READ ME

Streamlining your organization's IT policies and procedures is long overdue. BY KAREN CHAMBERLAIN

Today's employees are asked to do more tasks in less time than ever before. Software is continually changing to meet these demands, addressing bottlenecks and freeing companies to focus on their core competencies.

And then there are IT policies. We've figured out how to take most of those binders of paper policies and digitize them, and even how to slice and deliver them electronically to employees in smaller, more targeted packages. But in the process we haven't figured out how to reduce their size or number; in fact, we probably have added more policies to keep up with the growing number of regulations with which companies are required to comply.

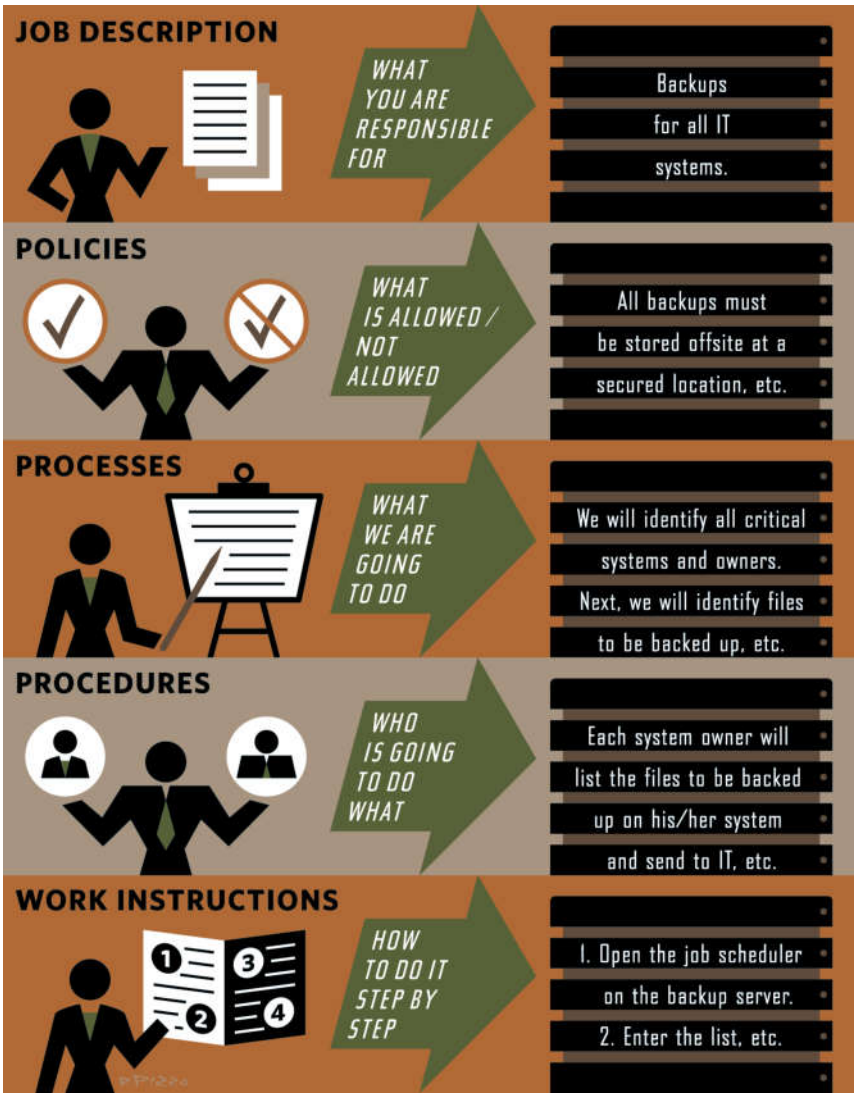

FIGURE 1 *(right)* outlines considerations for different elements of policymaking.

ILLUSTRATION BY ROBERT PIZZO

Like laws, you don't want your employees to learn about policies by violating them. So how do you go about getting them to your employees when they need them? And how do you train on them in a way that sticks?

RETHINK YOUR DEFINITION

In the past 15 or so years, I have become very good at policy writing. This is because, as soon as people figured out that I was able to write *one* IT policy, it became my job to write *all* of the IT policies.

It can be difficult to know where to start, especially if you are new to policy writing or if an auditor or manager is waiting for you to finish writing something new. The process of policy writing might be easier if your company has a template to use; however, the next step—whether you use a template or create one—is still to get the policy to your authorized users.

We don't write detailed policies for them to be read and then collect dust. Or worse, to collect dust without being read in the first place. Ideally, we want those policies in front of our employees every day, where they have ready access to them. The big question is: Who needs to know what and when?

First, we need to sweep away our preconceived notions about what a "policy" looks like. In the past, we detailed out the types of *documents* that we needed.

Please keep in mind: the "policy" is actually not a document; rather, the "policy" is what we are allowed or not allowed to do in a given company. Once we focus on the actual rules and requirements instead of the documents themselves, we can begin to define the who, what and when.

Fortunately for today's IT policy writers, there are several frameworks and standards (such as ISO27k, COBIT, NIST, PCI, HIPAA and GLBA) that can assist with identifying the policies that an organization needs to have in place. It is not a requirement that policy writers read through all available frameworks and standards; however, as a policy writer you should at least be familiar enough with them to know how they apply, if at all, to your organization.

Start by listing high-level policy requirements and the regulations they address, whether internal or external. This can simply be "the building and designated areas must be secured from unauthorized entry" or "all sensitive data must be protected." Here's where a read-through of the frameworks and standards can be most helpful.

THINK ABOUT YOUR AUDIENCE

Define your audience before writing (or revising) your policies. Each of the document types in Figure 1 *(p. 25)* are generally for different audiences. For example, a Process document is typically written for management, auditors and others who need to see the "big picture" of what is to be accomplished. The audience for a Work Instructions document is the worker whose job it is to perform the task. While the audience for the Process document probably cares about a "Purpose" section, this section is redundant for Work Instructions.

> **You don't want to leave it up to the reader to make inferences as to what parts of a policy, or which policies, apply to them.**

Providing clarity and direction to the employees is crucial in a policy document. A "one-size-fits-all" approach can be confusing, while many different versions of the same document can be just as confusing and costly. You don't want to leave it up to the reader to make inferences as to what parts of a policy, or which policies, apply to them. Rather, try using a table to identify the part(s) of the policy, procedure, etc., relevant to each type of audience.

For example, a decision matrix on when to use the change management procedure could include network scenarios, application scenarios, telecom scenarios, etc. Each of these audiences would use the same change management procedure for their own scenarios described within the matrix.

STREAMLINING YOUR POLICIES AND PROCEDURES

If you have both policies and procedural or work instruction documents, consider combining them and adding interactive documents such as forms. Your change management form could be created in your HelpDesk system as a template with a sequence of steps with user input. In the headings or descriptions for each step, the policy requirements could be added, such as: "Approval Signature: You must have this change approved by your manager before you move on to the next step."

If you can add all of your policy requirements to the form, your change management policy, procedure and work instructions could amount to one decision matrix and one

HOW TO...

Even if you don't adopt this methodology, the example below might get you thinking about how you can improve upon your own policies.

SITUATION A company has a 10-page PLC (SDLC) policy that details the phases and expectations for three types of projects: small, medium and large. A separate PLC procedural document is six pages. Templates, mostly in Word, exist for each of the deliverable documents. For each project, folders are created on an intranet site, and deliverables are placed in the appropriate folders. Some templates are not needed and therefore missing for some projects. A project plan is maintained in MS Project.

POSSIBLE SOLUTION

Create a new Excel workbook. On the third tab, first column, enter the project phases, one per row. In the second column, enter the procedural steps for a small project for each phase (all steps in one cell). In the third column, enter the deliverables needed for each phase (*can denote mandatory). In the fourth column, enter the alternate options and/or notes. Repeat for medium and large projects, each on their own tab (fourth and fifth tabs). Discard existing PLC procedural document.

On the sixth tab, place the first template. On the seventh tab, place the second template, etc. Repeat until each template is on its own tab. Remove sections such as Purpose, Objectives, etc. and keep only the fields that are required to be completed for the project. Give policy and other guidance on required fields. Auto-populate similar fields on multiple tabs. Discard all separate template documents.

Review the PLC policy document and add those policy elements to the second tab that are not defined already on any of the other tabs. You may include references to other tabs if necessary, but your policy should only be a few paragraphs at most. Add new requirements for new projects to use the workbook, retaining either the third, fourth or fifth tab, whichever is appropriate, and requiring "N/A" at the top of any template not required.

Add a legend to the first tab. Rename all tabs. Remove the requirement for multiple folders for the project—you will have only a project plan, the Excel workbook, approval emails and testing evidence to post on the intranet site. The project manager will be able to review the workbook to assist with assessing progress for the project plan. ■

form in total. If that form is included inside a HelpDesk ticket, the testing evidence, approvals, etc., could also be captured on the ticket (or attached) as well.

FINAL WORD ABOUT TRAINING

One of the things that drives process improvement is a user's natural inclination to question why things are set up and carried out the way they are. Regular training is the perfect opportunity to provide a background and purpose for your policies, procedures, etc., especially if they are combined. For successful training sessions, consider the following recommendations:

- Schedule training sessions multiple times a year to accommodate changes and new users.
- Make your training sessions interactive with a live trainer. Use the internet for remote sessions. A live trainer can give more detail, take questions, explain why some alternate solutions did not work and increase buy-in.
- Provide lunch. Most users have full schedules but can sit for an hour of training at lunchtime and would rather have lunch with you than read extra pages of explanation in a document. This also shows that you are willing to work around participants' schedules.
- Create fake situations with real people. Calling people out on mistakes or putting them on the spot to answer questions about something they just learned can create a negative impression. Assigning a participant to be in a pretend situation to illustrate a point can heighten understanding and increase retention of the material.
- Ask participants how you can improve. Tell them, we put this part of the policy here because we want you to know *this* whenever you do *that*. Ask them, is our strategy working?

Not every policy, procedure, etc. will be a candidate for consolidation, such as policies designed for specific audiences or regulations. However, if you take the time to tailor your documents toward your audience's usage requirements, you'll not only make it easier on them, but on you as the writer as well. ■

KAREN CHAMBERLAIN, *CISSP, has written and reviewed IT policies for 15 years. Her first experience with policy writing came while working at a company trying to become ISO 9000-compliant.*