Clearwater

Whitepaper

Build A Culture of Compliance Through Principle-Based Policy Governance

Table of Contents

Introduction 3

The shelving system 3

Organizational risk 4

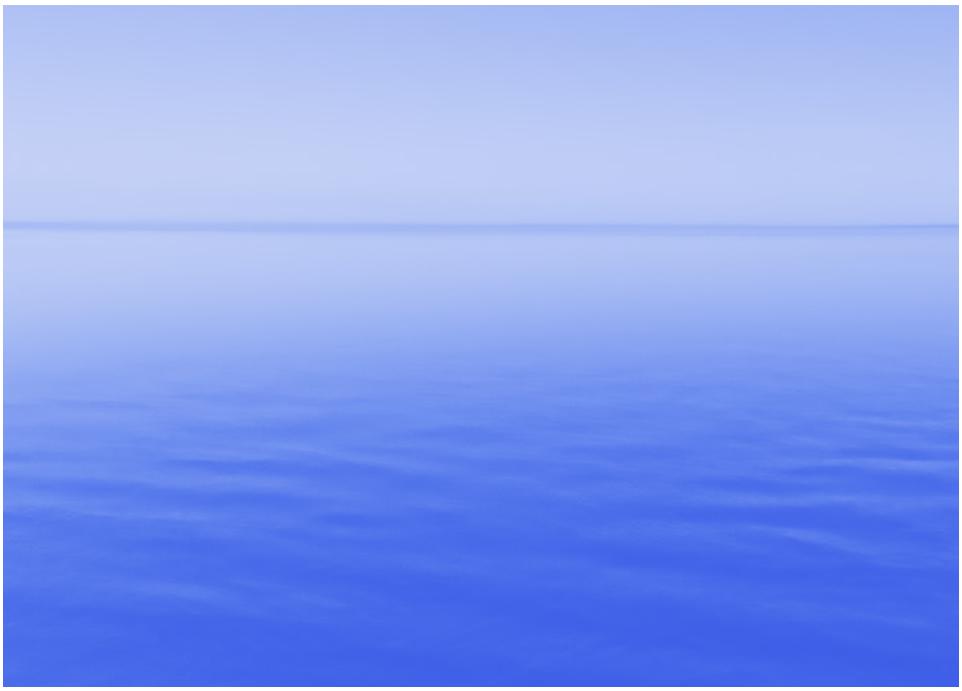
What is principle-based policy governance? 5

Begin with intent 6

Framework support 6

How to implement principle-based policy governance 9

Benefits 10



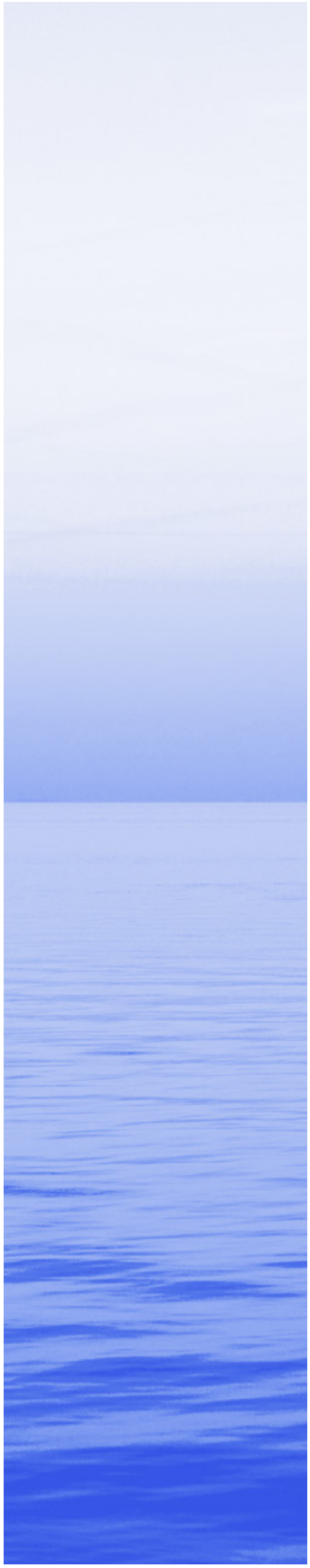
© Clearwater | All Rights Reserved | 10.5

Introduction

Organizations of all sizes struggle with embedding policies and procedures successfully into their day-to-day operations. That's because for many, these policies fill binders and shared drives, overwhelming employees with pages and pages of instruction about expectations for a growing list of compliance, regulatory, and safety standards and procedures.

Often, the first introduction to these policies comes during new hire onboarding, where team members are expected to watch training videos, read documents, maybe pass a quiz, and then sign off in acknowledgement they understand all of your company's rules and procedures.

And then what happens once an employee gets settled into your work environment? Over time, it's likely your company creates more policies or updates existing ones, and sadly, there's often a gap in both communication and training for your staff on these changes and new requirements. As a result, policy changes either aren't known or are just ignored.



The shelving system

In some organizations, policies can fill two, three, four, even more, binders, making it difficult for anyone to keep track.

The core documents generally live at a corporate office, with copies distributed to other locations. Whenever the executive team approves a change at the corporate level, those changes have to be printed out and shipped to each location with instructions about which old pages to trash and which new pages to replace. Your compliance officer, if you have one, may create checklists and protocols to ensure this is handled, but it's often a roll of the dice about when and where these tasks are completed.

Even in more modern environments where technology replaces paper, it's still difficult to update these files.

Oftentimes, editing restrictions make it difficult for the right person to access the right document to make timely changes. Or there are multiple versions of the same policy. Or the server goes down and the policies can't be accessed.

© Clearwater | All Rights Reserved | 10.5

And even when team members make all the required updates, it often doesn't trickle down to employees who do the day-to-day work. If it does, there's often little education about those changes or enforcement or penalties for non-compliance.

Organizational risk

For many companies, compliance standards are merely checkbox initiatives, set up and ticked off just to pass an audit, where things go cold until it's time for the next audit review or re-certification.

That's a big risk for healthcare organizations, especially where failure to meet standards could result in data breaches and violations that can cost thousands—sometimes millions—of dollars in response and recovery expenses and related fines and penalties.

Why do so many companies take the risk? That's because traditional policy creation and management practices are:

- Time-consuming
- Taxing on resources
- Error-prone
- Difficult to track and regulate
- Challenging to identify inaccuracies
- Lacking in employee buy-in or support
- So voluminous, no one wants to tackle them

There are also a number of consistent challenges for organizations when it comes to policy creation and implementation. Here are a few common examples:

- Policies exist, but they're not implemented
- There are no standardized or routine policy reviews
- Policies aren't updated and don't reflect current workflows or environments
- Policies don't align with implemented practices
- Policy requirements are too difficult to adopt
- Policies set expectations outside budget scope
- It's not clear who is responsible for policy enforcement

© Clearwater | All Rights Reserved | 10.5

- There is little to no policy enforcement
- There is little to no training about how to meet policy standards
- There is little to no support to implement policies budget
- Team members don't understand policy creation structure or how to get a new policy improved
- There is no policy manager
- Each department or manager just establishes his/her own policy
- Policy creation processes are so strict, (for example they require board or committee approval) no one wants to set them
- Policies are often at a variety of maturity stages

So how can we replace these outdated and cumbersome practices with more viable alternatives that don't just make policy creation and management easier, but also integrate them into workflows and build a culture of compliance? Is there a better way to define, implement, and manage policies and related expectations?

The answer is adopting Principle-Based Policy Governance and using existing frameworks to establish and maintain controls.

What is principle-based policy governance?

When we talk about Principle-Based Policy Governance, what we're talking about is facilitating and streamlining the adoption of key principles and policy statements at the board and/or executive level. We are not talking about setting the day-to-day tasks or requirements to meet those specific principles. Those will be hammered out by your subject matter experts—the key employees tasked with these responsibilities within your organization. Rather, the focus is on approving the core standards and framework to guide your policies in a way that meets your organization goals and objectives and your compliance and regulatory requirements.

This is where policy intent is set, which guides the rest of your supporting components and standards.

> Failure to meet standards could result in data breaches and violations that can cost thousands—sometimes millions—of dollars.

© Clearwater | All Rights Reserved | 10.5

Begin with intent

One of the big fail points for organization-wide adoption of policies and procedures is that employees often don't understand exactly what they're supposed to do or why, nor do they have a real understanding of how their role fits into the overall big picture for your organization and ultimately its success.

This is often the result of policy intent not effectively translating into practice.

To get started, when considering a new or modified policy, ask yourself:

- Will this policy have a positive impact on our organization?
- Does the policy help us meet or maintain a regulatory or compliance standard?
- Can we translate this policy into standards and procedures that are easy for our employees to understand and do?

By starting your processes with intent, you can then establish a set of principle statements that will effectively guide your policy statements, and from there, you can create directives that support these policy statements, and ultimately standards, procedures and guidelines that support those directives.

A few other important starting points for consideration:

- Create policy statements that are meaningful and impactful for your organization
- Align your policy statements to a framework that works for your organization
- Automate procedures that integrate your policy expectations across all environments

Framework support

One way to successfully create an organizational culture that supports Principle-Based Policy Governance is to use existing frameworks to build, manage, and mature your policies.

For example, if your organization needs to create a set of policies to meet your cybersecurity requirements, you might choose the NIST Cybersecurity Framework. This framework outlines standards, guidelines, and practices you can use to protect your critical infrastructure and manage cyber risk.

© Clearwater | All Rights Reserved | 10.5

The NIST framework has five core functions:

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover

These five areas, in this example, would guide the principle statements your board or leadership team would review and approve. These principles relay the intent of the board and define organizational information security expectations.

Then, there are 23 categories within the NIST framework, which are like control families or control groupings, that you can use to create policy statements. These policy statements should be defined and agreed upon by organizational leadership and then aligned to meet the intent of the security principles.

Next, still drawing on the NIST framework, there are 108 subcategories, which are controls. These controls can serve as directives for your policy and are used to define your policy expectations with alignment to your framework standards.

Your board would use these components to establish your core policies and then would hand off implementation of processes, standards, and guidelines to your organization's subject matter experts (SMEs)—the team members responsible for these activities—for example, the head of your IT and InfoSec teams.

Your SMEs can develop security standards from existing frameworks, but should customize these standards based on the unique needs of operational units and, at the same time, comply with directives.

Finally, procedures and guidelines, also developed by your SMEs, will outline all of the processes, activities, and methods your team members should do to implement and maintain the requirements set in your security standards.

Setting principle-based policies empowers your SMEs to take ownership of developing these processes and standards instead of the board—who isn't involved in these day-to-day processes—and telling your teams how to meet your policy principles.

Your SMEs essentially create the "how to" components to achieve your policy goals. They can use the guidance of the selected policy framework, for example here,

© Clearwater | All Rights Reserved | 10.5

the NIST Cybersecurity Framework, to determine how to comply with your policy expectations and set your security standards.

One of the great things about this approach is that your SMEs don't have to get board approval on every change or new procedure within their practice. Instead, your board guides your team on what the expectations are and then empowers the people who do this within your organization to set those standards.

In addition to setting these standards, your SMEs also play an important role in establishing performance levels for the procedures and guidelines, so you can monitor your success of meeting policy requirements and identify gaps where you have issues, with the goal of resolving them before an audit discovers a deficiency or an incident or event occurs.

Principles	The five principles relay the intent of the Board and defines organizational information security expectations.
Policy Statements	The twenty-three policy statements are defined and accepted at the leadership level of the organization and are aligned to meet the intent of the cybersecurity principles.
Directives	Directives align to the NIST Cybersecurity Framework Subcategory Level. Directives further define expectations or Policy Statements and are aligned directly to established cybersecurity framework standards.
Security Standards	Security standards are based on pre-defined standards from the NIST Cybersecurity Framework and its referenced controls from CIS, ISO 27002, and ISO 27005; however, these may be customized for organizationally based controls.
Procedures & Guidelines	Procedures describe security related processes, activities, and methods for implementing and maintaining requirements defined within the organization's Security Standards. Guidelines provide guidance and pragmatic advice about fulfilling the requirements established by the organization's Security Standards. Although the guidance and advice are discretionary, the underlying requirements are usually mandatory.

© Clearwater | All Rights Reserved | 10.5

How to implement principle-based policy governance

The process starts off with organization introduction and acceptance. This generally starts at the executive level and involves outlining the problem you're trying to tackle:

- We've got countless pages of policies.
- These policies aren't updated as often as they should be.
- The policies aren't accurate or they're not being followed.
- We need to restructure how we create policies and what we do with them, while still meeting our regulatory requirements.

After outlining the problem, explain that your goal is to restructure policies in a way that they make sense to your team members and they become easier to implement so it creates a compliance culture and sets the right expectations for all employees.

After getting executive buy-in, support, and approvals, it's time to bring in your SMEs. Here, you explain what your policy processes should look like and explain core terms such as the differences between policies, procedures, standards, and guidelines.

It's important to encourage your SMEs to work with you in this process, explaining the valuable role they'll play in developing the day-to-day processes that directly affect them and their teams. They have a unique opportunity not only to contribute, but also help write these standards. They will be the experts in developing how your company accomplishes these tasks.

After engaging your SMEs, it's time to create and implement policy standards, being sure to adopt processes that are both repeatable and scalable as your organization—and your requirements—change over time.

Here's a quick recap and checklist to help with implementation:

- Cultural introduction and social acceptance
- Management and leadership acceptance
- SME acceptance
- Develop plan to integrate with existing policy
- Prioritize control focus
- Prepare cascade expectations from principles to standards, procedures, and guidelines

© Clearwater | All Rights Reserved | 10.5

- Empower SMEs
- Empower SMEs to create and implement standards
- Relate standards to higher-level expectations
- Integrate expectations into repeatable functions using your IT management engine, HelpDesk system, or ticketing system to:
  - Enable alerts to integrate control procedures into daily activities of SMEs
  - Track SME time pertaining to control processes
  - Manage workforce change, ensuring standards survive workforce turnover
  - Create logging and audit trails of control activities
  - Forecast budget needs pertaining to controls

Benefits

There are a number of benefits of moving from the older, ineffective means of policy creation to a principle-based approach that's supported by industry frameworks. Here are a few:

- Stabilized cybersecurity program goals and measurements by using established guidelines and standards within the NIST Cybersecurity Framework
- Aligns organizational programs to nationally recognized standards
- Remediation roadmap development engages existing SMEs
- Prioritizes remediation efforts
- Enables expectations that address workforce turnover (SME and leadership) while maintaining organizational needs
- Assists in identifying multi-year strategic and annual tactical work plans

If you're still using traditional processes to create and manage important organization policies, now is the time to embrace automation and build your Principle-Based Policy Governance program with the support of industry approved frameworks.

© Clearwater | All Rights Reserved | 10.5

Clearwater is the leading provider of Enterprise Cyber Risk Management and HIPAA compliance software and consulting services for the healthcare industry. Our solutions enable organizations to gain enterprise-wide visibility into cybersecurity risks and more effectively prioritize and manage them, ensuring compliance with industry regulations. Clearwater's suite of IRM|Pro® software products and consulting services help healthcare organizations to avoid preventable breaches, protect patients and their data, and meet OCR's expectations, while optimizing cybersecurity investments. More than 400 healthcare organizations, including 64 of the nation's largest health systems and a large universe of business associates that serve the industry, trust Clearwater to meet their information security needs.

Have questions regarding this white paper? Engage with Clearwater for a specific discussion about your organization's approach.

- ClearwaterSecurity.com/Contact

© Clearwater | All Rights Reserved | 10.5