Exploring digital: empowering the Internal Control Function

Insight into four different digitization options to keep up with today's fast-paced world

The Internal Control Function, or second line of defense is a vital part of the organization tasked with devising and improving measures to prevent fraud, helping the company adhering to laws and regulations and improving the quality of internal financial reporting. The world is watching: companies, especially the larger ones have to adhere to global and local laws, expectations of the general public, shareholders, auditors, employees, the supply chain and other stakeholders. This internal and external pressure is causing the Internal Control Function to feel the urge to improve its way of operating. This article provides insight into different digitalization options to help improve the way the Internal Control Function operates, with the purpose of inspiring you to digitize your Internal Control Function too.

Sylvester van der Giesen MSc
is a senior manager at KPMG Enterprise Solutions.
vandergiesen.sylvester@kpmg.nl

Vincent Speelman MSc
is a senior consultant at KPMG Enterprise Solutions.
speelman.vincent@kpmg.nl

INTRODUCTION

The Internal Control Function (ICF) uses a wide set of controls to make sure business and compliance risks are prevented or dealt with in the benefit of the company's well-being. Many of these controls are manual. Using largely manual controls means a great deal of effort, time and money. Not only are these controls more time consuming and costly, they also cannot absorb the increasing complexity of today's business environments in time, leaving the company possibly exposed to risks.

Let's see what happening in the ICF market domain. The recently published Governance risk & Compliance (GRC) survey by KPMG ([KPMG19]) was initiated to get a better insight into the maturity of GRC, the level of internal controls and the adoption of HANA with organizations running SAP within the EMA region. More than 40 large organizations running SAP have been asked to participate in this survey. Relevant conclusions for ICF:

- Approximately 20% of these companies don't have a centralized internal control repository
- Approximately 50% of these companies have less than 10% of their controls automated
- Approximately 70% of these companies identify control automation as a top priority
- Approximately 50% of these companies want to reduce their control deficiencies

Following this survey, it seems that while the top priorities of companies include further automation and reducing control deficiencies, the actual number of companies relying heavily on automation, using digital solutions, is low. While the relevance of digitizing seems evident, it is difficult to start, having a large landscape of applications and different control options available to you as organization. A logical question to ask is: how can we start to digitize our ICF?

This article shares client stories of ICF that used digital options, simply tools, to improve the way they operate across a variety of industries. We will outline how digital options can be used to lower the cost of control and improve the level of assurance of four different control types and what pitfalls should be avoided. We will also share relevant lessons learned and next steps based on our own experiences.

DIGITALIZATION OPTIONS FOR THE INTERNAL CONTROL FUNCTION

Digitalization of the ICF can be achieved in different forms. Some organizations start by implementing a tool or system to centrally manage and govern their risk and control framework. Some choose to go for an end-to-end transformation, where various tools and systems are integrating with each other, controls are automated and manual activities are supported by robotic process automation and low-code platforms. In the end, all companies try to achieve the same goal: increase their level of assurance while decreasing their cost of control. To help reach this goal we analyze a number of digitalization options using the CARP model. This model helps to categorize the different control types that will effectively reduce risks within a process or process step. CARP stands for Configuration, Authorization, Reporting and Procedural (Manual), which represent different types of controls (see Figure 1).

In Figure 1, the left side (C+A) of the model represents more technical controls, which can often be implemented directly in the ERP system, whereas the right side (R+P) of the model represents organizational controls which are embedded in daily business activities. Furthermore, configuration and authorization controls are preventive in nature while reporting and procedural controls are detective in nature. For each of the control types indicated in the model, there are digitalization opportunities. In the next section, some examples and use cases are provided for each category to provide a peek into the different options.

Configuration controls

Configuration controls are related to the system settings of an ERP system that can help prevent undesirable actions or force desirable actions in the system. These kinds of configurations can exist for the business processes handled in the ERP system as well as for the IT processes related to the ERP system. Therefore, a distinction can be made between "business configuration controls" also known as application controls and "system configuration controls".

Examples business configuration controls

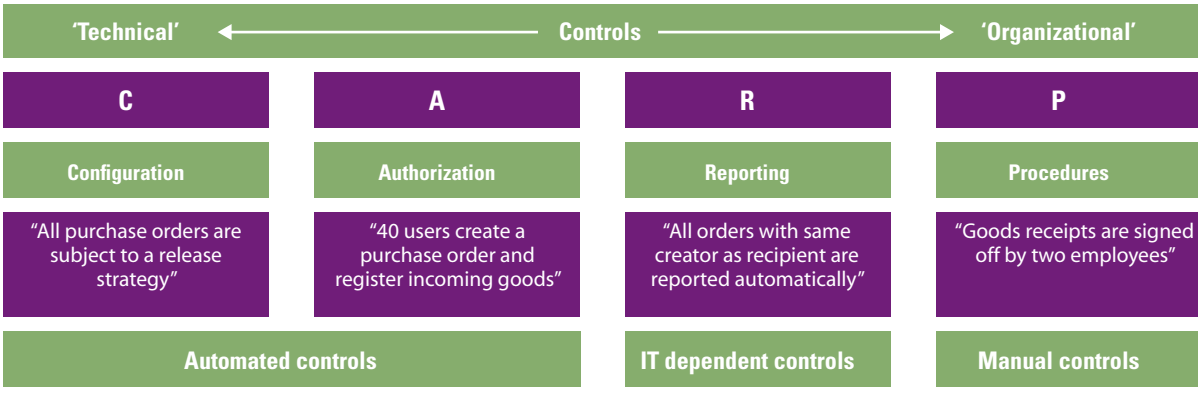
- Mandatory fields, such as a bank account number; when creating a new vendor in the system, these settings make sure no critical information is missing.
- Three-way match; this enforces that the purchase order, goods receipt and invoice document postings are matched (within the tolerance limits) with regard to quantity and amount.

Examples system configuration controls

- Password settings such as SAP parameters: "login/min_password_lng" or "login_min_password_letters" determine system behavior, such as the length of a password or the minimum number of letters used.
- More general system settings such as the number of rows that can be exported in a Microsoft Dynamics D365 environment determine a part of the system stability and are governed to make sure system performance is not impacted by frequent large exports.

In short, configuration controls are automated and preventive in nature which help organizations stay in control while not taking up any FTEs to execute the controls. Therefore, this type of control can be used to reduce the cost of control and increase assurance levels. However, there is a catch: how can the organization prove its automated configuration controls are set up correctly? And how does it prove that has been the case over time? To show how digital solutions can help solve this question, we present a use case of a large multinational where SAP Process Control was implemented to monitor the system configuration controls of 20 SAP systems.

Figure 1. CARP model.



Use case: using tools to go from quarterly parameter checks to continuous monitoring

Context
A large multinational with over 10 Billion euros in revenue. The company has over 20 centralized SAP systems. For each of these SAP systems, their (security) parameter settings, such as client logging (Rec/Client) or Password Settings (login/min_password_lng) needed to be monitored in order to adhere to their set SAP Security baseline. Their security baseline covers over 100 (security) parameter settings, which resulted in a lot of pressure on their testing resources.

State before Process Control
Before SAP Process Control was used, the 100+ security settings for each centralized SAP system were reviewed once per quarter. The review was performed manually and documented by creating screenshots of each relevant system setting. These documents were over 100 pages per system. The follow up on findings of these reviews were limited and rarely documented. If changes had occurred during the quarter (e.g. a setting was changed to an incorrect value and changed back to the correct value just before the review) there was no possibility to find these changes.

State after Process Control
By using continuous monitoring via SAP Process Control the system (security) parameters are now monitored on a weekly or monthly basis (dependent on the risk profile) and on top of that, all changes made to parameters are reported. Furthermore, the monitoring is now exception based. This means that parameters which are set to the correct values are passed and reported as effective whereas parameters that are set to the incorrect value are set to deficient and escalated through a workflow. The workflow requires a follow up action of the system owner, which is then captured in SAP Process Control.

Key benefits
By shifting the monitoring to SAP Process Control, the cost of control decreased while the assurance over control increased. By automating the parameter monitoring the focus shifted towards exceptions and follow up thereof. In the new situation, all results are also better auditable and more useful for the external auditor.

In this specific case, the client used SAP Process Control to perform continuous monitoring on their system configuration controls.

System authorization controls

Are preventative measures taken to control the content of technical "roles" and access for users to those roles with the intent of making sure the right people can execute the right actions? In their efforts to manage access, companies generally make use of the below authorization controls:

- *Segregation of duty controls*. The ability to change vendor bank accounts is limited to a technical system role related to master data management. That role is only assigned to personnel in the master data management department, to people who are not directly processing transactions. Another role is limited to be able to do purchase orders. This limits the risk that one person can change a vendor bank account into a private account, and create a purchase order against it, for a fraudulent pay-out. The outcome is that certain activities or "duties" are segregated. Issues like this example are called Segregation of Duties (SoD) conflicts.
  [Vree06] zooms in on the relevance of Segregating of Duties and its impact, along with multiple improvement suggestions and [Zon13] dives into solutions for managing acces controls.
- *Sensitive Access controls*. Updating credit management settings often falls under the Sensitive Access controls. These controls are essentially lists of actions that can have major impact on the business, and access to it should therefore be limited and closely monitored. Unlike SoDs, this is a single specific action. In the example of credit management, access to the transaction code and object in SAP and the Permission in Microsoft D365 are normally monitored periodically, where any users or roles having this access are screened and adjusted where needed.

In short, authorization controls are very similar to configuration controls because they are part of the system and once created and assigned, they automatically do their job. These controls are strong preventive controls if set up correctly. Like in the case of configuration controls, there's a catch: how can the organization prove that the authorization controls are set up correctly, and how do

you prove that has been the case over time? To show how digital solutions can help solve this question, we present a use case where a company used Access Control tooling to assist in managing their access controls and making sure their roles are SoD Free or SoD-mitigated in a way that increases assurance and lowers the cost of control.

Reporting controls

Reporting controls are pieces of information combined into a format where a user can get to conclusions about for example the effectiveness of a process or the state of a financial. They are used to detect anomalies so that action can be initiated. Examples are:

- Related to the SoD example mentioned under authorization controls, a manager in the internal control department wants to know how many SoD conflicts were reported last month, the actions that were taken to fix them, the status of those actions and the real risk the business is now facing. A dashboard, for example in BI tooling such as MS PowerBI, Tableau or Qlicksense or as part of a risk platform such as the earlier mentioned Sofy, SAP Process Control, can be a great tool to visualize and report on the status of the authorization controls. Especially on this topic, many lessons can be learned, and we highly recommend reading the 10 most valuable tips for analyzing actual SoD violations ([Günt19]).
- A manager in finance running a report that checks the systems for duplicate invoices, so that double payments to vendors can be prevented or payment of duplicated invoices can be retrieved from vendors that were paid twice.

In short, reporting controls are generally detective in nature as they present information about something

Use case

Background Sofy
The Sofy platform is a KPMG proprietary SaaS platform, hosting solutions in areas where KPMG built expertise over the course of years. Solutions on the Sofy platform aim to provide relevant insights into business-critical processes as well as triggering relevant follow-up actions by end users with the help of workflows, tasks and notifications.

Context
A large multinational operates in more than 150 countries and has annual global revenues of over 50 Billion euros. The core application landscape of the customer consists of 9 SAP production systems. Access of all users to these systems are to be monitored to limit extensive conflicting access rights and trigger quick resolution of access rights related issues by the appropriate end users.

State before KPMG Sofy Access Control
The organization struggles to get a reliable view on Access Risks within and between their business critical applications. Their previous solution only looked at the SAP landscape and analyzed their production systems in an isolated way without taking into account that users may have conflicting access rights in the intersection of multiple systems. There is a strong desire, driven by Internal Control and findings from the external auditor to get better insights into conflicting authorizations within the full SAP development stack as well as other business critical applications. Issues often exist with users that have access to multiple business critical applications and as such can perform conflicting activities in multiple systems. With the existing solution, the company was unable to detect these issues.

State after KPMG Sofy Access Control
By implementing the Sofy Access Control solution:

- transparency has been created within the complete SAP landscape.
- a preventive SoD check is now running continuously for every access request
- conflicting user authorizations resulting from role assignments are being reviewed and approved. This happens before they are actually assigned in the underlying system to prevent unauthorized access for end users.
- conflicting user authorizations are being reviewed continuously to ensure accurate follow-up, takes place in terms of risk acceptance, mitigation or remediation.

Key benefits
The solution helped the client gain control over their authorization controls because:

- it increased transparency in conflicting access across the full SAP stack
- continuous monitoring on each of these systems ensures quick resolution and remediation of access related risks.
- preventive SoD checks make sure unauthorized access in the system is avoided as the impact of roles changes or role assignments is clear upfront
- The implementation of this digital solution has shifted the minds from taking remedial actions in a re-active way to pro-actively avoiding and mitigating access related issues.

that already has occurred. While the Configuration and Authorization controls try to prevent risks, there is always a residual risk and this is where reporting controls come in, to detect any mistakes or fraudulent behavior that got past the preventative controls.

These reporting controls can be very strong when the executers of those controls are supported by strong dashboards and analytics. In the Compact special of January 2019, [Zuij19] presented a case on advanced duplicate invoice analysis. The article explains how they implemented smart digital tooling to create a duplicate invoice analysis at a major oil company. We advise reading this in-depth case, because it could provide helpful guidance on how reporting controls can be digitized to unlock the power to identify conclusions that were invisible or inaccessible before. This can directly increase the assurance level of this type of control because insight is provided that wasn't there before, and at the same time, it decreases the cost of control, opening up the possibility to gain back any invoices that are paid twice. Additional examples are:

- Automating the running and sending of reports using SAP Process Control
- Creating an analysis to identify the use of discounts in the sales process using SAP HANA or SQL
- Unlocking faster decision-making by providing the organization with real-time overviews of the state of internal controls. This can be achieved with a live Dashboard using Microsoft PowerBi in combination with Outsystems and SAP Process Control, or KPMG SOFY

Procedural (manual) controls

Procedural controls are manual actions performed by a human, initiated to prevent or detect anomalies in processes. They help companies cover residual risks that are not easily covered by Configuration, Authorization or Reporting controls. Examples of manual controls are:

- Signing off documents such as contracts, large orders, etc.;
- Manual reconciliation of received payments against invoices, with or without the use of a system;
- Manual data alignment between the sales system and invoice system.

Controls executed by humans, such as Reporting and Procedural controls compared to ones that are executed by a machine, have the inherent risk of the human operator making mistakes, because making mistakes is human, especially when the complexity and receptiveness of a control increases. As business complexity and the volume of data is increasing, companies are now looking into solutions that can replace or enhance human-operated controls with automated digitized ones.

To show how manual controls can be improved using digital solutions, we present a use case focused on reducing manual actions or at least reducing the effort and increasing the quality of their output. In this case, Robotics Process Automation (RPA) tooling was used to automate manual journal entries, resulting in fewer manual control actions. This reduces the cost of control because fewer FTEs are required to operate the control. Secondly, the level of assurance increases as a robot will not make mistakes even when the repetitive task is executed hundreds of thousands of times.

Use case: automating manual journal entries at a large telecommunication organization

Context
During a large finance transformation at one of the biggest Dutch telecom companies, KPMG was asked to help identify opportunities for automation within the finance department. During an assessment at the client, the processing of manual journal entries was identified as a suitable process for automation with the use of Robotic Process Automation (RPA). This happened because of the high repetitive nature of the process and the high business case value, as the process is time consuming and error prone. To show the viability of RPA within the organization and the potential benefits for the client, a Proof of Concept was initiated.

State before using RPA tooling

- Large finance team that is performing manual repetitive task daily.
- Low first-time right percentage for manual journal entries which leads to rework
- Inefficient input template for creation of manual journal entries
- Multiple human control steps embedded in the process to check journal entries before recording which is time consuming
- No clear visibility for management of prior recorded manual journal entries

State after the implementation

- Standardized a manual journal entry template for the usage of RPA
- Automated the booking of manual journal entries using RPA software
- Eliminated unnecessary steps within the manual journal entry process

Key benefits

- Higher first-time right percentage due to fewer errors performed in the process as a result of automating the process using RPA
- One fully automated process which resulted in FTE reduction
- Less human intervention necessary due to higher data quality caused by robotic input, which is more stable and less prone to error.
- Automated reports generated can be used for a better audit trail and management reporting.

LESSONS LEARNED: DIGITIZING THE RIGHT WAY

Like other projects, digitalization projects can be challenging and will have pitfalls. In this section, we will provide examples of the pitfalls we encountered, and explore how they can be prevented.

Determine the baseline

In several cases the goal of a project is set without first analyzing the starting point of the project. This can result in unachievable goals, which will cause the project to be a failure. For example, if the goal of a digitization project is: "we would like to fully automate the testing for 50% of the controls in our central control framework using tool XYZ" there are several prerequisites to achieve that goal:

1. Tool XYZ should be capable of automating the testing for these controls.
2. The feasibility of automating the testing of controls in the central control framework should be determined beforehand.
3. The end users should be part of the digitization journey to make sure they understand the tool and understand how it can be embedded in their process

In this example, setting the baseline would consist of analyzing the controls for feasibility of automation in general, then checking whether tool XYZ is capable to facilitate the aimed automation and then engaging the business users before the project starts.

Once the baseline is determined, an achievable goal can be set, and the project will have a higher chance of success.

A fool with a tool is still a fool

The market is full of tools and technology solutions, some with a very broad range of services, some with a specific focus. Each of these tools have strong points and weaknesses. These tools are often sold using accompanying success stories. However, even if the best tool is used in the wrong way, it won't be successful.

As an example, we could consider SAP Access Control, a tool which can be used to monitor potential Segregation of Duties conflicts in an ERP system. When the tool reports SoD conflicts, an end user should follow up on the conflicts. In the case of SAP Access Control, a user has the ability to assign a control to an access risk to let the system know the risk has been mitigated. In reality, many users assign a control in the system to hide the results of SAP Access control by showing them as "mitigated", while in reality the actual risk in the ERP system is still there as the control is not really executed. In this case, the tool is just as good because the end user decides to use it. Good examples of how to use this tool properly can be found in the article of van der Zon, Spruit and Schutte ([Zon13]).

To ensure that a tool or solution is used in the right way, make sure that the end users are involved and properly trained in the tool or solution. If they see the benefits, the adoption will be easier and the tool or solution can be used to the full extend, moving towards a more digitized organization.

Who controls the robot?

Governance is an important topic in relation to technology solutions. In a landscape where controls are tested automatically, reports are being generated by a data analytics platform and manual tasks are performed by robots there is still manual intervention of humans.

The automated testing of controls needs to be configured in the tool or solution. As part of the implementation project this is probably tested and reviewed, but what happens after that? How do organizations make sure that nobody changes the rule-based setup for the automated testing of the controls? This question is relevant for every tool or technology solution used for digitization of processes. If there are separated robots to perform conflicting activities within a process, but both robots can be accessed by the same person, the conflict and underlying risks still exist. To resolve this, proper governance of the technology solution or tool should be put into place.

Working together

In larger corporations, each department might have their own budget and their own wishes and requirements. However, if each department is working on digitizing individually, a lot of effort is wasted. Re-inventing the wheel is costly and will slow down overall progress.

When all powers are combined, requirements are bundled and effort is centralized, digitizing the processes will make more sense and implementation can be faster and cheaper. It's about connecting individual digitizing efforts to achieve the next level.

CONCLUSION

The digitalization of internal control entails more than selecting and implementing a new tool and learning how to use it; it is the use of digital technologies to change the way the business or a department works and provides new value-producing opportunities for the company. Onboarding new tooling will therefore require enhancements on your operating model to be set for success.

Different aspects of the operating model need to be considered. Think of the potential impact on the ICF when automation impacts the role between the business and internal control. People and skills are impacted when internal control takes a role in the configuration or maintenance of automation rules, requiring certain technical capabilities and skillsets. In today's digitalization, a more agile way of working is usually better, potentially impacting the required capabilities of the internal controllers. From technology perspective, automation has a major impact because of the integration within or connection with the existing IT landscape. This is even more so the case when RPA is used, impacting aspects such as governance, maintainability and security. Finally, automation within the internal control realm will have an impact on the current way of reporting, also considering auditability.

Taking the time and effort to define the impact on the operating model of your ICF and to devise a detailed plan on how to use digital control options, is the key to success.

Acknowledgements

The authors would like to thank Sebastiaan Tiemens, Martin Boon, Robert Sweijen and Geert Dekker for their support in providing use cases, feedback and co-reading the article.

References

[Cool18] Coolen, J., Bos, V., de Koning, T. & Koot, W. (2018). Agile transformation of the (IT) Operating Model. *Compact* 2018/1. Retrieved from: https://www.compact.nl/articles/agile-transformation-of-the-it-operating-model/

[Günt19] Günthardt, D., Hallemeesch, D. & van der Giesen, S. (2019). The lessons learned from did-do analytics on SAP. *Compact* 2019/1. Retrieved from: https://www.compact.nl/articles/the-lessons-learned-from-did-do-analytics-on-sap/?highlight=The%20lessons

[KPMG19] KPMG (2019, May). Survey - Governance, Risk and Compliance. Retrieved from: https://assets.kpmg/content/dam/kpmg/ch/pdf/results-grc-survey-2019.pdf

[Vree06] Vreeke, A. & Hallemeesch, D. (2006). 'Zoveel functiescheidingsconflicten in SAP – dat kan nooit', en waarom is dat eigenlijk een risico? *Compact* 2006/2. Retrieved from: https://www.compact.nl/articles/zoveel-functiescheidingsconflicten-in-sap-dat-kan-nooit-en-waarom-is-dat-eigenlijk-een-risico/?highlight=hallemeesch

[Zon13] Van der Zon, A., Spruit, I. & Schutte, J. (2013). Access Control applicaties voor SAP. *Compact* 2013/3. Retrieved from: https://www.compact.nl/articles/access-control-applicaties-voor-sap/

[Zuij19] Zuijderwijk, S. & van der Giesen, S. (2019). Advanced duplicate invoice analysis case. *Compact* 2019/1. Retrieved from: https://www.compact.nl/articles/advanced-duplicate-invoice-analysis-case/?highlight=Advanced

About the authors

Sylvester van der Giesen MSc is a senior manager at KPMG Advisory. He has been with KPMG since 2012 and focuses on the intersection between business and IT with a strong focus on risk consultancy. Sylvester is experienced in SAP Internal Control and technology solutions in the area of governance, risk and compliance such as SAP Process Control and SAP Risk Management.

Vincent Speelman MSc is a senior consultant at KPMG Advisory. Vincent has been with KPMG since 2017 and has a focus on the intersection between business and IT related to multiple ERP Systems such as Microsoft D365 Finance and SAP. Vincent has an all-round experience in Microsoft D365 and SAP on the areas of Configuration, semi-automated and Authorization controls.