Transcript: Five Steps to Effective Policy Implementation

Slide 1

Welcome to this short video on policy implementation. Stay tuned for about seven minutes, and I'll share what in my experience enables successful policy implementation and compliance.

Slide 2

Before looking at policy implementation, let's review all the related areas.

First, Policy is the foundation of security efforts. Each policy states what security objectives management wants to achieve. It states what needs to be accomplished, not how.

Policies are supported by standards, baselines, guidelines, and procedures. They are created or adjusted to ensure the policy objectives are met. Standards are required steps or controls that IT and other areas of the business must follow. A baseline is the minimum security a system, or device within a system, must meet. This is usually based on information provided by standards of best practice and vendors. Baselines commonly differ between systems, depending on the sensitivity of the data they process, store, or transport.

Guidelines are recommendations for security controls and procedures. Procedures are step-by-step approaches to completing IT and business tasks. Procedures should be designed to ensure all employees achieve both business and security objectives.

Governance is the development of policy to achieve outcomes commensurate with reasonable and appropriate risk management and regulatory compliance. Governance also includes monitoring and oversight (e.g. auditing) to ensure management's policy expectations are met. Even if the data goes into the cloud, no organization can relinquish its responsibility for governance to protect the data it collects and processes, regardless of where it resides.

Governance is one part of the GRC triad: governance, risk management, and compliance.

Slide 3

Policies are the basis of security, but they are often not properly implemented. It takes more than distribution and training to ensure compliance. We should consider the reasonable and appropriate attention to specific tasks. These tasks help to inform affected employees about additions or changes to what is or is not acceptable; to integrate changes into how we implement information management and delivery solutions; and to manage results.

Slide 4

The five steps we cover in this video include providing policy access, training, reviewing and changing our baselines and requirements, and ensuring that governance processes include the new policy objectives.

Slide 5

A general announcement that a new policy is available, and its general impact, is necessary to bring attention to potential needed changes in information projects and employee behavior.

Distribution of the policy to managers and supervisors begins with the process of discussing the impact of the policy on business operation. The announcement and distribution of the policy should precede the date the policy takes effect by about 30 days, if possible. This provides sufficient time to acclimate management and users to upcoming changes.

The policy should be posted where it is easily accessible by all employees. Managers and supervisors should be able to refer to it at will. In addition, access to information about the policy owner is important. If an employee has a question, or someone wants to report serious challenges to achieving compliance, they should be able to easily contact the person or team responsible.

Slide 6

The organization should create lesson plans for training relevant to management, business users, and IT. In many cases, the policy affects each of these groups differently.

Managers need to understand the affect the policy on business operation. They must be able to discuss the policy with employees, answer questions, and integrate necessary changes into day-to-day activities. Management training should include suggestions on how to provide oversight to ensure user compliance.

Business users are provided with a general look at how the policy affects them and how they use information resources. Since relying on user behavior is a control of last resort, user training should focus on the gaps left by implementation of automated controls. This includes changes made by their managers and supervisors to business procedures.

IT personnel need basic business user training supplemented with how the policy might affect the design, development, implementation, and management of new and existing systems, networks, and network devices.

Slide 7

IT and security should review standards and guidelines to ensure current standards, baselines, and guidelines will achieve compliance. This is done by referring policy outcomes to the organization's adopted standard of best practice. If changes are needed to standards, baselines, and guidelines, a review of all relevant systems, network devices, and user devices is necessary to ensure changes, or new standards or guidelines, are integrated into them.

Slide 8

Again, training received by the IT team should be followed by a review of system, device, network device, and network segment standards and guidelines. Changes to these must also be reflected in relevant build documents. Build document changes are completed in parallel with creating an action plan to make necessary changes to existing builds or builds in progress to ensure policy compliance.

Slide 9

Finally, management must take steps to ensure the policy objectives are consistently achieved. Governance requires integration of the new policy objectives into internal and external audits as well as daily management review reports. Security should demonstrate to management daily processes that ensure compliance, including inclusion in change management procedures and security monitoring.

Slide 10

If you have questions or comments about the content, you can reach me at tom.olzak@erudiosecurity.com.