WHITE PAPER

INTEGRATED RISK MANAGEMENT

End the Struggle with InfoSec Policies and Standards through Risk & Compliance Integration

Why CISOs Struggle with Information Security Policies and Standards

Information Security Policies and Standards are a Chief Information Security Officer's primary tool for communicating security expectations throughout the organization.

However, for many organizations, they are more a source of confusion, and worse, they can increase the organization's liability. Employees are forced to sift through bloated, complex, and frequently contradictory documents and then deduce what requirements apply to them in their particular role and circumstance. Neither security managers nor internal auditors can confidently attest they meet minimum regulatory compliance and risk management practices.

This is usually a result of a CISO taking a compliance-only approach meant to satisfy an auditor. The hallmark of such an approach is simply restating regulatory mandates into policies and standards or using generic "out-of-the-box" policies. Other symptoms of this mindset include the use of a generic risk register and overlapping assurance programs.

In this situation, policy and standards compliance processes are disconnected from other risk and compliance processes creating confusion for the organization. As regulations evolve, this burden only increases. This is an ineffective approach.

Eventually a complete rewrite becomes an easier task than attempting to review and update the current set of documents.

When this point is reached, we advocate CISOs take the time to correct the root cause of the problem as we see it: failure to build Policies and Standards with an integrated risk and compliance approach.

In this book, we will cover the 4 symptoms of a compliance-only approach and the benefits of a risk-integrated approach.

The Symptoms of A Compliance-Only Approach

Although the results of a compliance-only information security mindset show up at various levels throughout the organization, we've identified four common symptoms of this problem.

1. Simply re-stating regulatory mandates into policies and standards without first interpreting and right-sizing for the unique risk posture of the organization.

2. Use of "out-of-the-box" policies obtained through tools or websites that do not meet applicable federal, state, industry and internal mandates.

3. Use of a generic risk-register that doesn't include internal policies and standards.

4. Overlapping assurance programs, typically aligned against each regulatory mandate, which burden staff and complicate reporting requirements.

1 Simply Re-Stating Regulatory Mandates

The aim of a narrow, compliance-only approach is to survive an audit review of policy documents without any findings. Thus, the tendency is to add any and all mandates to governance documents to minimize chances of a gap.

The problem with this approach is it can actually increase an organization's risk level. Simply restating regulatory mandates into policies and standards can unnecessarily restrict an organization's compliance options. Whereas before it had the flexibility to identify alternate means to mitigate risk, it has now mandated itself to follow a prescribed approach. Further, many regulatory mandates are more appropriately enforced at the process or procedure level.

Take for example, the practice of testing in production. Although broadly recognized as non-ideal, for some environments and situations, it is simply unavoidable.

Do your policies generically state this common mandate, or is it tailored to your unique risk?

Do they identify alternative controls that equivalently mitigate risk?

If an organization fails to make this distinction, it increases exposure to any regulator, auditor, or insurance company that may evaluate the organization's policy compliance.

2 Use of "Out-of-the-box" Policies

A CISO may be attracted to this approach if they are trying to "check the box" on policy compliance. Many GRC tools and websites are populated with generic content for organizations to use. However, we find that such generic content generally has the following shortcomings:

- Excessive focus on a single regulatory source (e.g., HIPAA, PCI, or FFIEC only) and not sufficiently customized to other applicable federal, state and industry-specific sources.
- Not written for the organization's current InfoSec maturity and culture.
- Exclusion of or insufficient consideration for internally derived mandates applicable to the organization.
- Inclusion of controls the organization cannot meet due to technical or operational infeasibility.

The typical result is an organization that is over-controlled in some areas and under-controlled in others – exposing it to unnecessary costs and audit findings.

Where should a CISO start? After all, where does one begin organizing the mass of various topics and overlapping requirements? In our experience, CISOs are better off focusing their time on building a strong organization-specific risk register and using it as the spine for developing InfoSec Policies and Standards.

This leads directly to the next common symptom.

3 Use of a Generic Risk-Register

The key to simplifying the risk and compliance challenge is a well-defined, organization-specific risk register. Such a tool clarifies:

- What are the controls I must address to be compliant?
- How important are these controls to my organization (what is the inherent risk?)
- What are the mandates driving the need for those controls?
- How effective are these controls in my organization (what is the residual risk?)

However, such a tool has historically proven to be a barrier to entry. After all, it takes considerable effort to identify all regulatory sources, map them to a harmonized control library, and allocate associated risk ratings.

For this reason, many CISOs will either adopt a generic risk register from a GRC tool or website. Or fail to build a risk register at all–instead adopting a compliance-only approach.

We strongly caution CISOs against adoption of a generic risk register as they are typically impractical from an assurance perspective and can significantly drive up testing costs. Instead, we advocate a middle ground where organizations adopt a managed content library that can be rapidly customized to include incorporation of its own policies and standards as sources themselves. Such an approach lowers the barrier to entry, while keeping a practical implementation.

4 Overlapping Assurance Programs

A compliance-only approach will wastefully organize testing around individual regulatory sources. The burden for such an approach is acutely felt by IT staff. For example, a system owner must respond to a SOX compliance test. And then a PCI compliance test. And then, a round of tests for internal policy compliance.

This all adds up to high compliance costs and may overwhelm staff.

A better approach is to integrate all controls into a single framework, allowing a single assessment for control definition, and a single testing pass that measures compliance against all regulatory and internal mandates.

This approach treats Policies and Standards like just another regulatory mandate and positions the governance documents as the communication tools they're intended to be rather than a tool to placate auditors.

Tackle the Problem with An Integrated Risk & Compliance Approach

The root cause of the policy and standards stuggle is a failure to build them through an integrated risk and compliance approach.

We advocate an approach that tightly integrates policies and standards with a risk register linked to mandates; which is subsequently used to drive control planning and testing. This approach effectively integrates risk and compliance processes and avoids the common symptoms mentioned while allowing a CISO to overhaul their policies and standards in just 2–3 months.

An Integrated Risk and Compliance Approach...

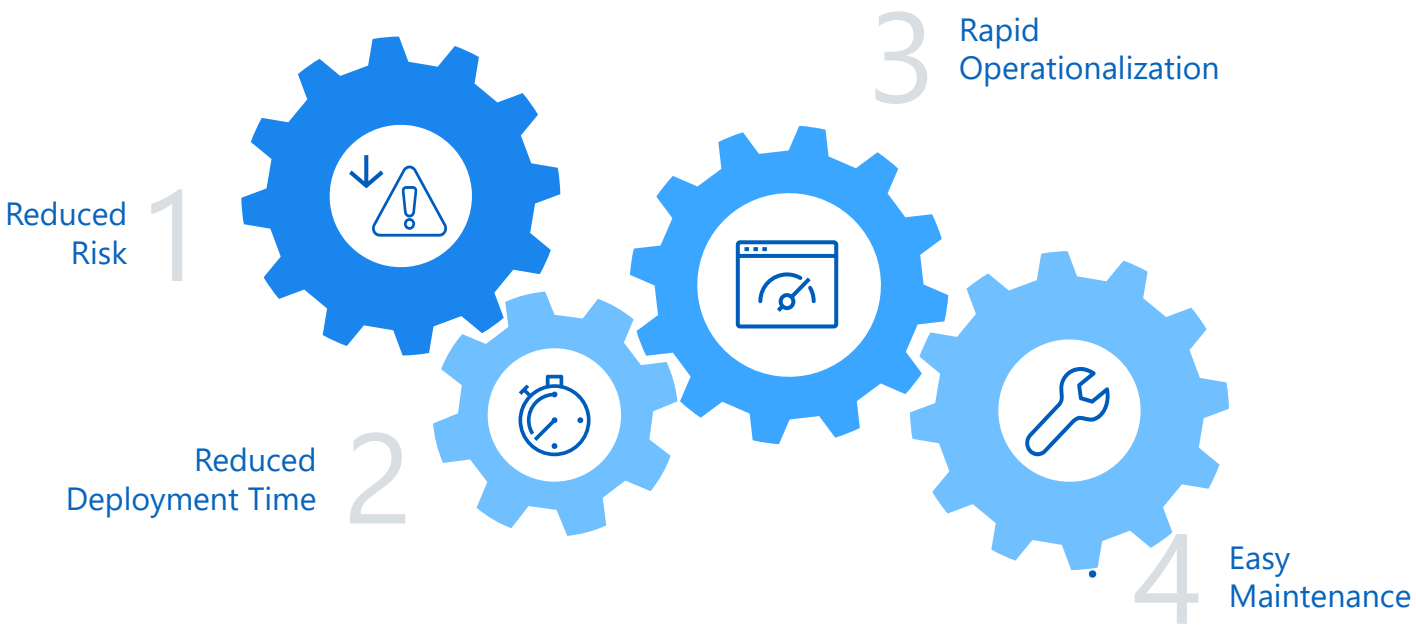
...Answers Key CISO Questions

- Do my Policies & Standards meet the latest regulatory minimums?
- Have I committed to a regulatory mandate we cannot meet?
- Where do my Policies & Standards under-control or over-control?
- Can I measure my Policy & Standards compliance?

Benefits of a Risk-Integrated Approach

This methodology has demonstrated its value with consistent success across numerous clients. Rather than being a one-off task for auditors, authoring governance documents becomes a central aspect of the risk and compliance management program, driving security controls throughout the organization.

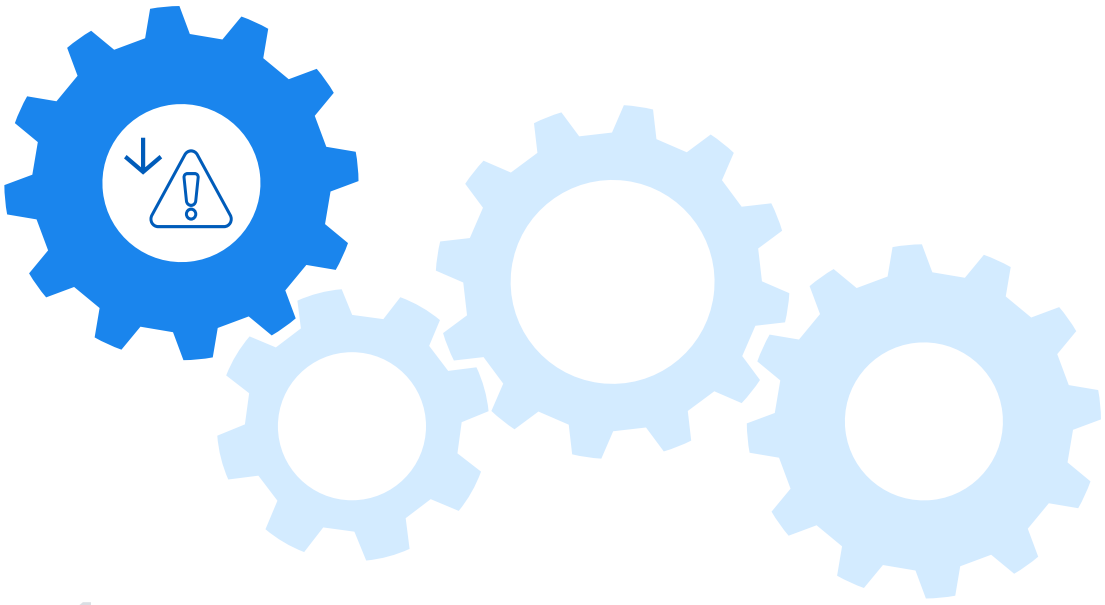
The top four benefits we've seen from this approach are:



Accelerate your journey

Leveraging our iGRC Content Library as an accelerator, Edgile can help you rapidly deploy a full refresh of InfoSec policies and standards. At the same time, we establish a GRC foundation that ensures you can:

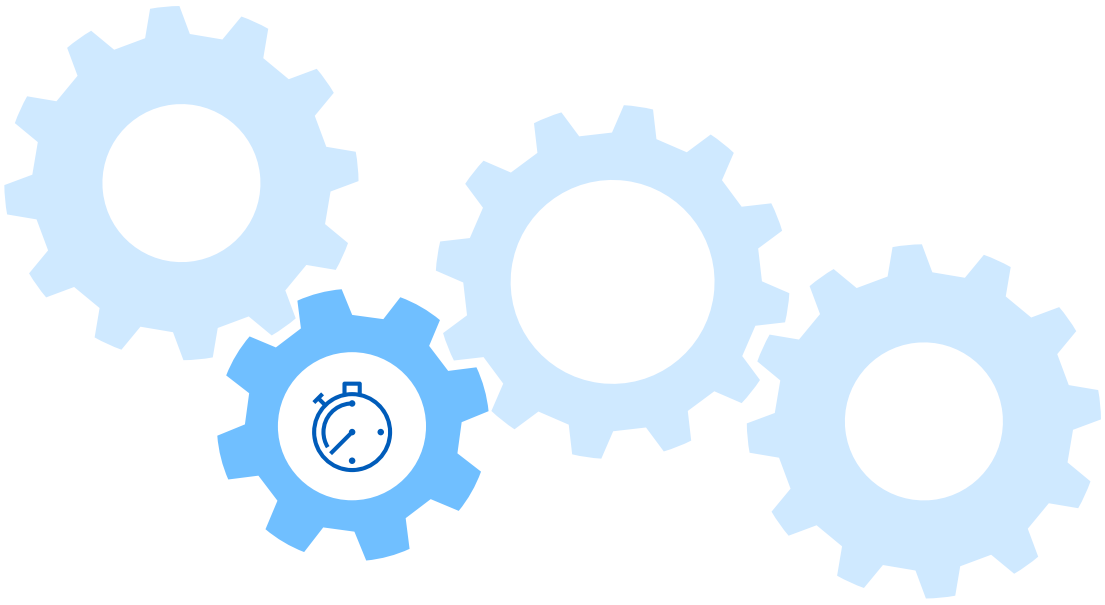
- Operationalize the controls in your environment
- Assess Once, Test Once and Satisfy both internal policy and standard compliance and external compliance (e.g. laws and regulations)
- Sustain a Risk Register with verbatim linkage to laws and regulations
- Easily maintain the documents as regulations evolve



1 Reduced Risk

The risk register becomes the CISO's "single source of truth" regarding compliance and risk mandates. When policies and standards are mapped to a risk register, an organization can confidently "right-size" the control environment in a manner commensurate with its actual and desired risk.

The result is the CISO now has both the insight and the ability to address areas where the organization is under-controlled or over-controlled.



2 Reduced Deployment Time

Historically, the barrier to entry for this approach is untenable: identifying all regulatory sources, mapping them to a harmonized control library, and building a risk register.

However, when using our iGRC Content Managed Service, the hard part is already done. Now, one can simply translate and apply the identified requirements into policy/standard language appropriate for the organization's desired risk posture.

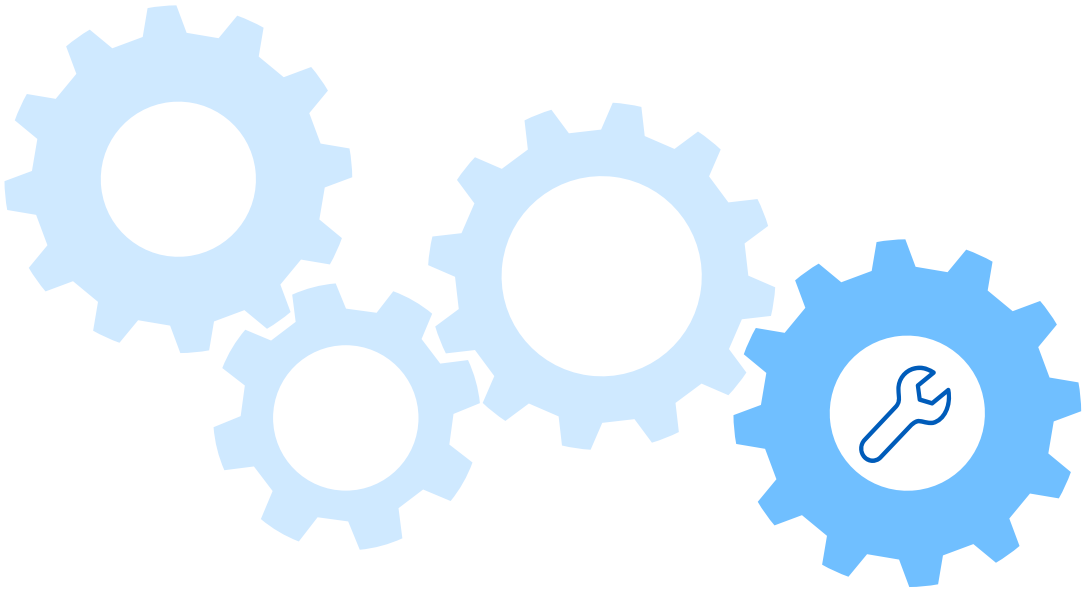
In general, we've been able to deploy a risk register and a draft full-spectrum set of information security policies and standards in as little as 2-3 months.

3 Rapid Operationalization

Our methodology integrates policy and standards compliance with other risk and assurance processes.

An optimized framework means simplified deployment and faster adoption.

This ensures every asset owner clearly knows what controls they must adhere to. Further, you can assess once, test once and report on compliance against multiple mandates using a common process that can be scaled up or down considering the organization's assurance requirements.



4 Easy Maintenance

Keeping track of new regulatory rules and guidance from state, federal, and industry-specific authorities is an intensive effort requiring legal expertise. For most organizations, this requires expensive, highly skilled dedicated resources.

Our content managed service provide access to the dedicated Edgile team of attorneys, risk and compliance, and InfoSec experts. Now you can have your mandates monitored and harmonized with quarterly updates with a consistent, high-quality Risk Register delivered at a lower cost to the organization.

Review

CISOs struggle with Information Security Policies and Standards because over time, these Polices and Standards become complex, bloated and frequently contradictory. Neither security managers nor internal auditors can confidently attest they meet minimum regulatory compliance and risk management practices.

The root cause of these problems:

Failure to build Policies and Standards with an Integrated Risk and Compliance Approach.

Instead, policies and standards are too often authored with a compliance-only mindset. There are four common symptoms of this problem:

1. Simply re-stating regulatory mandates
2. Use of "out-of-the-box" policies
3. Use of a generic risk-register
4. Overlapping assurance programs

Edgile's Integrated Risk and Compliance Approach leverages our iGRC Content Library to accelerate your deployment. The benefits of our approach include:

About Edgile

Edgile is the trusted cyber risk and compliance partner to the world's leading organizations, providing consulting, managed services, and harmonized regulatory content. Our strategy-first model optimizes IAM, GRC, and cybersecurity both on-premises and in the cloud. By transforming risk into opportunity, we secure the modern enterprise through solutions that increase business agility and create a competitive advantage for our clients.

For more information about Edgile, visit **www.edgile.com**.