iGrafx®

eBook

The How-to Guide: Building a Compliance and Risk Management Strategy

Introduction

Organizations in heavily regulated industries like banking, insurance, healthcare, and manufacturing face substantial financial and reputational risk in their operations, and the risk is magnified by an ever-expanding list of new regulations. The good news is that we've compiled a how-to guide designed to help businesses tackle these compliance and risk management challenges head on.

We'll cover how to:

- Make your business operationally resilient with technology
- Proactively uncover hidden risks and compliance gaps
- Transform your audit process into a faster, cheaper, and more accurate version of itself

The Challenge

Compliance is expensive, constantly evolving, and time consuming. In addition, the consequences of non-compliance can be colossal. In 2023, the SEC filed 784 enforcement actions for nearly $5 billion in penalties - and that's just one agency for one industry in one country.

So, what makes standing up an effective risk and compliance management program challenging? Many businesses run operations across many different geographies, meaning they're facing various regulations and laws they're required to comply with.

In the United States, you have Sarbanes-Oxley, HIPAA, OSHA, and other regulations. If you're in Europe, there's GDPR and ISO, just to name a couple. These regulations are constantly evolving and more continue to come into effect every year. Staying on top of this can often be dizzying.

Typically, organizations aren't intentionally disregarding these laws and regulations – rather it's the sheer complexity of the task at hand.

They need to adopt an effective strategy that:

1. Proactively manages business operations
2. Identifies and mitigates risks
3. Ensures internal and external requirements are met
4. Proves compliance

The Art of the Possible

Seamlessly shift from
“We’ve defined risks & controls”
to
“There is proof that our controls are effective”

There are any number of best practices teams can leverage when building their risk and compliance strategy. Here we outline the four pillars that are important when trying to achieve the art of the possible:

Perfect Harmony

The goal here is to achieve perfect harmony and collaboration between the three lines of defense: business units, risk and control teams, and internal audit.

Real Ownership

Ownership must come from the business teams because they are acutely aware of the risks and controls and can communicate gaps back to risk and compliance teams.

Easy Proof

Proof of compliance for audit purposes must be easy, accurate and acquired rapidly.

Resilient Operations

Teams need the ability to respond quickly and efficiently to changes in both the operational and the risk landscapes, maintaining compliance throughout.

3 Lines of Defense

An effective risk management program relies on three lines of defense – each with different roles and responsibilities. True success can only be achieved with clear communication across these three teams.

1

First Line: Business Units

Managing Operational Risk

Business units play a critical role in managing risk because they are the closest to the day-to-day processes where risks arise. Let's dive into what technologies can help these teams best meet their roles and responsibilities.

Standard Operating Procedures

Standard Process and Procedure Information helps ensure processes are being executed in accordance with regulations, and in a repeatable manner. This includes ensuring all risks and regulations are documented. Make sure the documents are easily accessible – this is helpful when training and onboarding new team members to ensure they are following established procedures.

Document Management System

A Document Management System acts as a single source of truth where all relevant documents are stored and referenced. You'll want a system that can be tailored to an employee's specific role, and with a robust permissioning structure. This ensures that teams can stay focused on the information that is relevant to their role or department.

Feedback Mechanisms

Feedback mechanisms will provide business units the ability to communicate with internal audit and risk and compliance teams. This means when risks, concerns or gaps in processes are discovered, this information can be communicated seamlessly across the three lines of defense.

2 Second Line: Risk & Compliance Teams

Identifying Risks and Developing Mitigating Controls

The second line of defense creates the policies and procedures that translate laws and regulations into meaningful actions (that need to be taken by the first line business units). From a technology perspective, there are also tools that can help these risk and compliance teams succeed.

Enterprise Risk Management Frameworks

Enterprise Risk Management (ERM) Frameworks provide a structured approach to identifying, assessing, mitigating, and monitoring risks. They can also help teams ensure risks are being appropriately quantified and that mitigation strategies are working. One such well-known framework is ISO 9001. Another is COSO ERM. You'll want the ability to tie the framework(s) you utilize to the actual processes operating the business.

Risk & Control Assessments

Teams also need the ability to evaluate risks and their mitigating controls through assessments and testing. One common form of this is a 'Risk and Control Self-Assessment' or RCSA. These assessments offer a common, repeatable way for teams to understand where the business is exposed and how well protected it is.

Reporting & Dashboards

Reporting and dashboards provide a crucial mechanism for communication between all lines of defense. This should include targeted risk reports like heat maps, the ability to see all the processes (and risks) tied to a particular regulation, and visibility into controls (and their effectiveness) that are mitigating those risks.

3 Third Line: Internal Audit

Verifying That Controls are Effective

The third line of defense ensures that an organization is operating in compliance with both internal policies and laws, and also makes sure nothing goes wrong ahead of an external audit. There are a number of ways to support this effort (and are relevant to the business units as well).

Single Source of Truth

Using a single, centralized repository to store and manage all key process information is critical – this can include processes and SOPs, policies, and risks and control definitions and assessments. This enterprise-wide visibility is important for internal audit because they're not simply looking at one process or department.

Process Mining: Conformance Checking

Process mining – specifically applied for conformance checking - can be extremely helpful in providing proof during the audit process that business units are following processes as designed. It can also help find root causes that explain why processes aren't being executed correctly.

Process Mining: Predictive Analytics

Another aspect of process mining is predictive analytics, which is a type of AI/ML that can establish triggers and thresholds to alert business units to potential problems in the future. For example, it could alert you that you are not likely to meet a GDPR guideline in the future if you don't respond to a customer in a certain time frame.

Putting the Technology to Work

The next step is to bring together all the capabilities and best practices we've covered to create a robust framework for managing risk and compliance. Here we'll examine four key areas where a new approach - and the right technology - can help.

Understand Your Risk Exposure

Discover unmitigated risks and assess non-compliance.

For example, with Process Mining, you can discover where a process is being performed that is not in compliance (or 'conformance') with designed and expected sequences. This includes discovering where key control steps are being bypassed, or standardized process and procedure information is not being followed. In addition, you may understand the number and types of process variation; the different ways the process is performed.

To answer questions like:
Where are we most exposed?
What is the scope of the problem?
Can I prove my controls are effective?

Contextualize Your Processes

Model your business context and record your changes.

With a centralized repository of process information, you can understand where operational risk and control is identified within the process, who owns the process, what regulations or other requirements have been identified, what systems are involved, and so on. In addition, with complete change history on process diagrams and related business modelling information, and complete reporting, all changes are recorded and auditable.

To answer questions like:
How do risks impact the business?
Does the first line know the risks?
Do I have change documentation?

Show Your Progress

Document and report risks, continuously monitor processes.

Extensive reporting capabilities from a centralized repository that defines connections between processes, resources performing the process (human and technological), and risk and control - all tracked and audited as things change - provide a holistic and detailed view of governance, risk, and compliance efforts. Whether that takes the form of 'Heat Maps' for risk, detailed tabular reports, or extensive dashboarding capabilities that allow presenting information in an easily understood and actionable manner.

To answer questions like:
What is the inherent and residual risk?
Who is responsible for each risk?
How are things changing over time?

Get Ahead of the Problems

Simulate regulatory impact and predict risk events.

Using Discrete Event Simulation allows answering 'What If?' questions that include the questions outlined to the right. For example, if a new regulation requires extra effort through a new control, what is the cost of performing those actions? In addition to Simulation capabilities, Process Mining has powerful AI / Machine Learning predictive analytics, enabling you to be better prepared for where current process performance is likely to violate SLA, policy, regulatory, or other constraints.

To answer questions like:
What impact will this control measure have?
What does reacting to regulation cost?
What risk events will occur?

A Proven Approach to Compliance & Risk Management

In this guide, we've highlighted the challenges that heavily regulated companies face, detailed technology that can help, and outlined a better approach to ensuring effective compliance and risk management.

The What:

- Processes are collaboratively modeled and understood the same way
- Risks and controls are brought to the front lines as part of their daily operations
- Risk and compliance becomes an integral part of process design and process improvement

The Why:

- Business becomes operationally resilient
- Narrative shifts from business prevention to business enablement
- Customer sentiment stays positive and financial penalties are avoided
- Business operates in a risk-informed manner
- Audits become faster and cheaper

Process360Live

iGrafx's proven approach centers on three main pillars:

Discover

Discover how your business processes run today

Design

Design the ideal future, compliant versions of your processes

Optimize

Optimize processes for maximum performance

Unlock the Power of Process Intelligence

For more than 30 years, iGrafx has delivered technology solutions centered around business processes – specifically, the continuous optimization of these processes.

Our all-in-one process intelligence platform, Processs360 Live, seamlessly integrates process mining, design, simulation and predictive analytics. Organizations worldwide rely on our platform to improve productivity, reduce costs, and comply with external regulations and internal policies. More than 2,000 global businesses are realizing value with iGrafx.

To learn more about iGrafx's Process360 platform and how process intelligence can help transform your operations, speak to one of our experts today.

Get in touch