What Makes a Good Policy?

Michael Barwise, Integrated InfoSec
mbarwise@intinfosec.com

In a previous paper - *"Instant Compliance for a Grand"* - I savaged the deficiencies of an industry-standard specimen security policy document. That policy addressed IT systems passwords, but the principles are essentially the same for any business policy. So while I'm continuing to use IT examples here for simplicity, the policy model I'm proposing applies anywhere within the enterprise.

It's indisputable that many corporate policies are "shelfware" - documents that exist but don't do anything very useful. So what makes a good policy? There are three fundamental principles.

First Principles

First and foremost, a policy must contribute at some defined level to the solution of a single specific (and real) business issue - not just its symptoms, and never a vague cluster of different issues at once. A classic example of one that fails is the "Acceptable Use Policy" that commonly restricts the private activities of staff on corporate IT. This usually consists of little more than a mish-mash of all the "bad things" the authors can think of, accompanied by a threatening prohibition against doing them. Activities that could harm the infrastructure rub shoulders in an unordered list with those that could cause corporate embarrassment or breach the law. To address each of these disparate issues effectively would need a separate policy, and each of them would have to specify the obligations of the IT department and others in addition to those of IT end users. This may sound complicated, but it's essential if we actually want to solve the real problems personal use of IT can expose the business to. Or indeed any other business problem.

Second, every policy must be consistent with common standards, understandable and demonstrably possible to comply with. So individual policies must not be created in isolation - they must be part of a coherent policy governance framework that specifies the necessary common standards and definitions.

The ideal framework is a logically hierarchical inverted tree from broad corporate governance at the root to specific instructions at the leaves. So if a given policy deals with, say, passwords, it will be a consistent child of an authentication policy that deals with when, where and why you use different kinds of authentication. The authentication policy will in turn be a consistent child of a broader systems access policy, which itself will descend from a strategic information management policy. At each layer there will also be other siblings, so in addition to systems access, the strategic information management policy might have children covering data classification ("protective marking"), data quality, retention, privacy and so on. Policies at some levels of a sub-tree may refer horizontally or vertically to policies in other sub-trees, but there should be no more than four layers of policies in any sub-tree between your governance standards and your procedures. If there are, it's worth reviewing your business analysis.

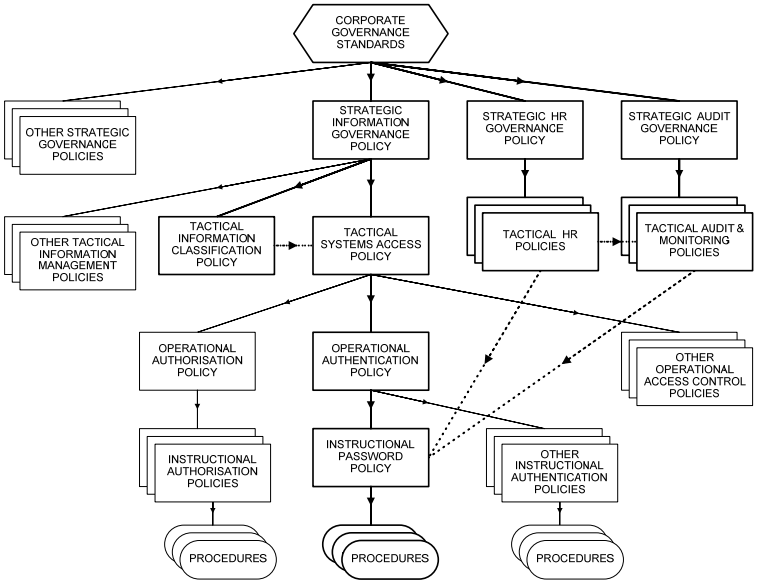
Third, a policy is not an end-user document. Even at the lowest level, the job of a policy is to inform the creation of procedures, which are the only things front line people should be concerned with day to day. The kind of "policies" we mostly have to sign off against when we're hired actually do very little to protect the organisation. They tend to be *"Polcedures"* - scrappy mixtures of policy snippets and procedures - and are generally non-functional because, being written individually on the fly without enough specialist input from business process owners and not being part of a coherent policy framework, they tend to be shallow, unfocused and mutually (sometimes even self-) contradictory. As a result, their requirements are almost always viewed as externalities by those who should follow them, and get ignored when the pressure is on to deliver for the business or in pursuit of personal convenience. And incidentally they're unlikely to be robustly enforceable, as they mostly wouldn't stand up to legal challenge.

A Rational Structure

The diagram below shows the significant structural elements of an optimised policy governance framework, with the major branches of the example password management policy sub-tree emphasised.

This structured framework assists both policy maintenance and efficacy. Even if some policy element within the framework proves less than optimum, it will have a consistent effect on all other policies that refer to it because the contributions it makes to them descend from its sole authority. So the source of the problem is easily identified and corrections can be made at a single point of adjustment. Without such a structure, you just have a disorganised pile of incoherent *ad hoc* documents that might pass audit because they exist, but won't contribute well to the business problems you're trying to solve. Such policy sets will also be difficult to maintain, as adjustments may have to be made in parallel in many different policies to prevent them getting ever more out of kilter with each other.

The Policy Governance Framework



Policies at the strategic layer express the broad governance obligations of each of the organisation's generic business functions. There should be no cross-references between a policy in any given sub-tree and a policy in another sub-tree within this layer, as the policies address individual obligations. These may be statutory or, very frequently, self-imposed. It is a major error to consider compliance as solely referring to regulatory obligations.

Policies at the tactical layer specify the generic business-oriented processes required to fulfil each of the strategic policies. At this level there may be horizontal cross-references, e.g. where the policy in question draws on a standard defined elsewhere - such as those between information classification and systems access and between HR and monitoring in the diagram. There may also be downward cross-references to the instructional layer where a tactical policy (e.g. audit) informs operational or instructional policies in another sub-tree.

Policies at the operational layer identify realisable sub-components of the generic processes specified in the tactical layer. No cross-references are allowed from policies in this layer to any other policies in this or other layers, as its sole function is to act as a translation interface between specific business-oriented policies in the tactical layer above and their functional implementations in the instructional layer below. A well-specified operational layer is crucial to the success of a policy governance framework, as it's the only way to ensure the solutions delivered by the implementation are a good fit to the business requirements they're supposed to fulfil.

Policies at the instructional layer define the specific process management tasks required to fulfil each operational policy. All procedures relevant to a given instructional policy are identified here in terms of their objectives, but not their content. There may be downward cross-references to this layer, from the tactical layer alone, where standards or processes from other sub-trees need to be invoked (e.g. the need to pass an incident to HR or audit for investigation). But there must be no horizontal cross-references within this layer as instructional policies are maximally granular, dealing with specific discrete procedurally soluble problems.

Documents at the procedure layer are the sole authorities on what front line people actually have to do to comply with each instructional policy. It's imperative that the procedures specified mesh well with the primary business processes to which they relate. That means different business groups, departments and functions may need different procedures, although they must all fulfil the requirements of the policy they support.

Although this framework might be misunderstood at first sight as advocating a vast mountain of paperwork, in fact almost all the higher level policies may be documented very briefly. Detail increases downwards through the tree.

Finally, the art of eliciting good compliance with procedures is in making the smallest possible changes to everyone's existing processes while achieving the objectives of the policy. So where procedures supporting different policies affecting the same front line business process turn out to be sufficiently similar, the procedural implementation can be simplified in practice by merging them, provided their multiple sources are fully documented to allow traceability back to all the individual policies from which they're derived. Complex governance can often be achieved via the implementation of quite simple procedures, but if you don't document what you've done, why you did it and how you did it, you can't manage the outcomes.

Author: Michael Barwise is a UK-based policy and risk management consultant with a background in information assurance and systems engineering. He has contributed to international policy and national legislation on Internet and information risk, has lectured on policy development at Masters level, and is widely published online. His special interest is assisting business to improve the quality of risk decision-making.