Pratum

First Steps in Compliance Initiatives:
Risk Assessments & Policies

WHITE PAPER

By: Dave Nelson, CISSP
President, Pratum

A NEW WAY OF THINKING

The regulatory environment governing information systems in both the public and private sector has exploded over the past several years. There have been varying responses in the approach each organization has taken in their effort to become "compliant". Many of the differences from organization to organization have been explained by quoting the industry profile or size of an organization. Other times it is the budget or process maturity that has defined their process, or lack thereof. Business leaders need to be challenged with this thought. **Compliance is not a technology problem, it is a business problem.**

So many times we look to technology to solve all of our problems. This goes back to the early days of IT integration into the business process. Back when technology could be applied to most processes and the efficiency gained would be off the charts. There wasn't a lot of thinking or justification needed for those projects. You knew if they came in on time and on (or close to) budget you'd have a winner.

We have moved into a new age though, and our thinking must transition with it. Gone are the days of all technology projects being a plus for the organization. We really need to identify which projects are worth the time, effort and expense.

Compliance is no different. Most of the regulatory environments your organization will fall under, SOX, HIPAA, FISMA, GLBA, etc., are not specific in how you meet the requirements. **However, one thing they do require is a risk assessment.**

UNDERSTANDING YOUR RISK

The underlying principle of each of these regulations is the reduction of risk. **Notice the term "reduction of risk" and not "elimination of risk".** When talking about business you will often hear the phrase "No risk...no reward", right? If you eliminate all of your business risk and can still make tons of money, wouldn't everyone do what you do? Where's the market in that? What we really want to do is reduce our risk to acceptable levels. From a business perspective we do this every day when deciding to open in new markets, launch new products, etc. We weigh the risk to the organization and determine if the risk is worth the reward. In the same vein, if you could reduce your risk significantly with little impact to your operations and budget you'd be crazy not to.

Information security must be approached the same way. Don't put in firewalls, email encryption or costly intrusion detection systems because "everyone else did" or you think you're required to. Assess the inherent risk to your organization without those controls and compare that to the residual risk which would exist after implementing them, and see which one you would rather live with. Why spend $10,000 to replace something that has a value of $1,000? Some things though are harder to quantify, such as reputation. It becomes much more complex to put a price on these items.

THE ROLE OF A RISK ASSESSMENT

Now this isn't a license to be negligent and do nothing, but there's certainly a difference between a $500,000 intrusion prevention system and a $50,000 intrusion detection system. Both might satisfy your compliance needs. Only after doing a risk assessment can you determine the level of risk your organization is willing to accept. **Risk assessments will help your organization build a profile for risk tolerance and help you prioritize your investments in security.**

Many times external consultants are better at leading these discussions as they can bring an objective viewpoint to your process, especially if this is the first time an assessment is being performed. Pick your assessors wisely though, and make sure they want to take the time to understand your company, its culture and how it makes (or loses) money. While there are best practices to follow, a cookie cutter approach will only take you so far.

Once you have your risk assessment completed, the next step is developing policy, procedures and controls to ensure only appropriate risks are taken. Ask any professional in nearly any trade what the secret to creating a repeatable process that works well is and they'll tell you...great policy/procedures/documentation.

POLICY, PROCEDURES AND DOCUMENTATION

Everyone has a technique they think works better than others. It maybe something someone discovered after completing a task multiple times, or possibly even just once. Have you ever wrecked a vehicle? You don't have to repeat it multiple times to learn how to avoid it. Why then do we continually try to reinvent the wheel when it comes to IT and our policy or procedures? We know some things work and others don't, however we never seem to write it down.

How can we expect a process to be followed if we don't have a way to distribute it, train employees to follow it and check up on it? This is where the Love/Hate relationship begins. ***We love to have policy as it helps define our organization***, gives us implementation guidance and sometimes even protects us. This is all fine and dandy when the policy doesn't impact our operations. When it does have a negative impact, either real or perceived, we go ballistic. ***We also typically loathe the process of creating policy.*** It tends to get bogged down in politics way too much, and many times we complicate the process due to one of the following:

1.) We either don't understand what a policy is and what it's used for, or...

2.) We don't want to put in the effort to build an effective framework for use in the future.

Not having a firm grasp on either of these will doom your policy projects. Writing policy is an art form, and new tricks and techniques are continually being developed to improve the process. Here are some points that may help you navigate the murky waters we call policy development.

TIPS FOR IMPROVING YOUR POLICY WRITING PROCESS

- **Policy has to be generic and specific at the same time.** Talk about conflict of interest. You need the policy to be general enough so as leadership, technology, laws and other external forces change, your policy remains valid and does not require significant reworking. The approval process for policy is tedious, time consuming and most importantly, POLITICAL. You want to avoid this whenever possible. So while being as general and non-committal as possible, you need the policy to have some sort of bite. It needs to be clear what the general preferences of the organization are.

- **Policy is only a guide.** It is a statement of fact in which management agrees a specific issue needs to be addressed and generally how they want to see it addressed. It is not a roadmap to remediation, so, don't try to make it one.
- **Policy alone isn't sufficient.** It takes a full set of documentation to manage risks and have any reasonable assurance of information security and privacy. Here are the 4 basic types of documentation you need.

  Policy – General accepted principals of an organization.

  Baselines – Standard accepted configuration for hardware and software. Deviations require risk assessment and management approval before being implemented.

  Procedures – Set of detailed instructions for how to implement security controls, manage changes, identify risks and remediate gaps.

  Guidelines – When no specific instruction is given, use these "common sense" principles as a guide.

- **Policy should identify responsibility and authority.** If everyone has input into every baseline or procedure that is created, you'll paralyze your organization. Policy should state who is responsible for implementing each section and what authority they have. In this mode, the server group may be responsible for creating the baseline for server hardware or OS configurations, but the application group gets to review it prior to being published in order to ensure their needs are met as well. Each organization will implement this a little differently, however the main idea is to limit the number of people who have to sign off. Don't leave out true stakeholders but don't give groups outside of the process too much weight in the decision.
- **Train your users.** Telling them a policy exists, find it…follow it…simply isn't enough. It shows a certain callousness on the part of the employer and more importantly would not hold up in court if your policy is challenged for any reason. If the policy is really that important to your organization then provide some training.
- **Review policy on a regular and frequent basis.** For corporate level policy, annual reviews should suffice. For baselines or procedures, quarterly might be better. Whatever schedule you choose, document this in your policy and follow it. Not reviewing policy can be as bad as not having one at all.

Following some of these simple guidelines will help you have some assurance of the confidentiality, integrity and availability of your critical data and systems. **Well documented policy and procedures used in conjunction with a risk based approach to information security will put your organization on the right track toward your compliance initiatives.**