eraneos

Whitepaper

Reducing the costs of your (Operational) Risk Management and Compliance

A redesign focused on requirements and control efficiency

August 2023

Content

Is your organization struggling with the rising costs of managing risk and compliance? You're not the only one. There are countless other organizations, especially companies in the financial services sector, that are facing very similar challenges.

Some interesting findings by various research institutes highlight this very issue:

- The budget required for making changes related to regulations has increased by more than 60% since the financial crisis.
- About 40% more banks each year are spending over 5% of their income on compliance costs, and this trend is expected to continue.
- Almost 80% of all compliance costs come from staff-related expenses.

Within Eraneos, we've developed a solution that helps clients significantly reduce the manual operational costs of handling operational risks and ensuring compliance. While this method is primarily developed for the financial services sector, it can also be used in other heavily regulated industries. In this whitepaper, we will share our insights and experience to guide you through this process.

A short summary of the approach:

- Ensure end-to-end (E2E) processes are leading in your Risk Self Assessment Approach.
- Make 'Requirements Engineering' part of your policy-writing efforts.
- Make the policy requirements accessible.
- Link the policy requirements to the systems and processes where they are implemented.
- Use CI/CD and process mining tools to prove the existence and functioning of regulatory requirements.
- Implement meta controls to oversee the continued correct functioning of controls.

In a nutshell, this approach reduces the costs of control efforts, empowers risk departments of organizations to make data-driven decisions, strengthens risk management, and enhances compliance efforts. It opens up new possibilities for improving risk systems, risk processes, and overall risk handling in a proactive and efficient manner.

But first, what are the issues we encounter in the day-to-day risk management practices that we want to address?

Issues in the current way of working

The way things are currently done has some challenges that we've noticed across different organizations and industries. In short, the current way of doing things is labor-intensive, error-prone, and might not be very effective in keeping everything doable and under control.

Here are the four main issues we've observed:

1. Policies

Regulations and strategies can often lead to a ton of policies, standards and procedures, making it hard for the frontline workers (1st line) to know exactly what they need to follow. In banks, for example, the number of policy pages can easily run into the thousands. This leads to mistakes and oversights, especially for those who are new to regulated industries.

2. Controls

The number of controls required to demonstrate compliance and manage risks keeps increasing. To cope, some organizations focus only on high or critical risks, leaving the rest less prioritized. Others create abstract controls to reduce their number, losing the link to the actual risks. This leads to operational errors and interpretations, and makes it harder to prove full compliance with regulations.

3. Adherence

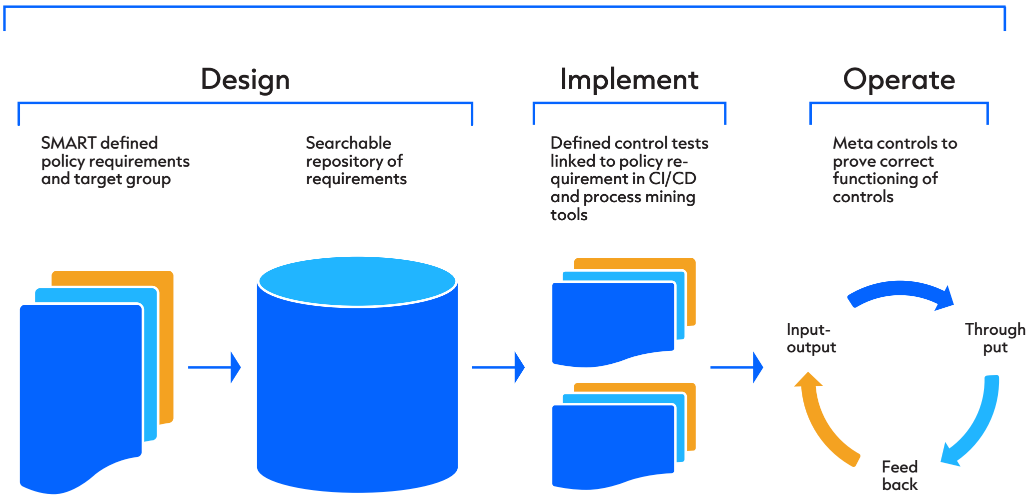
Demonstrating adherence to regulations, especially when regulators visit, is a complicated and time-consuming task, especially when considering the issues mentioned above.

4. Evidencing

Many processes are partially automated, but showing that the controls function properly often requires manual work like taking samples, testing the controls, and monitoring the testing process.

So, how do we solve this? We have a solid requirement, process, and data-driven approach, which we'll explain in more detail below.

E2E process orientation of controls


Design
Implement
Operate
SMART defined policy requirements and target group
Searchable repository of requirements
Defined control tests linked to policy re-quirement in CI/CD and process mining tools
Meta controls to prove correct functioning of controls
Input-output
Through put
Feed back

Ensure end-to-end (E2E) processes are leading in your Risk Self Assessment approach

In big organizations, Risk Self Assessment (RSA) are often done at the department level. While it's great that managers want to be in control of the risks in their departments, this approach can often lead to inefficiencies. The problem is that - at the department level - we might not know if a risk is already being managed or mitigated somewhere else in the process chain. To tackle this, we suggest doing RSAs on an end-to-end (E2E) process level, even though it involves more people.

There are some added benefits to doing RSAs on the E2E process level. We can also use E2E process mining for risk management purposes, aligning it with business process management.

Let's see how this approach delivered benefits in the financial services industry:

Example 1: By doing just one RSA on an E2E process level, one organization reduced 17 controls. Removing the need for these controls saved them between 1 and 2 full-time employees in the frontline. By extrapolating this over their E2E processes, the savings could easily amount to 1 to 3 million euros annually.

Example 2: In a bank, when redesigning an E2E process, we found that each department in the value chain would double-check the work of the previous department. This caused delays of several weeks, leading to low client and employee satisfaction with this process. By removing these double controls, the throughput time was reduced to just a few days, increasing client satisfaction, one-time right processing, and employee satisfaction.

So, by focusing on E2E processes in your Risk Self Assessment approach, you can make things more streamlined and efficient, and ultimately saving time and resources.

Make 'Requirement Engineering' part of your policy-writing efforts

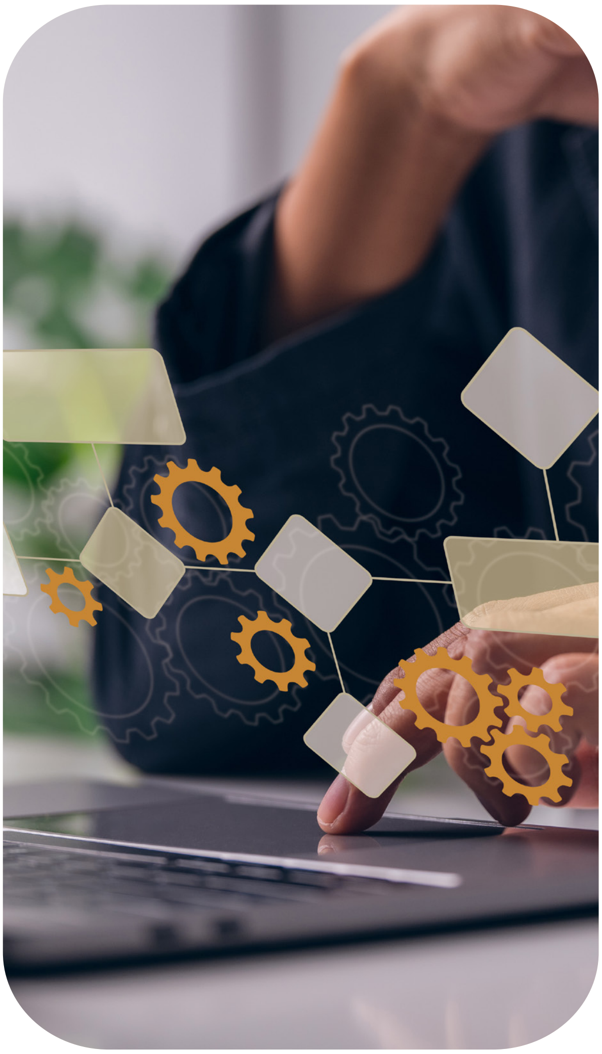
If there is one thing all IT departments have learned since the dawn of digitization, it's the importance of setting clear and unambiguous requirements for any project. The same goes for implementing regulations and writing policies. We know that policies must be clearly written and linked to regulations, but we can make them even better by making the requirements crystal clear. To do so, be sure to stick with the following:

- Ensure each policy rule is defined as a requirement and has a unique identifier. This way, controls and changes can be directly linked to specific policy requirements, making things organized and straightforward (we call these 'control objectives').
- Make certain that each policy requirement has a clear and unambiguous area of applicability. Too often, a requirement is stated to apply to 'the whole organization' or 'all staff,' when it may actually only apply to a specific group like 'data owners'. We'll define unique and precise areas of applicability, which can be a combination of terms like 'shipping clients + credits'.
- Make sure every policy rule is always SMART for the first line. In other words, they're Specific, Measurable, Achievable, Relevant, and Time-bound. This helps the frontline staff to understand and follow the policies with ease.

By incorporating Requirement Engineering into our policy writing efforts, we can create policies that are clear, effective, and easier for everyone to follow.

Discussing SMART formulated requirements

The difference between principle-based and rule-based legislation often leads to discussions during policy writing. Many compliance departments prefer to embed the principles in their policies and leave it at that. While it's correct to state the principle in the policy, all principles should, in our view, also be made specific and measurable and therefore translated into clear, unambiguous minimal policy requirements (including processes to deviate) for the organization. Stopping at the level of principles leaves the interpretation open to each individual and can lead to a multitude of interpretations including the ones you don't want.



Make the policy requirements accessible

Now that we've defined clear requirements, the next step is to make them more easily accessible. The challenge here is not so much about the tools we use to make a repository of policy requirements, but rather the culture within the second line (the people overseeing risk and compliance). To make requirements accessible, the second line needs to put themselves in the shoes of the first line (the frontline workers) and think like them.

Let's offer an example to illustrate this point: Imagine we create a policy about recovery and resolution, which is something that only applies when a bank is almost failing in Europe. The first line participants might not even know this policy exists, as they are not directly confronted with it in their day-to-day work. So, even if there's a requirement relating to their processes or data hidden in that policy, they won't know to look for it.

To overcome this, we need to add tags to the repository of policy requirements. One way to do this is by using the standardized area of applicability we mentioned earlier. This helps in categorizing and searching for specific requirements. Additionally, we should consider what changes the first line is making in their work: Is the policy requirement related to a system, a process, a product, and so on, they are changing? By adding these change categories as standardized tags, it becomes much easier to search for and find the relevant requirements.

In a nutshell, we want to make sure the requirements are not only clearly defined but also easily accessible to the frontline staff. By using tags and standardized fields, we can bridge the gap between the second line and the first line, making compliance and policy adherence a smoother process for everyone involved.

Example:

Let's assume that the first line is changing a system by showing in the application a field containing personal data. Suppose, in this example, only the system and not the process is changing, the process requirements are not relevant for this change, only the system and data (privacy) requirements. Selecting policy requirements for systems and for data (privacy) is thus sufficient.

The second line should apply this kind of structuring to make these requirements better accessible to the first line.

Link the policy requirements to the systems and processes where they're implemented

When we implement a policy requirement in a system or process, it's crucial that we are not only able to demonstrate that it has been designed and implemented correctly, but also that it is continuously working as intended, even after many changes have happened over time. This means we need to keep track of the connection between the policy requirement and the system or process it's applied to.

At first, many organizations might think of using tools like Jira or Confluence for this purpose, which makes sense from a change management perspective. However, these tools won't show if the control is still functioning correctly after later changes; they will only confirm that it's been designed and implemented.

We believe a better solution is to register this link either in a CI/CD (Continuous Integration/ Continuous Deployment) tool for fully automated requirements, or in a process mining tool like Celonis for process controls with manual, human actions.

Once the control is linked to the policy requirement in one of these tools, we can use it after every change to prove that the control or requirement is still working properly (known as integration testing). These tools will generate evidence, which can be summarized and automatically uploaded into, for example, a GRC (Governance, Risk, and Compliance) system as proof of operating evidence. This way, we not only prove the design and existence of the requirement but also its continuous and correct functioning.

If a requirement is not correctly implemented or a control is not functioning as it should, of course, we need to halt the go-live of the change or have it go through a formal risk acceptance process. With the solution mentioned above, your GRC tool can be automated to signal when such action is required.

By linking the policy requirements to their implementation(s) using the right tools, we can ensure that our policy requirements are met and prove correct functioning by monitoring our controls efficiently.

Meta controls to oversee the continued correct functioning of controls

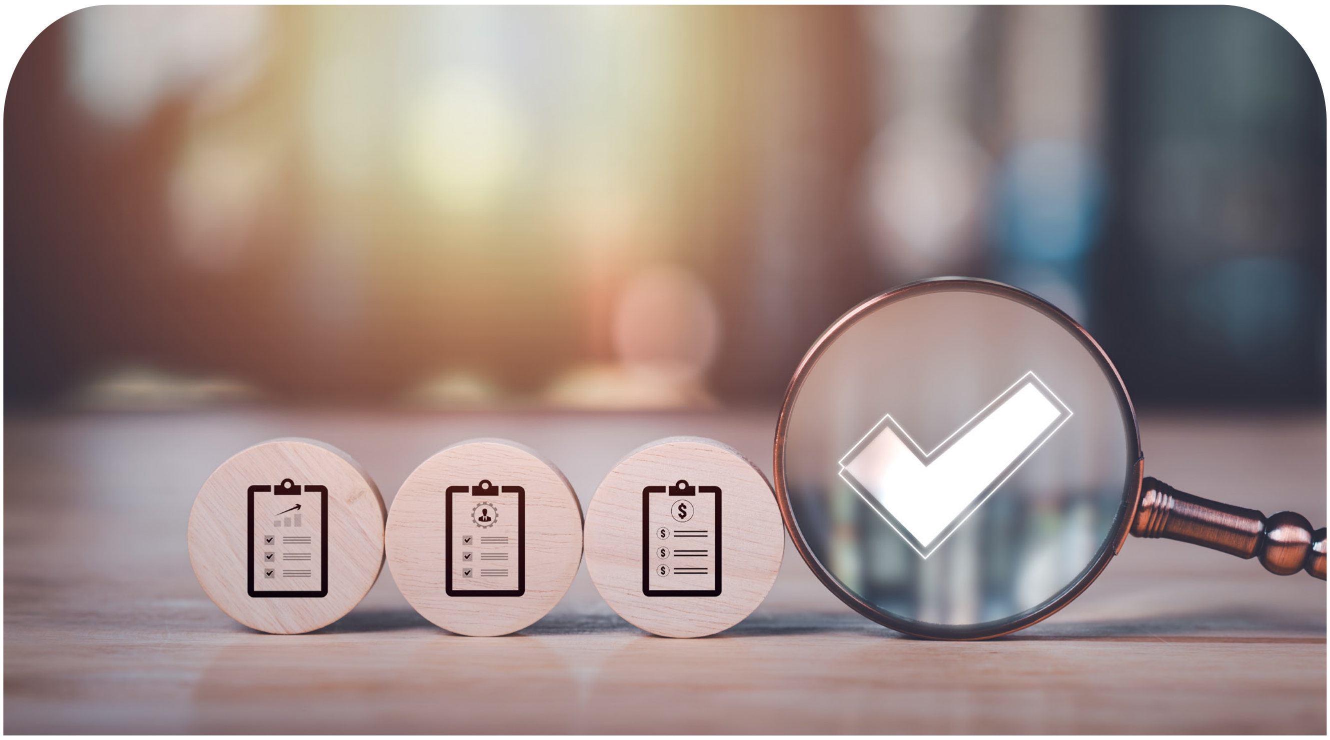
In day-to-day operations, it is a fact of life that things go wrong sometimes. For example, to make a process faster, someone might bypass a control. Or a program might stop working correctly, causing an automated control to fail. And there could be cases rejected by a control, but no one takes care of fixing them. So, how do we prove that controls are actually working without checking each one individually?

Well, there's a simple solution: we can use a set of generic meta-controls for the controls and requirements. Here are the most important ones:

- Input-output comparison: This control checks if the number of cases that enter the process matches the number of cases that go through the control and come out as output. We can automate this verification, and if there are any differences, it's a sign that we need to investigate further.
- Throughput: For process controls, we'll make sure that the steps are performed in the correct order. For instance, doing a 'four-eyes' control on a transaction after it's already executed undermines the control's effectiveness. Process mining can help us spot this. For automated controls, we'll check if the program is working properly, and if it's malfunctioning, we'll figure out which cases might be impacted.
- Feedback: This control verifies that cases rejected by a preventive control are corrected within an acceptable time frame. It can also check if the cumulative risk for a client or country stays within a predetermined limit. We can automate this too, for both automated and process controls.

By applying these generic controls to observe the operational functioning of controls, we can provide evidence that the controls are doing their job properly. In other words, we can confidently say that they are functioning correctly.

These generic meta-controls also make it easier for us to monitor their effectiveness in day-to-day operations.



Additional added value of this method

Apart from a reduction in controls, there are several additional benefits to organizing your control monitoring and testing as described above. Here are a few:

- A focus on the subjective element: risk managers can now concentrate on the parts that involve subjective judgment. For instance, in the financial service industry, defining a 'high risk client' might vary from one case handler to another, so an independent risk or compliance view is still essential.
- Quick feedback on daily operations: When using process mining tools and automated testing in CI/CD, the frontline employees can get feedback on errors in daily operations without much delay. This feedback can be fed directly to the frontline staff (first line), unlike traditional risk reporting, which often takes weeks or even months after cases are closed.
- Standardized and automated evidence reporting: With standardized evidence reporting, there's less room for different interpretations, and we can perform data analysis more effectively.
- Time savings for regulator visits and deep dives: During onsite visits by regulators or in-depth assessments by the third or fourth line, this approach saves a significant amount of time as adherence can be easily demonstrated.
- Proactive communication on requirement changes: If a policy requirement changes, the second line can now inform the relevant parts of the first line, like the application or process owners. With the approach we have described above, it is exactly known in what system, processes, products, and so on, a requirement is implemented. This ensures that all relevant staff know where and how the new requirements should be implemented, as well as monitoring this implementation.
- Data-driven risk management and compliance: By storing evidence in a standardized and accessible way, risk management and compliance can now use data analysis to identify anomalies and improve various aspects related to risk and compliance. For example:
  - Analyzing where policy requirements are implemented and where they are missing in systems and processes, and checking for any gaps by means of the 'area of applicability'.
  - Identifying processes with the most repair cases and understanding the reasons behind them.
  - Assessing knowledge and behavior within teams, for instance, if certain teams require more retests around controls, suggesting additional training, or having a risk manager attend their sessions to increase knowledge.

Can this solution always be applied?

Of course, this approach isn't a silver bullet. There are still some areas that will continue to require old-fashioned sample taking and manual testing and monitoring. Here are a few examples:

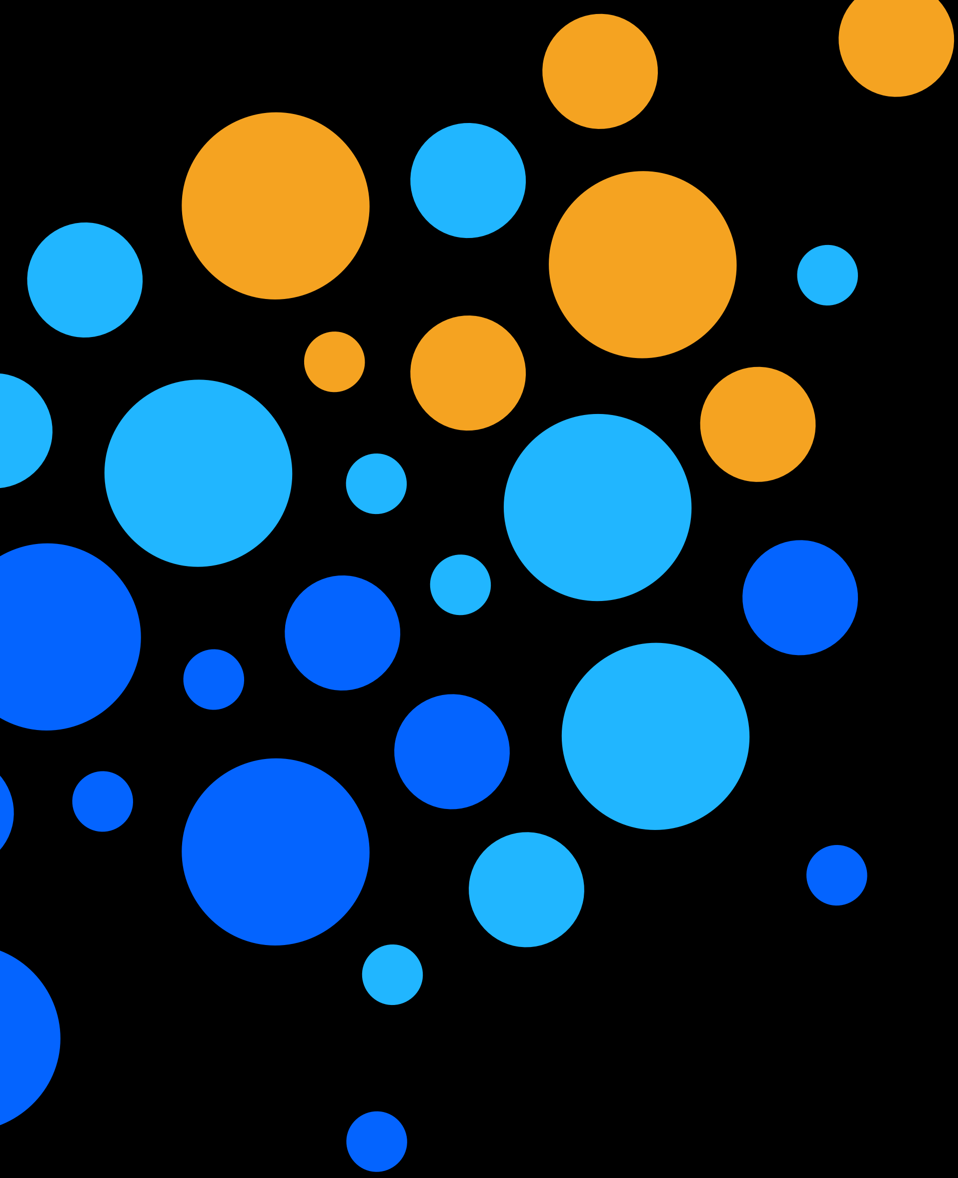
1. Purely manual processes without any system support or workflow tools, as well as most governance-related controls.

2. Controls on outsourced processes. While the outsourcing company is still accountable, they mostly have no direct control over the controls and implementation of the requirements in the organization of the contractor. The outsourcing company can rely on assurance reports, but analyzing them often involves manual work.

However, even with these relatively obvious limitations, the approach described above is still highly valuable. It brings cost savings and improves the overall quality, making the effort worthwhile. And while it might not be a one-size-fits-all solution, this approach also offers a plethora of benefits when it comes to efficiency and quality improvement for risk management processes.

Author:

Erik Zoetmulder
Senior Manager – Financial Services
erik.zoetmulder@eraneos.com



eraneos

Experienced in a wide range of industries

ABOUT ERANEOS

As a global Management & Technology Consultancy Group, Eraneos supports organizations in not only designing but successfully implementing a future-proof digital transformation strategy that can make an ever-lasting impact.

By listening to what businesses want and understanding their needs, we can fast-track and embed transformation with ease by aligning people with technology, processes and leadership, effortlessly.

Knowing your industry, technology and local context alongside a global perspective, gives us the advantage you need to succeed.

It's this deep understanding that enables us to shape and implement strategic transformation within your organization while providing the best service. That's why our customers trust us with even the most complex of challenges, from strategic digital transformation in finance to the ethical application of A.I. in healthcare.

We don't just listen to your needs, we understand them. We're more than ready to help you realize your potential in the digital age.

Contact us >

Our offices >

Visit our website >

eraneos.com