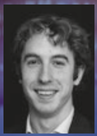
Trust by Design: rethinking technology risk

Enhancing technology risk management in agile environments to ensure auditable trust!

Swatantra Kumar, M.Tech, PGDAC, BE
is a senior manager and Head of Solution Design and Development Function at KPMG.



Stefan Jacobs
is a manager at KPMG.

Tom Koehler
is Chief Technology Officer, KPMG NL, and Global Head of the KPMG Citizen Developer Program.

In society, there is a growing call for trust in technology. Just think about the data leaks and privacy issues that hit the news almost on a daily basis. Organizations tackle these issues through risk management practices and implementing controls and measures to ensure meeting the risk appetite of the organization. But the implications go further, last year the Dutch privacy watchdog stated that organizations should be very careful in using Google cloud services due to their poor privacy practices. This is not only challenging for the vendor but also for the clients using the services. Another example is Apple. They are doubling down on privacy in their iCloud and iOS offerings, so users trust them more as a brand, which increases their market share.

This raises several questions: What is trust? When do we decide to trust someone or something? And how can you become trusted? Do we overlook what trust really means, or do we have an innate sense for "trust"? But how does that work for organizations consisting of hundreds or thousands of people and complex business-to-business structures?

INTRODUCTION

The questions above seem to be easily overlooked when someone says, "trust me on this one", or "have some trust in this". For example, imagine you are buying a used car and the salesperson shows you a car and says "trust me, it is in perfect condition" we first want to look under the hood, open all doors, ask for a maintenance log, and of course do a test drive. Then imagine a colleague with whom you have been working for years tells you to trust them on some work-related topic, you tend to trust that person in an instance. That is looking at trust from a personal perspective. For business to business, the easiest direction to point at are contracts and formal agreements. But these only go so far and do not protect organizations or, maybe to a greater extent individuals against every risk. It's important to not only look at whether a solution works well, but also if it meets your trustworthiness requirements across the wider value and supply chains. In our hyper-connected world, we rarely see stand-alone technology solutions anymore; we see systems of systems interacting in real-time. The ability to govern technology comprehensively can help you avoid potential ecosystem risks while fostering stronger alliances based on shared governance principles.

THE CONCEPT OF TRUST

In the audit, we use the saying "tell me, show me, prove it" (or something similar) where we list three ways to support a claim in order of lowest to the highest level of assurance. This implies that trust is the lowest level of assurance which is, strictly speaking, of course true. However, despite this, humanity has built many constructs of trust which we rely on, on a daily basis: money, legal structures, law, and governments, just to name a few. In the book *Guns, Germs, and Steel: The Fates of Human Societies* by Jared Diamond ([Diam97]), the concept of creating these "fantasy" constructs in which we put a lot of trust, is posited as a cornerstone of human progress.

The concept of trust is hard to define

In the risk management world, an example of trust we often come across is assurance reports. Frameworks such as ISAE, SOC, and ISO are trusted to be relevant and properly applied. These are all tools or constructs that we trust to keep our data, investments, or processes safe. These constructs are used as ways of trusting each other in the B2B world. These types of trust concepts are, to an extent, widely accepted, and rightfully so. However, isn't it strange that we put so much trust in the authors of the frameworks or the independent auditors that validate these frameworks? Is this a case of blind faith or is it the trust we have and put in these types of constructs based on something more that we might take for granted?

The concept of trust is hard to define. You can look it up in a dictionary and depending on the one you use, the definitions vary. However, you can leave it up to academia to relentlessly structure things. In a meta-analysis, a well-founded concept of trust has been derived ([McKn96]). The act of trusting, or trusting behavior has 5 different precursors, where trusting intention (1) directly causes the trusting behavior. Trusting Intention is the extent to which one party is willing to depend on the other party even though negative consequences are possible. In general, people tend to form trusting intentions based on their beliefs, or trusting beliefs (2). These are formed from current, and prior experiences (dispositional trust (3)). In addition to that, there is a component that is caused by the system (4), and trust in that system (5). The system in this context can be a wide variety of systems given the situation, for example, an IT system or a management system.

Another concept of trust is that individuals want to have an amount of certainty that positive events unfold, and do not like risks that might reduce the certainty of said events. Trust could therefore also be considered as a feeling that there is low exposure to risks. This concept of risk exposure is also used in research to understand technology adoption, and trusting behavior ([Lipp06]). This research mentions predictability and reliability as two core features that can be used to evaluate trust in technology.

Most of these conceptions of trust are based on personal trust, or the trust behaviors of an individual ([Zahe98]). There is however a distinction between personal trust and organizational trust. The latter is considered to be a function of the combined personal trust of the employees of an organization. This seems to indicate that the predictability, reliability, and usability of technology can increase trust in a technology through the reduction of risks towards the potential benefits of using said technology. This, however, does not explain how organizations trust technology or other organizations. On the other hand, organizations consist of individuals that work together, so there is a clear connection between personal and organizational trust ([Zahe98]). There are different views on how this works, and the debate on how trust complements or replaces formal agreements and contracts seems to be ongoing. A lot of research was done into various facets of *trust* and how it works between two actors (e.g. [Noot97]). What literature does agree on is that trust can work as a less formal agreement between organizations and allows for less complex and costly safeguards when compared for contracts or vertical integration ([Gula08]).

Based on this, we broadly derive that trust will always play an important and above all positive role in organizational and interpersonal relationships (although the exact implications might be not completely understood at this point). It does however show us that trust can complement governance models and operationalizing this concept can be beneficial to organizations on various levels, bringing efficiency gains and maybe even competitive advantage ([Sydo06]). Trust in technology can be achieved by the demonstration of predictable and reliable positive outcomes, and a high degree of usability.

ACHIEVING TRUST IN PRACTICE

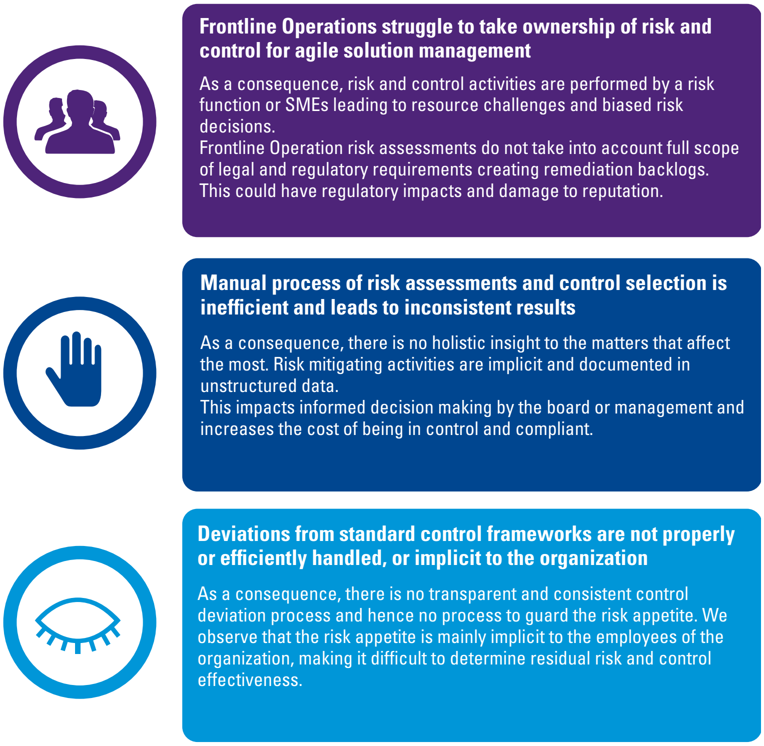
Now that the theoretical concept is uncovered to a degree, we can look at the practical aspect and a framework that is capable of governing how a trust should operate. First, we should probably set some conditions. As the concept of trust is very broad, we cannot cover the entire topic; we will therefore first look at the internal organization, the way organizations adopt technology and perform innovation and change projects.

Usually, these types of changes are governed by risk management processes that try to optimize the benefits while at the same time reducing the risks of non-compliance, security deficiencies, or reduced process effectiveness.

"*Risk management*" is the term used in most cases, but we also see that "*risk management and a lot of other stuff*" is sometimes more applicable to reality. With "other stuff" we mean a lot of discussions on risks and mitigation, creating a lot of controls for things that might not really need controls in the first place. Then we come to testing these, sometimes overcomplete, control frameworks, to a degree that some organizations are testing controls for the sake of testing them. Testing is followed by reporting and additional procedures to close gaps that are identified. Usually, this has to be done on top of regular work instead of having embedded or automated controls that just operate within the processes themselves. In various industries, regulators impose more and more expectations regarding the way that risks are managed. In addition, there are increasing expectations from society on how (personal) data is protected, and the way organizations deliver their services. This includes far-reaching digitization and data-driven processes, required to support customer requirements. These expectations, technological advancements, and the ever-increasing competitiveness in the market create a gap between often agile-driven product delivery and risk management. Unfortunately, we also see that, as a natural reflex, organizations tend to impose even more controls on processes which further inflates the "other stuff" of risk management.

From a classical risk management standpoint, risks are mostly managed through the execution of controls and periodic testing of said controls. These controls are usually following frameworks such as ITIL or COSO. In many organizations, this type of work is divided between the so-called first, second, and third lines of defense. Recently we have seen that especially the first and second lines of defense are positioned closer to each other ([IIA20]). In practice, this results in more collaborative efforts between the first and second lines. Regardless of how exactly this structure should be implemented, the interaction between the first two lines of defense is increasingly important: organizations' risk management practices often struggle to keep up with the momentum of the product teams that are releasing changes, sometimes multiple times a day. These releases can introduce risks such as privacy or contractual exposures that can be overlooked by a delivery-focused first line.

Innovations and technology adoptions are performed by the collective intelligence of teams that have a high-risk acceptance and focus on getting the highest benefit. Collective intelligence can be broadly defined as the enhanced capacity for thought and decision-making through the combination of people, data, and technology. This not only helps collective intelligence to understand problems and identify solutions – and therefore deciding on the action to take – it also implies constant improvement. The experiences of all involved in the collective are combined to make the next solution or decision better than the last. However, risk management practices are required to be embedded within the innovation process to ensure that the risk acceptance of the organization as a whole is not breached. Take for example the processing of personal data by a staffing organization. This can be extremely beneficial and lead to competitive advantages if done properly. However, this is not necessarily allowed



Frontline Operations struggle to take ownership of risk and control for agile solution management

As a consequence, risk and control activities are performed by a risk function or SMEs leading to resource challenges and biased risk decisions.
Frontline Operation risk assessments do not take into account full scope of legal and regulatory requirements creating remediation backlogs. This could have regulatory impacts and damage to reputation.

Manual process of risk assessments and control selection is inefficient and leads to inconsistent results

As a consequence, there is no holistic insight to the matters that affect the most. Risk mitigating activities are implicit and documented in unstructured data.
This impacts informed decision making by the board or management and increases the cost of being in control and compliant.

Deviations from standard control frameworks are not properly or efficiently handled, or implicit to the organization

As a consequence, there is no transparent and consistent control deviation process and hence no process to guard the risk appetite. We observe that the risk appetite is mainly implicit to the employees of the organization, making it difficult to determine residual risk and control effectiveness.

Figure 1. The issue at hand.

in the context of European legislation. This is where risk management plays a significant role in, for example, limiting the usage of personal data. In innovative teams, this is however not always perceived as beneficial. Risk management can therefore be seen as a limiting factor that slows down the organization and makes processes murky and bureaucratic. Unfortunately, this compliance pressure is true and present in a lot of organizations, see Figure 1. There is, however, another perspective that we want to highlight.

A good analogy is a racing car, which purpose is to achieve the fastest track times. This is achieved by a lot of different parts all working together to reach the fastest time. As racing tracks usually consist of higher and lower speed corners; a strong engine and fast gearbox are not enough to go the fastest. Good control with suspension and brakes that can continue to operate under a lot of stress, is just as important as the engine. This is no different with business teams, they need a powerful engine and gearbox to go forward quickly, but the best cars in motorsports have the best brakes. These roles are performed by an organization's risk management practice. Data leaks, hacks, and reputational damage can be even more costly than slow time to market. However, there is an undeniable yearn from business teams to become more risk-based as compared to compliance-based.

In an agile environment this is also, or maybe even more, true. To achieve risk management in an agile world, risk management itself needs to become agile. But with the ITIL or COSO focused periodic testing of controls, the outcomes will lag behind. Imagine that testing changes every quarter. Before this has been tested and reports are written, numerous new changes will have been triggered already. With a constantly changing IT landscape, the gap between the identified risks from these periodic controls will no longer be an accurate representation of the actual risk exposure. This is called the *digital risk gap*, which is growing in a lot of organizations.

To close, or at least decrease the gap, the focus should be on the first line process; the business teams that implement changes and carry forward the innovations. It is most efficient to inject risk management as early in the innovation process as possible. In every step of the ideation, refinement, and planning processes, risk management should at least be in the back of the minds of product owners and product teams.

To achieve this risk awareness and to close the digital risk gap a framework has been developed that incorporates concepts from agile, software development, and risk management to provide an end-to-end approach for creating trust by reducing risks in a proactive and business-focused approach. This is what we call **Trust by Design**, and takes the concepts from the integrated risk management lifecycle (see Figure 2) into practice.

The goal of Trust by Design is to achieve risk management practices in an agile world where trust is built by design into the applications and solutions by the people who are building and creating them. Due to the high iterative and fast-paced first-line teams that are almost coming up with new cool ideas on a weekly basis, the second line struggles to keep up. To change this, we should allow the first line teams to take control of their own risks, and build a system of trust. The second line can digitize the policies into guardrails and blueprints that the first line can use to take all the risk that is needed as long as the risk appetite of the organization is not breached.

Looking at how trust is achieved, there are three main principles we want to incorporate into the framework. The first is predictability. This can be achieved by standardizing the way that risks are managed because a highly standardized system functions in a highly predictable way. We strongly believe that 80% of the risk procedures that are taken within organizations, which seem to be one-of or custom procedures, can in fact be standardized. This is, however, not achieved overnight, and can be seen as an insurmountable task. The Trust by Design framework takes this transition into account by allowing processes to continue as they are at first but standardizing on the go. Slowly, standardization will be

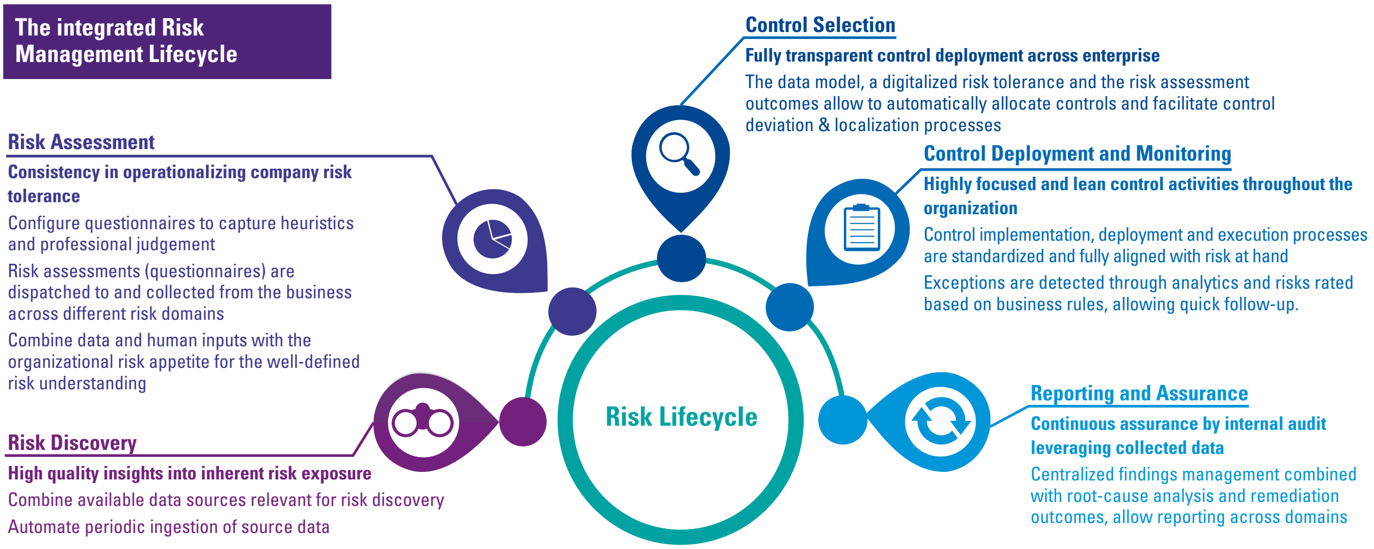

The integrated Risk Management Lifecycle
Risk Assessment
Consistency in operationalizing company risk tolerance
Configure questionnaires to capture heuristics and professional judgement
Risk assessments (questionnaires) are dispatched to and collected from the business across different risk domains
Combine data and human inputs with the organizational risk appetite for the well-defined risk understanding
Risk Discovery
High quality insights into inherent risk exposure
Combine available data sources relevant for risk discovery
Automate periodic ingestion of source data
Control Selection
Fully transparent control deployment across enterprise
The data model, a digitalized risk tolerance and the risk assessment outcomes allow to automatically allocate controls and facilitate control deviation & localization processes
Control Deployment and Monitoring
Highly focused and lean control activities throughout the organization
Control implementation, deployment and execution processes are standardized and fully aligned with risk at hand
Exceptions are detected through analytics and risks rated based on business rules, allowing quick follow-up.
Reporting and Assurance
Continuous assurance by internal audit leveraging collected data
Centralized findings management combined with root-cause analysis and remediation outcomes, allow reporting across domains
Risk Lifecycle

Figure 2. The integrated risk management lifecycle.

achieved, and trust will grow because the procedures are much more manageable and can be easily adapted to new legislation or technological advances.

Secondly, there is reliability. A standardized system allows for much better transparency across the board, both on an operational and a strategic level. But determining if processes are reliably functioning calls for transparency and well-articulated insights into the functioning of these processes. By using powerful dashboards and reporting tools pockets of high risk, developments can be made insightful, and even be used as steering information. Imagine if an organization is undertaking 100 projects of which 50 are processing highly sensitive personal data. Is that in line with the risk appetite, or should it be reconsidered? By adopting the Trust by Design framework these types of insights are available.

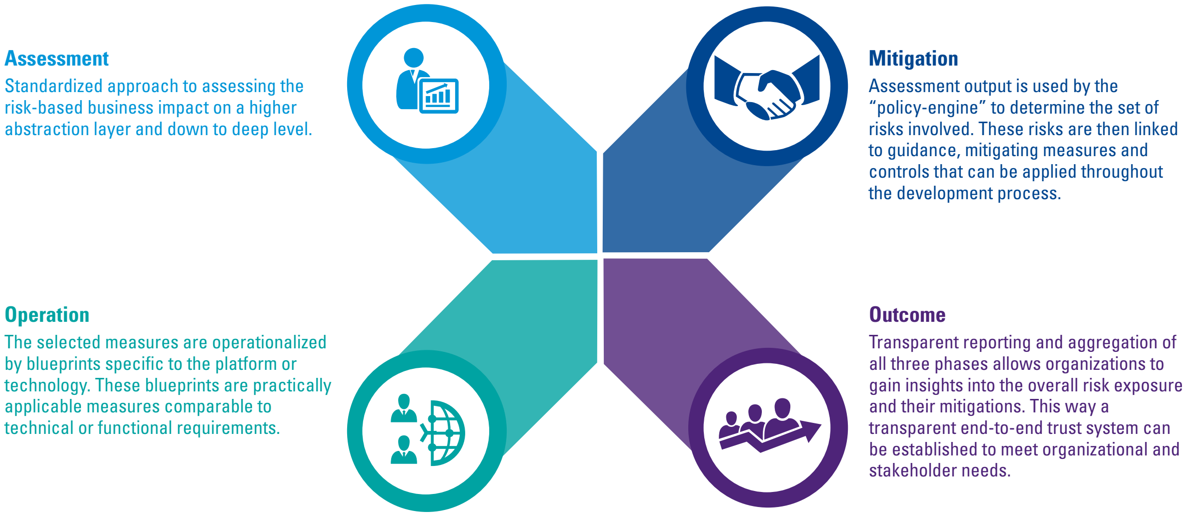
Lastly, there is a usability component. This is how the business teams perceive the guardrails and blueprints that are imposed. The Trust by Design approach is meant to take risks into account at the start of developing applications or undertaking changes. To achieve this, there are three basic building blocks that need to be defined. The first is the process itself, which also includes the governance, responsibilities between various functions, and the ownership of the building blocks themselves is defined. The second building block is the content, consisting of the risks, control objectives, and controls. And the third is where this content is kept, the technology to tap into the content and enable the process.

Following the three components of trust, the Trust by Design framework aims to reduce the complex compliance burden for business teams and increase the transparency for decision-makers and the risk management function within organizations. The Trust by Design framework aims to reduce the two most time-consuming phases in risk management for innovations and developments; determining the scope of the measures to be taken, and implementing said measures, while at the same time creating trust within the organization to leverage the benefits.

In practice, the framework is meant to be embedded within the development lifecycle of innovation, development, and changes. In Figure 3 the high-level framework overview is shown and consists of four major stages.

The first is the assessment stage, where through standardization business teams use business impact assessments and the following deeper level assessments to determine the risk profile of innovation or development. These are standardized questionnaires that can be applied to a technology, product, or asset throughout the development journey. The results of the questionnaires are used to funnel risk assessments and lead to a set of well-articulated risks, for which control objectives are defined. These control objectives can then be used to determine the risk appetite that the business is allowed, or willing to take, resulting in controls/measures. In the third stage, these can be implemented into the product at the right stages of the development cycle. These controls/measures can be seen as a set of functional/technical requirements that are added from a risk-based perspective. By applying this approach, by the time a development is completed or migrated into production the major risks are already mitigated in the development process itself. By design.

Lastly, there is the outcome where products are "certified" as the assessments, risks, the associated measures and the implementation can be transparently monitored.



Assessment
Standardized approach to assessing the risk-based business impact on a higher abstraction layer and down to deep level.

Mitigation
Assessment output is used by the "policy-engine" to determine the set of risks involved. These risks are then linked to guidance, mitigating measures and controls that can be applied throughout the development process.

Operation
The selected measures are operationalized by blueprints specific to the platform or technology. These blueprints are practically applicable measures comparable to technical or functional requirements.

Outcome
Transparent reporting and aggregation of all three phases allows organizations to gain insights into the overall risk exposure and their mitigations. This way a transparent end-to-end trust system can be established to meet organizational and stakeholder needs.

Figure 3. High-level Trust by Design framework.

These stages are constantly intertwined with the development processes. As circumstances change, so can the assessments or controls. Moreover, in environments where stringent controlling of certain risks is not necessary, guidance or blueprints can be part of the operation stage, helping innovation teams or developers with certain best practices based on the technology being applied, or the platform being used.

A CASE STUDY

At a major insurance company, this approach has been adapted and implemented to enable the first line in taking control of the risks. The approach proposed at this organization is based on four steps:

1. a high-level scorecard for a light-touch initial impression of the risks at hand,
2. a deep dive into those topics that actually add risk,
3. transparently implementing the measures to mitigate risks, and
4. monitoring the process via dashboards and reports.

By using a refined scorecard on fifteen topics that cover the most important risk areas, product teams understand what risks they should take into account during the ideation and refinement processes. But also, which risks are not important to the feature being developed. This prevents teams from being surprised when promoting a feature to production, or worse once it is already out in the open. By applying risk-mitigating measures as close to the process step where the risk materializes, an acuminate risk response is possible, preventing over or under control. This requires specific control designs and blueprints that allow teams to implement measures that fit their efforts. The more precise these blueprints are the less over-controlled teams will be. It is important to note that for some subjects organizations might decide that over-controlling is preferred to the risk of under-controlling depending on the risk appetite.

Based on the initial impressions the scorecard is used to perform a more specific assessment of the risks and the required measures. This deep-level assessment sometimes requires input from experts on topics such as legal or security. In several organizations, a language gap exists between the first and second lines. One of the product owners we spoke to said, "*I do not care about risk management, I just want to move forward as quickly as possible. For me this is only paperwork that does not help me accomplish my objectives*". Risk management consultants are also often guilty of speaking too much in a 2nd line vocabulary. It is important that we understand the 1st line and their objectives towards effectively designing a scorecard. In a way, this type of scorecard can be seen as the "Google Translate" between the 1st and 2nd lines. By asking the right questions in the right language the risks can become more explicit, and the required measures to mitigate the risk can be more specific. This reduces overcontrolling and leads to lowered costs and more acceptance from the product teams. The communication between the first and second lines is imperative to a successful implementation of a Trust by Design approach. This is also in line with the earlier mentioned IIA paper, in which the second line will become a partner that advises the first line, instead of an independent risk management department.

Since true agile is characterized by fast iterations and does not plan ahead too far, using a scorecard with an underlying deep level assessment helps product teams to quickly adapt to changes in the inherent risk of the change at hand. This "switchboard" approach allows much more agility, and still allows organizations to mitigate risks.

Developing this type of "switchboard" that leads users from high-level risks to more specific risks and the required standard measures, should be done iteratively. We also learned during our implementation that there is no way to make such a system exhaustive. At best we expect that 80% of the risks can be covered by these standard measures. The remainder will require custom risk mitigation and involvement of the 2nd line.

IMPLEMENT MEASURES, MEASURE THE IMPLEMENTATION

Once the specific risks are identified, the agile or scrum process can be followed to take measures into account as if they are (non) functional requirements. This way, the regular development or change process can be followed, and the development teams can work on these in a way that is familiar to them.

The technology used by our insurance client to manage projects is Azure DevOps. It is used for both developments and more "classic" project management. This tooling allowed us to seamlessly integrate with the process used by teams in their daily routines. In addition, by structuring the data from the scorecard, risks were made transparent to all lines of defense. Through structured data, it is possible to create aggregations or to slice and dice data specifically for different levels of management and stakeholders. Using PowerBI or the standard Azure DevOps dashboarding decisions regarding risk mitigation and risk acceptation is open for all to see. In addition, the Power platform can be considered to further automate the processes and use powerful workflows to digitize the risk policies and inject these directly into the change machine of the 1st line.

HOW ABOUT THE CONTROLS?

This leaves us with one more question, how do we connect these measures to the controls in the often exceptionally large and complex control frameworks? Especially since ITIL/COSO worlds are looking back, by periodically (weekly, monthly, etc.) testing controls using data and information from events that have passed. Based on this testing, the current, or even future situation is inferred. Agile is more responsive, in the moment and per occurrence. So, this inference can no longer be easily applied. Of course, large organizations cannot simply change their risk universes or control frameworks. So how do we connect these measures to controls?

This is a difficult question to answer, and counterintuitively, one to at first ignore. Once the first line starts to work with the standard measures, gaps between the operational risk management and the control testing world will become apparent. These can then be fixed relatively quickly by adapting the measures to better align with the controls. In other cases, we expect that controls also need to be reassessed. Especially given huge control frameworks of highly regulated organizations this will also be an opportunity to perform rationalization and cull the sometimes overcontrolled nature of organizations. In addition, it also presents the opportunity to further explore options of control automation that can lead to further savings and efficiency.

Measure or control?

We make the distinction between control and measure. In the first stages of implementing the approach, this will be apparent. Controls are periodically tested, whereas measures will be an explicit part of the development process, just like any (non)functional requirement. But we expect that this distinction will fade as the change process itself will eventually become the only control to mitigate risks in the future.

> Communication between the first and second lines is imperative to a successful implementation of a Trust by Design approach

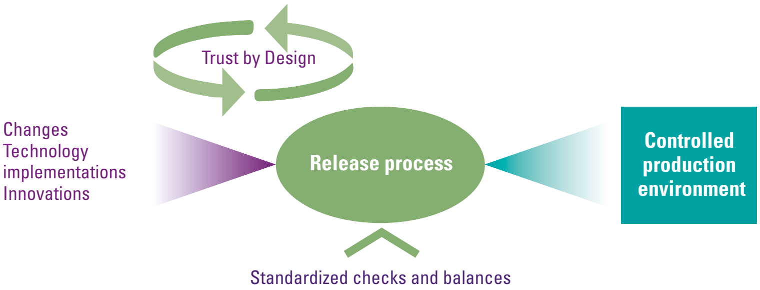


Figure 4. The release process as a pivotal function in managing risks.

CONCLUSION

In our vision, a major part of risk procedures will migrate into the changing realm instead of control testing procedures that are static in nature (see Figure 4). As organizations become more software-development oriented (in some shape or form), it allows us to reconsider the approach to testing controls and mitigating risks. Imagine a bank changing the conditions on which someone can apply for a loan, nowadays this involves a lot of manual checks and balances and testing before all kinds of changes are applied and manual interventions are needed. Since the risks of these changes are not holistically considered during the development process, controls are needed in the production environment to ensure the proper functioning of the systems after the change. The digitized organizations of the future will converge their risk processes into the release cadence and will never worry about testing controls other than access controls and security. They know the as-is state, and they know the delta, that which is being added, changed, or removed is done according to the appropriate risk appetite *by design*. Finally, Trust by Design will also provide the foundation to develop digital trust metrics. Digital trust captures the confidence that citizens have in the ability of digital technology, service, or information providers to protect their interests. This allows internal organizations, their clients, and society to *trust* the processes and technology.

References

[Diam05] Diamond, J. M. (2005). *Guns, Germs, and Steel: The Fates of Human Societies.* New York: Norton.

[Gula08] Gulati, R. & Nickerson, J. A. (2008). Interorganizational Trust, Governance Choice, and Exchange Performance. *Organization Science 19*(5), 688-708.

[IIA20] Institute of Internal Auditors (IIA) (2020). The IIA's Three Lines Model: An update of the Three Lines of Defense, Retrieved from: https://global.theiia.org/about/about-internal-auditing/Public%20Documents/Three-Lines-Model-Updated.pdf

[Lipp06] Lippert, S. K., & Davis, M. (2006). A conceptual model integrating trust into planned change activities to enhance technology adoption behavior. *Journal of Information Science, 32*(5), 434-448.

[McKn96] McKnight, D. H., & Chervany, N. L. (1996). *The Meanings of Trust.* Minneapolis, Minn.: Carlson School of Management, Univ. of Minnesota.

[Noot97] Nooteboom, B., Berger, H., & Noorderhaven, N. G. (1997). Effects of Trust and Governance on Relational Risk. *Academy of Management Journal, 40*(2), 308-338

[Sydo06] Sydow, J. (2006). How can systems trust systems? A structuration perspective on trust-building in inter-organizational relations. In R. Bachmann & A. Zaheer (Eds.), *Handbook of Trust Research* (pp. 377-392). Cheltenham/Northampton: Edward Elgar.

[Zahe98] Zaheer, A., McEvily, B., & Perrone, V. (1998). Does trust matter? Exploring the effects of interorganizational and interpersonal trust on performance. *Organization Science, 9*(2), 141-159.

About the authors

Swatantra Kumar MTech, PGDAC, BE is a senior manager at KPMG. He has over a decade of experience in software development & delivery, application performance, and solution architecture design. Swatantra has been involved in digital transformation, DevOps, IT strategy, SaaS & cloud consulting for various organizations in the BFSI and SMEs sector, and carried out numerous assignments with a wide range of clients around the globe helping them meet the challenges of the ever-changing IT landscape. Swatantra heads the solution design and development function and is responsible for citizen development proposition, low-code services, and Trust by Design framework.

Stefan Jacobs MSc is a manager at KPMG and advises organizations on risk management in agile and highly digitized environments within the development and innovation processes. After extensive experience with data analytics and automation in various IT audit- and advisory work, he switched to product management and software development with a strong focus on risk management and agile principles. Stefan is currently part of the digital excellence hub within KPMG that is responsible for developing the Trust by Design framework.

Tom Koehler is specialized in enterprise risk management and securely bringing an organization's innovation and digital transformations to life. Tom serves as Chief Technology Officer for KPMG in the Netherlands and was appointed Global Head of KPMG Citizen Developer Program. The goal of this initiative is to give employees more autonomy and responsibility to create digital solutions while empowering them with the right tools, the proper guardrails and the support they need to bring technology to life. It's about building trust in our global systems and creating a thriving community of like-minded colleagues. He is also the co-founder of the Munich Cyber Security Conference (MCSC), founded in 2014. MCSC offers a unique space for exchanging and discussing solutions to the manifold challenges in information technology and cyber security.