Reuters Legal News

Building and updating organization policies and procedures

By John Bandler, Esq., Bandler Law Firm PLLC

JUNE 18, 2024

Organizations of every type need to create and update their policies, procedures, and other governance documents.

We call this "policy work" but recognize it is about more than just policies. These internal documents come in all sizes and forms and are essential to manage and lead the organization. They may be required for compliance too.

Lawyers are frequently involved in policy work because of its connection to law and compliance and because attorneys should be proficient with words.

Attorneys may specialize in certain areas of law and compliance but the following principles for policies and procedures are universal. Whether it is cybersecurity, privacy, employment law, occupational safety, or how the organization should build a product or provide a service, we can look to some important principles to build and improve our documents.

Consider three platforms for compliance plus two more components

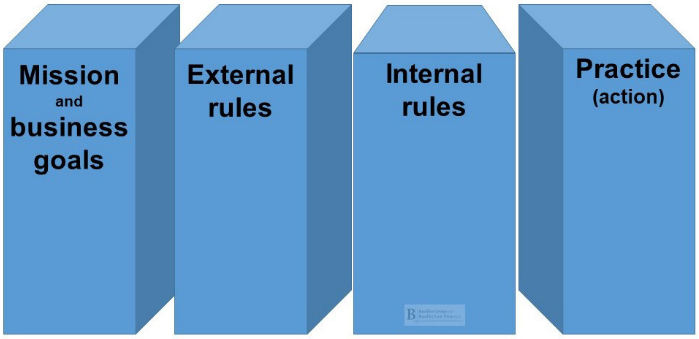
As I laid out in my previous column, we first think of Three Platforms to Connect for Compliance which consist of:

- Laws and regulations (external rules);
- Policies and other internal rules;
- Practices (action).

A compliant organization aligns all three platforms. (John Bandler, "Management, policies, cybersecurity and compliance," Reuters Legal News, April, 23, 2024, https://reut.rs/3RkwBAX). They start by assessing external rules, which are established mostly by government and may also include contractual requirements with third parties. The organization then builds and maintains a platform of their internal rules (many in writing) and another platform of what they do — practices.

Then there are two more components to consider.

We need to consider mission, our fourth platform, the organization's reason for being. Mission is tied to how the organization obtains revenue to pay salaries, rent, and maybe turn a profit. We want all four platforms to align nicely like this.



Bandler's Four Platforms to Connect

Courtesy and copyright John Bandler from his book Policies and Procedures for Your Organization

Finally, we need to consider best practices (external guidance) which also might inform what our policies and practices should be. That is our fifth component, all are important for policy work on any topic.

The internal rules platform analogy

We do policy work by thinking about the internal rules platform concept. We think about what this platform should consist of and how to build and improve it. It includes all governance documents such as policies and procedures which is what most people call "policy work."

But it also extends to all areas of management and leadership, including verbal instructions, tone, and culture. Let's call these "unwritten rules". No organization can or should write down every rule because that is impractical.

Verbal rules are essentially the words conveyed orally. Tone is essentially the way they are stated and the meaning that conveys. And culture is the vaguer notion of what is expected and what will be tolerated or not.

Now let's consider two situations:

- An organization with excellent culture and tone can get things done properly, efficiently, ethically, and in compliance with the law, even if it lacks certain written policies and procedures.

Thomson Reuters is a commercial publisher of content that is general and educational in nature, may not reflect all recent legal developments and may not apply to the specific facts and circumstances of individual transactions and cases. Users should consult with qualified legal counsel before acting on any information published by Thomson Reuters online or in print. Thomson Reuters, its affiliates and their editorial staff are not a law firm, do not represent or advise clients in any matter and are not bound by the professional responsibilities and duties of a legal practitioner. Nothing in this publication should be construed as legal advice or creating an attorney-client relationship. The views expressed in this publication by any contributor are not necessarily those of the publisher.

Thomson Reuters™

- An organization with deficient culture and tone can fail to comply with legal requirements, do things wrong, and have difficulty accomplishing the mission, even if their governance documents look excellent "on paper."

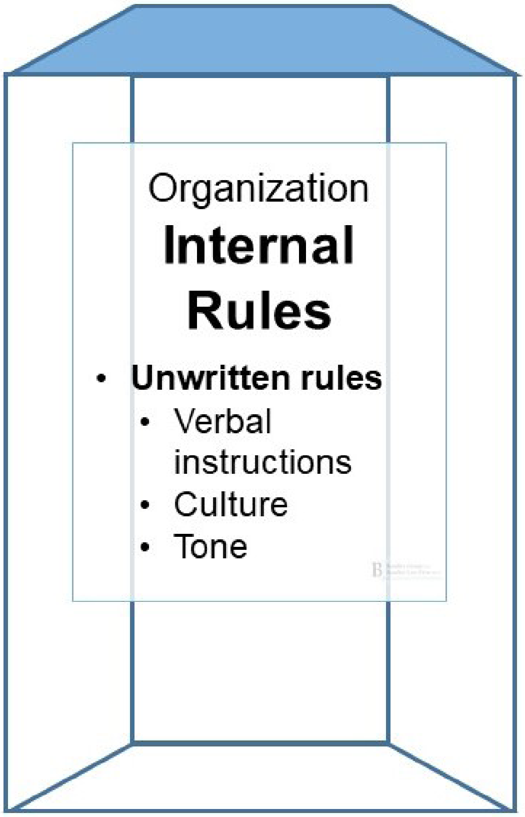
The platform concept accommodates both examples.

Unwritten rules are the sides of the platform

We construct the faces (sides) of the platform with culture, tone, and verbal rules. These faces could be super strong (like structural steel) or a flimsy facade (tissue paper, paper mâché, rotted wood, or rusty sheet metal).

In an organization with solid culture, tone, and verbal rules, the faces are the proper dimensions to align with other platforms. They are strong because employees make good decisions and act properly since they know what is expected of them to achieve the mission and comply with laws. Even without a single policy or procedure written down, employees, managers, and leaders know what to do.

In a deficient organization, these sides are poorly constructed and crumbling from neglect. Even if employees read a policy, they are told "that's now how we really do it."



Internal Rules Platform Faces
Unwritten Rules

Courtesy and copyright John Bandler from his book:
Policies and Procedures for Your Organization

Some rules need to be written down

Organizations need to write down some rules eventually. Large organizations have huge libraries of policies and procedures.

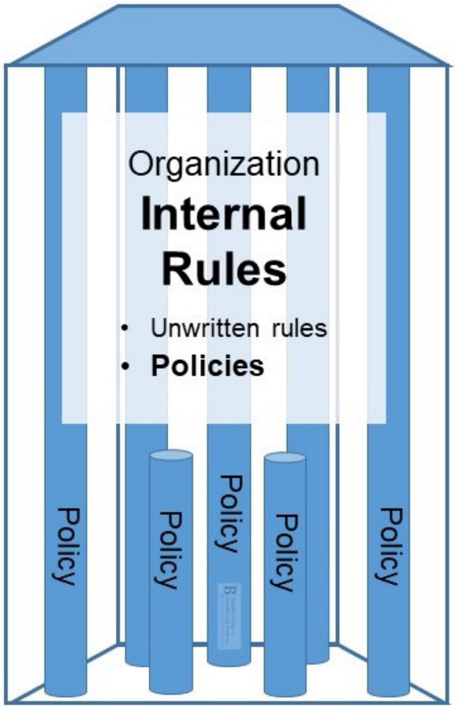
Consider a start-up or small business needing to write their first governance document. Some organizations might start with policies, a more general type of rule that covers things broadly and should be able to last a while until updates are needed. They are like large pillars which help support the platform faces.

Then procedures are more detailed rules; step-by-step instructions to accomplish a task. They may need more frequent change because of their level of granularity. Procedures are smaller pillars like this.

Since the documents are like pillars that help support the platform, we can visualize adding more, rebuilding some, or strengthening some. Management and policy work is a process of continual review and update.

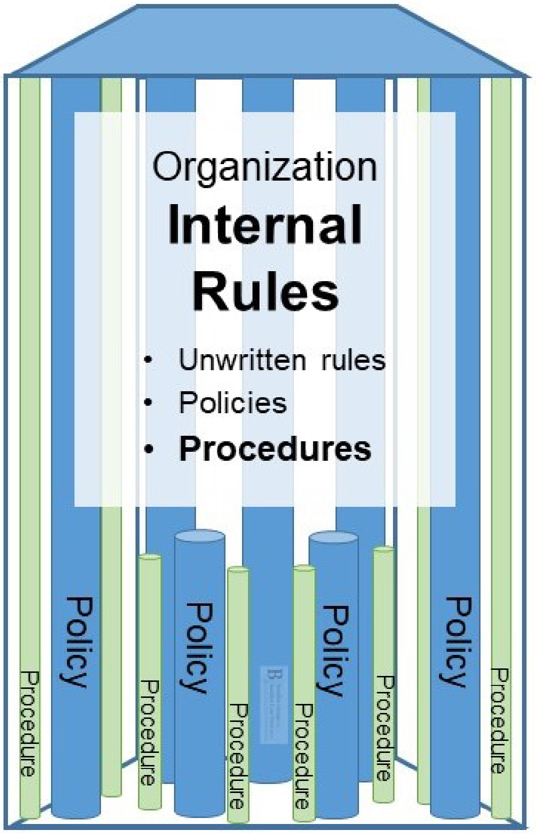
We also see how a verbal instruction could either undermine or reinforce the written documentation. Consider two scenarios a new employee might encounter:

- "Take a look at these policies and procedures then sign the form. It's just a formality we have to do with all new hires. Then your trainer will tell you how we really do things here."
- "Read these policies and procedures and let me know if you have any questions or suggestions. We regularly review and update them for compliance, clarity, and to improve the organization. Then you will sign to acknowledge that you will follow these important rules."



Internal Rules Platform
with written policies (general rules)

Courtesy and copyright John Bandler from his book:
Policies and Procedures for Your Organization



Internal Rules platform with policies and procedures

Courtesy and copyright John Bandler, adapted from his book:
Policies and Procedures for Your Organization

What if an organization has no written rules?

Some organizations have no written rules at all.

Some organizations have no written rules on a particular topic (e.g., cybersecurity, incident response, privacy, employee responsibilities, safety, a sales process, product manufacturing process, etc.).

There may be valid reasons why organizations don’t have certain documents yet.

A start-up needs to allocate resources effectively and policy work and governance may not be their priority. In small businesses, leaders and employees wear many hats, and policy work will be a lower priority.

Most organizations could stand to improve their policy work and be more regular with the update and creation of documents. But an absence of documentation does not mean they are noncompliant *per se*.

The traditional “policy pyramid” analogy falls short

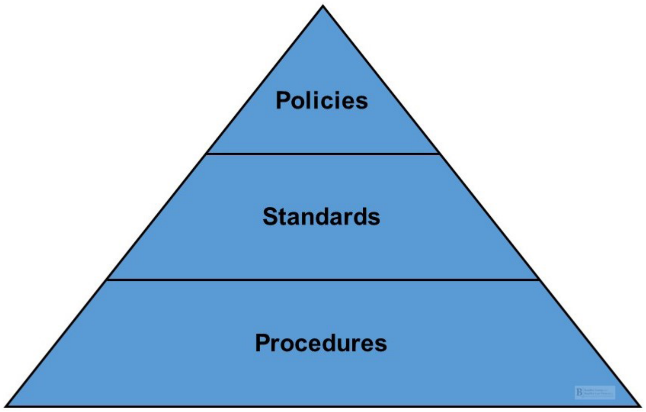
Those working in governance, risk, and compliance (GRC) or other policy work may be familiar with the “policy pyramid” or “rules pyramid” analogy. The most frequent depiction is like this, with policies at the top.

Putting policies at the top recognizes they are a high-level document but creates other issues. This shape does not help visualize a place to start except at the bottom. Nor a place to stand as it is being constructed and once complete, nor how to reinforce it.

> *Most organizations could stand to improve their policy work and be more regular with the update and creation of documents. But an absence of documentation does not mean they are noncompliant per se.*

Pyramids are excellent for ancient tombs but there are reasons you don’t see many business or residential buildings in that shape.

The pyramid analogy also fails to interact with other important aspects of management and policy work, such as laws, best practices, mission, and practice.



Traditional “Rules Pyramid” Concept

Courtesy and copyright John Bandler from his book:
Policies and Procedures for Your Organization

Building our internal rules platform — implementation

In contrast, the internal rules platform can be built quickly and then continually improved and reinforced over the life of an organization. And it is easy to conceptualize how it should align to the other components.

We implement our policy work by getting the right stakeholders and experts involved, and assessing the five components for policy work:

- Mission
- Laws
- Guidance
- Internal rules (current and desired), and
- Practices (current and desired).

We outline, draft, discuss, and move our governance document towards a final approved version. At all stages there may be differing opinions with decisions to be made. As always, we identify options, assess and weigh pros and cons and make sound decisions for the good of the organization.

Solid principles apply across topic areas including cybersecurity

Good principles for management and policy work apply across topic areas, and especially for complex areas such as cybersecurity.

Policy work is often neglected and even more so for cybersecurity policy work.

> *Good principles for management and policy work apply across topic areas, and especially for complex areas such as cybersecurity.*

Any organization evaluating their policy work and management must also consider cybersecurity, privacy, and information governance. This is essential for the mission and compliance with laws surrounding data breach reporting, cybersecurity, privacy, and negligence.

When we review organization cybersecurity and information governance, we apply the same good principles for management and policy work that we should apply to other areas.

Organization leaders (and their legal counsel) should not procrastinate their work on cybersecurity and information management. The legal requirements are here and the subject is imperative for mission success.

Neither should they abdicate their leadership responsibilities and decision-making duties for this topic. Instead, they must seek advice and guidance, follow it when appropriate, and thus retain their duty and decision.

As leaders and managers assess complex areas of cybersecurity, privacy and information governance, they can apply sound principles to make decisions and build policies. That means assessing and following the law, be guided by best practices and expert consultation, and seek to achieve the mission.

John Bandler is a regular contributing columnist on cybercrime and cybersecurity for Reuters Legal News and Westlaw Today.

About the author

John Bandler is a lawyer, consultant, author, and adjunct professor at Elisabeth Haub School of Law at Pace University. He helps protect organizations from cybercrime, improve cybersecurity, and better manage information assets. His latest book is "Policies and Procedures for Your Organization" (2024). His firm, based in New York, is **Bandler Law Firm PLLC**, and he can be reached at JohnBandler@JohnBandler.com.

This article was first published on Reuters Legal News and Westlaw Today on June 18, 2024.