

## Compliance Consulting

You can waste a lot of resources complying with regulations—and often, when you’re finally done, you find that while you’ve checked a lot of checkboxes, you haven’t actually improved your security. Instead, proactively meeting regulations can help merge security into the overall security strategy for your business, rather than adding it after the fact. Consultation with an outside expert should be an integral part of your compliance strategy.

If your business falls under multiple regulations and standards, consultation is even more important. It's very costly to approach each requirement separately, but when they're combined, the process can be extremely complex. An Alliance Technologies compliance consultant can help to ensure that the resources spent achieving compliance benefit the business as much as possible.

### Compliance Consulting Areas

Regulation / Standard	Focus
<b>HIPAA/HITECH</b>	All businesses that work with medical or insurance information fall under HIPAA or HITECH rules. These regulations typically focus on, but are not limited to, medical clinics, insurance processors and hospitals.
<b>PCI DSS</b>	Most businesses that accept credit cards must comply with at least some aspects of the PCI Data Security Standard. This standard covers, but is not limited to, retail establishments, restaurants and the hospitality industry.
<b>FTC Red Flag</b>	All businesses that provide services to be billed later must comply with the Red Flag Rules to limit the likelihood of identity theft. This regulation covers, but is not limited to, utilities and service providers.
<b>Sarbanes-Oxley</b>	Public businesses must comply with the Sarbanes-Oxley Act. The act focuses on auditing standards, financial disclosures and documentation. Although it typically only applies to large companies, any publicly traded company is affected.
<b>Gramm-Leach-Bliley</b>	Financial and insurance companies must follow the data handling requirements of the Gramm-Leach-Bliley Act. This act is concerned with financial privacy, data protection and social engineering as they apply to customers of the company.

### Typical Consulting Timeline \*

Activity	Hours	Description
<b>Planning</b>	4–12	Determine the top priorities for the business and compliance, and draft a rough plan for the consulting engagement.
<b>Data Gathering</b>	40–80	Gather documentation needed to identify current business practices, as well as those that are planned for future implementation.
<b>Gap Identification</b>	20–40	Compare data to the “gold standard” in the regulation to identify necessary and recommended areas of improvement.
<b>Project Layout</b>	40–60	Determine what project dependencies and priorities must be addressed to achieve compliance while improving security.
<b>Project Management</b>	10–40 per month	Ensure that projects are properly managed to achieve both security and compliance within a reasonable amount of time.

\* Based on average engagements. Actual times may be higher or lower based on business complexity and size.