TRANSCENDENT GROUP INSIGHT

What type of governance model and culture is required to overcome the increasingly complex risk picture?

Introduction

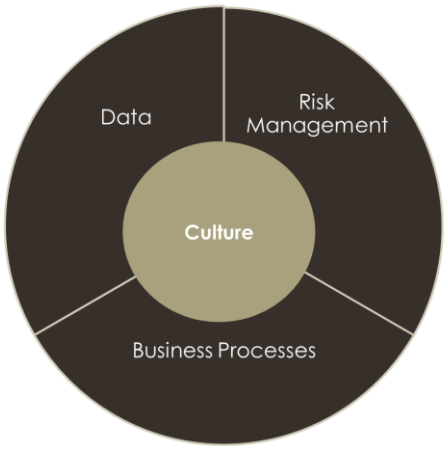
On the one hand, despite increased investments in governance, risk management and compliance programs, control failures are still making headlines in the Nordics and Europe. On the other hand, the demands on businesses and their governance, risk management and compliance programs are ever more heightened, complex, frequent, and costly.

- Regulators expects more. Regulatory requirements are increasing. Some industries are used to complex regulatory environments, while for others have meet a new world with GDPR. And some expectations are not always clearly defined, i.e. regulation on Culture and Corporate Values (EBA)
- The outside world (customers, society) expects more. Cultural pressures also raise the bar for sound governance, as organisations respond to pressures from both regulators and customers. Organisations are subject to moral and ethical standards with their impact on their surroundings being measured and judged in media.
- Push from within the organisation for cost reductions. But at the same time, "risk fatigue" is increasing due to the inefficient implementation of requirements and responsibilities
- Technology demands. Digital and mobile tools may help realize an organisation's strategic objectives by facilitating collaboration among employees and communication with customers, but this must be seen within the context of a complex and fast moving world. In addition, globalization puts pressure on each local company in order to meet market and customer demands.

Governance systems differ from one organisation to another. There are several suggestions on why this is. Literature points to no one definition of a governance system, nor what makes one system different from another. Political and regulatory factors may play a role, in addition to basic factors, such as social structure (in the case of industrial relations) and the level and character of economic development (in case of financial systems). However, once a governance system has acquired its character, it rarely changes significantly in the organisation.

Example of a governance structure:

Governance systems comprise several elements. In our experience, one element is not more important than another, just like one element may vary from another. One element might be a methodology used, i.e. risk management, while another is integrated in everything we do, i.e. processes. Based on our experience, we see a tendency towards increasing understanding of the link and coherence between culture and risk management, data, and business processes in order for organisations to efficient and effectively meet business objectives.



What we have seen in the last year under COVID-19 is the importance of organisations applying agile governance while at the same time maintaining a stable organisation and managing risks. Known risks are what risk management methodology supports. Many organisations have, however, not been able to act fast enough in balancing governing change with ensuring a normal level of thoroughness remains in place. This is because risk management, data and culture has not been an integral part of managing the business. The maturity of these elements –risk management in particular – as a methodology - and how well they are integrated into corporate governance has become clear to many organisations this year. Many organisations do not have a structured approach to risk management, understand the importance of or utilise culture and data in their decision-

making processes. Of course, every organisation approaches risk management in one way or another, but not only a proportion of these have a comprehensive understanding of the top risks for the company or risk management as an integrated part of daily business. Some organisations perhaps did not even fully understand the risk of securing operations in a worldwide pandemic.

The use of actual data and quantification in assessing risk or consequence. This is something that is done within some areas. Banking and insurance quantify and sensitivity calculate certain parts of their portfolios, and have risk managers that monitor this. Other sectors often adapt this approach to governance, but don't base it on or link this to actual data.

This insight aims to highlight two areas of great importance for all organisations in order for them to have a **corporate governance system that supports fast decision-making without forcing decisions that may risk the sustainable growth of the organisation**. In this regard, we want to discuss; 1) the importance of building a corporate culture and 2) the use of data in governing and running the daily business.

Culture eats [……] for breakfast – the importance of your culture.

Many argue that "culture eats strategy for breakfast". We argue that culture is in everything we do, hence it impacts our processes, risk management methodology, our capability to digitalize operations etc.

The board of directors has the responsibility to practice good governance, which also generally includes working to develop a healthy corporate culture. This may sound good in theory, however it's our experience that culture can be hard to define and even more difficult to put into practice.

"Culture" is defined as set of values, symbols and rituals shared by the employees of a specific organisation, which describes the way things are done in order to solve business challenges and problems, both internal and those relating to customers, suppliers and the business environment. Or to put it simply, culture is the behaviour in the organisation which influences how employees act, see, feel, and believe.

To execute corporate governance effectively, organisations need to understand the ways culture influence business processes and decision-making processes. Employees are people. They exhibit both good and bad behviours, different values, different ways of working, different ways of adhering to authorities, regulations etc. But culture in an organisation may also vary from one department to another, from one country to another and even from one level in the organisation to another. Gert Hofstedes defines six types of cultural dimensions in his 10-year study on culture[1]. From that perspective, corporate governance should help to consolidate organisational culture. Or put in other words; The "right" behviours are to be defined, practiced and supported by business management in order to effectively reach the vision and mission required by the owners of the company.

The past few months, many organisations have been influenced by various pressure due to COVID-19, i.e. requiring business model transformation, liquidity, work environment, operational availability etc. This has required transformation in anything from a small to a very large scale. Transformation is very common in many organisations, however, it is very rare that organisations goes through several transformations at the same time or fundamental changes of re-designing the business model.

[1] Geert Hofstede, "Culture's consequences: Comparing values, behviours and institutions across nations,"

We believe that COVID-19 can teach us several things of what will be required of organisations in the future. Organisations often base transformations or decisions upon qualified data, historic events, thoroughly risk analysis of new demands. We believe organisations in the future will be challenged to be more agile, with the hallmark of agility being the ability to be both stable and dynamic. It will be those companies that can integrate the contrasting elements of stability and speed to functional, modern unit winning. For that perspective mind-sets and behaviours of the employees and functions inside the company will be crucial for organisation to dynamically reaching the strategic and economic priorities, or change business objectives if required while keeping sound, stable character to its stakeholders.

In our view, organisations which consciously focus on the importance of their culture and continuously work on its enhancement have a stronger basis for transformation or crisis management having already created organisationa common starting point and common language.

In our experience, the following three factors are necessary in order to establish a common culture:

First and foremost, it is important that business leaders talk about “why” the organisation exists. According to Simon Sinek; "People don't buy what you do; people buy why you do it." In many organisations, functions, units or even in teams there is a habit of talking about "what we do" and "how we do" it, to instead talking about "why we are here and what we believe in."

The business **culture must reflect your "why."** This will encourage and inspire employees, customers, stakeholders, and community members to support, and patronize the business for delivering optimized outcomes in a time of crisis or in time of business growth and prosperity. Organisations that are heavily regulated (e.g. financial services, pharmaceuticals, medical device industries etc.) or which have a more complex company structure risk management or where compliance is recommended to be an integrated part of the culture. One example is General Electric, a global technology and service company present in over 100 countries and with approximately 300,000 employees. One of their core values is “Integrity”, which is implemented in their governance system, in employee evaluation processes and in risk appetite.

Secondly businesses should **define which cultural attributes constitute the culture** - the list of cultural attributes needs to be simple, short, and effectively support the "why". Is important so that employees understand its meaning and importance to human behaviour. For some organisations requiring more agile work processes or methodologies more principle based attributes can be considered enabling the employees to reach the right decisions on their own as the governance process may not be risk mitigating enabling. Rick Diviney is a former Navy Seals which in his book “the Attributes” describes how beneath obvious skills are hidden drivers of performance, such as cunning, adaptability, courage, even narcissism.

As mentioned in the beginning to develop a healthy corporate culture may sound good in theory, however it’s hard to put into practice. So how to?

First and foremost understanding and promoting culture has so much to do with who people are and how they feel. **Understand both the current and the desired culture**: Business leaders should closely examine current business processes step by step to identify which practices are aligned with the desired culture and which are destructive and require change—which begins by uncovering the values and behviours that allowed those practices to develop. **Promoting a strong and specific culture** means that business managers must strike a chord

with their employees that speaks to their emotions. Establishing this connection makes everyone share the same purpose and motivation from the top to the bottom.

Secondly, culture cannot be delegated. It must be on the CEO's list of responsibilities and top priorities: It must be clearly understood and communicated consistently from top level in order to train and raise awareness of the cultural values throughout the organization Business management must also determine how they relate to business strategy, and **take responsibility for shaping them**. This must be strengthened through measuring culture and making themselves account for failures by using data and tools to understand if employee behaviours and attitudes are in line with the cultural attributes. If measurement shows that current behviours conflict with desired culture, this needs to be accounted for by deciding on refinements. For this purpose, we cannot promote *Whistleblower processes* enough. Communication channels in order to speak up should be an integral part of every organisation, enabling employees to be the ears and eyes of management[2]. Another core element in supporting responsibility and accountability is the *remuneration processes*. Often remuneration programs support the economic and strategic results. Less frequently, they include through which means these results are achieved. HR – perhaps supported by Compliance – is an important function in this effort. Many organisations build teams to better communicate leaders' vision of the desired culture, but these teams do not always connect cultural change programs to behviours and business strategies.

Building a solid corporate culture is a continual work in progress. Economic and technological forces are more and more requiring change for how organisations function. The future is in many aspects uncertain. The only thing that the board of directors can count on is that major issues affecting their operations will continue to evolve in various and unexpected ways over the next decade or more. What will not change is the importance of a sound corporate culture and a strong commitment to good governance.

Through our many years of experience from Governance, Risk Management and Compliance, and through corporate scandals and regulatory or similar transformation projects, we know that a healthy corporate culture increases the ability to transform, increases productivity and generates positive long-term shareholder value. Regulators are placing more and more emphasis on sustainable growth[3] and know that organisations with weak cultures are susceptible to having leaders or employees who have bad conduct. Organisations with a healthy corporate culture will improve their branding and reputation; which will likely increase their customers'and/or stakeholders' sense of loyalty.

Where many corporate boards get it wrong is that creating and maintaining a good corporate culture is not a one-size-fits-all. Culture starts at the top, but it requires everyone to work within and stay connected with the entirety of the organisation's cultural values.

The importance of data for good decision-making

Actual data is often used in risk management in finance, but there are other areas where data can be used. For example, more and more organisations are beginning to understand the importance of risk management within digitization, privacy and information security. All too many still rely on methodologies that are not based on much more than guess work and gut feeling.

---

[2] In December 2019 the EU has enforced a the Whistleblowing Directive - DIRECTIVE 2019 1937. The Directive needs to be transposed in national law by 17 December 2021. The Directive introduces a general obligation for organisations above 50 employees or an annual turnover of 10m Euro to establish an internal whistleblowing reporting channel.

[3] https://op.europa.eu/da/publication-detail/-/publication/e47928a2-d20b-11ea-adf7-01aa75ed71a1/language-en

There are well known and accepted ways of working with risk in quantifiable and scientifically verifiable ways, as has been done for decades within domains like finance, insurance and medicine. But there seems to be a combination of lack of both knowledge and culture based on misplaced trust within digitization and data management.

The burden of weakening knowledge is often placed on leadership because they are said not to understand all the ins and outs of digitization. What is apparent though is that the steadily growing numbers of people working within digital business of some kind, do not necessarily have a firm grasp of the concept of risk and uncertainty. This is especially when it comes to putting their understanding of risk into a business context and communicating it to leaders. What's the cost of the risk being expressed and how does it measure up to what it takes to fix it?

The misplaced trust come into play when these two worlds collide. Often based on a very thin, sometimes poorly documented and seldom verifiable grounds, the work force of digitization creates an impression of simplicity, urgency and certainty. If we can say anything about digitization it is that it comes with a lot of uncertainty, it is often a lot less simple than it is sold to be and very seldom simple.

You may have heard the expression "Data is the new gold". Well, there's no question as to whether data is critical to all business. Data shares a lot of inherent properties with gold. It holds a large value for the business but is at the same time just as valuable to our threat actors. If we don't have full and complete control of where we store it, how we secure it, where it comes from, who has access to it, how we use it and what we use it for, and so forth. We run an increasingly growing risk of going out of business.

Digitization is all about using technology to get even more out of the information we already have and using it to do what we do in an increasingly effective way. Technology, however, also creates weaknesses. Weaknesses that, left without scrutiny and careful consideration of the associated risks, can set us up for some serious surprises. The risk of digitization should not be left to the technocracy of our business, but rather be managed in cooperation with information security and privacy professionals who can base their reasoning of risk on something other than gut feeling and experience alone, let alone express it in an understandable way.

It is time to start tracking the level of uncertainty within information security and privacy in a more holistic way and measure risk of digitizing your "gold", or information values if you will, by real numbers. We know what requirements are put on the business when it comes to securing our data, we know what should be done to secure our data, and we should know if that job is done or not. If the requirements on security are not met, we should also know that the uncertainty of evil threat actors having a field day with our data is increasing on a day-to-day basis.

By using well-known methods within statistical science like Bayesian inference and Monte Carlo simulations, we can measure and track uncertainty over time and be much more precise in expressing what kind of losses we could expect if something unwanted were to occur with regards to our data.

It is not too difficult to measure risk on a micro level and reporting the risk on a macro level of an evil threat actor attacking our business in an understandable way. On a management level shouldn't have to be technical at all. It is all about following the information flow. Every part of the organisation must take part in information handling at some point. Build a culture of figuring out what the risks of every single link in the chain represents from an information security perspective, and it will be possible to aggregate risk on a macro level in understandable ways.

The risk of an attack by evil threat actors, the risk of too much technical stuff going wrong, or the risk of not living up to the requirements put on your business, is not new. It's all about how you use your data to build a sound, measurable and accountable grounds for making the best decisions for the business.

So, what does it mean to have an unacceptable risk within information security? It should mean that we are too uncertain to carry on doing what increases the risk. When we have whole slew of red, unacceptable and completely incomprehensible technical risks reported by the IT-department to base our decisions on, what do we do? Firstly, we should require risks to be reported in an understandable manner, following the flow of information throughout the business, and measured in an accountable way. Secondly, we should require an answer to the question of what will most effectively decrease the risk and how the effects will be measurable.

If you as a leader are not satisfied with the way information security and privacy is handled from a risk management perspective, it is time to require more accountable handling of risk in your business, based on quantified, scientifically verifiable measuring of your security posture. This should be combined with a thorough and ongoing analysis of your threat landscape, enabling the creation of a culture of risk-based decision making throughout your business. Build risk in as a part of every nook and cranny of your business. Aggregate risk of an attack, aggregate risk of costly mistakes both technological and manual, or aggregate the risk of costly compliance breaches. That is what you as leaders need to have. If it is possible to measure, it is possible to express as the probability of loss understandable by any business leader regardless of technical understanding.

This is where governance maturity and culture come into play. Information security and privacy is not a technical concern for the IT-department anymore. It is core strategic business. If you want to survive in the data driven "wild west" you need to sharpen your business's measuring and governance skills and build a culture able to express information security and privacy risk from the ground up. Then you will have a risk management that is relevant for top management and have it integrated in you daily business.

Concluding reflections:

Our point of view in summary is therefore that if you want to develop your corporate governance - work with culture and make risk management even more relevant by maximising the use of data.

Please reach out

Heidi.Gliese.Hylleborg@transcendentgroup.com

+45 51 63 14 46

Goran.Breivik@Transcendentgroup.com

+ 47 984 88 995

Christian.stensrudk@Transcendentgroup.com

+ 47 911 78 986