POLICY MANAGEMENT:
THE UNSEXY SIDE OF IT SECURITY

By Todd Nielsen

I'd venture to say that most CIOs and executives I know would prefer getting a root canal over writing and managing IT polices. Good policy management is the kind of strategy that often gets overlooked and ignored when it comes to information technology and security. In the financial services industry, it is not enough to have strong IT security controls; auditors and regulations are now requiring organizations to prove they have policies (and procedures) around security and privacy, as well as the use and confidentiality of customer information.

In such a regulated industry, strong security controls coupled with strong policies provide tangible results that are definitely sexy and very desirable. Here are four sexy benefits of policy management:

1. Increased Regulatory Compliance

There are so many aspects to financial and security audits. Having been through a SOC II Type 2 audit at JMARK, as well assisting our clients with thousands of bank audits, it is clear that audits are getting more and more complex and frequent. It is not enough to have a control in place; you also have to have the policy around the control, and often show proof that employees have acknowledged the policy.

Image © NicoElNino/iStock

A great policy management program helps to solidify controls because the act of writing the policy helps to identify weaknesses in operational controls that can be corrected to improve regulatory compliance requirements.

2. Reduced Risk Mitigation and Legal Expenditures

Policy management is not just creating a policy and putting it in a binder for new employees to read. Policy management entails writing a policy, verifying the policy meets regulatory and organizational requirements, implementing controls to enforce the policy, and then training all relevant employees on the policies. After that, there is ongoing reevaluation of polices and controls, and then constant retraining. This entire process helps to reduce risk by identifying needs, establishing guidelines (the policies), refining the controls, implementing improvements and training everyone on the policies. In a recent survey, more than 63 percent of organizations believe their policy management program reduces legal costs and the time it takes to resolve regulatory issues and fines.

3. Improved Employee Knowledge and Acknowledgment

A great policy management program ensures that every employee reads and acknowledges the policies as soon as possible after a change or addition has been made. This provides opportunities for employees to ask questions so they can truly understand what is being expected of them. It improves accountability as well because you will have a date and time when that policy was acknowledged, if there are questions or issues regarding individual employee compliance. All of this also improves knowledge throughout the organization and provides tracking and proof for auditors.

4. Solid Consistency and Centralization

A great policy management program will be centralized and consistent. What often happens in organizations is document and policy silos occur in different areas that often create conflicts with corporate policies and regulatory compliance. Without a centralized system, policies become inconsistent and distributed, which leads to compliance risks and poor operational controls.

The Challenges of Implementing a Policy Management Program:

At JMARK, we have seen many organizations struggle to implement a policy management program, which is why we ended up developing one to help our banking and financial services clients. The pitfalls we have seen organizations struggle with include:

- Lack of knowledge in translating regulations to policies. Let's face it; the regulations' world is often confusing and frustrating. Here are just a few of the regulations that someone needs to understand, in order to put in place a good policy management program for financial institutions:
  - The Bank Secrecy Act.
  - Sarbanes–Oxley Act.
  - Anti-Money Laundering.
  - Dodd-Frank Wall Street Reform and Consumer Protection Act.
  - Cybersecurity Act.
  - Health Insurance Portability and Accountability Act (HIPAA).
  - And more, plus they are always changing.
- Lack of copywriting skills by those that do have the knowledge. Writing is not something everyone can do, even though almost everyone claims they can. Regulations have to be interpreted into policies, in a format and style that makes them understandable to the employees who have to comply with the policies. If the policies are not easy to understand, employees will not comply with what they do not understand.
- Too many choices over the format and software to use. There are a lot of options out there that can bring an onset of paralysis analysis, along with constant double guessing on what is needed for compliance and regulations. There are many ways to do this. The important thing is to keep it simple and automated as much as possible. Audit trails must be kept and it can't be laborious to do so. Hence the importance of simplicity and automation.

Policy management is already a critical and necessary component of compliance in banking institutions. If your policy management program is lackluster, it's time to turn that around in order to meet increasing demands in security and compliance regulations. To get an idea of the kind of scale that exists in policy management for financial institutions, shoot me an email at tnielsen@jmark.com and I'll send you a large list of IT security and regulation related policies that you likely should have in place at your banking institution. Implementing a policy management program is not easy, but doing so will result in some real sexy benefits. ■

Todd Nielsen is an executive, writer and speaker. He currently leads strategy execution initiatives as chief strategy officer of JMARK Business Solutions, Inc. His almost 20 years of diverse experience — dealing with rapidly changing markets and technologies has made him a strong leader and business advisor. He can be reached at tnielsen@jmark.com