nagarro

Compliance Now

SoD Decision Guide

Scope and Impact of Segregation of Duties (SoD) in an SAP environment

Table of contents

Introduction

This is an overarching guide to help you navigate the complex world of tool selection, use case identification, implementation processes, and discussion of special considerations in relation to SoD tools for SAP. It aims to offer insights and knowledge to enable readers to make informed decisions about the tools they choose and discover how to set up the organization to use the tools efficiently.

By reading this e-book, you will be aware of the factors you need to consider when selecting and implementing tools and be better equipped to make informed decisions, aligned with your goals and objectives. This e-book is specifically designed to help those who are looking to mature their risk management process with an SoD tool and navigate through complexities of the process. By covering special considerations and providing guidance on typical areas of confusion or debate, it aims to make the project feel more manageable and approachable for anyone looking to make informed decisions about their toolset.

Through the e-book, you will learn about the key considerations that you should consider when selecting and implementing tools and the potential pitfalls to avoid. While the e-book cannot cover every detail in depth, it offers a valuable starting point and an overview of the most important aspects to consider.

We have followed a logical structure based on what we observed our clients go through when undertaking an SoD project in ComplianceNow. We have focused on things to consider while selecting a tool and how to build a business case internally for the tool. The book then segues into a technical discussion on implementing an SoD tool, avoiding potential pitfalls, and navigating the SoD tool project to success.

Introduction to Compliance Now

ComplianceNow is an innovative product division of Nagarro, providing high-end SAP compliance solutions to improve the productivity, efficiency, and transparency of compliance processes in companies and organizations running SAP. Our goal is to innovate, build, and deliver proven compliance products that will make a difference to our customers in their efforts towards managing the wide-reaching system complexity while adjusting to the ever more restrictive governance standards on the path to compliance. The product suite includes components supporting areas such as internal control, segregation of duties, authorization testing, and compliance analytics.

Proactive Risk Management

Access Control

- SoD mitigation in SAP
- Preventing workflow
- Fast implementation/ Low operation costs

Privileged Access Management

- Self-service firefighting
- Audit & logging
- Audit management process

Internal Control

- Centralized internal controls
- Control library - SoD risks
- Workflow & logging in a trusted system

Compliance Operations

Authorization Process Manager

- Remove project risks
- Reduce testing time by 75%
- Improve quality and satisfaction

Usage Monitor

- SAP Access analysis
- Enable data-driven decisions
- Optimize & reduce costs

Password Reset

- 24/7 self-service
- Lower admin costs
- Improve user experience

Your Assurance

- SAP certified any-premise & ext. cloud
- ISAE 3402 Type II Certified

Handholding Trough Installation

- Hosted/On-premise
- Fixed price installation support
- Full CN Suite installation in 2 - 3 weeks

Facilitated Adoption

- CN specific extended services
- CN devoted managed services

Low Total Cost of Ownership - Why?

- Fair pricing
- Dedicated support center in DE/DK
- 3 yearly releases with updates & innovation

What is Segregation of Duties

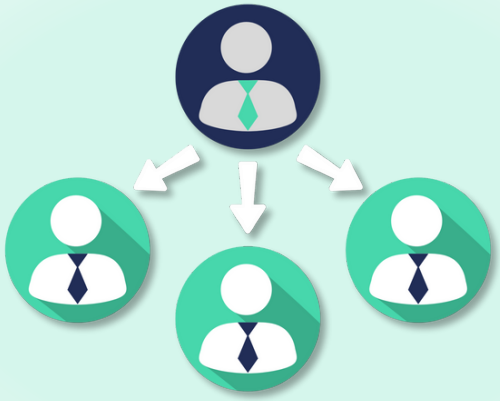
When discussing Segregation of Duties (SoD), we must first talk about risk, as we are trying to manage and prevent risk. To that end, we can briefly discuss what constitutes a risk in our world.

In essence, a risk in SAP is anything that can destroy, negatively impact, or disrupt processes in the business. This is a rather broad definition, and risk assessment and evaluation depend on the individual business, as the severity of risk can vary between companies.

The problem with risk identification is that what constitutes a risk can stem from either a combination of accesses (SoD risk) that can be used to instigate a malicious/negative event, such as fraud, or it can stem from critical access. Critical access is a single-sided risk, meaning that the access itself is a risk, not a risk due to a combination with another access. These two categories broadly summarize all risks in SAP – critical access and SoD risks. Unsurprisingly, what we focus on with an SoD tool is SoD risks. However, the SoD tool also impacts critical access, but we will return to that subject.

Segregation of Duties Definition

- **Segregation of Duties (SoD)**
  - SoD is an internal control created to prevent risks such as error and fraud, by ensuring that at least two individuals are responsible for separate parts of a particular business process.
- **SoD involves**
  - Breaking down tasks within a process, which could feasibly be accomplished by a single person, into multiple tasks to ensure that no single individual carries sole responsibility and control.



The fundamental goal of SoD

The fundamental goal of the SoD process is to remove risk by separating processes and handing out the different parts of the task to different people so that one individual cannot manipulate and misuse a process. SoD risks are challenging to manage due to several reasons. Employees tend to accumulate access over time, and keeping an overview of who has what without a tool is close to impossible and not realistic. Additionally, when adding accesses to a current employee, you are always at risk of suddenly creating an SoD risk if you have no tool that runs a background risk analysis on the role combinations. Further, the deep complexity of what is in each access on an object field and values level is too complex an analysis to handle without a tool.

As mentioned earlier, a portion of risks are what we call critical access or single-sided risk. The problem with critical access is that we cannot segregate the risk away because the risk is inherent in a single given access. We also cannot broadly remove the access from all employees, because then there are one or more tasks that simply cannot be performed, which paradoxically would be a potential disruption to the business process – the very same problem we are trying to prevent! So, how does an SoD tool and critical access fit together?

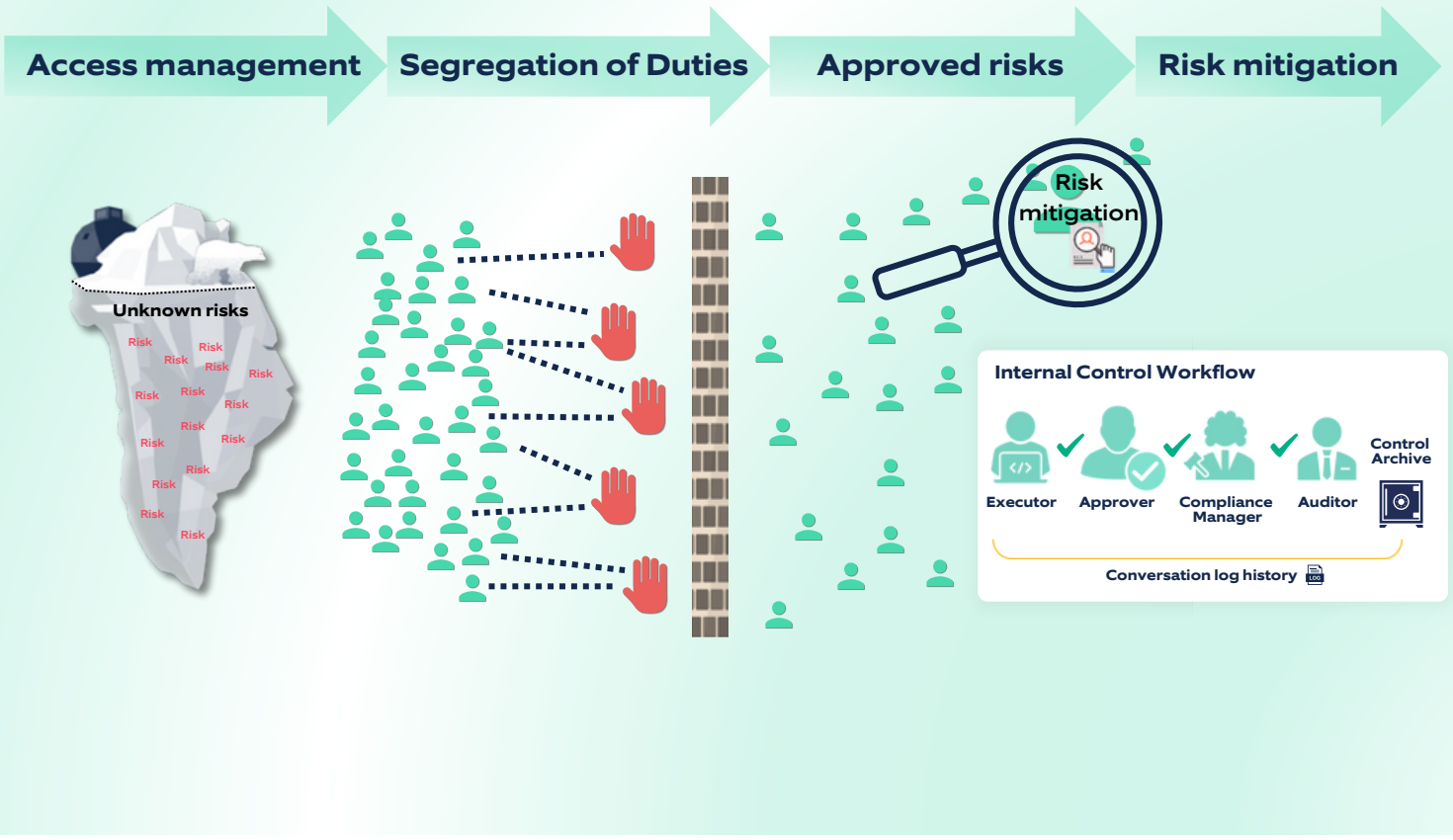
Apart from preventing risk by enabling the ability to segregate access, an SoD tool also provides an overview and transparency of the risks in the organization and which employee(s) have the risk. Transparency of who has critical access is exactly how SoD tools and critical accesses interconnect. Having a full overview of who has the critical access enables the ability to remove it, should the employee in question be evaluated to not require the access. Removing critical accesses from employees who do not need them would already reduce the pool of single-sided risks in the organization. The remaining critical accesses that are not removed are still a risk, but with an SoD tool, they are known risks. Having transparency and knowing your risk situation is a huge advantage, as you can only prevent and mitigate risks you know exist. The organization can mitigate the risk of critical access by implementing controls.

What is Segregation of Duties not?

Mitigation is a topic that should be touched upon when talking about what SoD is and what SoD is not. Mitigating controls are a related part of the SoD tool and process. Controls should mitigate risks you cannot prevent by segregating them away. The risk that you cannot segregate away can be SoD risks where an employee needs accesses that, in combination, constitutes a risk to perform their job, or it can be a critical access that, as mentioned above, can only be managed by an internal control.

By implementing control on the risk, you can ensure that the employees with the critical access or SoD risk have not used it maliciously. An example could be the combination of the ability to post payments to vendors and creating bank and maintaining bank data. This combination allows you to create a fictitious account and post vendor payment. If an employee needs to have both of these to perform their job, there should be control in place to manage the risk. This control could be a four-eye principle, meaning that a colleague (often a superior) should approve whenever both accesses are used for the change to be enacted. This will mean that while the risk might not be prevented, it is mitigated, and your organization has still managed the risk.

To sum up, mitigating controls are part of a good risk management process and can help diminish risks by mitigating accepted SoD risks and critical access. However, mitigating controls in SAP is not directly a part of an SoD process or SoD tools but is closely related. In combination, an SoD tool and a well-established mitigating control process can be seen as two halves of a good risk management process, and internal controls is a logical step to take either in combination with an SoD tool or as a natural next step.



How to build a business case for SoD tools?

Investing in compliance and risk management tools is exactly that – an investment. Risk exists in an organization regardless of whether you handle them or not – but we promise you that having a strategy and dealing with risk is a lot less costly than not handling risk preemptively.

If you think compliance is expensive, you should try non-compliance.

Building a business case for compliance and risk management can be difficult at first glance. After all, the payoff of risk management tools is to prevent and minimize unknown and not yet existing costs. But is this true? No, there are benefits besides removing potential costs.

Only some areas we can look at are directly translatable to monetary costs and benefits, making it difficult to measure. Furthermore, there are two sides to a good risk management strategy: handling the problem areas today and setting up a mechanism for handling tomorrow's problems. Because risks will exist, and new risks will emerge. Risk management is not about fixing all the issues at a specific moment in time, it is about enabling your organization to manage, mitigate, and prevent risks as they emerge over time. In other words, compliance is never a finished project, so investing in good tools and processes will give your organization returns on investment over time due to risk reduction, and continuous returns due to efficiency gains in risk management.

This section will help you understand and build a business case for SoD and enable you to make the benefits more tangible for you and your organization.

Risk management is not about fixing all the issues at a specific moment in time, it is about enabling your organization to manage, mitigate and prevent risks as they emerge over time.

Potential hurdles to the SoD project

In this e-book, we argue that SoD tools are important and should be a priority for all companies. But before we can dive into how one could build the business case for an SoD tool, we have to explore why there might be a push-back. After all, there must be some reason why everyone doesn't have an SoD tool implemented already – so, counterintuitively to the topic of this e-book, we would like to shortly dive into why some companies experience pushback regarding the implementation of an SoD tool. When building the business case, it is important to understand why some management might expect a negative impact or, in some way or the other, are against the implementation of an SoD tool.

First, the potential risk that has yet to turn into actual incidents is an invisible problem. This, of course, does not make it any less of a real problem, but this is one reason management might need help prioritizing it.

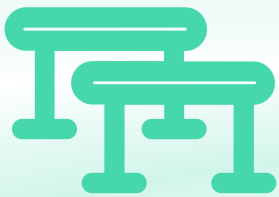
Secondly, management might believe that their current control and risk management processes are perfectly fine and that there is no reason to change anything. In other words, the current practices can be lacking, but the consequences have yet to reveal themselves; therefore, the current practices are deemed sufficient. Paradoxically, low maturity of risk management also has hidden consequences, as it is only a high-level maturity risk management practice which brings transparency to the organization.

Thirdly, there is the question of performance and flexibility. When you have no Segregation of Duties, everyone can cover for each other, and if people are out sick, on vacation, etc. the flexibility allows for everything to run smoothly. This is of course without a doubt also a performance benefit, but a security issue.

Lastly, there is a question of uncertainty regarding the cost/benefit of an SoD tool. This is of course, always something that is questioned when evaluating whether to undertake any project, but especially in the case of SoD tools, a lot of value does not spring to mind for many people. Therefore, SoD tools are often judged on very few parameters, creating a false evaluation of the SoD tool, ultimately leading to the project's abandonment. The subsequent chapters in this section of the e-book will try and cover the most important aspects of how an SoD tool delivers value and how you can utilize these points to build a business case for an SoD tool that correctly includes all important parameters to make a well-educated evaluation of SoD tooling.

Typical hurdles for SoD projects

- **Problem not visible**
- **Current practice consequences not yet revealed**
- **Don't want to lose flexibility**
- **Cost/benefit uncertain**



Reputation & trust

While it is difficult to ascribe value to it directly, reputation is important in business. Reputation fosters trust, and trust creates better client relationships and better public relations. Fraud and mismanagement of assets can reach the public, harm the public's trust in your company, and directly influence your business performance. On the other hand, having a spot-free record and advertising a high governance, risk management, and compliance (GRC) standard can boost trust and serve as a marketing tool.

Furthermore, there is also a client and partner perspective. Think about what type of company you would like to have business dealings with – probably one that is committed to protecting your data and does not represent a potential liability.

A company with a mature and good GRC strategy can more easily retain and acquire clients and partners and can dissuade public mistrust.

Efficiency gains

Efficiency gains are a huge benefit of investing in GRC and can easily be communicated in a business case. Implementing SoD (and, in general, GRC tools) allows for centralizing your GRC control. It allows you to create standardization and consistency in risk assessment, prevention, mitigation, controls, and documentation. This removes many inefficiencies in processes, breaks down informational silos in the company and reduces events that can interrupt the business processes. This approach starkly contrasts with the risk management of a less mature organization. These companies will often handle everything in Excel. They will often be driven by varying departmental approaches, which need more alignment across different organizational units, resulting in a lack of clear standardization or coherence in execution and documentation. Essentially, this type of compliance management will rob the organization of a true overview of risks and thereby, open the organization up to liability and inefficiencies.

Furthermore, by implementing tools for SoD (and GRC), you enable data reports and a dashboard of real-time information that can support you in making informed decisions. In contrast, manual data handling, analysis, and report generation will be based on data already dated when the report is finalized.

As a final efficiency argument, we must mention a big one – auditing. Auditing is a costly and unavoidable process. SoD enables fewer audit findings due to risk management being in place and a faster and easier auditing process due to proper documentation and paper trails in all the relevant processes that auditing will look at. This results in fewer hours needed for auditing and improved auditing quality.

Legal liability & regulations

When discussing the business case for GRC, it is crucial to address one of the most prominent points: achieving compliance to meet governmental regulations and mitigate legal liability. This point is undeniably significant and serves as a crucial driver that directly impacts the company's performance while reducing or eliminating the risk of fines and sanctions. This is a very relevant point, and meeting regulations can often be enough of an argument to help drive the SoD project.

The cost of fraud

The ACFE estimates that around $4.7 trillion in revenue is lost yearly on average[1]. That equals roughly 5% of all revenue globally is lost due to fraud. The average loss per case is $1.7 million with a median loss of $117.000. This tells us that even though the loss per case has a large variance, the loss is generally very substantial. It is even to the point that, depending on your choice of software and the size of implementation costs, even a single prevented fraud case could be enough to offset the cost of an SoD tool. Internal fraud control mechanisms are proven to result in lower monetary loss due to fraud and much quicker detection. Further, half of all fraud cases occur in organizations with no internal control mechanism, and the most effective internal control mechanism is proactive data monitoring and analysis – such as an SoD tool. It is also very telling that 64% of organizations increase their investment in proactive data monitoring and analysis after a fraud case. We believe it makes more sense to establish and invest in SoD before an eventual fraud case, as even a single avoidance prevents a high cost for the organization.

It is also important to remember that these figures are just for fraud with malicious intent. SoD also drastically reduces the risk of costly human error, and can even mitigate external threats such as stolen credentials.

The cost of fraud globally in 2022

Revenue lost yearly

4.7 Trillion $

5% revenue on average

Loss per incident

117.000$ Median loss

1.700.000$ Avg. loss

Increased investment

64% after fraud detection

[1] https://acfepublic.s3.us-est2.amazonaws.com/2022+Report+to+the+Nations.pdf

Human error

You might have full trust in everyone in your organization and believe that fraud is a completely irrelevant issue to you. Of course, this is often not the case in a big organization, but it is very good if everyone trusts each other. While this is, of course, great that you have an organization with full trust, we can all agree that human error will happen regardless of trust.

Furthermore, if you have full access to everything in SAP, the potential consequence of human error is correlatedly very large as the potential for damage is close to limitless. In reality, human error is responsible for the vast majority of security incidents, and the logic follows that it should, therefore, always be a prime priority to reduce human error in the organization, because it is the most typical cause of security incidents.

By segregating duties and ensuring that employees are only allowed access to the processes within their area of expertise, organizations can drastically reduce the risk of human errors due to lack of understanding or knowledge of a particular process. Therefore, the business case for a segregation of duties tool is even stronger when factoring in the impact an SoD tool has on human error.

External threats

Many people only think about the segregation of duties tool as a tool that restricts access and reduces risks stemming from employees. However, there is a very simple and important argument for why the segregation of duties tool is essential to a security strategy for defending your organization against external threats. According to Ponemon Institute & IBM security[2], stolen credentials along with phishing are the most frequent type of cyber-attack. If an outside threat gains access to employee credentials, it is quite obvious how segregation of duties is a factor in mitigating the damage they can cause. It is in everyone's (except the hacker's) best interest that the credentials that the hacker has gained access to have limited access and have no combination of accesses that can easily be misused for misappropriation of funds or other malicious actions.

[2] IBM Security & Ponemon Institute, Cost of a Data Breach Report 2023

Just think about the other end of the spectrum, where no matter what credentials a hacker gains access to, they are enabled full access to the organization's SAP system. It would be a catastrophe.

It is very logical that when stolen credentials is one of the most common types of cyber attack, that you limit these credentials access to only include necessary access. That is why, it is ComplianceNow's opinion that when you build a business case for a segregation of duties, one should include the cyber-security value that an SoD tool adds against external threats. It would be a mistake to only view it as a tool that prevents risks from internal sources.

Summary

A segregation of duties tool is not just an insurance against fraud, but it is an efficiency tool that easily pays for itself when you include all the dimensions where a segregation of duties tool add value, such as risk reduction of fraud, human error, cyber-attacks, negative public image and an increase in organizational trust and ability to uphold regulations.

Tooling

Choosing the right SoD tool for your organization has a major impact on your post-implementation work. It is important that the organization makes an educated choice based on correctly identifying internal ambitions and circumstances and matches them with a suitable vendor that has fitting capabilities and understanding of your organization. You will have successful implementation project and post-implementation work only by starting with the right tool. This chapter will focus on some things you should consider before choosing a tool.

Internal factors

Ambition versus being realistic

It is important to be ambitious when starting your risk management maturity journey. It is also important to remember that you are just starting. The chances that you can go from a somewhat immature risk management process to a world-class process in six months is not a realistic goal. We generally recommend objectively evaluating your organization's ambition and maturity level before choosing a vendor. By understanding how mature your risk management processes are, you can better understand what the next step is and what is a realistic project to undertake. This will help you look at market availability, as you know what you are looking for and what vendor might fit you. We have created a simple maturity model hereunder to help you identify your current maturity level.

	Minimal	Ad Hoc	Preliminary	Defined	Integrated	Optimized
How is risk managed?	It is not	Individuals take some responsibility Emerging risk management but only reactive	Manual handling Departments handle their own risk processes	Manual handling Processes are defined and repeatable Accountability established, risk assessment/ response process in place Risks prioritized	Tool supported risk management processes Cross department strategy for managing risks, supported by tools Extensive collaboration between business and IT Compliance factored into key business decisions	Automation of many risk management processes High level of tools that support strategy Extensive collaboration between compliance and Business, and extensive understanding of processes and risks Predictive risk analysis
Auditing Impact	No audit trail	No to little audit trails	Some documentation, but no centralization	Some documentation, but no centralization	High level of documentation Centralized Standardized	High level of documentation Completely centralized & Standardized
Main Challenge	Incidents might already have happened, no way to be sure Auditing difficult and costly	No ownership, monitoring or processes defined Reliant on individuals taking charge	Disconnect between departments (siloed) No standardization Manual handling No measurements or overview of effectiveness	Disconnect between departments (siloed), lack of integration between departments No tools integrated to make the defined processes easily manageable No measurements or overview of effectiveness	Finding new opportunities for streamlining risk management General agility in risk management, as processes have become structural and fixed	Finding new opportunities for streamlining risk management General agility in risk management, as processes have become extensive

Organization size

Another factor to look at is the size of your organization. The larger your organization, the more complex it generally gets, and then they require a large and complex tool as well that is specifically designed to deal with complex landscapes. This does not mean that a large organization cannot be simple enough and therefore does not require complex and large tools. But it does mean that a small to medium-sized organization rarely benefits from purchasing the market's biggest and most complex tools, as they will end up paying for a lot of functionality they probably won't need. So, if a tool is large and complex, the implementation project and post-implementation work will likewise be more complex; therefore, there is an increased risk of project postponement and project abandonment.

External vendor

After assessing the current internal maturity level, you are ready to look at the tools in the market. Choosing the right vendor and looking at all the different properties is important. Choosing a supplier for GRC tools is like choosing a partner. As your organization changes and matures, your supplier will need to be able to accommodate this. It would be best if you match your organization with the correct partner. We recommend that you investigate some basic things about potential vendors.

Support

When selecting a vendor, it is crucial to consider the level of support they offer to ensure a successful partnership. Whether you have an experienced in-house team or not, having qualified and responsive support can make all the difference in resolving questions and challenges that may arise. Therefore, it is important to evaluate the support quality, including the level of technical expertise. Will you have direct access to a knowledgeable technical specialist, or will you only have access to basic customer support? Additionally, it is essential to research the vendor's support repositories, such as FAQs, user guides, and online forums, to determine whether they have the resources you need to get the most out of their product.

Certifications

Certifications are like cheat sheets when it comes to choosing a tool and a vendor. You cannot just put in 'best SoD tool 2023' in a search engine and expect to find the perfect match for your organization. However, certifications offer a quick and easy way to get valuable information. By looking at a vendor's certifications, you can see at a glance if their tools are compatible with your platform and how up-to-date the vendor is. It's also worth checking if your potential vendor follows industry certification programs, such as the SAP certification program. This shows that they're dedicated to keeping up with all the latest updates and that their tools are future-proof.

When you're investing, it's always good to know that it will continue delivering value over time. It’s important to consider all the available information when choosing a vendor to ensure a successful partnership that meets your organization's needs, and certifications are a good place to start.

Road map – geared for the future?

One thing to know that the tool can keep solving the issue that initially sparked your search for an SoD tool and filled your requirements. Another very interesting thing, if you are assessing vendors, is to investigate whether they have a road map for the product. By seeing a road map and investigating the planned future for the product, you can better determine what you are buying into and what value you can expect the tool to deliver in the future. When you talk about SoD, it is always important to balance what you get now, what you get in the future, and what the maintenance requirement and support level is. By gauging all of these, you can make an educated decision that can help ensure long-term success.

Maintenance requirements

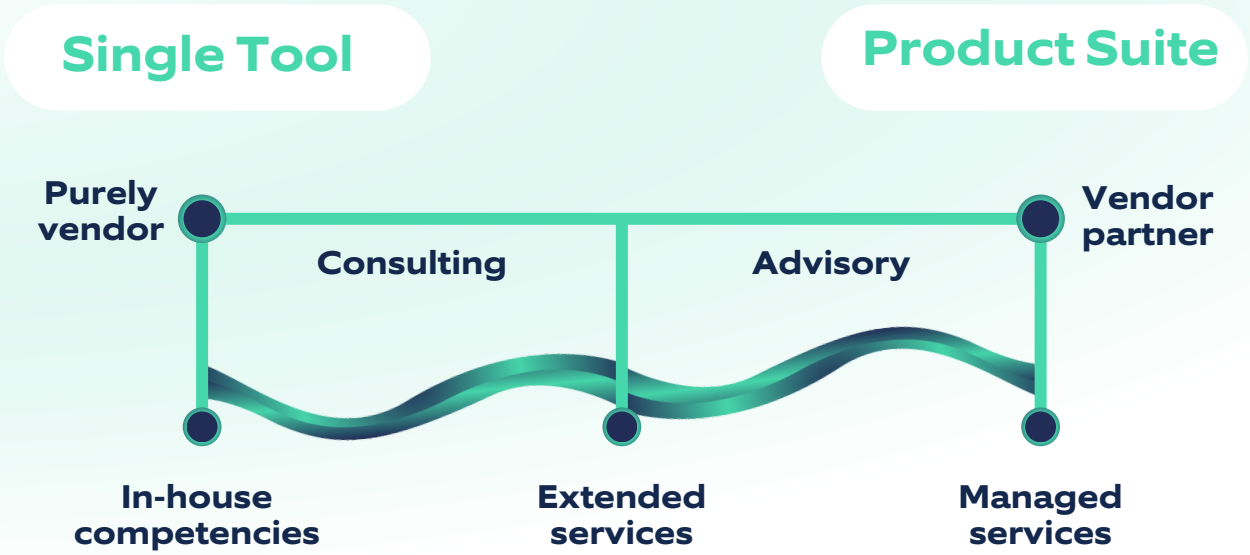
Choosing the right SoD tool for your organization involves assessing the features and functionality and understanding the maintenance and setup costs. More complex large tools typically require a higher level of maintenance and setup, which can result in significant one-time and ongoing costs. For example, on a technical level, some heavy tools may require their own system, while lighter tools can often be integrated as add-ons to existing systems. The cost of implementing a new system can be substantial, and ongoing maintenance costs can add up over time. It's important to consider the total costs associated with each tool and weigh them against the benefits of its features and functionality. By taking a careful and informed approach to evaluating SoD tools, you can choose a tool that meets your organization's needs while also fitting within your budget and resource constraints.

In-house competencies vs. vendor service support

Your organization’s in-house competencies matter when you are deciding on an SoD tool. You need to have a team in place that has the expertise which enables them to learn the tool. Your chosen vendor will likely help you get started with the tool by providing initial training, but you need to have people that are able to anchor the information internally in the organization. Again, this might seem obvious, but it might not be so apparent. After an initial implementation, everything can run well. But if it is dependent on a single individual in the organization, the tool can become ineffective and unmaintained, resulting in the tool delivering diminishing value. To secure maximum value for your investment, we recommend that you have a team in place that can absorb the knowledge from the vendor, spread it in the organization, and make an effort to assign a specific product owner for the tool. This will help create an understanding of the tool and its criticality for the organization's business and anchor the tool in the company.

On the other hand, if you evaluate that you need more in-house competencies, you will need to contract third-party consultancies to help you fill out the necessary gaps. In the meantime, you can build your internal competencies to make your organization less dependent on external contractors in the long term.

Suppose you evaluate a gap between your required expertise and your current expertise. In that case, you can investigate how much service and support your potential vendor provides and what extended implementation support they offer. This way, your vendors' expertise in their product and the SoD risk management area can benefit you. This vendor/customer relationship type would be more akin to an advisory role. This can be a beneficial way of quickly closing the gap and accelerating your risk management maturity.



Preventive vs. reactive

When analyzing SoD conflicts in the organization, one can choose between a preventive or a reactive approach. The two approaches are characterized by when the analysis is done concerning assigning privileges to the user. If the analysis approach is to detect SoD conflicts after the privileges have been granted, then it is a reactive approach. It is a preventive approach if the analysis detects conflicts before granting privileges. These two approaches each have their strengths and weaknesses.

The preventive approach will generally be the best practice when speaking from a risk management perspective. With a preventive approach, you are always aware of the risk, as risk is dealt with upfront. Furthermore, it is good practice to prevent issues rather than rectifying and correcting them continuously. On the other hand, a preventive approach has some negative impacts. The preventive approach carries a set-up cost concerning defining the process and training approvers.

Furthermore, it carries the burden of being a slower way of delegating access.

The pay-off for preventing risk existing in the first place is adhering to the predefined process, which means that the access request will take time to handle in contrast to simply accepting the request. This can result in an interruption in the business.

The reactive approach is a pragmatic approach that gets privileges delegated fast. There is less risk of interruptions in the business, and risk handling is postponed until after privileges have been granted. This will, however, also mean that you are postponing the problem instead of dealing with it upfront. Risk still has to be managed, but now you have to put out fires instead of never having set the fires in the first place.

A reactive approach will always mean a higher risk exposure because even if you manage the SoD conflict right after the access has been granted, there is a period when that risk exists in your organization.

However, as mentioned earlier, the preventive approach has a set-up cost that the reactive does not have, so if you manage fairly few risks, you can argue that the reactive approach is sufficient and most beneficial in terms of cost/benefit. However, this approach needs to scale better with growth as more risks are introduced, and managing them reactively becomes a larger task.

Another aspect to consider in the preventive versus reactive approach discussion is the psychological aspect. Remember, when you are granting privileges, employees will get used to having the accesses they have, and even if they do not use them, they might not be very keen to remove them. It is more difficult to take access away from someone than to never have given them access in the first place.

Pros and cons of reactive vs. preventive approach

Reactive

- **Fast access delegation**
- **Can better support small risk management scope**
- **Pragmatic**
- **Postpone problems**
- **Identify risk later**
- **Higher risk exposure**
- **Most likely a more expensive way of handling equal risk level**

Preventive

- **Slower access delegation**
- **Identify risk straight away**
- **Less risk exposure – all risk approved before delegation of access**
- **Prevent problems**
- **Preventive process must be defined (higher setup costs)**
- **Training of approvers**
- **In the long run a more efficient and scaleable risk management model**

Final thoughts on tooling

You need to be able to produce a clear requirement list. Knowing your requirements for the tool is essential to matching yourselves with a fitting vendor. This point needs to be stressed. Knowing your needs reduces your uncertainty, and uncertainty can drive poor decisions.

In our experience, organizations that are uncertain about their requirements will often choose too complex tools for their needs and thus end up with a too-heavy and complex solution that requires excessive maintenance and is very cost inefficient. Moreover, we often also see failed implementations due to tool complexity, where the tool never gets implemented after purchase as the organization cannot handle even getting the implementation off the ground.

So, why should you gain some certainty before buying a tool?

Uncertainty can drive the purchase of too big and complex tools for your organization. There is a certain logic: if you are uncertain about what you need at minimum, you can buy something expensive and complex because that product should cover your needs. However, this idea is not correct when it comes to SoD tools and GRC tools in general.

More expensive will often mean more complex and bigger. Many large and costly tools are built for huge enterprises and serve the specific requirements of huge enterprises. Buying large and complex tools for an organization with a smaller size, a lower need for complexity, and a thousand moving parts in the tool, is a recipe for an unnecessarily costly project with a large potential for failure.

More is not better when it comes to SoD tools – a well-thought-out requirement list, and a good vendor fit is the ultimate goal, ensuring that you make the best investment and setting yourself up for successful post-implementation work. Remember that in the purchasing phase, you are setting yourself up for what work you need to do in the future, so doing your due diligence will save you costs and headaches in the long run.

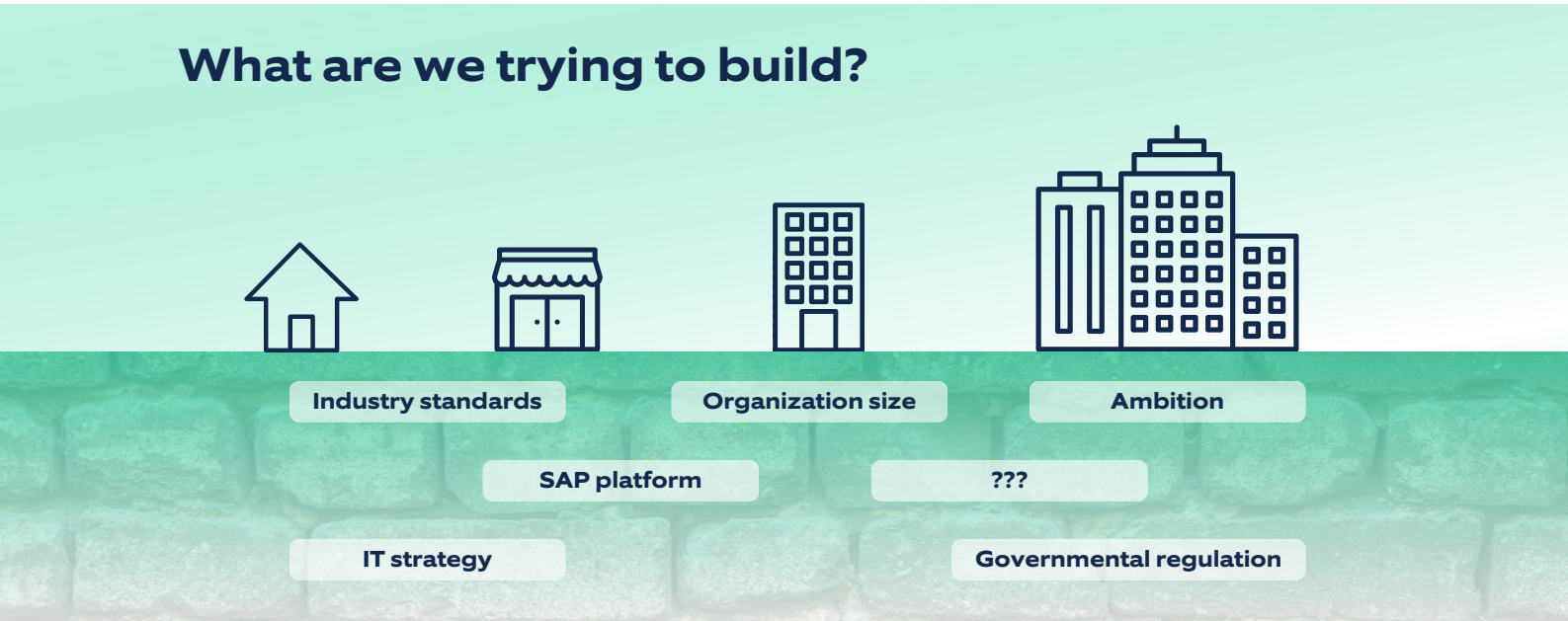
Organizing the organization

When embarking on an SoD project, it is important to have a good plan involving different parts of the organization, not just the IT department. This chapter will focus on different aspects of what an organization should do to become ready for an SoD tool project and guide you through the process. The chapter also provides you with tools, such as a 'pre-flight' checklist, that you can go through to verify that your organization is ready to start the SoD project.

Aligning the organization – what are we trying to build?

When deciding to implement SoD, it is crucial to lay the foundation with careful planning and organizational groundwork to ensure successful execution. Implementing SoD requires pre-planning and thoughtful consideration to achieve desired outcomes. Equally important, gaining alignment, personal investment, and ownership within your organization is paramount. In essence, an SoD project shares similarities with constructing a house. Just as a blueprint guides the construction process, having a well-defined plan helps stakeholders align and comprehend the project's scope. Additionally, involving employees at various levels and fostering their motivation to take ownership and responsibility are key to successful implementation and smooth day-to-day operations. A solid plan or blueprint sets the stage for alignment, ownership, and, ultimately, a successful SoD implementation.

Herein, it is important to think about what your goal is and what your foundation is. By foundation here, what goes into the project should be a deciding factor for the project's goals. Are you in a highly regulated field? What is your IT strategy? Is your company huge and complex? There are plenty more questions, but the point is that what you are trying to build with the SoD project should be aligned with your company's foundation.



Assessing risk situation

There are a variety of things you should consider in an SoD implementation. First, in an implementation plan, you should consider your organization's specific risk situation. What things influence what your risks are? What is important for the company? What things could happen that would damage your business? The point herein is that it is important not to think that an out-of-the-box concept is just ready to go for your specific organization.

You can find assistance in having predefined risks and conflicts, but you must contextualize them to your organization. Sometimes it can be very easy and tangible to define this, but sometimes it can be a bit more complicated. For example, organizations might overlook that their profitability and competitive advantage stems from proprietary knowledge/technology, and therefore protecting the leak of this knowledge should be of a much higher priority than adhering to an "out-of-the-box" standard rule set.

Returning to the initial point of aligning the organization, it is crucial to consider what drives your organization and identify risks that could hinder its functioning. This leads to an important but often overlooked realization: defining risks and determining what matters to the entire business is not a task that can be accomplished by the IT department alone. Because after all, how should the IT department have all knowledge about all business processes?

To effectively identify the areas that require coverage in your SoD implementation, it is crucial to determine the individuals capable of fulfilling those roles. This process necessitates the active involvement of the business side of your organization. By engaging stakeholders from different departments and levels of hierarchy, you can ensure a comprehensive approach to the project. The participation of employees at various ranks brings diverse perspectives and expertise, fostering a sense of ownership and accountability throughout the implementation.

Why and how do we involve people in the organization?

IT should only make decisions on behalf of the business side with their involvement. Here's an elaboration on why and how to involve individuals from different departments:

1. Inclusion of business side

IT should not make decisions on behalf of the business side without their involvement. SoD tools impact the entire organization's day-to-day operations, so representatives from functions heavily affected by the SoD project should be included when deciding the basic plan and configuration logic of the SoD tool. This vertical approach typically starts with the Chief Information Security Officer (CISO), or other high-ranking roles with similar responsibilities, to identify significant risks and organization-specific considerations. It then extends to engaging different business process owners to uncover any additional risks they are aware of but may still need to be identified.

2. Ability and motivation

When determining who to involve, it is important to consider both the ability and motivation of individuals. Look for employees with the knowledge and expertise relevant to mapping risk areas.

Additionally, establish motivation by highlighting the project's impact on their roles and emphasizing that having representatives from various departments is in everyone's interest. The SoD tool can provide real-time actionable data and dashboards, which can be attractive to business-side stakeholders. Ideally, each chosen department should have a designated 'sponsor' as the liaison for the SoD project.

3. Clear agreements

To ensure the success of the relationship with the involved departments, it is beneficial to have clear agreements in place. These agreements outline how the specific department's time, resources, and personnel can be utilized. By setting expectations and establishing mutual understanding, you can facilitate effective collaboration and ensure that the department's resources are appropriately utilized for the SoD project.

Make sure that you have an answer to these questions

To summarize this short chapter on alignment, we have created a checklist. The idea here is that you know what questions you should have an answer to and if you have an answer to all of the questions, you can be rest assured that your SoD project has a good foundation.

Correlation between risk mitigation and cost

Finding the right balance between risk mitigation and cost is crucial in an SoD project. While organizations may aim to eliminate all risks, it's important to consider the associated costs. In this context, costs mean not only monetary costs but also what they practically imply for the organization.

Adopting a "zero risk" approach involves segregating all SoD risks and removing critical accesses, which would impede essential functions. This way the risk management process would end up being a huge disruption to the business – one of the main things we are trying to avert when we are preventing risks. It is vital to acknowledge the impracticality and lack of sustainability in achieving complete risk elimination.

Zero risk is an unrealistic goal. It is both impractical and costly. Instead, organizations should prioritize a pragmatic and balanced approach to risk management. These entails implementing mitigating controls alongside an SoD tool and ruleset. It's important to recognize that it's impossible to prevent all risks since risks and the ability to perform actions are inherently linked. Accepting a certain level of risk becomes necessary.

Organizations should establish a well-configured internal control process to prevent risks from being exploited. By combining effective internal controls with an SoD tool, organizations can make significant progress in enhancing risk management maturity and ensure that the accepted risk is controlled and documented, mitigating the risk. Implementing mitigating controls at the same time as implementing the SoD tool would be beneficial. This might be insurmountable for your organization, but it can be the logical next step if it is not done in parallel.

While complete risk elimination remains unattainable, implementing robust controls and tools allows organizations to achieve a realistic and practical equivalent of a zero risk environment. By striking the right balance between risk level, uncertainty, and cost, organizations can effectively navigate the complexities of risk management.

Discussion on project approach

When starting with an SoD tool implementation there can be different expectations and requirements from stakeholders. Which tool should you choose, and which modules will be used?

It is important to know your company's maturity regarding risks and controls. Answering these questions can point you to which approach you should take:

- **Is there an overview of all internal risks, and if yes, are they thoroughly described?**
- **If we do not have a complete overview of internal risk, can we create it?**
- **Do we have an overview of all the roles? What is the content of those roles, and are there any embedded risks in those roles?**
- **Can we benefit from hiring external support?**
- **Are we ready to involve the business and change internal processes within role approval, user administration, access reviews, key stakeholder training, risk administration, role development, risk reporting, etc. (see also "pre-flight check list" in earlier chapter)**

Based on some of these questions and your knowledge of your company, an approach can be decided upon. Regardless of the chosen approach, the goal is to achieve the same result—a complete map of internal risks in your SAP system.

1. Enable full ruleset

Start by enabling the built-in risk library that comes with your tool. Make sure to refrain from activating any process integrating functions in order not to start sending out emails, activating any approver workflows, or integrating into user administration functionality. The first target is to run a full system analysis and gather information about current risks in the system. Based on this information, it is possible to start cleaning up the role concept, prioritizing your activities by area, functionality, or any other parameter you determine. This process can be iterated until you feel confident enough to introduce the concept of risk owners and an approval process, a preventive check interrupting a role assignment in the user administration, and any other process-specific functionality available to you.

The ruleset will be changed according to findings during the process.

2. Enable partial ruleset

Similar to the process above, it is possible to start with a narrower approach where a handful of risk definitions are selected. The same activities are executed for this narrowed-down scope as for the full ruleset. This will allow you to focus on the chosen scope and implement all the processes for a single portion of the business instead of going all in.

3. Validate ruleset internally before enabling

When deciding to validate the ruleset included with the chosen tool or even create your own ruleset from scratch, it is important to involve people from your organization with extensive knowledge of the processes covered by the ruleset. It can be one or more people, and they are good candidates for risk owners when rolling out the solution to your organization.

Going through each rule/risk definition is a time-consuming process and might cause a prolonging of the implementation project for the risk/SoD tool.

Validation of risk library

An important part of implementing a risk tool is to create, select, and validate a risk library. The risk library collects general and detailed definitions of what constitutes a risk in your system. Some tools come with a built-in or available risk library. Some external auditors supply a risk library, and sometimes, a company might have a risk library created based on external audits over an extended period. Regardless of the level of detail and whether it covers current processes within the company, the risk library must be reviewed and perhaps updated.

Some questions that need answers are:

1. **Have all internal processes been analyzed to identify potential risks?**
2. **Are risk definitions described in enough detail?**
3. **Are owners assigned to the risk definitions?**
4. **What happens to a user with a system access, where those accesses contain one or more risks?**
5. **Is there an approval/rejection process?**

An important factor to note is that tools with an included risk library will cover standard system functionality, so all custom-built applications, functions, etc. are not covered by the risk library by default and must be considered during the validation of the risk library.

The validation process will involve a lot of different people within your organization. Should you involve:

- **Internal audit:** Will be interested in what is reported and how the process is defined.
- **Compliance officer:** Should be involved in order to ensure that external regulations and internal procedures are adhered to.
- **External audit:** Will typically have input to the risk library based on ongoing system and process audits. Ensure to include them in the ongoing development of your risk library.
- **Process owners:** With extensive knowledge about the processes and the inherent risks.
- **Managers:** Will have input on the organization of teams and the practical implications of implementing SoD in the organization.
- **IT personnel:** How to manage and operate the tool. Focus on system-specific risks.

Bringing the best people into play is key to a successful risk library validation.

Remember: Validating and extending the risk library is an ongoing process and should be assessed regularly.

Discussion on IDM and Access Control

IDM (Identity and Access Management) and Access Control are related to managing access to resources, but they have some differences. This section will be a discussion centered on IDM and access control, and therefore, we must first outline some definitions and characteristics.

IDM focuses on managing the digital identity of users, including their authentication (verifying their identity) and authorization (determining what resources they are allowed to access). IDM systems typically provide a centralized interface for managing user accounts, access rights, and authentication methods across applications.

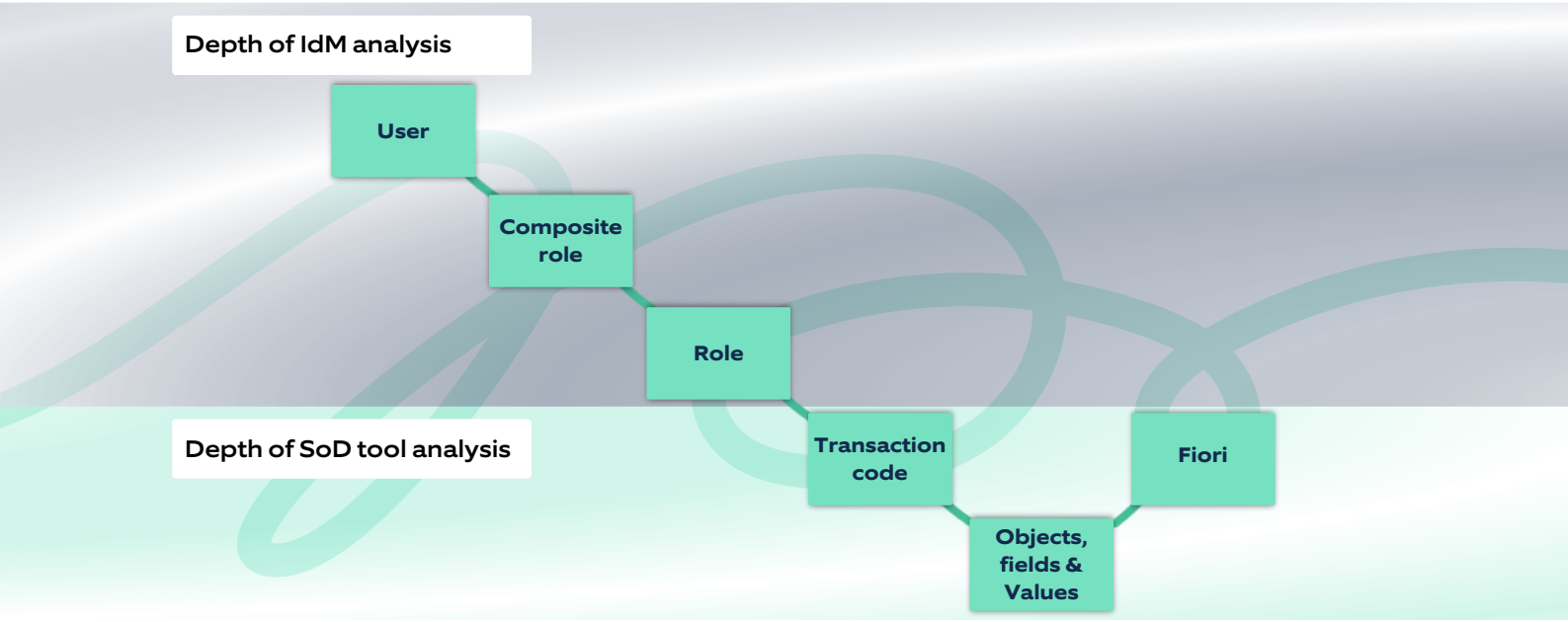
Access Control, on the other hand, is the process of limiting access to a resource only to authorized users. Access control systems can take many forms, such as physical access control to a building, network access control to a computer network, or file access control to a shared folder. Access control systems typically rely on authentication methods to verify the user's identity before granting access to the resource.

To summarize, IDM is a broader concept as it encompasses the management of user identities and access rights across multiple applications, while Access Control specifically focuses on the mechanisms and processes that limit access to resources based on authorization and authentication.

Can IDM execute Segregation of Duties analysis?

Sometimes there is a discussion, or uncertainty, whether an IDM tool can also perform SoD analysis of SAP accesses. It is correct and incorrect to a certain degree – an IDM application can typically perform a segregation of duties check, but only on a role level. This means that the IDM application, in the user provisioning process, will check if "Access X" is about to be combined with "Access Y" on the same user account and whether this is defined as a conflict. Analyzing the combination of transactions, objects, and field values assigned to users through SAP roles requires a dedicated SoD application for SAP.

The next level of this discussion is the statement that the check of SoD is sufficient on the role level since we are very careful in designing the roles. This might also be true, but one thing is to design the roles, and another is how the roles will evolve and how the roles are combined with the end-users. Here, you will manually need to consider many transactions, objects, and field values in combination; you will have to consider this on the individual user level. More and more teams realize that doing this manually is very close to impossible without a dedicated risk library (supporting transactions, objects, and field values) and a risk engine to analyze the roles and end-users.



What to be considered around Access Management and implementing SoD

After this initial clarification, we can discuss further considerations around access management and SoD. First, the relevant question is, how is SAP access management or user provisioning handled in your productive environment?

Is it done through a manual process (typically User Administration), or is it done through an IDM system? If the access in SAP is approved and distributed through IDM, you need to consider how this will impact the risk approval process. Risks are typically distributed to appointed Risk Approvers, where line management handles general access approval. This means that Risk Approval will often be a separate approval workflow needed to be processed before or after the access approval.

One thing to consider looking at the access approval and risk approval process is that it is two different processes handled by different people in the organization, and approving access is probably a faster process than approving risk. Secondly, it can be technically complex to integrate the risk approval process as part of the access approval, but it is not impossible. Some vendors of SoD solutions are offering an API, so every user creation or access change will be directed to the SoD engine for analysis with a response back to the IDM system if a risk is to be considered as part of the access approval process. Further, information from the IDM can be directed back to the SoD tool concerning the approval of risk to be included in the documentation.

An alternative to integrating the access and risk management process is to have the two processes running in parallel. In the ComplianceNow Access Control module, there is a function called Legacy Risk Management – other SoD tools might have a similar function. LRM will list all identified risks in the system, and the risk can either be automatically processed for workflow approval or manually processed to risk approval. Since access is applied to the end-user before processing for potential risks, this is to be seen as a reactive way of handling risk management. Some organizations will not accept this approach. The benefit is that IDM and the SoD tool can both perform and execute their respective tasks without needing to make a potential complex integration between the two applications.

There are many angles to discussing whether you should integrate the SoD into the IDM process. Both access management and risk management are important processes but with different frequencies, different participants, and possible integration challenges.

Access management

- **Ensuring right accesses to the right processes and to the right people**
- **Granting access to enable people to work**
- **Access approval can be fast tracked**
- **Line manger approves/process owner**
- **Focus is business processes**

SoD management

- **Validate and approve an SoD critical access in a controlled framework**
- **Not always possible to fast track access (risk) approval**
- **Risk owner approves**
- **Focus is risk management**
- **Less approvers, but centralized organ**

Introducing SoD in an existing live system

Introducing SoD in an SAP environment that has been implemented years before is more often the case than introducing SoD in a new system. The consideration with a live environment is that the authorization concept has already been implemented and the users are provisioned. This also means that introducing SoD in an already running SAP environment will most likely result in adjustment of both the role allocation to the user as well as the authorization and role concept.

The Risk Library and the activation of the individual risks will directly impact the possible number of risks identified in both the roles and on the end users. In the section “Discussion on project approach,” the process of implementing SoD is addressed. Thus, in that section, the focus is more on the actual result of activating the risk in a live system and a few overall directions on how to address these results.

Legacy risk management

As mentioned earlier, SoD will most likely be introduced in an already live system. Therefore, implementing an SoD tool supporting a preventive risk approval process might raise the question of how to handle the risk introduced on the user before the process had started. This is what we normally refer to as legacy risks, and the most optimal scenario is to get these processed and approved by the risk owners, ensuring an equal documentation of all risks – both, the risks introduced in the past as well as all future risks.

In ComplianceNow Access Control, we call this function Legacy Risks Management. In LRM, you will be able to have a full overview of all risks on users with indicators of when, how, or if they are approved – or perhaps awaiting approval in the workflow. Such a function will allow you to push out all risks introduced before SoD was introduced, supporting your SoD engine holding the entire documentation.

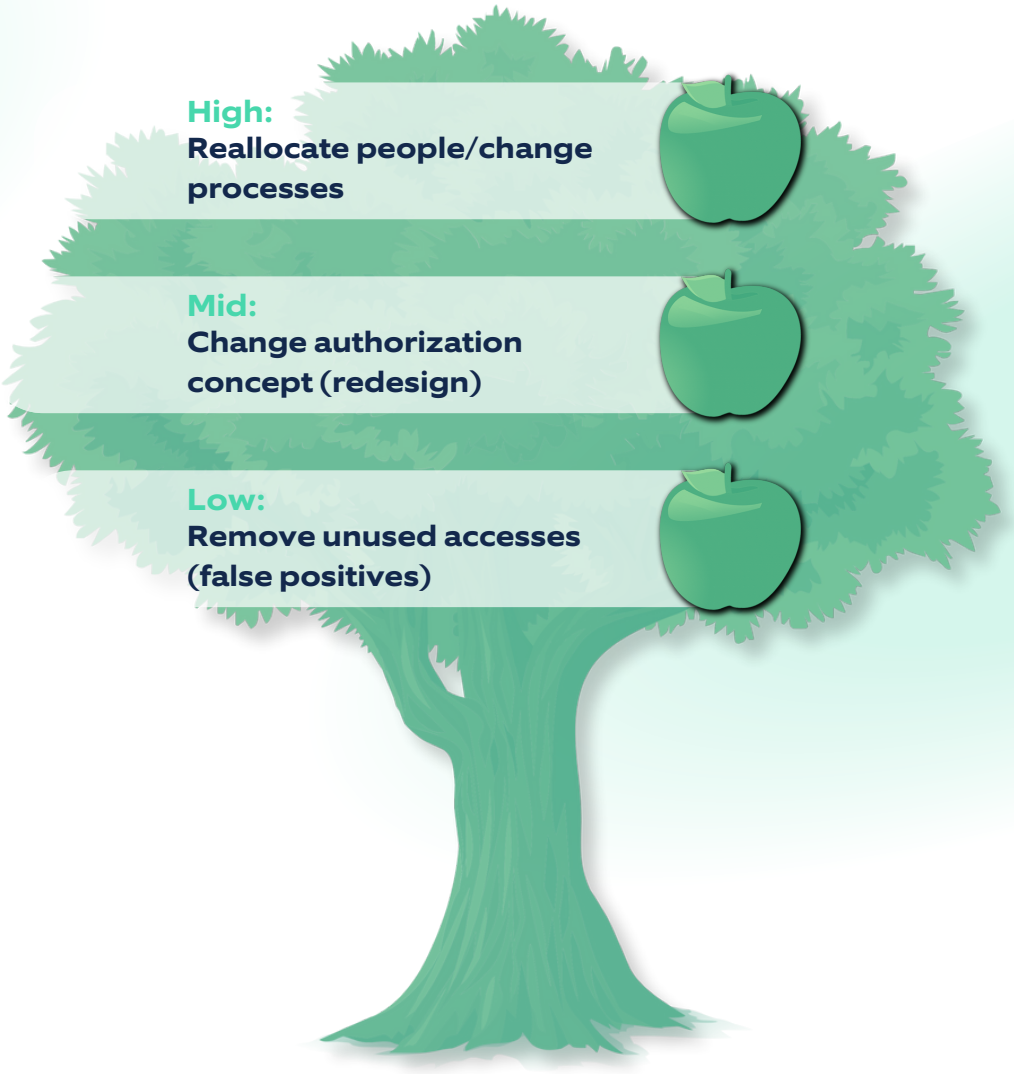
Addressing the risks identified

Implementing an SoD tool and running the first overall end-user risk analysis can be an interesting experience, showing a surprisingly high number of risks. The good thing is that there are some 'low-hanging fruits' actions to reduce this number initially. The first recommendation would be to look at roles assigned to users with no usage for the last 6-12 months. SAP standard does not have very good functionality to support this. Still, most SoD tools either have an SAP compliance analytic component incorporated or a separate tool supporting SAP access and usage analytics. Such a tool will be critical in the continued work of reducing the number of risks.

The next suggestable step in reducing the risks could be performing a false-positive SoD analysis. False positive means looking into the users having access to both functions of what has been defined as a risk but is only using one of the functions. In some SoD tools, such an analysis will be possible directly as part of the data delivered in the risk reporting.

The next measurements will be more far-reaching and could be a full redesign of the authorization concept and user mapping. It is far from the case in many companies, but changes to the existing roles are necessary depending on the decided acceptance of the number of risks on users. Such changes could be splitting up a role, making it possible to assign the two functions in a risk to two individual groups of users. Changing roles or part of the role concept is extensive, requiring the involvement of people line of business, process owners, and risk owners. Again, all changes need to be tested.

The most extensive action would be to reallocate people to allow the separation of duties to be more comprehensive or even redesigning whole processes.



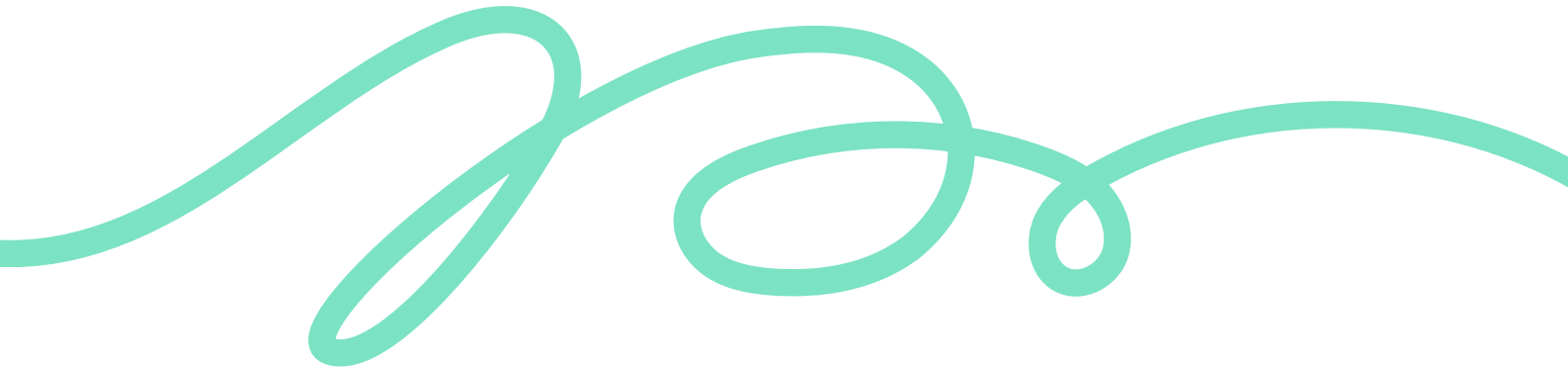
Backdoor risks

Now, we will delve into the 'backdoor risks' concept and explore its relevance in risk management. While the term 'backdoor risks' is a self-made term we use in ComplianceNow and might go by a different name elsewhere, it is a common problem. Understanding that new risks can emerge through alternative pathways, even with preventive measures and approved legacy risks is important. This is a backdoor risk.

Backdoor risks can manifest when making changes to the risk library or modifying individual or composite roles during the development process, which are subsequently forwarded to the production environment. Surprisingly, even a seemingly small change has the potential to introduce a substantial number of new risks on users.

Although changes to the risk library are infrequent, modifications to the role concept are more common. Therefore, it is important to understand how an SoD tool addresses this situation and how the risks associated with such changes are presented to risk administrators, enabling them to respond effectively. In ComplianceNow Access Control, for instance, all new risks, regardless of their origin, are listed in Legacy Risk Management (LRM). This overview provides administrators with a clear understanding of whether the risk is processed or not.

Furthermore, functions like LRM support the distribution of annual re-approvals for all identified risks, ensuring ongoing alertness. By leveraging functionalities like LRM, organizations can effectively manage and mitigate potential backdoor risks, thereby, strengthening their overall risk management framework.



How does an SoD tool support your S/4HANA journey?

We have experienced that many organizations start looking more seriously at SoD tools when they are migrating to S/4HANA. We wholeheartedly agree that this is a good idea and that an SoD tool can actually help support the journey.

When the decision to migrate to S/4HANA has been made, many new technologies are to be evaluated as part of the S/4HANA project. Deciding on which processes need to change, which new functionality to embrace in SAP, and which potential Fiori apps to start using might impact the entire authorization concept.

The time might be right to consider implementing an SoD tool to support the process. An SoD tool will enable you to add the concept of a risk library into the planning and execution.

Consider using statistical and usage analysis functions in the beginning of a project to determine the scope of your current authorization concept for the migration. This will enable you to minimize the as-is concept and narrow down what is being analyzed for future changes.

Introducing a risk library when all roles are being evaluated for upgrade purposes makes it possible to have a complete discussion of processes, responsibilities, and access within your future S/4HANA system.

The risk library will ensure that rules are risk free to the extent of your requirements, enabling you to determine where it is required to create controls to mitigate any necessary areas. You will end up with a list of current and future accesses that can be assessed based on the risk library.

Not only will the introduction of an SoD tool enable you to minimize the project scope, but a tool will also help you prepare for the expanding requirements of auditors and stakeholders.

Make sure that any tool you choose can support a risk library that covers standard ECC as well as S/4HANA including services/Fiori applications.

Concluding remarks

Segregation of duties might be a large project, but it is a necessary step to truly maturing your SAP risk management processes. We hope this book provides some initial guidance and has helped operationalize the project.

As you move forward, we encourage you to leverage the knowledge shared in this e-book to enhance your risk management processes. Make informed decisions, establish effective internal controls, and navigate the complexities of risk management with confidence.

Thank you for reading this e-book. We sincerely hope it has been a valuable resource for you. May you embark on your SoD journey equipped with the tools and understanding necessary to achieve compliance and prevent risks effectively.