How To Avoid Compliance With IT Policies:
10 Real-World Tips For Non-Conformists

Regulations – who likes them? Not innovators, nor power-brokers, nor managers behind schedule on a critical deadline. Whether imposed by the government and enforced through legal sanctions, or concocted by bureaucrats within an organization and monitored through quality assurance audits, they're bound to get in an IT executive's way sooner or later. Who isn't nostalgic for the good old days of laissez-faire technology when a DOS C> prompt and a dream could make a talented developer and his company rich?

I'm joking, of course. Sort of. Actually I am paraphrasing the mindset of many IT managers I have worked with over the past decade. I'm a business anthropologist who often leads transformative organizational projects, re-engineering workflows and processes when new regulations demand that people change their customary behaviors. Following the 2008 worldwide economic meltdown, the financial services industry has experienced a major outbreak of new regulations affecting IT systems. But they are not alone. Health care, energy, education…the growth of on-line communication and digital interconnectivity has created new risks to be monitored and mitigated in every sector.

Sometimes a new regulation is obviously a good idea, because it addresses damage that has already been done and aims to prevent a recurrence. Few would protest safeguards designed to protect information systems from hacker attacks, malware, or data theft. Rules whose purpose is to improve end-to-end reliability also make sense to most technologists.

The regulations that cause chronic heartburn and passive-aggressive mutiny among IT managers are those generated by models of transactions among a system's users, the checklist determining which category of user is allowed to do what, where, when, and how. (In the world of finance, for example, the most common rules stipulate separation of duties – one person enters a transaction and another person approves it, so that there are always two separate individuals witnessing any movement of money.)

Why should this be so? For one thing, it has become increasingly rare for the people who write the code to have any direct experience of the end-users' work processes and environment. Back in the days of standalone PC/Mac yore, many information systems were first created by "power users" who knew exactly what they and their colleagues needed. Today it is not unusual for the user, business analyst, developer, tester, and instructional designer for the training materials to be located on different continents, speak different native languages, and have different educational backgrounds. This situation provides a wealth of opportunities for ongoing confusion and endless refactoring.

Also, the user transaction model changes far more often than security or reliability rules. It might happen when a legislative committee overturns a decision made by an administrative agency. Or when a corporate acquisition or divestiture adds or subtracts user types. Or when the marketing department decides to give special privileges to a certain class of users. Or all of the above, all the time. Eventually the systems architects may come to suspect that their once-elegant design has morphed into a Rube Goldberg-style contraption, and the coders to regard the business analyst or product manager in the way an exhausted parent trying to serve dinner feels toward a child who is a very picky eater.

In the beginning, as I first became involved with such projects, I assumed that the IT managers I encountered were beleaguered, defensive, and cynical (because in fact they were) but the regulators who invented the rules were zealous, righteous, and idealistic. This illusion persisted for several years until I found myself at on a client's project team with an executive who had switched sides: she had once been an inspector at a regulatory agency, and now she worked for the regulated company managing compliance. According to her, many of the bloodhounds were just as alienated as the foxes they pursued.

"Here's how it goes," she told me. "When the regulators come in to a company to perform an inspection, first we look for signs of intelligent life among senior management. Next we state the obvious to them. Then we shoot the wounded. After that we tell the naughty boys and girls what they need to do to make it look like they are behaving properly. We listen to a lot of promises nobody believes, we agree on a date for the next ritual, and we leave."

Let's say you are an IT executive who is quite fed up with the exorbitant amount of time and resources it takes to follow ever-changing rules. Your staff would work more effectively, your product would be more marketable, and your division would earn more revenue if only you had a little more…wiggle room. If you are lucky, the regulator or auditor assigned to inspect your domain will be like the character I described. Regrettably, not all of them are so flexible or empathic.

The most important point to remember is not that you should comply with the rules, but that you must be *seen to be* in compliance. To accomplish this goal, you must have a lot of documented IT policies. However, to give yourself that essential wiggle room, the policies must be drafted and communicated in such a manner that nobody understands them, and adherence to them cannot be easily measured or even verified.

Does this sound like a tough challenge? True, it is not easy. Yet over the years I have worked with some of the most talented compliance-dodgers in the capitalist realm, and as a public service I hereby present some of their best practices.

1. Do not distinguish between a policy, a procedure, and a standard. A policy is an abstract statement of principle. A procedure is a list of actions to be performed by a human being or machine in order to turn that abstract principle into a tangible reality. A standard describes a condition that can be verified or a level that can be measured to determine if the procedure has succeeded. For example, an organization might create a policy such as: "We support telecommuting as a means of making our staff more productive." Procedures might include logistics for VPN access, protocol for teleconferences, instructions for time tracking. The standards would establish qualitative and quantitative criteria proving whether or not telecommuters were adequately productive. However, unless you are a philosopher these fine distinctions are blurry and not really important.

2. Encourage each business unit and infrastructure owner to draft their own policies, procedures, and standards using technical terminology that the specialists clearly understand. Limit the participation of professional writers, editors, taxonomists, or risk managers. Attempts to establish a common language across the organization and develop a consensus about acceptable levels of risk are a waste of time because this sort of collaboration has no impact on anyone's personal bonus or performance evaluation.

3. Resist the urge to centralize the storage of policy documents, because the budget necessary for the hardware, software, and labor will become a political hot potato. Each group responsible for creating IT policies should be empowered to choose the location and format of its contributions. Methods of version control should also be left to their discretion.

4. Allow the list of IT policies to grow organically. When someone creates a new policy, procedure, or standard, he or she should add it to the end of the list. There is insufficient ROI to justify providing an index, or a set of keywords for each entry, or a map showing relationships between the policies, procedures, and standards. Any of these lookup functions imposes an arbitrary, artificial order that is more of a hindrance than a help. Today's intranet search tools are effective and enable a more holistic approach.

5. Hold frequent meetings to discuss IT policies, and provide multiple drafts of documents for stakeholders to review. Respect the subject matter experts' busy schedules and permit them to delegate their participation to junior associates.

6. People love making up rules, especially when the rules will be imposed upon others who annoy them. An effective IT policy operation will inspire managers everywhere in the organization to propose new procedures and standards for the general good. With so many helpful ideas to choose from, it is impossible to create a review and prioritization process that everyone believes is fair to them. Empower the policy developers to decide how many new procedures and standards they need, and which suggestions should be implemented.

7. Reorganize the IT Policy team at least twice a year so that the function benefits from a continuous supply of fresh perspectives, and people throughout the IT domain learn to appreciate its importance. Assign overall management of the operation to a long-term employee who gets along well with other managers – someone who is good at planning team-building events, office parties, and charitable campaigns – but whose contribution to the business will not be sorely missed.

8. If there are innovators within the organization whose rule-bending behaviors have caused trouble with regulators in the past, do not include them in developing policies that will govern their behavior in the future. They will slow down the drafting of the policies by raising too many objections, and they will go along only if they receive assurances that the new rules are "aspirational" rather than mandatory. Since they will probably not comply with the new policies anyway, they will appreciate being able to claim that they had no idea what was going on.

9. When regulators and internal auditors discover a violation of IT policies, procedures, or standards, the perpetrators should be severely punished. The problem should be logged in a company-wide database where everyone can read the lurid details. Their compensation should be reduced, from the lowest level employee responsible for the error all the way up the hierarchy to the manager of the division. This approach will ensure that most risks will be kept secret. Under no circumstances should a financial reward or public honor be offered to anyone who proactively reports issues before they are discovered.

10. Educate your staff about the policies, procedures, and standards through automated intranet training webinars. Provide multiple choice questions that show the correct answer after the user has completed each question, and permit the user to run the training several times until

he/she achieves the minimum passing grade. The staff will be able to maintain their usual level of productivity by running the training while multitasking. Alternatively, each department can designate one person to log in many times using others' credentials and run through the training for everyone. The one-for-all-and-all -for-one approach is especially recommended if departments are in competition for fastest compliance and highest scores.

The foregoing list is by no means exhaustive. For an IT executive eager to improve his or her dodging style, there are two key principles to keep in mind regardless of your industry or IT environment.

First, end-users never tell the truth about their behaviors. They may not intentionally lie, but nobody remembers or is aware of everything they do. This works to your advantage, so believe your users' reports. Do not engage an observer, install video cameras, record keystrokes, or analyze data logs.

Second, end-users support what they believe in. Participatory design techniques help win the users' hearts and minds for compliance. To ensure the wiggle room you desire, these methods should be avoided. Policies invented by an elite cadre of experts and imposed upon the end-user work communities yield far more unpredictable results.

So now – go for it. Hone those obfuscations skills and champion the principles of laissez-faire technology. Remember, you're wiggling for a worthy cause.