Reuters Legal News

Management, policies, cybersecurity and compliance

By John Bandler, Esq., Bandler Law Firm PLLC

APRIL 23, 2024

Organizations need to manage themselves appropriately and efficiently which will require creation and maintenance of policies and procedures. These documents and other internal rules help the organization comply with legal requirements and accomplish the mission.

Cybersecurity and other aspects of managing information systems require effective governance and compliance processes to satisfy increasing legal requirements and to ensure efficient business operations.

Governance documents serve many purposes — including compliance

Governance documents include policies, procedures, manuals, handbooks, and other documents that organizations create to manage their people and processes. For convenience we can refer to "policies" and "policy work" while understanding policies are one type of governance document.

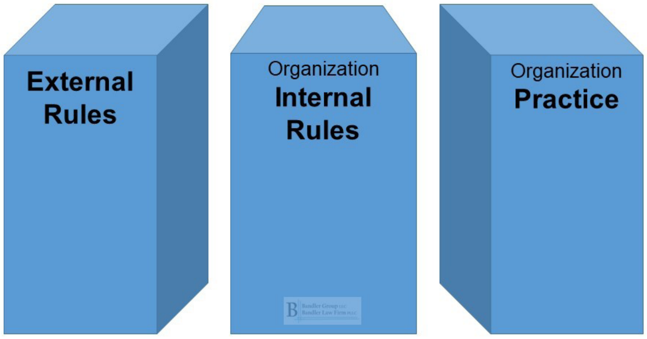
The Three Platforms takeaway is that every organization and every policy need to assess what laws apply and then be compliant with them. Next, practice needs to follow policy and law.

Compliance is an important purpose but not the sole purpose. If there is a compliance issue then the first layer of review is with the documents.

Consider my 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 as depicted in the diagram. 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 actually do — practices.



Bandler's Three Platforms to Connect for Compliance

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

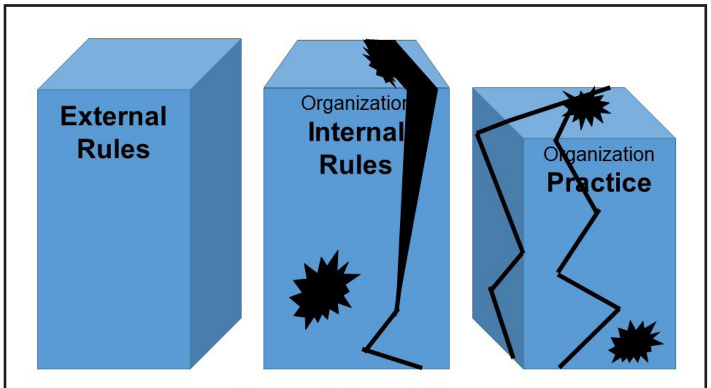
If all organizations were compliant then regulators, plaintiff's attorneys, and even some prosecutors would be idle and bored. But rest assured that many organizations fall short of perfection on the compliance (and efficiency) fronts.

No organization is perfect. Most people have worked in organizations where there was room for improvement in policy or practice — or both. Improvements that could lead to better compliance and more efficient operations.

A non-compliant organization may fail to assess — or consciously disregard — relevant legal requirements. They may haphazardly create inadequate platforms that do not align with those external rules and may be structurally deficient. Their written policies might have been copied and pasted from elsewhere without thought or adaptation. Then they gather dust, untouched. Leaders, managers, and employees may not have read them, might not have even heard of them, and generally don't follow them.

Thanks to the courts and news, we know examples of organizations that had severe deficiencies in their compliance and were then found civilly liable for monetary damages or even convicted of criminal offenses. A woefully deficient organization's three platforms might look something like this diagram and have poor alignment and structural failings.

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.



Noncompliant organization

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

The Three Platforms takeaway is that every organization and every policy need to assess what laws apply and then be compliant with them. Next, practice needs to follow policy and law.

Compliance is not everything

Legal compliance is important but is not everything.

That's because organizations exist to fulfill a mission, not merely to comply.

Every policy should incorporate the mission in some manner. Mission might be called business goals or objectives or something else, but the principle is that policies (and compliance) further and support the mission. They don't fight against it.

> *Effective policies and procedures help organizations properly manage their information assets and systems, protect themselves, and comply with legal requirements.*

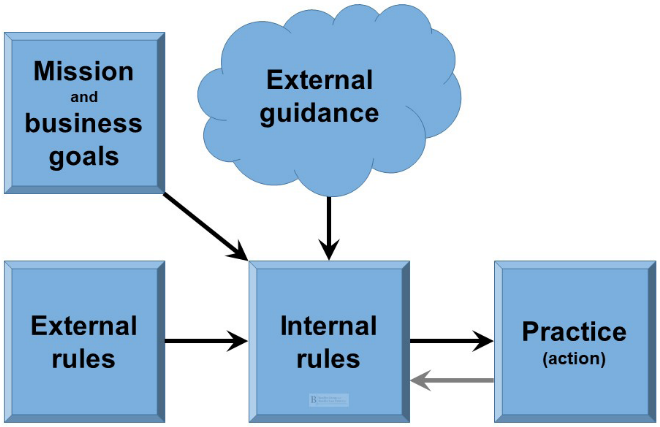
As a corollary, good organizations need to do their good work within the boundaries of legal requirements.

After mission, a fifth consideration is required because reinventing the wheel can be time-consuming. Policies should evaluate and consider "best practices," an amorphous term which includes any guidance that comes from outside the organization and is relevant to that policy topic.

In sum, to conduct effective policy work we need to add two more components to our three platforms:

- Mission and business goals;
- Best practices (external guidance);

and that means we now have Five Components for Policy Work as depicted below.



Bandler's Five Components for Policy Work

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

Proper assessment of these five components allows us to effectively create and update organization governance documents, as I explain in my new book, "Policies and Procedures for Your Organization."

Cybersecurity and privacy

Cybersecurity and privacy are complex areas at the intersection of technology, data, cybercrime, business, and evolving laws and regulations.

Cybersecurity is a requirement for compliance and cybercrime protection. Then consider that organizations that properly manage their information systems can protect, comply and also better accomplish their mission. Translation: less costs and more revenue.

Organizations need to assess what cybersecurity and privacy laws apply to them as we introduced in an earlier article (''Cybersecurity law, compliance and protection,'' Reuters Legal News, Sept. 19, 2023, https://bit.ly/3UhD1Tx). In sum they need to assess legal obligations for:

- Mandated reporting of certain cybercrimes (data breach reporting);
- Cybersecurity;
- Privacy.

For example, laws or regulations may require an organization to maintain a cybersecurity program which consists of documents plus proper processes and practices to address issues and risks.

The laws of negligence (not to mention voluntary principles of good management) suggest the organization should maintain a reasonable and diligent cybersecurity program. The law may require the entity to take certain actions and notify certain people and organizations if there is a data breach. Contracts impose cybersecurity related duties. With those external rules identified, the organization now builds internal rules and assesses what it does and should do.

Cybersecurity policies and procedures

Cybersecurity almost always requires written policies and procedures because it is too complex and otherwise would be poorly communicated.

Although verbal instructions and communication are essential with every part of business management (including cybersecurity) writing is necessary to address the nuanced intersection of criminal threats, legal requirements, technology, business needs, internal policy, best practices and employee action.

Effective policies and procedures help organizations properly manage their information assets and systems, protect themselves, and comply with legal requirements.

Following from this is the realization that cybersecurity professionals, including executives, managers, lawyers and consultants, need to write effectively. And then employees need to read and be able to understand what was written.

These policies and procedures are necessary but can be daunting to write, read, review, and update. A multitude of overlapping requirements and best practices means there are different categories and terminologies with both overlap and distinction. This can cause fear, uncertainty, and doubt (FUD) throughout the policy process.

Can we use AI tools to write our policies?

Some are tempted to see if artificial intelligence (AI) tools can create the perfect written product. This temptation exists even when the topic area is simple, and these areas of information governance, cybersecurity, cybercrime prevention, and privacy are rarely simple. There are overlapping and evolving areas of law, best practices, technical and cybersecurity issues, plus nuanced decisions of risk management.

Perhaps AI is the simple and easy button we can press to get our work done?

Unfortunately, AI is not the magic panacea, as we discussed in an earlier article ("AI's promise and problem for law and learning," Reuters Legal News, Feb. 21, 2024, https://bit.ly/3VZsDks).

The answer here — as always — is that humans need to read and understand the written word, and that means humans need to play the dominant role in shaping it. We need to understand the legal requirements, best practices, mission, and desired organizational action.

Policy writing is both a journey and a destination. The journey helps inform the destination and helps build individual and organization strength. Organizations that take short cuts might not get to the right destination and will deprive themselves of the learning process that the journey provides.

The final takeaways

Cybersecurity is complex and may seem unknowable to some. But we simply need to bring good principles of management, decision making, and policy writing to it.

Organizations need written governance documents to comply, protect themselves, and accomplish their mission. The final document is important, but so is the journey to get there. Policies should never sit on a shelf gathering dust but are important for action and mission, and with all the organization does. Especially cybersecurity.

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 April 23, 2024.