Compliance

Compliance Complexity Is on the Rise

70% 70% of compliance practitioners surveyed expect an increase in the amount of regulatory information that the regulators will publish next year[1]

59% 59% of compliance practitioners surveyed expect the personal liability of compliance officers to increase in 2015[2]

As data breaches grow increasingly sophisticated, government and industry are rushing to safeguard sensitive data against emerging threats. The result is a growing maze of regulatory red tape that is becoming increasingly difficult for enterprises to untangle. Ever-changing compliance regulations are straining operations at every level—from budget to systems to experienced compliance personnel. Something's gotta give—and it's unlikely to be the regulations.

Further exacerbating compliance complexity is the rise of the cloud and its accompanying SaaS boom. The proliferation of specialized cloud applications is a double whammy on the issue of compliance: not only increasing the number of data sources that must be secured, but also obscuring data visibility as a result of ease of adoption. Enterprises are struggling to get a handle on the many applications—think Google Docs, Box, Trello, etc.—being implemented across lines of business with no central oversight.

"Citizen Integrators" Are Not Helping

65% Analysts have predicted that by 2017 the line of business will develop 65% of integration flows

Compliance with government and industry security standards is an enterprise-wide affair. Stringent rules and processes must be followed to ensure there are no cracks in the armor. However, in the self-service integration environment championed by iPaaS providers, the many business stakeholders (i.e. citizen integrators) that have been enabled to configure integrations outside the realm of IT may not be aware of the multi-tentacled dimensions of compliance. Or, if they are, they may find themselves limited by specific compliance to their vendors' tools that aren't broad enough to provide end-to-end compliance. As a result, compliance is often sabotaged (knowingly or unknowingly) and the enterprise finds itself at risk of exposure.

Compliance Is a Continuous Cost

$60,000 Minimum

It is estimated that annual PCI DSS audit costs for larger entities start at $60,000, but often rise sharply from there once the considerable costs in hardware and software remediation required to remain compliant are taken into account[3]

Generally speaking, there are three major compliance certifications, which are broadly classified under security, controls and privacy:

- For security, especially around sensitive payment card data, the industry standard is PCI DSS (Payment Card Industry Data Security Standard).
- For controls, SOC 2 (Service Organization Control 2) is a strict set of guidelines and requirements around control at a service organization as it relates to security, availability, processing integrity, confidentiality and privacy.
- For privacy, typically pertaining to the healthcare industry, HIPAA (Health Insurance Portability and Accountability Act) is the most common compliance standard and often a requirement to do business.

Businesses that process data that falls under one (or more) of these compliance certifications often face huge one-time costs to assess and meet the governing compliance standard. And while these upfront costs are usually anticipated, many organizations overlook the fact that compliance certifications come with an expiration date and must be renewed—often annually. Ongoing compliance costs can reach hundreds of thousands and even millions of dollars as companies struggle to keep up with ever-changing regulations that require ongoing investments into new technologies and expertise.

The Massive Consequences of Non-Compliance

$440 Million

Target reported a profit drop of $440 million for its 2014 fiscal fourth quarter as a result of a large-scale and highly publicized credit card breach[4]

50

More than 50 class-action lawsuits were filed in less than a month following the data breach of health insurer giant Anthem[5]

Regardless of complexity or cost, businesses are responsible for compliance. There are no excuses and the consequences of non-compliance are massive. An article in Forbes details seven critical consequences[6] for failing PCI DSS compliance:

- Compensation costs
- Federal audits
- Lost revenue
- Legal action
- Remediation costs
- Damaged reputation
- Bank fines

These consequences aren't unique to payment card non-compliance; most apply universally across other types of compliance certifications as well. In fact, more severe punitive damages and punishments could be doled out if an organization is found to be non-compliant with federal regulations such as HIPAA.

Liaison's Continuous Compliance Model Advantage

Every aspect of your operations is impacted by compliance. But you can minimize that impact by choosing an integration provider that is keenly aware of compliance issues. In fact, you can take your integration operations almost entirely out of scope by choosing an integration solution, such as the Liaison ALLOY Platform™, that manages your integration and data management operations on its certified infrastructure. Data, whether in motion or at rest, is secure at all times on the platform and Liaison diligently keeps all certifications up to date.

Taking it a step further, Liaison can help you take the majority of your systems—even those on-premises—out of scope of industry and government compliance standards. This is accomplished through our cloud tokenization solution, which substitutes sensitive data throughout your back-end systems with format preserving tokens.

The following table illustrates how ALLOY, the industry's first Data Platform as a Service (dPaaS), overcomes the limitations associated with other integration approaches.

Integration Approaches	Limitations	ALLOY Advantages
In-house integration	All compliance onus for integration operations is in on the enterprise True cost of ownership is extremely high, guaranteeing expensive ongoing compliance costs Leads to delay and compliance complexity as in-house solutions require three environments: development, test and production Requires expensive integration and compliance experts Does not facilitate real-time data processing; thus, does not cover compliance of data in motion Is not ideal for supporting today's poly-structured information; thus, limited compliance for this type of data	Holistic, data-centric approach to compliance Lower compliance costs as integration operations are taken out of compliance scope Unifies integration and data management disciplines to better handle compliance complexities Provides detailed views into the integration layer to enable better compliance, security, and governance while still allowing for full control and access Provides full visibility into the heuristics of the data flow, helping enterprises mitigate risk Data compliance in all states, whether at rest or in motion Integration provided as managed services, allowing enterprises to leverage our compliance expertise
iPaaS	Although integrations are built from the cloud, iPaaS relies on the enterprise to create its own integrations, thereby placing all compliance onus on the customer Decentralized approach to integration makes centralized compliance oversight more difficult	

[1, 2] Thomson Reuters, Cost of Compliance 2015, May 2015

[3] Gary Glover, SecurityMetrics Blog, How Much Does PCI Compliance Cost?, August 2015

[4] New York Post, Target's profits down $440M after data breach, February 2014

[5] Modern Healthcare, Legal liabilities in recent data breach extend far beyond Anthem, February 2015

[6] Forbes, 7 Critical Consequences Of Failing PCI Compliance, July 2014