

What's Wrong with Compliance?

By
Thomas Witwicki CISSP, CISM, CIPP
Principal, Assurance Point LLC

As a CISO, what do you say when your CEO asks you the infamous question, “Are we secure?” Can you only respond, “Well, we’re in compliance with ABC Regulation and XYZ Industry Standard?” If that’s the only answer you can give, your security program is in need of some attention.

Compliance can be a *driver* of your security efforts, but it cannot be the complete story. Your security program should not be *driven* solely by compliance needs. Compliance cannot replace a security program although it is seductive to listen to its siren call. Your business people say it’s important and thus you have management support and attention. Shouldn’t you therefore be aligned with the business?

But there is also a rather troubling fact that few regulations have an accompanying certification process to actually determine if you are compliant. Even if there is a certification process, it may be based on a rather high level audit that does not include very extensive controls testing. So compliance alone is not a very firm foundation on which to gauge the state of your security.

On the Positive Side

Certainly there are some positive benefits that come with achieving compliance. Compliance with a State or Federal law is not an option – you simply have to do it or your company will face possible fines and civil or possibly criminal penalties. The effort to achieve compliance also brings a project oriented discipline to the security mission that is helpful for motivating staff and comes with a sense of accomplishment and tangible results achieved when the compliance project is completed. I’ve already mentioned budgetary and management support which can help with needed investments in security infrastructure and controls.

Compliance not a Substitute for Risk Management

The real problem with an external compliance driven security program is that the actual information risks in your organization are not being managed adequately. There may be hidden risk that can negatively impact your company and may be neglected or you may not even be aware of. To borrow a turn of phrase from and with my apologies to Bill Blanchard, author of *The One Minute Manager*, “Risk not assessed means squat!” Also, criminals are always a step ahead of any compliance standards in exploiting vulnerabilities for monetary gain.

The steps to risk management are summarized below:

1. Assess the risk to information assets.
2. Mitigate risk through controls to reduce risk.
3. Accept risk according to your policy.

AssurancePointLLC.com
Security • Privacy • Compliance

Phone: 207-272-6976 Email: twitwicki@AssurancePointLLC.com
P.O. Box 2887, South Portland, ME 04116



It is beyond the scope of this paper to fully cover the subject of performing a risk assessment. A useful guide to the process is *NIST Special Publication 800-30*. The key point that I want to make is that risk is made visible and then a deliberate decision is made whether to accept risk or not. Only three possible decisions can be made regarding information risk:

1. Accept the level of risk as assessed.
2. Mitigate to reduce risk to an acceptable level.
3. Stop the business activity which is creating the risk.

Note that risk acceptance is a decision to be made by a business owner and not Information Security. Who in your organization can accept a given level of risk should be documented in your top level information security policy.

Compliance Oriented Controls or Comprehensive Control Framework?

The other problem with a compliance driven approach is that the resulting security controls are usually created specifically for individual compliance requirements. Although this can make it straight forward for a compliance assessor to evaluate your security policies, procedures and standards, in the long run it leads to a set of redundant and overlapping controls which are costly and inefficient to maintain. Most organizations need to maintain compliance with more than one regulation and new security oriented laws and standards, especially concerning privacy, are being passed by legislatures and industry standards groups on a regular basis.

The preferred approach is to adopt a comprehensive “framework” of controls to which you can map your compliance requirements. Some widely used control framework options are ISO/IEC 27002, NIST Special Publication 800-53, and COBIT. The common feature of such control frameworks is that their taxonomy is designed to comprehensively cover all conceivable control objectives. Your organization then determines if a give control objective is applicable based on risk and compliance requirements.

Mapping your controls to a comprehensive frame also enables your organization to perform a baseline assessment of its controls. This baseline assessment produces useful metrics that can be used to communicate the comparative state of your company’s security to your senior management. It can be a very useful tool for determining whether your organizations desired security state is in fact in place and being maintained on a sustainable basis.

In Conclusion

I hope I’ve given you some helpful and perhaps different ways of thinking about compliance. Of course, achieving compliance with laws and standards should be a desired goal of your information security program – it just can’t be the only one.

AssurancePointLLC.com

Security • Privacy • Compliance

Phone: 207-272-6976 Email: twitwicki@AssurancePointLLC.com
P.O. Box 2887, South Portland, ME 04116

