IS audit basics

The Auditors, IS/IT Policies and Compliance

Do you have something to say about this article?
Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

Every organization tries to formalize aspects of its culture through policies. These policies define what is expected of members of the workforce and describe how noncompliance is dealt with.

A compilation of policies is usually issued in the form of an employee handbook and/or is posted on an intranet. Keeping the policies updated and ensuring everyone who needs to know is aware of the changes grows in complexity with the number of people and their locations.

Making sure the workforce understands their purpose and agrees to comply with policies is not easy either. Noncompliance may require management, human resources (HR), legal and the auditors to get involved. If this is not the case, perhaps the policy in question has little value.

Ed Gelbstein, Ph.D., 1940-2015
Worked in IS/IT in the private and public sectors in various countries for more than 50 years. Gelbstein did analog and digital development in the 1960s, incorporated digital computers in the control systems for continuous process in the late '60s and early '70s, and managed projects of increasing size and complexity until the early 1990s. In the '90s, he became an executive at the preprivatized British Railways and then the United Nations global computing and data communications provider. Following his (semi)retirement from the UN, he joined the audit teams of the UN Board of Auditors and the French National Audit Office. Thanks to his generous spirit and prolific writing, his column will continue to be published in the *ISACA® Journal* posthumously.

The Policy Portfolio

Policy portfolios may differ from one organization to another to reflect their specific needs. For example, policy portfolios will differ depending on the areas where compliance with legislation is mandatory. Also, each organization has its own policies on general employment matters such as the consumption of intoxicating substances, "fraud, impropriety and extravagance," code of conduct (including bullying, harassment and violence), and conflict of interest. This article examines policy issues concerning information systems, services and data (SSD), such as:

- Nondisclosure of company information
- Data protection
- Personal use of the company's information resources
- Use of social media
- Bring your own device (BYOD)
- Information security

There are many other areas where policies may be desirable, but the portfolio should contain only those that have clear purpose and value. Having too many policies can be difficult for the workforce to absorb. Besides, policies that conflict with the organizational culture may lead to the loss of management credibility and demoralize the workforce to the point of disengagement.

Auditors' Focus #1
Assess the scope of policies issued and review their key parameters. These should include:

- Whether there are policy guidelines defining requirements such as readability and understandability, use of version control, need (or not) for the acknowledgment of each policy by individuals, etc.
- Extent of the portfolio against assessed risk impacting the availability, confidentiality and integrity of SSD, and identification of other topics that would merit a policy

- Currency of the policy (i.e., when it was last reviewed and possible need for updating it)
- Dissemination (on paper requiring acknowledgment, on paper without acknowledgment, self-service intranet site. In the latter case, review its usability and access statistics.)
- Mechanisms for monitoring compliance

There are many examples of poor policy development collected by the author over the years. The following one was "missed" by the information systems auditors.

A chief information officer (CIO) drafted a two-page policy on appropriate use of corporate resources that addressed issues clearly and concisely. It used terms such as "forbidden" and "right to monitor" and stated that noncompliance would lead to sanctions.

As the CIO had no authority to issue this draft, the HR function was asked to review it. Several months later, it emerged as a four-page document cross-referenced to other policies and personnel rules.

At this point, HR invited staff representatives to review it. Their response, offered some months later, objected to the use of "forbidden" and other terms considered too restrictive. "Forbidden" was changed to "limited personal use" (leaving "limited" undefined).

This was then sent to legal counsel. Their review took several months and resulted in a nearly incomprehensible 11-page document written in legal jargon with many clauses, subclauses and footnotes.

A year after the first draft was produced, the policy was printed and distributed together with a bundle of assorted circulars and administrative trivia. Employees were not required to acknowledge receipt. During a subsequent independent audit, few were able to produce their copy and many claimed they "never got it." This policy was also not part of the documentation issued to new recruits.

Human Nature

Auditors' Focus #2
Assess the extent of the commitment to comply with policies and the degree to which this is recorded in individual personnel records.

> **"Whenever the workforce regards policies as restrictions that make little or no sense, they will be ignored if they are not enforced by systems."**

Whenever the workforce regards policies as restrictions that make little or no sense (because they really make no sense or because they require guesswork to interpret them), they will be ignored if they are not enforced by systems (e.g., forcing a password change every month). Even when enforced, people may look for (and find) a workaround.

The assumption that policies are matters of common sense is questionable. A quotation attributed to Albert Einstein states, "Only two things are infinite, the universe and human stupidity, and I'm not sure about the former."[1]

During an audit a few years ago, an auditor came across the emergency exit shown in **figure 1**. The obstruction had been there for some time and was too heavy to be moved by one person. The notice on the left of the door was noted and ignored.

In any case, it is not unusual to find a cleaner's bucket propping open a secure door, passwords

being shared, online trading being conducted or computer games being battled during working hours.

Figure 1—Blocked Emergency Exit

Source: E. Gelbstein. Reprinted with permission.

Mixed signals from the top do not help. "Executive exceptions" demonstrate that policies for the workforce do not apply to the executive ranks (e.g., government employees using their private email for official purposes rather than the corporate, more secure, system).

Those well versed in organizational politics will remember Grace Hopper's quote—"It is often easier to ask for forgiveness than to ask for permission"[2]—which makes compliance even more of a challenge.

Compliance With Internal IS/IT Policies

Auditors' Focus #3
Assess the extent to which policies are monitored and with which they are complied.

Human history tells us much about noncompliance. For example, there are Hammurabi's Code of Babylonian law (~1700 BCE), the Ten Commandments, other codes of conduct and a huge volume of legislation. It is also true that law enforcement, courts of law and prisons are unable to meet demand, suggesting that noncompliance may be a fact of human behavior.

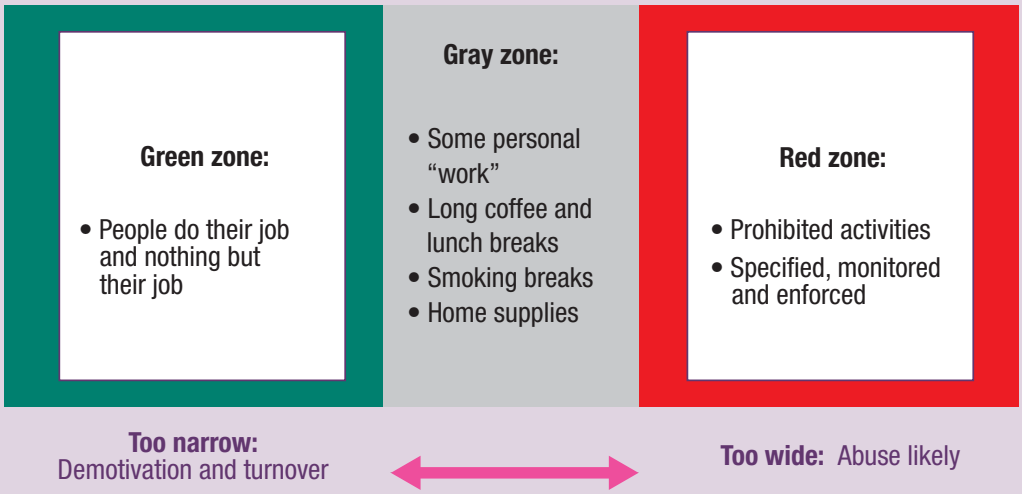
This leads us to the "zero tolerance" that some organizations target, with variable success, as enforcement creates martyrs and can reap undesirable media attention. A balanced approach to policies could consider three domains as shown in **figure 2**.

The gray zone recognizes human imperfections and needs (Is it okay to take home a box of paper clips or a few pencils? And a laptop? Where should the line be drawn?). The red zone should have few policies to avoid it becoming a straightjacket and a demotivator. The rise of the mobile worker and BYOD creates new challenges to what can be monitored and enforced. Senior management, the CIO, risk managers and auditors should consider these limits and address them to reflect the organization's specific culture and needs.

Machiavelli, the 16th century management consultant, stated that for those in authority, "…(there is) greater security in being feared than in being loved," followed by "…love is secured by a bond of gratitude which men, wretched creatures that they are, break when it is to their advantage to do so; but fear is strengthened by a dread of punishment which is always effective."[3]

Auditors' focus #4
Determine the extent to which the organization tracks innovative technologies that could have an impact on the organization and introduce new risk. Use this information to identify the potential consequences of adopting these technologies before adequately thinking about associated controls that are reflected in policies.

Figure 2—The Three Zones of Compliance Requirements



Source: E. Gelbstein. Reprinted with permission.

Conclusions

Good policies should reflect the concept of the perennial favorite of stylish women, the "little black dress": elegance, versatility and simplicity. This is rarely the case in policies, and some employee manuals can be as big as a small-town telephone directory and just as readable.

> **"The rise of the mobile worker and BYOD creates new challenges to what can be monitored and enforced."**

Having policies may be a mandatory requirement (e.g., to gain certification to the International Organization for Standardization [ISO] 27001), but this, while necessary, is not sufficient to ensure compliance.

Auditors should encourage and support those issuing policies by making them aware of these issues and subsequently following up on the actions taken.

Endnotes

1 Brainy Quotes, Albert Einstein Quotes, *www.brainyquote.com/quotes/quotes/a/alberteins100015.html*
2 Brainy Quote, Grace Hopper Quotes, *www.brainyquote.com/quotes/quotes/g/gracehoppe170166.html*
3 Machiavelli, N.; *The Prince*, 1513, chapter XVII