational costs and risks that endanger your earnings and reputation.

Without the real-time continuous audit of a partner's information practices based on ISLC terms and conditions, operational integrity suffers. Today's practice of periodically conducting service level audits, then assessing financial penalties, happens well after damage to your business has already occurred. ComplyChain delivers real time management of ISLC with service network partners.

ComplyChain Rewards for the Collaborative Business Manager

- Enable proactive compliance to regulatory mandates for information accuracy, security, and privacy
- Reduce the risks and costs when you share sensitive client information
- Protect your brand and your clients by reducing security, privacy and business failure
- Minimize the business impact of service level failures by enabling a real-time response
- Increase the efficiency, effectiveness and speed of your ability to manage multiple business partners

How does ComplyChain work?

STEP 1:

A ComplyChain Certified Partner™ reviews existing information service terms to determine where our patent-pending Information Service Level Compliance (ISLC) service can help you gain control of the business and regulatory risks associated with your external information-based activities:

| Compliance Issue | Information Service Risk | ComplyChain Control Solution |
|---------------------------------------|---|---|
| Performance & Quality | A partner changes their application (i.e. information processing routine) without proper testing. Your information is now corrupted. | Monitor supplier's software change management and request review of application changes and updates. Capture the time of application changes for transaction back-out file recovery. |
| Security & Privacy | A partner does not apply operating system security patches on a timely basis, leaving your information exposed. | Monitor application of system security patches for compliance to a reasonable time-based standard. If a patch was not applied, an automated response isolates the partner from your network, thus reducing the risk of security failures. |
| Regulatory & Certification | A file containing your client's sensitive personal and financial information is left unprotected, leading to unauthorized access. | Monitor backup, security and configuration activities. Immediately notify key personnel when security specs or information controls are violated. |
| Personnel & Training | A partner's key employee with access to sensitive information on your systems is promoted or leaves a partner's organization, and your organization is not notified to update passwords or system access. | Systematic or email monitoring of partner's critical employees for immediate notification to changes in their job responsibility or employment status, thus enabling you to perform a timely security profile update. |

STEP 2:

ComplyChain helps you quickly and easily work in a collaborative manner, on a per contract basis, with each of your business partners to establish and manage, over time, an efficient and effective set of ISLC controls for each unique relationship:

- What are the business issues that require Information Service Level Compliance?
- What are the resultant systems, data and personnel that require controls?
- What constitutes an incident/violation, and how will both organizations coordinate the responses?
- Which existing performance or security tools can be re-purposed to monitor, test and improve system, network, security and change management "vital signs?"
- How can we quickly achieve ROI?

STEP 3:

When the initial collaborative effort is complete and the controls are deployed, ComplyChain real-time continuous monitoring, joint incident response and settlement, control testing, and continuous improvement processes automatically begin. Now you and your business partner have the confidence that both organizations are **in compliance** with the ISLC terms and conditions set forth in your agreements.

When a violation occurs, a ComplyChain "**Joint Incident Response (JIR)**" coordinates a response for both you and your partner to quickly minimize the impact on business operations. ComplyChain processes also continually ensure proper settlement, testing, and improvement of ISLCs between organizations.