ISOPlanner

Compliance Automation for Information Security

PUBLISHED BY ISOPLANNER ©2023/2024

Contents

Introduction

Automation offers more and more opportunities for organizations, such as **optimizing work processes**.

Ensuring that automation meets the relevant laws and regulations (compliance), can create **scalability issues**.

Especially when compliance is **not an integral part** of it.

In this white paper, we discuss how compliance can become an integral part of automation, which **conditions** apply, and which **best practices** are applicable.

Compliance

The trend in politics and the market seems set: organizations need and want to meet more and more **compliance frameworks**.

Consider legal obligations (e.g., GDPR) and other regulations (e.g., NIS2). These **new requirements** work their way down supplier chains.

For example, many obligations require that a company not only have its own **data in order.** But organizations further down the chain have this as well.

Therefore, if organizations are not certified (e.g., SOC-2 or ISO27001), it becomes increasingly **difficult to do business**, especially with the larger clients.

While this presents challenges, especially initially, compliance in the area of automation also provides **benefits**. Both for the organization itself and socially.

Information security is better implemented and monitored, thereby **better protecting** the **confidential data** of companies and citizens.

Organizations also reduce their risks and thus the risk of fines. The challenges for organizations are:

- **Increasing burden on employees** to comply with compliance.
- **Rising costs** due to increased manpower requirements and/or procurement of services.
- **Increasingly complex information** for decision making.

Automation

In recent decades, organizations have been growing along with the opportunities offered by automation.

Productivity increases and human **error** can be **reduced**. There are plenty of other benefits (and drawbacks) that we overlook here.

In terms of information security, we see that implementation of most forms of automation comes with **increased complexity**. Both in infrastructure and processed data.

The number of applications and integrations increases, **increasing the surface of attack**.

Or **more confidential data** is processed (for example, personal data or intellectual property).

This leads to the following challenges:

- **Increasing burdens** (in both time and knowledge) to manage the IT landscape.
- Information security **risks** are increasing.
- **Dependence** on suppliers is increasing.

Interplay and consequences

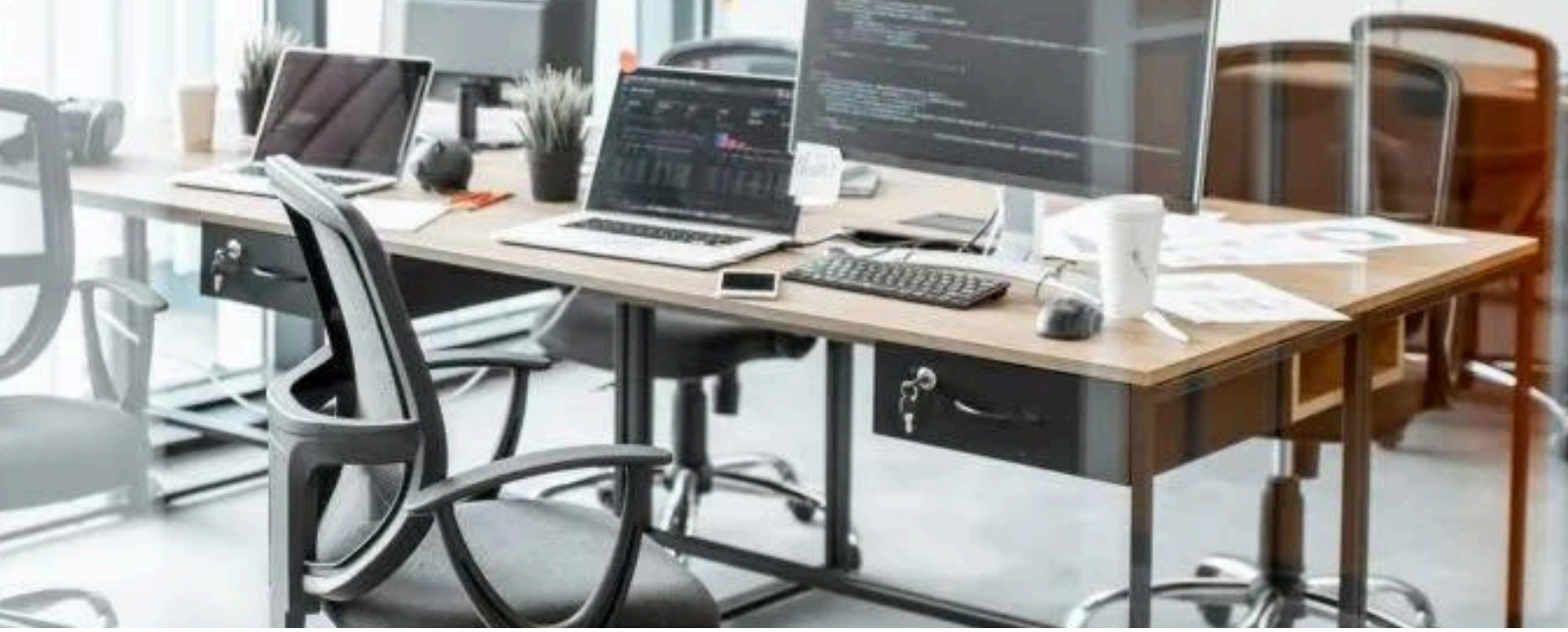
The interplay between compliance and automation is multifaceted.

Suppose an organization chooses to automate a **process with a software (SaaS) vendor** that processes sensitive data. This increases dependence on suppliers and increases the burden of verifying that those suppliers are compliant.

Or an organization wants to save **travel time** by allowing employees to work more remotely. Implementing the necessary IT infrastructure increases costs and increases information security risks (think of laptops getting lost). It is also becoming increasingly difficult to create policies on what employees may or may not do remotely.

Thus, compliance is seen as extra work that increases (linearly) with the degree of automation. After all, anything automated must also be compliant. Otherwise, an organization will lose its certification or worse. If so, then **compliance is not scalably implemented**. How can an organization recognize this?

- Compliance is implemented as a **manual action** with employees.
- Employees receive a **lot of training** to properly perform their manual actions.
- **Root cause analysis** of incidents mostly points to employees.
- Lists and actions are maintained in **Excel**.
- Use of software solutions increases workload or is **perceived as cumbersome**. If the number of compliance frameworks also increases, manual work may even increase exponentially.



The benefits of compliance automation

Automation of compliance particularly provides a benefit in **saving time and reducing risk**.

It relieves employees of (repetitive) work and prevents errors.

In addition, the following additional benefits arise (source):

- **Consistent digital experiences** for all users.
- **Less training** is required for employees.
- **Faster decision-making** due to better information.

To realize the benefits, an organization should make compliance an integral part of automation. Both project-based and in operations-based.

An integral approach for organizations worth considering:

- **Include compliance in the project**. Reserve time and knowledge so that the aforementioned interaction is addressed during the project.
- **Automate manual compliance steps** from the beginning by including them in the design. This also saves time for the compliance department afterward.

- **Consider what impact compliance has on operations**. Are changes in work processes necessary? Inform affected teams as soon as possible.
- Many compliance frameworks require an updated risk register. **Explore and address project risks and organizational risks**.

Organizations may also have processes that are not automated or run on legacy systems, that need to be compliant.

In these cases, compliance automation makes less sense but can still **increase scalability**.

Consider an automated reminder to check the paper filing cabinetfor expired retention periods. The more papers the more work but handling the **resulting incidents** can be **automated.**

Besides the integrated approach, the way compliance is automated is very important in its ultimate effectiveness.

Prevention of making mistakes (being non-compliant) is very important in **reducing costs and risks**. Also, control remains important as a safety net.

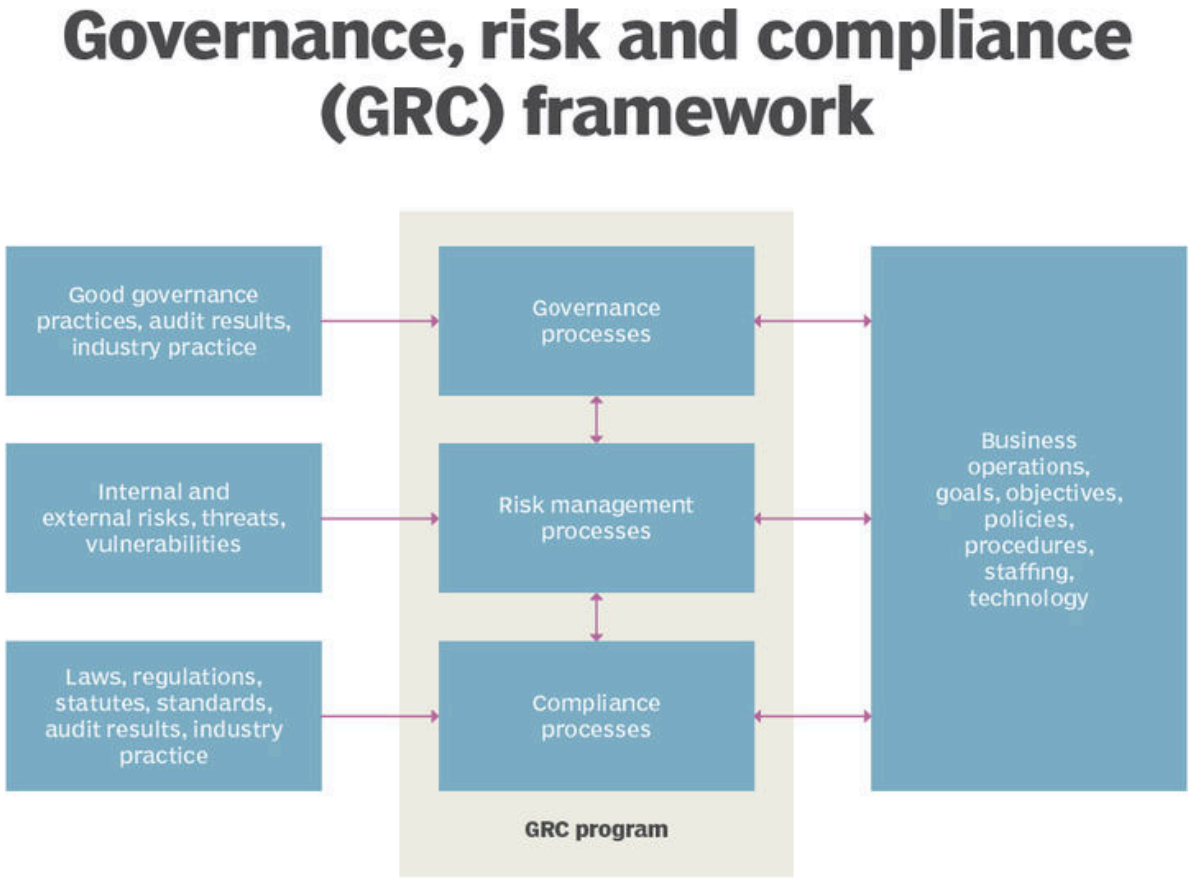
And everything must be auditable: building a record deserves attention, otherwise, there will be a **high workload just before the audits**.

The conditions you can put on the automation of compliance are:

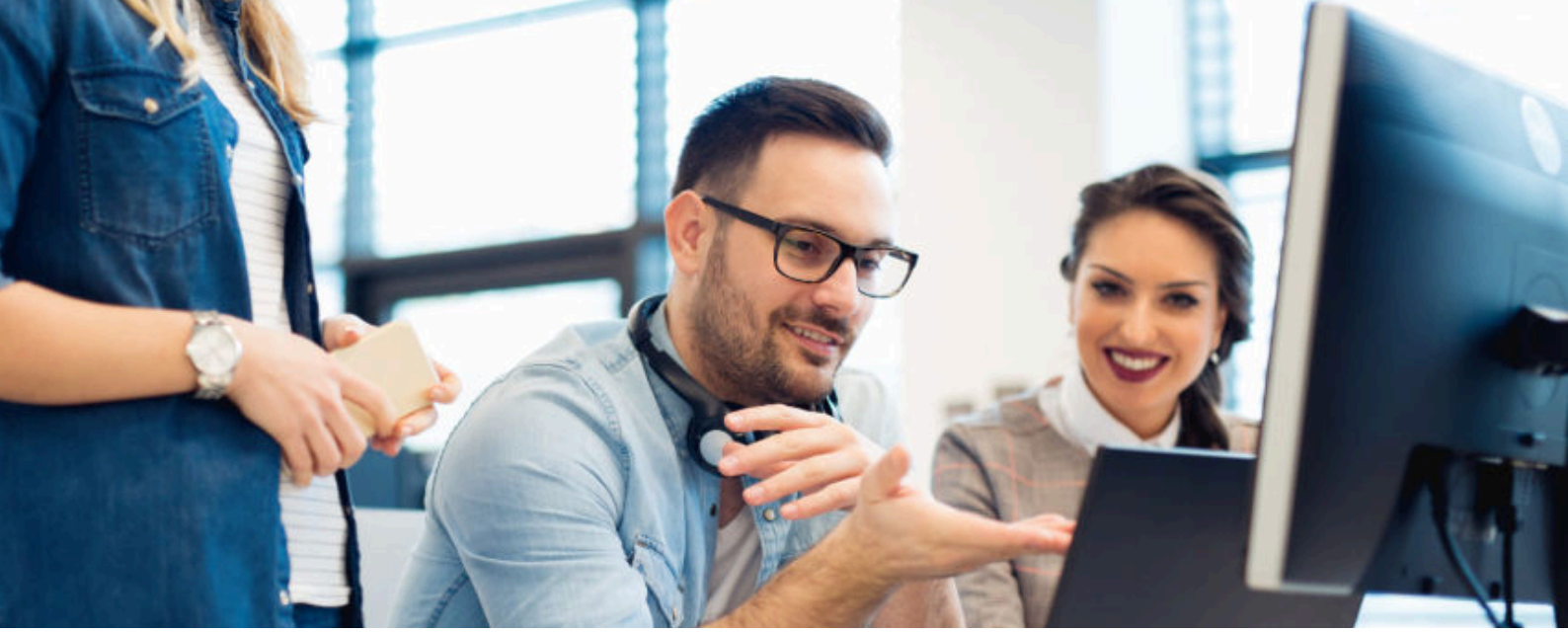
1. **Compliance controls should be built into automated processes.** This eases the burden on employees and saves costs in the future. Employees begin to see compliance as part of their work rather than extra work. Employees receive instruction and guidance during the process wherever compliance is required. Notably, the preventative effect ensures that the investment in automation is recouped (source).

2. **Detection of deviations.** Detection of compliance deviations should occur automatically and in response, the incident management process can be initiated. Automatic retrieval of compliance check status and supporting evidence saves a lot of time.

3. **Building Records.** Organizations must demonstrate compliance. Automated actions must be logged with supporting evidence. Presentation in a clear file for the (internal) auditor saves time and thus makes the audit process more scalable. If the file is incomplete or not reliable, the burden on the (internal) auditor actually increases.



Source: techtarget.com

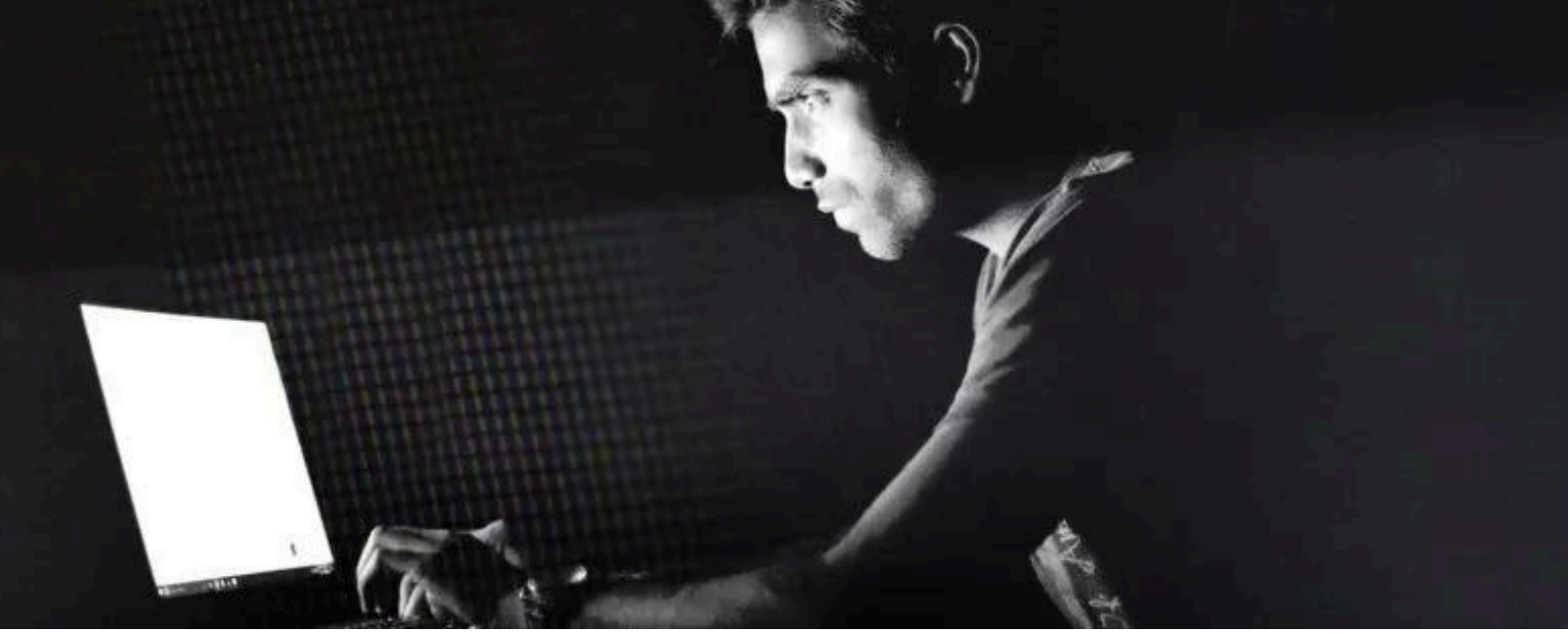


Risks

Implementing compliance automation is subject to the same challenges noted above as other automation.

The benefits must outweigh the drawbacks, and a **risk-based test** makes sense. To reduce risks, organizations can follow the following recommendations:

- **The automation solution processes compliance data that may be sensitive**. If that data is not shared with a new vendor, except perhaps for statistical purposes, this reduces risk and cost in vendor management.
- **Determine which compliance process is most at risk** or places the most burden on employees and start a pilot with it. Measure the cost of automation and contrast that with the benefit (payback time).
- **Automate in a way that makes it more simple for the user**. Help employees remember when compliance should occur, explain why they are doing it, what their responsibilities are, and help employees implement it (source).



Generative AI

Much is expected from this technology in automation in general. In terms of information security, AI already plays a big role, especially in **detection**.

Generative AI is very useful for threat detection in **large amounts of data** such as log files. When it comes down to automation of manual steps, generative AI makes less sense.

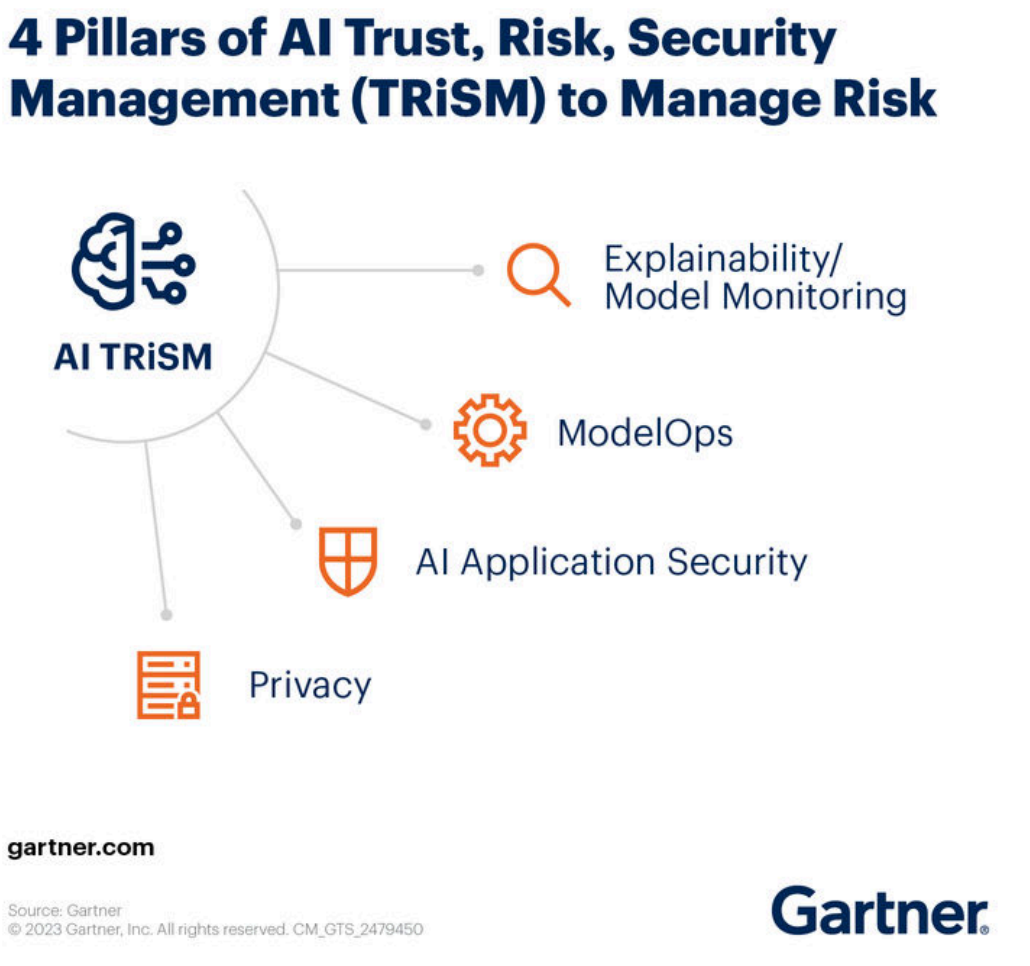
Of the manual steps to be automated, clear requirements can be written down. A deterministic automation may be better, it won't introduce the **additional risks** of AI doing incorrect actions or answers.

Generative AI can reduce the burden on employees in terms of **knowledge and administration**.

For example, consider summarizing all root cause analyses for executive review. Or **answering questions about exceptions** that are not automated by the process.

AI also seems useful for **gaining knowledge** about new compliance frameworks. For example, about the complex overlap of these frameworks or their implementation.

Caution is needed with this technique which is still **in its infancy**. To introduce as few new risks as possible, implementing TRiSM in AI models seems a good direction (source).



Source: gartner.com

1

Case

Implementation capacity management for ISO 27001

Once the policy is in place, evidence can be collected automatically. How? By retrieving the available space. For example storage on servers and databases and memory/CPU usage **via an API**.

If this data is retrieved via a fixed interval and stored in the control A.8.6 file, 1) the auditor can **monitor** this and 2) this can **generate an alert**.

For example, if the value goes above or drops below a set level.

With a follow-up link to this - for example, creating an action for the right employee - it **saves even more time**. Or even automatically increasing capacity based on a preset policy.

Don't forget to determine whether the ever-increasing automation makes sense in terms of **costs and benefits**.

This is an example of **reactive** automation.

2

Case

Assessing new suppliers

When an employee creates a new (critical) supplier in the ERP system, it is possible to start a workflow that contains **built-in compliance checks**. This engages the employee and enforces a consistent process.

For example, include a step that passes information security requirements **directly to the appropriate employee** who performs the review.

After completion (or automatic retrieval of a proposal), the **result is automatically evaluated** based on preset policies. In case of deviation, the possible inclusion of an escalation step is possible.

The result is **included in the file** for the auditor who oversees whether the processes have been executed according to policy.

The final step is to automatically approve the supplier to receive payments.

This is an example of **preventive** automation.

Conclusion

Automation of compliance provides value to the organization if current compliance processes are not implemented with sufficient scalability.

An automated integrated handling of compliance **emphasizes prevention**. Compliance checks are built into the processes. Subsequent checks are also automated.

The documentation of these processes is embedded in the system so that it can be demonstrated at **any time** that the organization is compliant.

As a result, **employees save time and make fewer mistakes** leading to **fewer business risks**.

ISOPlanner

With Compliance Management solution ISOPlanner, it is possible to implement compliance automation that meets these three important conditions.

1. Preventive

Because the system is **integrated into Microsoft 365**, it schedules tasks as appointments in Outlook and shares knowledge via Teams and SharePoint. The system also creates workflows in Power Automate (and similar solutions such as Zapier).

It is possible to **flexibly** integrate compliance checks into (part of) the work process. As a result, the operation experiences automation as easy and approachable.

Compared to other software solutions - where people often have to log into other systems - employees are already familiar with Microsoft 365 and often already have Outlook and Teams opend. As a result, **training is nearly unnecessary**.

2. Reactive

ISOPlanner **retrieves compliance data from other systems** and compares it to policies.

It **issues alerts** or starts new workflows based on thresholds. **Dashboards** show the current compliance status.

Compared to other software solutions, the advantage is that the confidential compliance data is only processed in the organization's protected Microsoft environment.

With this **low-risk profile**, it is conceivable to roll out solutions immediately after the response. For example, automatically increasing capacity in previously mentioned example about capacity management.

3. File

Since ISOPlanner has a task system that also **supports repetitive tasks**, it is possible to include all collected data in the **overview of tasks**. For example, performed process steps and evidence. And then view those tasks from different angles, from a process, risk, or measure point of view.

This provides a **clear picture and clear timeline**, without dependencies on external task systems.

This allows an (internal) auditor to quickly check if compliance is executed **consistently throughout the year**.

ISOPlanner simplifies ISO compliance with an easy-to-use solution for Microsoft 365

Want to become and remain compliant with ISO standards with an easy-to-use software solution?

Start Free Trial

ISOPlanner

More than 300 companies rely on ISOPlanner

LEVEL SOFTWARE & CONSULTANCY

SPIE

sales manager

FinData