Control by Design: risk-free processes as the holy grail

An important concept for saving costs and increasing your risk management. Nice theory, but what about practical application?

Thomas Schoonhoven MSc
is Risk Control Partner at Rabobank.

Robin Polder MA
is Lead Data & Technology of Team Customer Remediation at Rabobank Retail NL.

Risk management is gaining an increasingly prominent role within organizations. In a rapidly changing environment, increasing digitalization and more stringent regulations regarding service delivery, good risk management is a challenge. For a more automated risk management, the term Control by Design is used regularly, not only within financial institutions but also as an important risk trajectory for the future at other organizations. But what does this term mean? And why should it be necessary to embrace and apply this way of thinking? This article explains the background and opportunities of Control by Design. It also looks at the application, the possible barriers and how to deal with them to make the concept more concrete.

Bart Olieman
is Product Manager Businesses at Rabobank.

Mourad Fakirou MSc RE
is a manager at KPMG Digital Transformation.

This article is also a call to other organizations to exchange views.
Please send an email to info@compact.nl if you want to share your ideas.

INTRODUCTION

Business processes change continuously. Optimization takes place, (sub) processes or IT systems are outsourced, new products or services are developed, and old products or services are discontinued but still need to be managed. Laws and regulations or (internal) policies are introduced or modified, new risks appear or existing risks are weighed differently. In addition, reorganizations take place, responsibilities and priorities shift. This translates into more complex processes, the implementation of (manual) workarounds in order to meet new requirements. All this often happens faster than many IT departments can manage. This is also reflected in the controls, where manual checks on the workarounds and exceptions continually drive up costs and include the risk that those manual checks are not carried out adequately.

The complex and constantly changing and more burdensome regulations mean that important risks can no longer be mitigated by manual control measures alone. Further, in addition to the increasing costs of the process itself, there is increasing pressure on monitoring. Assurance on the operation of the control framework is sought through increasing first-, second- and third-line controls, driven by the Three Lines Lines Model (3LM). The costs of the manual work involved in implementing the control measures *plus* the costs associated with manually monitoring the operating effectiveness of the control measures lead to an ever-increasing cost of control.

Three Lines Model

The Three Lines Model (3LM) consists of three lines that together oversee the management of risk. The first line consists of managers and employees who are responsible for identifying and managing risks as part of their daily work. The second line provides support and guidance by offering guidelines, policies and control frameworks. In addition, the second line also takes care of monitoring to determine that the risks are correctly managed. Finally, the third line focuses on an independent review or audit of the control framework as a whole or parts thereof, including the activities of the first and second line. Often this role is fulfilled by an internal audit department ([CIIA21]).

Besides the complexity mentioned above and the increasing cost of control, we see increasing digitization. Financial institutions are increasingly serving customers online, adapting processes and IT systems. Customer journeys are designed and adapted and new systems are purchased and/or developed. Redesigning and re-implementing processes gives you an opportunity to also manage your risks differently or, better yet, to prevent them. By including the (process) risks as early as possible in your design, you can organize the control of these risks much more efficiently. Read "Control by Design"! A groundbreaking and new idea? Well, no, but it is one that needs to be put into practice in order to actually reduce the cost of control. To achieve this, we will first consider the definition of Control by Design and offer thoughts on how to embed it into the change processes of the organization. We will subsequently explore scenarios in case optimal Control by Design is not feasible, and we will conclude with a number of obstacles and pitfalls one may need to overcome during the implementation of Control by Design.

CONTROL BY DESIGN: RISK MANAGEMENT AS A FIXED PART OF THE (IT) DEVELOPMENT PROCESS

The term Control by Design is not new. And so-called Application Controls have also been used and implemented for quite some time. The benefits are clear. A well-programmed IT system will do the same thing every time, even on a Monday morning or Friday afternoon. In addition, in terms of monitoring, you don't need to do labor-intensive customer document monitoring, but instead the Application Control can be tested during the implementation or system change. For the Application Control to continue to function, you can rely on well-designed IT processes (General IT Controls) to ensure that the system continues to do what it is supposed to do. Adequate General IT Controls guarantee a controlled system change process, effective authorization management, and assured system continuity ([ISAC11]). These elements are a prerequisite for determining that an automated control (Application Control) continues to do what it is supposed to do.

Yet within organizations we see that such automated control measures are not always used to their full potential. Several things can stand in the way of broad automation. One example is that the implementation of automated control measures can be complex, expensive and vulnerable to change. It may also be that these measures are not given sufficient priority in change processes because such change processes generally focus on realizing business value. For example, choices are made to automate only *key* risk mitigation.

The difference between Control by Design and reactively implementing Application Controls (or automating existing manual controls) where risks become manifest, is that Control by Design is about setting up a process in such a way that certain risks are controlled (prevented or

mitigated) directly from the process design. This means that the process and the associated risks are the starting point of the risk mitigation, instead of the automation of already existing control measures. It is important to ensure good interaction between the process owner (who knows how his process is structured), the risk manager (who knows where the risks and controls manifest themselves in the process) and the IT specialist (who knows what systems and data are used in the process). By aligning the risk management process to the development process of a product and/or IT system (modification), it is ensured that identifying the root cause of the most important risks, and automating the associated controls, becomes a part of the organization's standard change mechanism. When prioritizing the change calendar, make sure that it is clear which risk-related changes (e.g. implementing a hard input control) can be included in planned changes (e.g. modifying input screens). After all, it is cheaper to replace the sewer pipe if the street is going to be opened up anyway to install the fiber optic network.

The idea here is as, for example, Elon Musk mentions in his First Principles approach: go back to basics. When you set up the process from scratch instead of adapting an existing process, you are more likely to come up with a different and possibly better suited design. This works best in a greenfield situation, where design choices can still be made and less restrictions exist resulting from an existing system landscape. The reality is that those situations are rare. So you should strive for a situation where the change processes take into account the objectives of Control by Design by default. This article focuses on that challenge.

Example

An example is offering a discount on a customer rate. Of course, this can be done by configuring manual discount authorization/approval levels in the system. A more efficient step, as well as less error-prone, is to let the system determine which customers are eligible for standardized discounts and to apply them automatically. And if the business operation can also work from fixed rates, then the process should already be set up so that discounting is not possible at all. The risk of incorrect or unjustified discounts is therefore enforced from within the process. Going back to basics: the (re)design of process and IT system.

Control by Design essentially focuses on preventing as much risk as possible in the system design of the process

APPLYING CONTROL BY DESIGN IN PRACTICE

To apply Control by Design, traditional risk management or process models remain in place. Indeed, for broad acceptance and proper operation, it is important to embed Control by Design into the models that are already used by the organization.

It is important to bring different disciplines together as much as possible: the process owner, risk management and the IT delivery partner. This is where two processes come together: the risk management cycle and the (IT) development process. It is in these processes where the Control by Design philosophy needs to be applied.

We recognize four important preconditions for the success of Control by Design. The first precondition is to *apply Control by Design during the implementation of new IT systems and the digitization and/or adaptation of processes.* The development process goes through the various phases of intake, analysis and determination of the requirements, in order to then build and implement these requirements. Whether you work according to a waterfall, agile or other development methodology, it always comes down to the fact that during the development process several steps of the risk management cycle are integrated, from identifying risks to mitigating and determining the monitoring strategy. In Control by Design, you want to align these steps and look specifically at where IT systems can be adapted to reduce certain risks or, better still, to eliminate them.

To do that, it must be clear which part of the end-to-end process is planned to be changed. To mitigate the risk, it is important to focus on the root cause of the risk. The BowTie and Five Times Why methodologies can be used to identify these root causes. The BowTie method breaks down the risk description into cause, event and effect

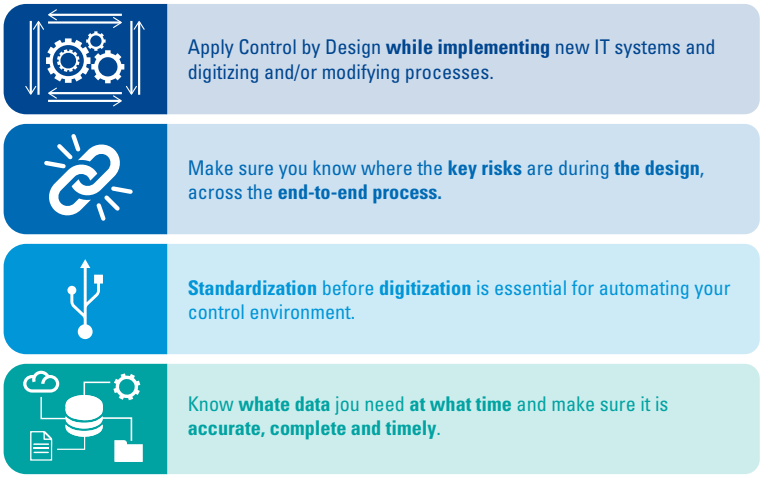
([Culw16]), after which elaboration on the cause can be achieved by asking several times why the risk arises. This is how you arrive at the final root cause ([Serr17]). If this root cause occurs in the part of the end-to-end process where a change is planned, Control by Design becomes particularly important. In order to be able to identify a risk, to perform the root cause analysis *and* to come up with the best approach to eliminate or (automatically) mitigate a risk in the process, the broad expertise of business, risk management and IT needs to be brought together at the right time during the change process.

This brings us to the second precondition; make sure that *during the design you know where the key risks are* located across the entire width of the business process. The end-to-end insight based on broad expertise is needed at that moment, because the actual root cause of a risk can occur in a completely different part of the process than where the focus lies at the moment of change. An example is when clients provide incomplete documents when requesting a product, which may result in incorrect advise or product approval. This risk can be mitigated in the closing phase by asking the client to submit these documents to complete the request, but carries the risk that the whole assessment and advise process needs to be reperformed to take the information of this documentation into account. Ideally, the cause of the risk can be eliminated in the intake phase, prior to the assessment and advise processes. With the end-to-end process approach, risks are identified across the process and system chain and control measures can be implemented at (or as close as possible to) the place where they arise. This prevents the duplicate implementation of control measures that mitigate the same risk and thus benefits efficiency. From the traditional risk analysis perspective, this step for Control by Design is of additional importance to shape the design in the right place and in a timely manner. You can replace the sewer pipe where the street opens up, but if the real problem is that far too much water needs to be drained, you're better off replacing the pavement with urban gardens.

The third precondition is to *standardize before you digitize*. For Control by Design, the principle is that the more a process is standardized, the simpler the process and the easier it becomes to avoid a risk. This is not a new concept but it is an important basis, although it is not always possible. An indication of a lack of standardization is there being too many deviations/workarounds in the process. We will discuss this in more detail later in the article.

The fourth precondition is to *have the right and accurate data* to be able to use a properly functioning automated control measure (Application Control). It needs to be clear what data is needed at what point in the process. This data must be accurate in order for the control to function properly. After all, garbage in = garbage out. Data needs to be collected from reliable sources, after which the accuracy, completeness and timeliness of the data needs to be determined before its use as a basis for an application control.

Figure 1. Four preconditions for Control by Design.



Example

Customer relationship management is important as a part of overall customer service. Does the customer still have the product that best matches his situation? In order to properly conduct customer relationship management, it is necessary to schedule customer contact in order to assess financial product suitability ,to record the notes of conversation and to plan the necessary follow-up actions. High workload and operational errors pose risks to this process. Using IT system support, several process risks can be reduced. CRM software builds in triggers for scheduling the customer appointments. During the appointment, the advisor walks through a workflow process within the IT system with the customer, completes the questions and automatically records the choices in the system. The report cannot be completed in the IT system until the advisor has provided their explanation of any exceptions or specific customer choices. The IT system then automatically saves the report in the customer file and e-mails it to the customer. Many actions are taken over by the IT system. The risk of not engaging in a timely conversation with the customer, not ensuring that all required questions are addressed, not having a record of the conversation, and not actually receiving the relevant information is reduced.

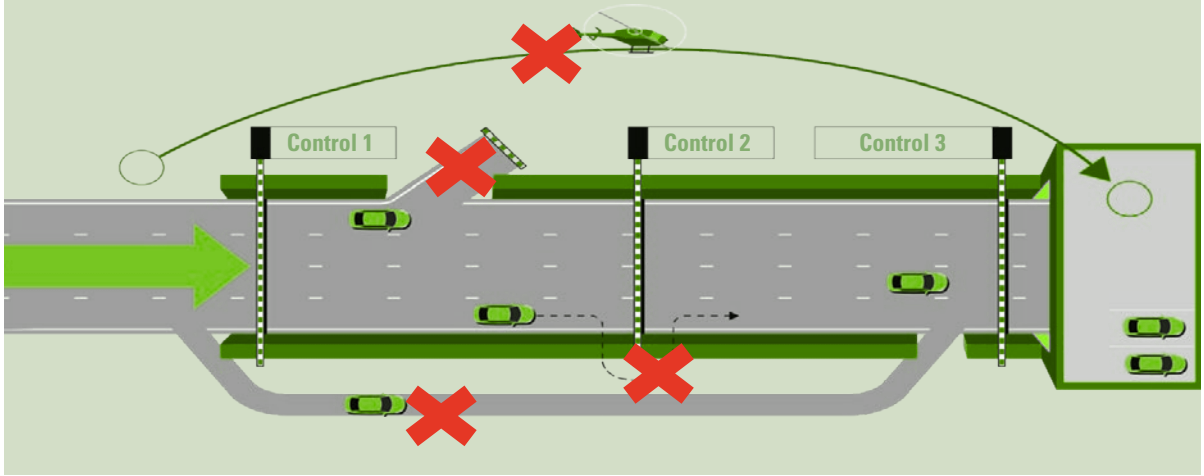
Applying Control by Design is easier said than done

It looks simple on paper and the idea finds many supporters who recognize the benefits, not the least from the cost savings perspective. Who wouldn't want to make more use of automated control measures to prevent manual work or make it impossible to make mistakes in the first place? However, the reality is different, especially in a more complex organization and a complicated IT landscape that has grown evolutionary. Without specifically taking into account the dilemmas raised by Control by Design, the chances of successful application are greatly diminished.

Some important things to consider in advance:

1. **Control by Design is not necessarily (just) automating the existing manual controls**
   Manual controls in the process are performed in a different way than Application Controls or IT Dependent Manual Controls. For example, there may be more professional judgment involved, information needed to perform the control may have to reach the reviewer in different ways through different IT applications, information is recorded in documents instead of structured data, and so on. Automating the action performed by the controller is not the goal of Control by Design: ideally, the step should become redundant (e.g. through a preventive control at the right place in the process). This difference must be clear in order to avoid disappointment in the application of Control by Design and thus hinder its success.
2. **Control by Design is ineffective when there are too many deviations in the process**
   A complex process is more difficult to control. When there are many product/process variations, it can be a lot of work to implement an automated, preventive control measure on all deviations that actually mitigate the risk in the process. Professional judgement necessary to perform a control and a lot of room for overruling business rules make it difficult to adequately mitigate risks via application controls. Theoretically, everything can be automated, but at irresponsible costs and with the result that the systems themselves become too complex.
   The better the processes are standardized, and the more product rationalization has taken place, the better the systems can be set up for preventive automated controls.
3. **Control by Design also takes change capacity and thus requires priority**
   Implementing and applying Control by Design requires commitment and investment prior to the actual IT implementation, at the expense of the available change capacity. Agile development teams with overflowing backlogs steer towards realizing as much business value as possible. A conscious prioritization of the requirements of Control by Design is therefore necessary but not popular – the value only becomes apparent when avoiding manual activities the cost of

Figure 2. The highway. Control by Design standardizes the primary process and eliminates or monitors possible deviations that can bypass controls.



which is usually not adequately weighed against the return of other changes prioritized in a sprint. Therefore, when implementing Control by Design, its rules should be enforced: i) deviations from the Control by Design principles and steps in the change process should be made visible; ii) deviations should require formal approval; and iii) temporary acceptance of deviations should be monitored to ensure the right priority on the backlog later on. For example, when an IT system change involves a manual check instead of removing the root cause, this is a deviation from the Control by Design principles and should thus follow the above mentioned steps.

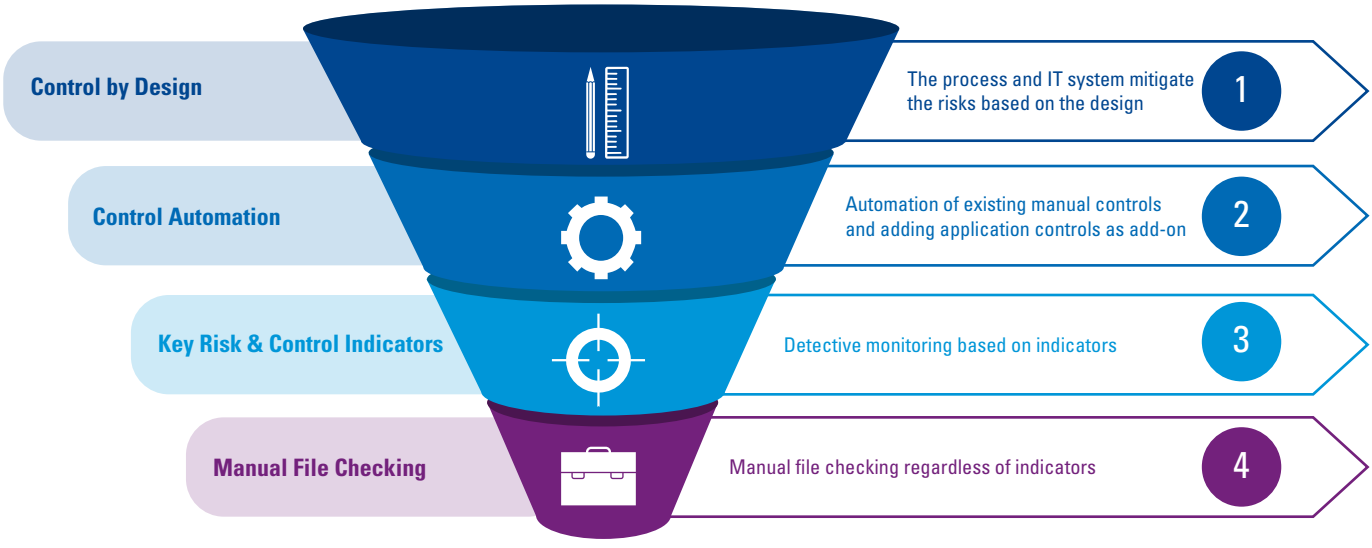
4. **Combined insight into the end-to-end process, IT and risk helps to make the right design choices**
A key objective of Control by Design is that risks should be prevented where they arise. But where is that? End-to-end processes are often long and complex, and transcend the responsibility of individual teams – at the functional, infrastructure and IT application levels. Parts of the process or technology may have been outsourced. Other parts may be using legacy IT products. Making changes in such cases is often complicated, costly and not future-proof.
In practice, it is difficult to bring all the necessary knowledge together to deliver the right insights. Process documentation may be outdated, incomplete or insufficiently detailed. There are few employees who can oversee the entire process and their time is scarce. A (key) risk analysis at process level with a good understanding of the root causes of risks is indispensable. The importance of involvement of the complete "triangle" of process, IT and risk with the aim to strengthen each other and speed up the development process cannot be stressed enough. Additionally, we emphasize the need to ensure enough time to properly map out the risks and their root causes.

5. **The responsibility for implementation of an IT change that addresses a root cause may differ from where the risk manifests itself**
Even if a solid risk analysis identifies a clear root cause and the necessary (IT) change to prevent or mitigate the risk, the IT change needed does not in all cases fall within the responsibility of the team that feels the impact of the risk.
Other scrum/development teams have their own responsibilities and priorities. Implementing a fix on a root cause may not score high on their list at that point in time. As a result, quick fixes and workarounds are often implemented, which take the pressure off the necessity to tackle the real root cause and leads to suboptimal solutions (... and go back to item 3 on this list). The parks department doesn't have time to realize the urban gardens at present, so maybe just replace the sewer pipe for now?

CONTROL BY DESIGN FUNNEL AS AN ALTERNATIVE

At the beginning of the article, lowering the cost of control was mainly broken down into two parts. With the (automated) prevention of risk, control costs in the primary process are decreased. Another way to reduce the cost of control is by more effective monitoring of the effective operation of controls. Manual file checking is the most labor-intensive form of monitoring. The Control by Design Funnel (see Figure 3) can be applied. This funnel indicated that the highest possible level of (automated) risk control lies in the development process. A lower level should only be examined if higher levels are not possible or the benefits do not cover the costs.

Figure 3. Control by Design Funnel.



In order to apply the funnel properly, it is important to not only assess the control measures during risk analysis, but also to adopt a monitoring strategy. As mentioned in the introduction, we see that more and more assurance is sought within organizations by intensifying the testing of operating effectiveness of controls and monitoring whether certain risks still occur. Automated control testing (funnel option 2, see Figure 3) and smarter control testing by using data (funnel option 3) will in that sense contribute to reducing the cost of control. Requirements to enable this automated or smarter indicator-driven control monitoring need to be provided to the software development team as an outcome of the risk analysis, subsequent assessment of the Control by Design (im) possibilities and selection of the alternative according to the funnel.

Example

In an ideal scenario, the risk of not having a record of a customer conversation is prevented by the CRM process as mentioned in the previous example. If automating the process to such an extent is unfeasible at the moment, one could consider automated monitoring to determine whether all the customer appointments conducted that week have resulted in a record saved in the customer file. If this monitoring cannot be automated either, then one can look at the next layer in the funnel, which is based on indicators. It has been established that the cause of an incorrect customer conversation record is a lack of time on the part of the advisor writing a report of his conversation with the customer. If the report is prepared within a day of the conversation, errors are almost never found. Should it take longer, the chance of a faulty record has grown exponentially. Thus, the time between the appointment and storing the record of the interaction is a quality indicator, a means of determining whether the control measure is working adequately. If the indicator shows that less than 95% of the advisor reports are saved within 2 days of the appointment, additional quality checks become necessary. Such monitoring does require that you are able to get the right data from the systems. The method of monitoring must therefore be included during the development process and introduced as a requirement during development. If these requirements are not included, often the only remaining option to assess whether the process is "in control" is the least favored, labor intensive level 4: manual file checking.

CONCLUSION: CONTROL BY DESIGN IS AN IMPORTANT CONCEPT FOR COST SAVINGS AND BETTER RISK MANAGEMENT

There is no universal blueprint for implementing Control by Design. Organizations differ from each other, and the way Control by Design is implemented can therefore vary. This depends, for example, on time, the maturity of the organization and the willingness to embrace the concept. It is therefore important to work towards objectives that are achievable for a specific organization.

Control by Design is an important concept to better manage risks and reduce the cost of control. Implementing the concept sounds simple, but in practice it can be

There is no universal blueprint for implementing Control by Design

problematic. There are several challenges to be encountered. Implementing Control by Design requires priority, an end-to-end process perspective and the right expertise to be at the table. It is a long-term process to adopt Control by Design as an integral part of the IT change process. Rollout comes down to small evolutionary steps, rather than radical change. It is important to make the right choices in how to deal with the scarce IT capacity: make sure you only have to develop control measures once by applying them in the right place. The effort that is invested during IT development will be more than returned after implementation. Expensive monitoring can be avoided as well as labor-intensive manual file checks to see whether the process is running smoothly.

This requires good anchoring of Control by Design in existing IT development and risk processes. Make the steps and tools as concrete as possible and make it mandatory, measurable and visible.

In addition, there are often other initiatives in the organization associated with Control by Design. Examples are Security by Design and Privacy by Design, Business Process Management or implementations of agile software development methods. These initiatives can reinforce each other and accelerate the transition to Control by Design. So take advantage of this to join forces.

Do you recognize the desire to apply this, are you curious about the experiences or do you want to know more? We warmly invite you to exchange views with us.

References

[CIIA21] Chartered Institute of Internal Auditors (2021). Position paper: The three lines of defence. Retrieved from: https://www.iia.org.uk/resources/delivering-internal-audit/position-paper-the-three-lines-of-defence/

[Culw19] Culwick, M.D. et al. (2016). Bow-tie diagrams for risk management in anesthesia. *Anaesthesia and Intensive Care 44*(6), 712-718. Retrieved from: https://journals.sagepub.com/doi/pdf/10.1177/0310057X1604400615

[ISAC11] ISACA Journal Archives (2011, September 1). IT General and Application Controls: The Model of Internalization. *ISACA Journal*. Retrieved from: https://www.isaca.org/resources/isaca-journal/past-issues/2011/it-general-and-application-controls-the-model-of-internalization

[Serr17] Serrat, O. (2017). Proposition 32: The Five Whys Technique. In O. Serrat, *Knowledge solutions* (pp. 307-310). Retrieved from: https://www.researchgate.net/publication/318013490_The_Five_Whys_Technique

About the authors

Thomas Schoonhoven MSc is Risk Control Partner at Rabobank. After several risk management positions in the first and second line, he is currently thought leader Control by Design and is responsible for the implementation within the Retail NL domain.

Robin Polder MSc is Lead Data & Technology of Team Customer Remediation at Rabobank Retail NL. He has a background in IT audit and major IT transformations within the financial sector. Within Rabobank, he is responsible for the deployment of data analytics and technology solutions to identify, prevent and, if necessary, execute (potential) recovery programs.

Bart Olieman is Product Manager Businesses at Rabobank. He has held various positions in the field of corporate finance. Currently he is involved in risk management. He is a strong advocate of making the management of risks within organizations more automated and efficient. He carries out the work within the Squad Control by Design.

Mourad Fakirou MSc RE is a manager within KPMG's Digital Transformation department. He built up extensive experience in the financial and tech sectors over the past five years, combined with expertise regarding IT strategies.