Understanding the Impact of Policies on your IT Organization

By Harris Kern's Enterprise Computing Institute

This article outlines a simple plan of action to help you identify and understand key policies that can have a substantial impact on your IT organization. Along with other important domains like technologies, facilities, and processes, policies capture key elements of your IT organization – elements that must be well planned and well deployed in order to provide cost effective IT services. Because they define the minimum requirements for key technologies and processes, knowledge of policies is essential. As such, this article outlines some steps to help you identify important polices and related elements that affect the way you manage your IT organization.

Step 1: Identify key management policies

First you need to identify management policies. These are the internal guidelines and mandates placed on your IT organization by management and other areas of the business. They are the business rules under which the IT organization operates.

Covering a wide scope, management polices are key links between the IT organization and other business functions. In this way they provide a common basis to align IT with the rest of the business. Management policies affect many aspects of your IT operations. They determine the way you implement key processes and technologies, so you must ensure they are factored into your IT strategies and plans.

Human resource policies are an important example. Efficient and effective business operations depend on staff. Because information security depends greatly on the behavior and actions of staff, human resource policies play a key role here. This means their are often many linkages between human resource polices and security policies. This often starts with hiring new staff, managing security incidents and terminating staff.

For example, Human Resources and IT follow common procedures to identify sensitive positions and qualified staff. Sounds simple, but this is not an effective process in many companies. It is neither well defined nor executed. IT needs to clearly identify sensitive positions and special qualifications, while Human Resources needs to set guidelines for background checks. There also needs to be an effective process for IT to promptly communicate information about security incidents so Human Resources can take appropriate actions. There are major security concerns in most IT organizations and they have a major impact on the way incident response procedures are deployed.

The IT organization is affected by other management policies too. These include policies related to privacy, procurement, shipment and receiving, asset management, document control, data retention and archival, accounting, and auditing, among others. Asset management is a well-known issue. With the proliferation of personal computers and networks, managing hardware and software is a major concern in many IT organizations.

Asset polices set guidelines for IT procedures like asset tracking procedures, licensing procedures and technology life cycles, as well as technologies like inventory management systems and desktop management applications

Also with more attention given to privacy, the company's privacy policies set important guidelines for key security technologies like firewalls, Virtual Private Networks and encryption, which are protections mechanisms for confidentiality. Privacy polices l set criteria to evaluate these technologies, and the way they are implemented and managed.

Step 2: Identify external policies

External policies are the all the policies, regulations, rules and laws that provide guidelines and set constraints on the company and your IT organization. These come from governmental or quasi-governmental entities, equipment suppliers, communications carriers, foreign agencies and others.

The key objective here is to identify the external policies and regulations that have the greatest impact on your IT organization, and factor these into your IT strategies and plans. For example, the healthcare industry must follow HIPAA guidelines. The financial industry must follow the privacy requirements outlined in the Gramm-Leach-Bliley Act. To comply, IT organizations must make major enhancements to their security architectures and processes.

Then there are the European Union's special privacy policies. The Directive on Data Protection prohibits electronic transfer of personal information about European citizens to countries where privacy protection laws are *inadequate*. From the European Union's perspective the United States' privacy laws are not adequate. If your company has European operations your IT organization will be affected. While there are special agreements between the European Unions and the United States, you must ensure there are sufficient provisions in your security architectures to protect confidentiality, integrity and availability of personal and information now and be ready to implement new provisions in the future. It all depends on the policies.

Also if you company's network spans international boundaries, you need to understand the telecommunication policies in different countries. This can be challenging, particularly in countries where telecommunications is closely regulated, or entirely controlled, by the government. This will have a major impact on costs and network architectures, network operations and problem management procedures.

Step 3: Identify IT policies

Ideally, management and external policies drive IT polices. These are all the policies that all are the company's internal guidelines that govern IT operations and the use of information resources. Security and acceptable use policies are two of the most prominent examples. With the objective of ensuring confidentiality, integrity and availability, security policies set guidelines and requirements that affect all technology architectures including applications, databases, networks and servers. They also influence incident detection and response procedures.

Acceptable use policies are intended for all users of IT services and describe internal guidelines to prevent unauthorized use and misuse of information and IT resources. They typically cover the use of e-mail, and computer and network resources. Their objective is to ensure that information technology resources are used appropriately, efficiently and effectively and have an impact on the way your IT organization monitors its information resources.

There are other IT policies to consider too - anti-virus policies, backup policies, network addressing standards, incident reporting policies, PDA policies, and many more. All of these have to be factored into your IT management plans.

Step 4: Evaluate the impact

We have already examined the impact of policies on your IT organization. You need to formalized this step and evaluate policies and determine the minimum requirements they establish for key technologies and processes:

Technology architectures - Policies set key guidelines, requirements, and constraints for technology architectures. For example, security policies establish guidelines for physical and logical access. As such they define key requirements for authentication, authorization and access control technologies. These may include strong authentication systems, firewalls, encryption and Virtual Private networks. The same applies to other security controls such as physical access. You need to ensure that physical access policies are factored into your data center facilities design. External telecommunications policies will define important constraints that affect your network architectures and the technologies you use.

Processes and procedures – Polices are the key drivers for IT processes and procedures. They define key objectives and process flows. They also set important criteria for service levels, metrics and reporting. Well-deployed processes and reporting procedures must be in place to ensure compliance with policies and regulations. They affect change management, problem management, help desk management, backup management, release management, and many others. For example, backup policies define how often backup are taken and how long data is retained. Problem management policies define how priorities are assignment to problems, how problems are escalated and whom they are assigned to. Change management policies define the key elements of how change requests are initiated, evaluated and implemented in a controlled way.

Organization and staffing – Policies establishes key roles and responsibilities. Also, in order to comply with policies and regulations you may need to create new positions, or partition sensitive tasks between two or more groups or staff. To manage an effective IT organization it is critical to understand how the key roles and responsibilities established in different policies will affect your organizational structures, and plans for staffing and training.

Cost – Finally you need to evaluate how policies affect costs. In some cases, complying with policies is not feasible. Take the case of the European Union privacy policies. For United

States companies, the cost of complying is prohibitive. However, the costs of not engaging in business is even higher, so special agreements have been made.

Summary

You must understand IT policies manage a cost-effective IT organization. They establish the basic guidelines and constraints for your technology and IT processes. If key staff in your IT organization are not aware of these policies and understand their impact, there will be major disconnects with the rest of the business.