eraneos

Whitepaper

Quality
Assurance
in a digital era

October 2023

Content

Traditionally, Quality Assurance focused on ensuring the quality of (manufacturing and delivering) a service or product. Main focus was on preventing mistakes and defects, with techniques like Statistical Process Control, Total Quality Management and Company Quality. The goal was to assure 'fit for purpose' (maximizing customer acceptance) and 'first time right' (minimizing rework afterwards).

The worldwide financial crisis has forced financial services firms operating in an intensely complex and challenging environment, where increasing spend on risk and compliance conflicts with the evolving field of Operational Excellence. With organizations becoming more complex and subdivided, the Three Lines of Defense Model (short: 3LoD) — consisting of the first line of defense (operational management), the second line of defense (serves, among other things, risk management and prescribing policies) and the third line of defense (internal auditing) — offered an integrated risk based approach on quality control.

However, in the last years entering a new era of digital, many industries have been undergoing a digital transformation, with data and analysis muscling out embedded quality improvement. In a true digital transformation, Quality Assurance is present in virtually every aspect of every employee's everyday work. As a result, there is a shift from bolt-on to built-in going on in the field of Quality Assurance.

So, what is the impact of this digital transformation on the Quality Assurance field of expertise? What is this shift towards 'built-in' in the field of Quality Assurance? What does this mean for these three lines of defense?

In short: The answer is **Exponential.** Let us explain a bit, starting with a simple equation:

"Business processes consist of input, throughput and output. This input, throughput and output consists of data and information streams. The

sum of all this data and information streams counts up into the financial statements. If all these business processes remain unaltered during the year and are in control, so will be the financial statements..."

But we all know this example is not the world we are living in today, which is a world that is changing at a fast and by some even described as an exponential rate. So imagine if all business processes are changing continuously during the year, how do you assure quality?

The traditional Quality Assurance approaches are outdated. To put it even stronger, only the ones able to continuously secure accuracy and completeness will survive the digital age. We need to look at the three lines of defense in a different way, as they hold the key to Quality Assurance in a digital era. Digital transformation leads to rethinking the traditional Quality Assurance field of expertise. Our strong belief is that digital transformation can empower the three lines of defense in such a manner, that Assured Quality is the future status quo.

"Only the ones able to continuously secure accuracy and completeness will survive the digital age"

Offense is the best defense

In our introduction we stated that digital transformation leads to rethinking the traditional playing field of Quality Assurance and the Three Lines of Defense in particular. With a simple equation we illustrated the growing importance of securing accuracy and completeness directly within the first line. Let's dive a little deeper into this evolution.

A thought experiment: *"It's the year 2025 and all your first line processes are fully automated, including the controls required to assure accuracy and completeness."*

Then what has become of the first line of defense? And how does the concept of built-in quality come in here?

The first line of defense is ultimately responsible for the choices they make and the risks they take in daily practice, impersonated by the business. Ideally the first line is intrinsically motivated to have clear objectives, to reflect, to regularly conduct the quality dialogue and to ask about incidents and learn from them. The first line is therefore the most important form of quality assurance.

When coming to executing operational processes, controls (e.g. Management Controls, General IT Controls, Process Controls and Application Controls) are often used to assure quality (e.g. accuracy and completeness). When your processes have become fully automated, automating your controls seems a logical next step. However, this is not as simple as it sounds and sometimes even impossible...

Application Controls are the most straightforward to automate, they are specific and within system boundaries. Process Controls are more difficult, they are also specific but often overarch several systems. Management Controls and General IT Controls are the most difficult to automate, being

generic and adherent to frameworks (such as COBIT and IT4IT) resulting in processes of and on their own.

This is where the built-in quality comes in! As a process or system evolves, its design must also evolve to support them. Agile frameworks such as SAFe use built-in quality practices to ensure that each change, at every increment, meets appropriate quality standards throughout development. A similar approach is seen in the, from Lean originated concept called, Quality by Design. The key to success lies in integrating controls in quality standards and directly capturing them as requirements when designing change.

In conclusion, in order to prevent quality assurance to stay behind while automating the work, offense is the best defense. Next paragraph we'll look at another line of defense, the second line, and see what is changing there. Just to give a small hint: quality, data, automation and design are all invited to the party...

"As a process or system evolves, its design must also evolve to support them"

The second line becomes first

In our introduction we stated that digital transformation leads to rethinking the traditional playing field of Quality Assurance and will impact the Three Lines of Defense in particular. In our previous paragraph we showed that quality should be built-in from the start, to tackle guidelines upfront instead of afterwards. Now we explain what the implications of this shift mean for the second line of defense.

Let's follow up on the thought experiment from previous paragraph, assuming not only all your first line processes but also all associated controls are fully automated...

Then what has become of the second line of defense? What is the added value of this second line? And what opportunities and threats arise in this situation?

The second line of defense develops the systems for a good process of quality management and control, always in support of the business. This second line of defense often includes many different functions, including legal, finance, compliance, internal control, security and quality. Each function works with their own identification and reporting processes often resulting in duplication of work.

In the previous paragraph we saw that technology has delivered new capabilities to distribute services and reduce the traditional costs of doing business. When done properly, as described in our thought experiment, this will lead to an excessive amount of data along with new methods to capture it. Let's dive a little bit deeper into three drivers:

Like many transformations, we will start with **technology.** As organizations begin to manage data effectively, they'll be able to use the faster computer power and data storage capabilities available to enable advanced analytics, developing better risk and quality management techniques

and decision support. As a matter of fact, second line functions in many companies have started venturing into big data analytics supported by technology to strengthen their assessment processes. Over the past years we have seen methodologies like process mining gaining territory in the improvement area.

The second driver we will address is **synergy.** Merging functions may not be possible in some cases, but leading organizations have already started to identify operational efficiencies by studying second line activities and integrating them where it makes sense. Cooperation and alignment between Compliance, Risk, Finance and other operational risk functions is key over here.

Finally, **people** are fundamental to driving change, and the traditional field of QA can't be upgraded if you don't have people open to and capable of doing it. The second line needs to have depth of capabilities like data management, advanced analytics and advanced mathematical and statistical training. This demands strong support from the Board and HR functions. It also requires additional skills like curiosity, analysis and creativity.

So, turning the first line of defense into offense and further building upon that driven by technology, synergy and capability, the second line becomes first. Now it's time to move on and see what happens to the last internal line of defense, the third line...

"The traditional field of QA can't be upgraded if you don't have people open to and capable of doing it"

There are only winners

In our introduction we stated that digital transformation leads to rethinking the traditional playing field of Quality Assurance and the Three Lines of Defense in particular. In our previous paragraphs we showed the digital revolution taking place within the first and second line of defense. Then what are the implications for the last hurdle: the third line of defense? Let's take a closer look.

The third line of defense provides top management with assurance about the quality of risk management and control. Internal audit is therefore a temporary capstone of the PDCA cycle and not directly responsible for the quality of being in control of the organization, but for the extent to which it is able to analyze and visualize the inconsistencies in the design and existence of the control frameworks.

So what is the impact on this third line of defense? And what does this mean for concepts like Risk and Control?

Before we start answering these questions, we want to consider the basics of Risk Control. Risk Control is focused on operational risks, which are related to internal processes, people and systems. These non-financial risks can also lead to serious problems for organizations and, in the worst case, have an impact on the 'License to Operate'. But when looking at organizations, which can be divided into portfolios, value streams, processes, applications and systems: How many risks are there? How do you keep an overview?

Being 'In Control' is constantly changing. How can organizations be In Control, improve and focus on the quality of the core business with the right effort in Risk Control at the same time? An issue that occurs almost in every organization. A well explained model is People, Process and Technology. A similar subdivision were described as three pillars of transformation in the previous paragraph. Coincidence?

When we zoom in on the implications for the third line, the number of performed internal audits or a good amount of audit points is not the objective. The goal is to mitigate risks and improve organizations, especially in key processes. With the approach of the Three Lines of Defense Model, the focus would be on the most important risks of the organization that could have an impact on the objectives of the organizations. This with minimal effort from the business (first line) enabling them to primarily focus on value creation.

As we know, auditors mostly focus on the processes and the information that flows through them. Traditionally on the financial processes, but business auditors are making their entry at a fast pace. These focus more on the effectiveness and efficiency of risk management measures, where the information is ultimately reflected in the annual accounts which in their turn must be correct and complete. In summary, the control of processes can be divided in: (1) identifying risks and determining mitigating measures; (2) testing whether these measures are effectively organized in design, existence and operation.

And this is where it gets **interesting!** Once again looking at organizations, from the perspectives of portfolios, value streams, processes, applications and systems, countless information (data) exists that can tell something about the effectiveness and efficiency of the risk management measures. If we then receive signals where risks go beyond certain norms or show more variation than a normal standard running process, 'something may be going on there'. Consider that when a process is highly automated and largely built up by business rules, a risk could arise if certain values are exceeded. Optimizing processes with Lean Six Sigma and seeing every 'outlier' as an opportunity for (quality) improvement has been done in industries for years, like the famous example of Toyota with Andon. Imagine that we will also start seeing these opportunities in optimizing the In Control measures...

And there is more, as serious steps can be taken towards checking the business rules, when moving more and more towards automated controls. The less manual work, the more automated controls, the more effective an audit can be in prioritization, frequency and depth based on risk classifications. This phenomenon is called Risk Based Auditing. As a result, when an organization can learn and optimize, the fewer processes are 'bothered' by internal audit. In the end this completes the circle by helping an organization with gaining grip on the most important risks and allowing guidance on the objectives to be achieved, being a big win for all the three lines!

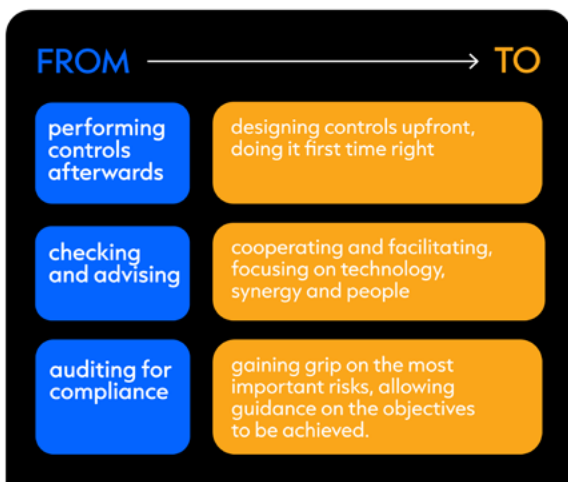"When an organization can learn and optimize, the fewer processes are 'bothered' by internal audit"

Digital Transformation shifts Three Lines of Defense

In our introduction we stated that digital transformation leads to rethinking the traditional playing field of Quality Assurance and the Three Lines of Defense in particular. In our three paragraphs we showed that offense is the best defense in order to prevent quality assurance to stay behind while automating the work, we illustrated that the second line become first by turning the first line of defense into offense and further building upon that driven by technology, synergy and capability, and we described helping an organization with gaining grip on the most important risks and allowing guidance on the objectives to be achieved being a big win for all the three lines.

So we can state there is definitely impact of digital transformation on the Quality Assurance fields of expertise, with clear consequences for all three lines of defense, leaving us only one question unanswered...

What is this shift towards 'built-in' in the field of Quality Assurance?

In the introduction we already answered in short: **Exponential.** The longer answer is this: Digital Transformation shifts Three Lines of Defense. Because of these shifts the work of Quality Assurance shifts along:

These shifts lead to 10 Digital Do's for Quality Assurance to reach the full potential of digital.

In the introduction we stated our strong belief is that digital transformation can empower the three lines of defense in such a manner, that Assured Quality is the future status quo. This means organizations should invest in an integral GRC (governance, compliance and risk) approach with appropriate mandate and the Quality Assurance professional, no matter what line operating from, will have to acquire new skills. So the shift towards 'built-in' takes Defense out of the Three Lines Model (short: 3LM), preventing double work, irritation, lack of responsibility and accountability and low risk awareness, reaction speed and alertness on incidents.

Author:

Koen Boomsma
Manager Organizational Excellence & Transformation

Co-authors:

Marcel van der Laan

Experienced in a wide range of industries

ABOUT ERANEOS

As a global Management & Technology Consultancy Group, Eraneos supports organizations in not only designing but successfully implementing a future-proof digital transformation strategy that can make an ever-lasting impact.

By listening to what businesses want and understanding their needs, we can fast-track and embed transformation with ease by aligning people with technology, processes and leadership, effortlessly.

Knowing your industry, technology and local context alongside a global perspective, gives us the advantage you need to succeed.

It's this deep understanding that enables us to shape and implement strategic transformation within your organization while providing the best service. That's why our customers trust us with even the most complex of challenges, from strategic digital transformation in finance to the ethical application of A.I. in healthcare.

We don't just listen to your needs, we understand them. We're more than ready to help you realize your potential in the digital age.

Contact us >

Our offices >

Visit our website >