Reporting about culture and behavior increases confidence in outsourcing

Soft controls and ISAE 3402

Many organizations have outsourced business critical processes to service organizations. Through ISAE 3402 reports, many service organizations report on the quality of their internal control. Internal control includes the combination of so-called hard controls (e.g. authorization, segregation of duties or automated controls) and culture and behavior within the organization (soft controls). Soft controls are an important foundation and precondition for the successful execution of hard controls. The cause of non-effective hard controls usually originates in shortcomings in soft controls. However, reporting on soft controls by service organizations is still very limited. In our experience, this causes tension in the relationship between the outsourcing organization and the service organization. By reporting on soft controls, mutual trust can be strengthened and both organizations are therefore "in control" to a greater extent. In this article, we provide concrete examples of the way in which this can be executed.

Laura Ploegsma
is senior consultant at KPMG Advisory – Governance, Risk & Compliance Services.

Corine Tol
is senior manager at KPMG Advisory – Governance, Risk & Compliance Services.

Jacco van Kleef
is partner at KPMG IT Assurance & Advisory.

OUTSOURCING DOES NOT DISCHARGE FROM RESPONSIBILITY

Organizations are expected to be demonstrably in control of their operations. This also includes activities that they have outsourced to other parties (so-called service organizations). However, how often do you read about data breaches, frauds, or other incidents in the chain of operations? Despite internal (hard) controls that are effective in design, errors and incidents still occur. Evaluations often reveal that this is caused by poor quality of soft controls in the outsourcing organization or the service organization. This advocates that parties have to pay more attention to soft controls.

ACCOUNTABILITY FOR OUTSOURCING ESPECIALLY TOUCHES THE HARD CONTROLS

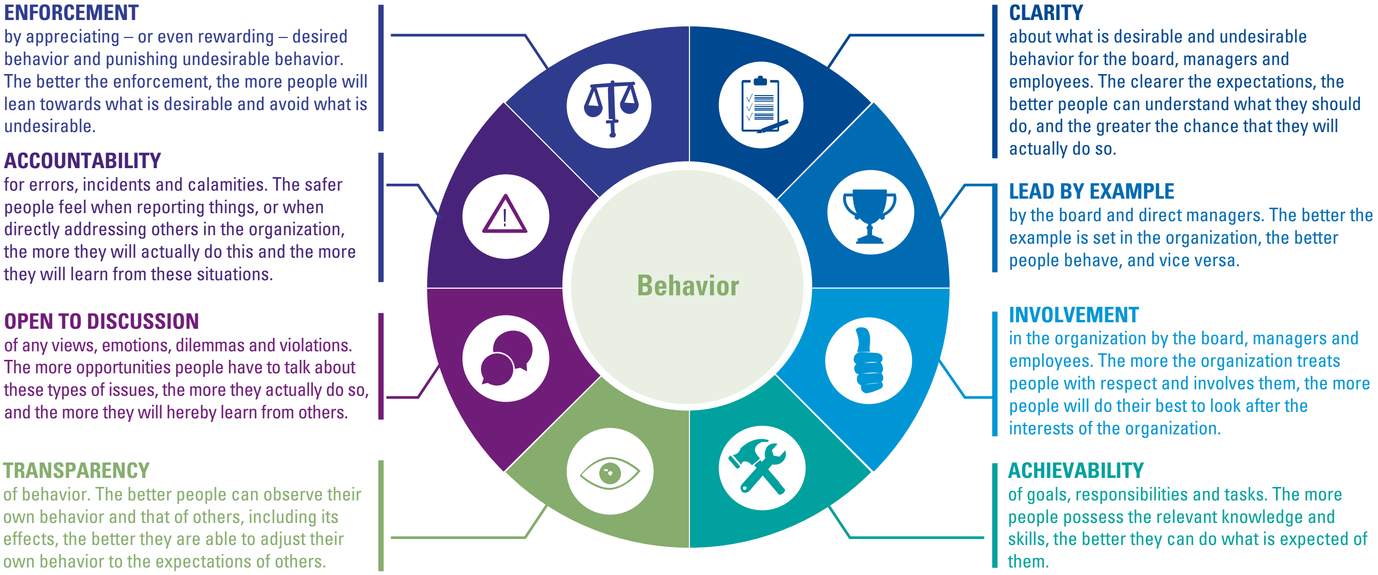
It is customary that service organizations report on the quality of their internal control through International Standard for Assurance Engagements 3402 reports (hereinafter "ISAE3420 reports").[1] In these reports the internal controls of the organization are audited by an independent auditor.

However, in most ISAE 3402 reports of service organizations, the focus is on hard controls. Little to no attention is paid to human behavior, which is a prerequisite for effective hard controls. This is remarkable and is the reason why we publish our vision on reporting on soft controls in ISAE 3402 reports.

In the meantime, the importance of culture and behavior is underlined in the guidance for Dutch auditors, Practice Note 1148 ([NBA22]) of the Royal Netherlands Institute of Chartered Accountants (NBA). This guideline calls for more attention to culture and behavior in audits of financial statements and other engagements of the auditor where the effectiveness of the internal control environment is relevant. As service organizations report on their internal controls to their users in ISAE reports, we are advocating for more explicit attention on culture and behavior in these reports to increase the value of these reports for their users. This is in line with the requirement in ISAE 3402 in which attention is requested for (other) aspects of the control environment of the service organization ([IFAC11][2]). The question is: in what way can culture and behavior be included in an ISAE 3402 report?

[1] Or other Service Organization Control (SOC) reports on internal controls like ISAE 3000, SOC2/SOC3.

[2] Standard 3402, article 16 sub viii ([IFAC11]): "Other aspects of the service organization's control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls that are relevant to the services provided."



ENFORCEMENT
by appreciating – or even rewarding – desired behavior and punishing undesirable behavior. The better the enforcement, the more people will lean towards what is desirable and avoid what is undesirable.

ACCOUNTABILITY
for errors, incidents and calamities. The safer people feel when reporting things, or when directly addressing others in the organization, the more they will actually do this and the more they will learn from these situations.

OPEN TO DISCUSSION
of any views, emotions, dilemmas and violations. The more opportunities people have to talk about these types of issues, the more they actually do so, and the more they will hereby learn from others.

TRANSPARENCY
of behavior. The better people can observe their own behavior and that of others, including its effects, the better they are able to adjust their own behavior to the expectations of others.

CLARITY
about what is desirable and undesirable behavior for the board, managers and employees. The clearer the expectations, the better people can understand what they should do, and the greater the chance that they will actually do so.

LEAD BY EXAMPLE
by the board and direct managers. The better the example is set in the organization, the better people behave, and vice versa.

INVOLVEMENT
in the organization by the board, managers and employees. The more the organization treats people with respect and involves them, the more people will do their best to look after the interests of the organization.

ACHIEVABILITY
of goals, responsibilities and tasks. The more people possess the relevant knowledge and skills, the better they can do what is expected of them.

Figure 1. Soft controls model (Muel Kaptein).

In order to specify and measure culture and behavior, the generally accepted soft controls model, developed by Muel Kaptein ([Kapt14]; [Kapt03]) can be used. This model is also used by the NBA as basic assumption in its guideline. Before we address the question on how culture and behavior can be included in ISAE reports, we will explain the soft controls model in the next paragraph.

> *"Sound insight in soft controls together with the analysis of hard controls provides a more complete representation of the internal control environment and the possible effectiveness of the internal controls taken"* ([NBA22])

STRUCTURED MODEL FOR ANALYZING AND MEASURING SOFT CONTROLS

In Kaptein's model, soft controls are defined as eight non-tangible behavioral factors in an organization, that are of importance for realizing its organizational objectives. In figure 1 this model is represented with an explanation of the eight soft controls.

We consider effective soft controls as the foundation and precondition for the effectiveness of hard controls. It is not about replacing hard controls by soft controls but increasing insight in the effectiveness of the internal control environment by including an evaluation on soft controls.

EFFECTIVE SOFT CONTROLS CONTRIBUTE TO SOUND INTERNAL CONTROL

Admittedly, soft controls are less easy to measure and qualify, but ultimately, they do affect the effectiveness of internal controls. Below some illustrative examples.

Examples of the relationship between hard and soft controls

Example 1
An authorized signatory's task is to approve payments on a daily basis. In addition to that, this person has multiple daily tasks and responsibilities. Usually, the payments' approval takes place at the end of the day. In extreme cases, it occurs that this employee is approving payments at 11 o'clock at night.

Therefore, there is a less effective soft control: achievability is too low. Chances are that the quality of the approval of the payments is negatively influenced by a lack of time. Despite the fact that hard control seems to be working, the likelihood of wrongful payments is increasing.

Example 2
A process description of steps that need to be taken by the employee could work properly to increase clarity and achievability. However, in practice, such a process description could be seen as inconsistent and could be experienced as insufficiently clear which could cause that the procedure in the process is not being carried out in the same way by every employee.

In Figure 2 we represent the relationship between hard and soft controls schematically. In this figure, soft controls are also shown as the foundation for effective hard controls. The soft controls instruments in the figure are examples of means that can be used to make the soft controls more effective.

By addressing soft controls in the execution of – and reporting on – internal control, a service organization could provide a more complete view of its control environment to the clients of their services. This contributes to the preventive side of controls, by providing the right circumstances for the execution of hard controls. In addition to that, it also contributes to a detective side as attention is being paid to findings in the context in which observations are being made. A few examples:

- Are mistakes allowed to be made?
- To what extent does one learn from incidents that occur?
- To what extent are employees enabled to properly do their job, which reduces the chance of mistakes?

The soft controls model is also highly effective to analyze the "why" of findings and to identify the root cause. Identifying the root cause leads to more sustainable improvements and with that to a structurally better internal control environment. At the same time, this contributes to more trust between the service organization and its client. Both are demonstrably better "in control".[3]

SUGGESTIONS FOR SOFT CONTROLS IN AN ISAE 3402 REPORT

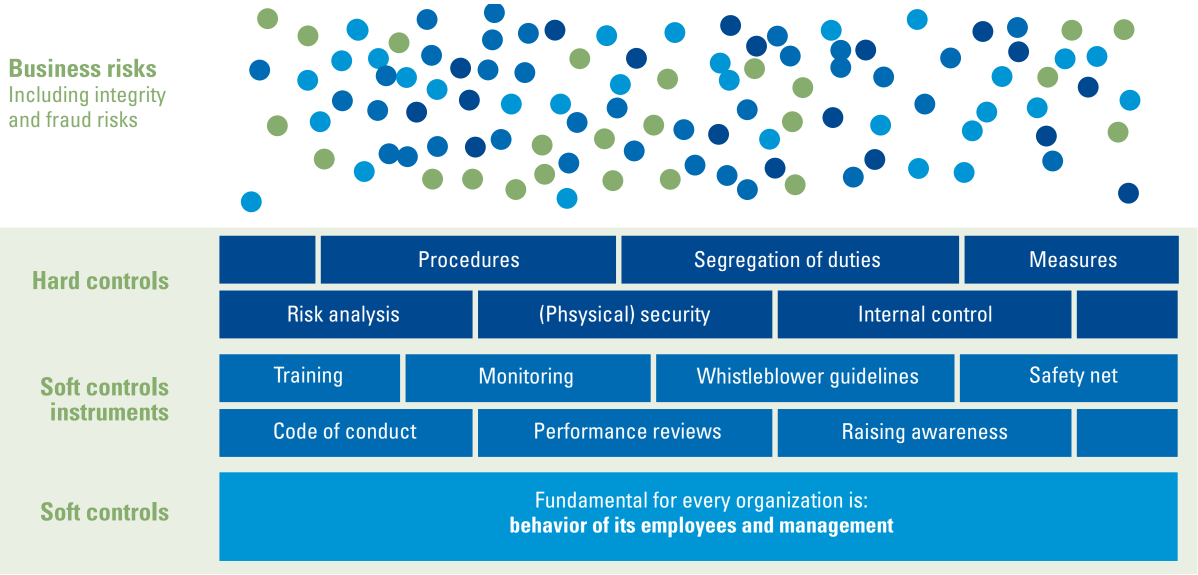
When an organization identifies risks, (hard) internal controls are implemented to mitigate these risks. In an ISAE 3402 report, these controls are subsequently tested for their operating effectiveness. An ISAE 3402 report roughly consists of two parts: the description of the service organization and the chapter with the control objectives, the related controls, and the findings of the auditor as a result of the test work. Next, we will describe some suggestions on how soft controls can be included in these two parts of an ISAE report.

Soft controls in the description of the service organization

In the description of the service organization, we see, in practice, that only a few soft controls instruments are being addressed (such as a code of conduct, personnel policy, regulations concerning integrity or whistleblower protection schemes). In our view, as an organization, you would not only detail the set of soft control instruments being used for managing culture and behavior, but rather the quality and effectiveness of these tools. This could be done by for example detailing the results of an annual employee's satisfaction survey. It's not about the survey itself but rather the fact that the greater part of the employees experience unclarity in what is expected of them in their job. Such a result may provide context to findings on the internal controls.

[3] For additional examples about the relations between Soft Controls and IT General Controls see [Bast15].

Figure 2. Relationship between hard and soft controls.



As far as we are concerned, a good example of how to reflect on instruments is Nationale Nederlanden's 2021 annual report. On page 54, for example, it is clearly described how Nationale Nederlanden monitors their values and standards and how they keep these alive: “Living our Values programme” ([NN22]).

As already mentioned before, soft controls are also highly effective for performing root cause analyses. For example, the description of service organizations may explain the extent to which root cause analyses are performed, including a description of what this analysis includes, what the results are, and what actions have been taken. An example of such a description is:

> *To gain more insight in our culture, the organization annually performs a root cause analysis on incidents of which the size of the consequences is important to the organization and on findings that involve multiple organizational units. The root cause analyses are being executed by a team that has been specifically trained for this and are mainly executed based on interviews with the people involved.*
>
> *The analyses of the past year show that especially the quality of the soft controls clarity and open for discussion require attention: Several employees had insufficient clarity about their role and responsibilities and were not comfortable enough to ask questions about it. In response to this, the organization communicated and defined tasks and responsibilities more clearly. In addition to that, several intervision sessions were arranged to increase the openness to discuss.*

Soft controls in the chapter on control objectives

Also in the second part of the report, the chapter on control objectives, soft controls can be integrated. It is common practice in this chapter to provide management comments to identified findings by the auditor, often as an appendix to the report.

In practice, we often see management responses about the hard component of a control, for example: “*We acknowledge the findings of the auditor and adjusted the procedure for the coming year.*” The positive aspect is that the finding is acknowledged by the management and that action has been taken. The comment however does not contain a reflection on the context of the finding such as an answer to the questions why there was a finding and what the organization has learned from this. An example of a stronger response in our opinion could be:

> *“We acknowledge that this control has not been effective. Immediately after observing this, we have investigated the cause. The objective of the control and execution of this control were insufficiently clear to the owner of the control, resulting in the control not being performed correctly in August. In the initial development of the policy, no coordination had taken place with employees who had to execute the policy. The language of the policy therefore did not connect to the experience of the control owner. We have simplified the work process for this control, and we have discussed this with the employees in the unit. For establishing new policies, coordination with control owners has now been included in the process. Therefore, we expect the control can be executed effectively next year.”*

A FURTHER STEP WITH SOFT CONTROLS AS PART OF THE CONTROL FRAMEWORK

Through the last example, the question arises whether soft controls can also be part of the internal controls in the control framework on which the auditor performs his test work. In our view this could be done in two ways:

- First you can connect specific behavioral risks to a control objective. From this behavioral risk it can be indicated in which way soft controls support the effectiveness of the hard control.
  An example: *a hard control that describes that a manager needs to approve an invoice, is only effective if that manager actually determines that the invoice complies to all conditions with the proper knowledge. The manager needs to feel responsible for this; it needs to be clear what is expected of the manager and the manager needs to have sufficient time for this.*
  As far as we are concerned, the trouble here is the demonstrability of soft controls. An ISAE 3402 engagement aims to provide reasonable assurance on the effectiveness of internal controls. This requires high-quality documentation and controls. In most organizations, the demonstrability of soft controls is not as mature to provide reasonable assurance. In addition to that it also is difficult to demonstrate whether the soft controls were effective for a specific period.
- A second way to include soft controls in the control framework, which is easier to apply, is by including hard controls on soft control instruments. Consider, for example, conducting an annual risk awareness survey, where you measure the extent to which soft controls support or impede effective risk management together with control owners, and then formulate action items accordingly.

GETTING STARTED WITH SOFT CONTROLS

Above, we illustrated how a service organization could start reporting on soft controls in its ISAE 3402 report: the description of soft controls, including soft controls in management responses and the execution of root cause analyses or soft controls as part of the control framework.

In order to be able to structurally report on soft controls in the internal control environment and actively work on this as an organization, the following step-by-step plan could be followed:

- Soft controls start with management. The first step is getting support from the service organization's management: is management open to this? Are they prepared to be vulnerable?
- The gradual training of the organization in the area of soft controls: This ensures that people within the organization speak the same language when it comes to culture and behavior. A sound route for this is to start with the control owners, compliance, and internal audit. Thereafter it can spread to the rest of the organization.
- Setting up a model for analyzing root causes. As stated above, a sound root cause analysis leads to a better internal control environment; however, this does need a robust method and process.
- The execution of soft control surveys: for example, by executing a survey as mentioned before (through questionnaires) amongst employees that execute controls. Also include the reflection of the organization on these results in the ISAE 3402 report.

CONCLUSION

If an organization outsources critical processes to a service organization, this organization is not discharged of the responsibility of being in control of these processes. As this responsibility is largely supported with ISAE 3402 reports, these reports should give a complete view of the quality of the internal control environment at the service organization. We are of the opinion that, without attention for soft controls, fundamental insights are missing.

As we illustrated in this article, you cannot be sure about the quality of the hard controls without paying attention to soft controls. This is why we plead to also report on soft controls, which increases trust between organizations, and helps the outsourcing organization as well as the service organization itself to be "in control" to a greater extent.

> You cannot be sure about the quality of hard controls without paying attention to soft controls

References

[Bast15] Basten A.R.J., Van Bekkum, E. & Kuilman, S.A. (2015). Soft controls: IT General Controls 2.0. *Compact, 2015*(1). Retrieved from: https://www.compact.nl/articles/soft-controls-it-general-controls-2-0/

[Kapt03] Kaptein, M. & Kerklaan, V. (2003). Controlling the 'soft controls'. *Management Control & Accounting, 7*(6), 8-13.

[Kapt14] Kaptein, M. & Vink, H.J. (2014, January 13). *The Soft Side of Hard Controls: A Control Coding Theory*. Retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2378437.

[IFAC11] IFAC (2011). *International Standard on Assurance Engagements (ISAE) 3402: Assurance reports on controls at service organizations* (article 16 sub viii). Retrieved from: https://www.ifac.org/system/files/downloads/b014-2010-iaasb-handbook-isae-3402.pdf

[NBA22] NBA (The Royal Netherlands Institute of Chartered Accountants) (2022, February 8). *NBA Practice Note 1148: Obtaining an understanding of soft controls relating to an audit of financial statements – Impact of culture and behaviour on the risk assessment*. Retrieved from: http://www.nba.nl/globalassets/wet--en-regelgeving/nba-handreikingen/1148/english-translation-of-nba-practice-note-1148-soft-controls-febr.pdf

[NN22] NN Group (2022, March 10). *Serving customers in times of change: 2021 Annual Report* (p. 54). Retrieved from: https://www.nn-group.com/nn-group/file?uuid=fe0ed772-850a-4697-95e5-06a1fe376e0f&owner=84c25534-c28a-4a64-9c78-5cc1388e4766&contentid=11805

About the authors

Laura Ploegsma is senior consultant at KPMG Advisory – Governance, Risk & Compliance Services. She supports organizations in performing assurance engagements (ISAE3402) as well as performing soft control assessments and embedding soft controls in the risk domain.

Corine Tol is senior manager at KPMG Advisory – Governance, Risk & Compliance Services. She supports all kinds of organizations in embedding soft controls in their full risk domain, such as internal audit, ORM and compliance.

Jacco van Kleef is partner at KPMG IT Assurance & Advisory. In his role as financial auditor and IT auditor he engages with clients in financial statement audits and assurance engagements (ISAE 3000/3402).