Internal Control over Financial Reporting

ICFR Benchmarking Survey 2016

pwc

www.pwc.no

Welcome

Welcome to our report on the Internal Control over Financial Reporting (ICFR) benchmarking survey for 2016. Designed to provide ICFR leaders (e.g. internal control officers, CFOs, Corporate Accountants and such) the benchmarking data they need in order to understand common practices today, and plan for more effective and more efficient ICFR operations in the future.

"Which ambition level should we set for our ICFR maturity and how much effort does this typically require?"

"How many internal controls have similar companies implemented for their transaction processes?"

"How do others monitor operational effectiveness of internal controls in practice?"

"What are common challenges and weaknesses amongst my peers?"

We are frequently asked these kinds of questions when we discuss internal control over financial reporting with our clients. In our experience, different companies who are seeking to improve the effectiveness and efficiency of their internal controls tend to meet similar challenges and ask themselves the same questions, regardless of their industry and size. Although ICFR should be adapted to the nature and needs of the business, there are a number of best practice elements any company that seeks to implement an effective and efficient internal control should adopt. This report aims to provide answers to some of the many questions posed to our clients regarding what peers are doing and also highlight key gaps between common practice in Norway and our views on best practice and global trends.

We received 26 responses to our 2016 survey, mainly from large global companies, of which almost half are listed on Oslo Stock Exchange. The Survey responses were received from a broad cross section of companies representing 13 different industry sectors, whose revenues ranged from less then 5 billion NOK to more than 25 billion NOK. Therefore, the report provides a view of ICFR over a wide variety of organisational settings.

We have organised the responses into themes based on elements of a good practice ICFR framework. In each chapter, we present the findings and discuss how they compare with our expectations and to what leading companies do. In general, the findings support our view that the area of ICFR is still immature in Norway relative to other countries, where listed companies are subject to more stringent regulation. As this is our first survey of its kind, some results are difficult to evaluate and derive trends from, due to the spread in responses and different interpretations of the questions. As we expand the benchmarking database and as the responding companies become more mature and standardised in their approach to ICFR, we believe this will become less of an issue. We look forward to following the development going forward.

The PwC ICFR benchmarking survey is available on the www.pwc.no website. From 2017, an online survey tool will be available on the website, where companies may respond to the survey and receive feedback directly. As the number of respondents increases, the analysis will be expanded to better address correlations between company characteristics such as organisational size, complexity and industry and their ICFR operations. We will provide periodic updates of the survey report, where we incorporate insights from the previous year while keeping some core questions the same for comparison purposes.

We hope you find the information in the PwC ICFR benchmarking survey report insightful and valuable. Our intention is that the report serve as a useful tool to help you improve the effectiveness and efficiency of your organisation's ICFR operations.

Aase Lindahl and the Business Controls team
RISK Advisory Services Oslo, Norway

Table of content

”Overall ICFR maturity shows room for improvement”

”Scoping is an underutilised tool for establishing an efficient ICFR system”

”Many lack a control design that in total addresses all critical risks”

”Periodic self-assessments are widely used for monitoring, but provide low levels of assurance”

Internal control maturity

Most Norwegian companies have implemented controls over their financial reporting to varying degrees, depending on their size, nature and complexity and on external and internal requirements. However, ICFR has typically been informal with a high degree of implicit trust involved. Over recent years, larger Norwegian companies have moved from control systems based on trust to "trust and verify." The latter requiring a more systematic, formalised and monitored approach to internal control. Many companies are seeking ways to ensure that their ICFR addresses risks in an efficient manner and derive more value from ICFR by taking a holistic view on risk management in the business.

The level of ICFR maturity in Norwegian companies depends on many factors, both internal and external. This benchmark survey aims to identify some of the most common factors that significantly impact the level of maturity. One key factor is external requirements, such as stakeholder and regulatory requirements. We expect the most mature companies in this survey to be found amongst companies listed in the USA, Canada and Japan that are required to comply with the Sarbanes-Oxley-Act (SOX) and its variations. Equally we expect institutions required by Norwegian law to implement risk-based internal control systems to be more mature. Other companies listed on the Oslo Stock Exchange operate under less strict requirements, but are expected to be more mature than non-listed companies due to reporting requirements and recommendations provided by The Norwegian Code of Practice for Corporate Governance. In general, the acceptable and most common level of ICFR for Norwegian listed companies is assumed to be around level 3 (See Formalised description in the "Levels of internal control maturity" box below).

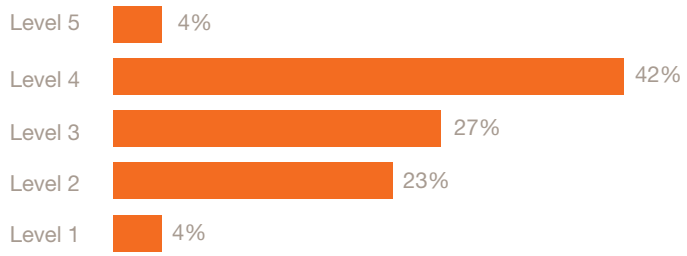
The survey starts by asking the survey respondents to assess the maturity level of their company's ICFR. 40% responded that they have implemented formalised and standardised controls, which are periodically tested for effective design and operations, and reported to management. Not surprisingly, over 60% of these presumably most mature companies are required to comply with either SOX, J-SOX, Canadian SOX or Basel III/CRDIV and Solvency II requirements. Over a quarter of the respondents have assessed their level of maturity to be at level 2 or lower, which is below the acceptable standard for Norwegian listed companies. 40% of these companies are listed on the Oslo Stock Exchange. Over half of the respondents rate their level of maturity at level 3 or lower, indicating that there are a number of companies who would benefit from a more systematic, formalised and monitored approach to ensure that financial reporting risks are adequately and efficiently mitigated by well-functioning controls.

Levels of internal control maturity

1. ***Unreliable*** Unpredictable environment, no or few control activities designed or in place
2. ***Informal*** Control activities in place, but not adequately documented. Little or no formal training or communication of expected minimum control activities
3. ***Formalised*** Control activities designed and adequately documented but not standardised. Deviations may not be detected on a timely basis
4. ***Monitored*** Standardised controls with periodic testing. Automation and tools may be used to support ICFR
5. ***Optimised*** Integrated internal controls with real time monitoring. Automation and tools are used to support control activities

Figure 1

How would you rate your company's maturity with regards to ICFR?

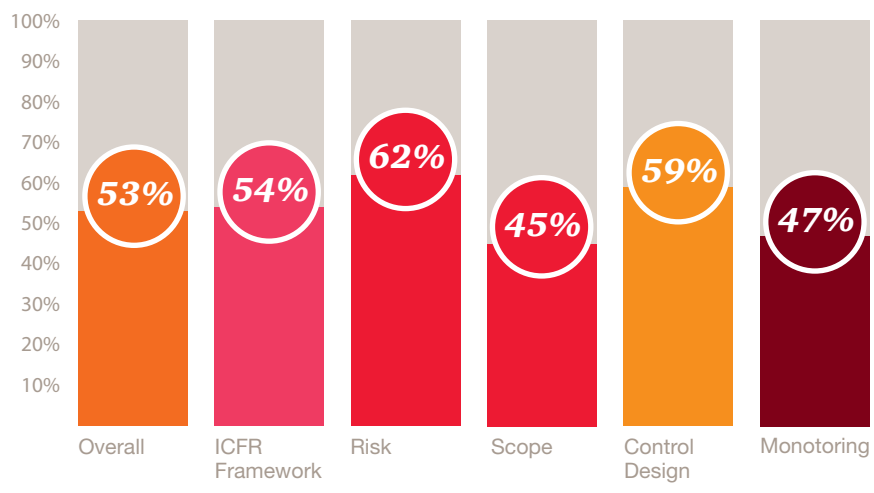


The majority of respondents rate their ICFR to be formalised or monitored.

The survey then proceeds to ask more detailed questions regarding key elements we would expect to find in a best-in-class internal control system (Optimised level 5). To gain an overview of the general gap between the responses to these detailed questions and a best-in-class level of maturity, we have benchmarked the responses to our understanding of an Optimised level of internal control over financial reporting. The consolidated average of all scores is presented in figure 2. Responses vary; some companies are well above average while others are well below. The level of ambition most likely varies between respondents but the results support our general findings that there is considerable potential for improvement among the responding companies. Interestingly, the companies' individual scores also show that a number of companies assess their maturity level to be higher than what is evidenced by their subsequent detailed responses. We have discussed our findings in more detail over the next chapters.

Figure 2

Total average score per internal control area compared to maturity level 5.



The overall maturity shows room for improvement, especially in the areas of scoping and monitoring.

Do Norwegian companies know what good internal control looks like? And does management know the true status of internal control in their organisations?

ICFR Framework

Leading companies have adopted a holistic and integrated framework for risk management/internal control, of which ICFR is an important component. A structured framework helps companies build and organise complete and effective ICFR systems. However, an ICFR framework cannot be effectively implemented and provide value to the business without systematic processes and well-defined roles and responsibilities.

Most respondents use an acknowledged framework and a defined annual process to implement ICFR

An ICFR framework provides structure and guidance for management on how to design, implement and maintain internal controls that effectively and efficiently address financial reporting risks. Using an acknowledged framework provides assurance to oversight boards, stakeholders and regulatory bodies that the company is taking a systematic approach based on good practice. COSO is one commonly used and acknowledged framework (see coso.org for more information). An ICFR framework is often managed and maintained by implementing an annual process. This typically consists of risk and scope assessments, design maintenance and improvement, communications and training, continuous or periodic monitoring and testing and reporting on status and results.

A majority of the surveyed companies have implemented an acknowledged framework for ICFR. Most of these have rated their internal control maturity at level 3 (Formalised) or higher. However, almost a third of the respondents state that their companies have not built their internal control based on an acknowledged framework. Interestingly, over half of these latter companies have assessed their internal control maturity to be at level 3 or higher.

Although using an established internal control framework, in our view, is fundamental to ensuring that a company's ICFR system contains all key elements, is not in itself sufficient to achieve high ICFR maturity and effectiveness. The quality of processes, such as scope and risk assessments, control design, implementation, maintenance and monitoring is key to effective ICFR. We recommend to implement an annual overall process for governing the ICFR processes, to ensure that the ICFR is risk-based, efficient, well-planned and -managed, implemented, operating effectively and continuously updated and improved. Most of the survey participants using a framework for ICFR have implemented such an annual process.

Figure 3

Q *Is your company's ICFR based on an acknowledged framework?*

of the respondents have implemented an acknowledged framework for ICFR.

Q *Does your company have a defined annual process for governing ICFR?*

of the respondents who use acknowledged framework, most have defined an annual process for governing ICFR.

Roles and responsibilities are defined, but how well are they implemented?

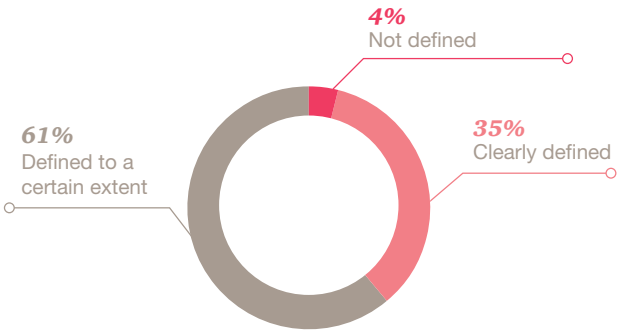
Clearly defined, communicated, understood and agreed roles and responsibilities are the backbone of any well-functioning ICFR system. They ensure that all involved personnel, functions and bodies understand and accept the respective responsibilities and duties they are expected to fulfil and that they are held accountable for their performance. A well-designed ICFR responsibility hierarchy enables the distribution and implementation of control ownership throughout the organisation, thereby building an integrated and resilient ICFR system.

All but one of our respondents state that they have defined roles and responsibilities for managing and overseeing ICFR within their organisation. However, less than half of these ensure that the defined roles and responsibilities are communicated, enforced and maintained. In our experience, this is a common challenge, which may lead to the gradual decay of ICFR responsibility hierarchies, involving lack of or reduced ownership, misunderstandings, reduced learning and improvement, inefficient and/or insufficient performance of key tasks and controls etc., thereby threatening to undermine the company's ICFR system.

As figure 6 illustrates, roles and responsibilities are in most cases formalised at corporate or group level. Interestingly we also see that the roles of control owners performers and process owners are often not defined at the unit level. This may impact the organisation`s ability to standardise and acheve an optimised internal control throughout the organisation.

Figure 4

Q *Has management defined roles and responsibilities regarding managing and overseeing ICFR?*



Only about a third of the respondents have clearly defined roles and responsibilities.

Figure 5

Q *How are the roles and responsibilities communicated, enforced and maintained?*

73% communicate roles & responsibilities to all relevant personnel

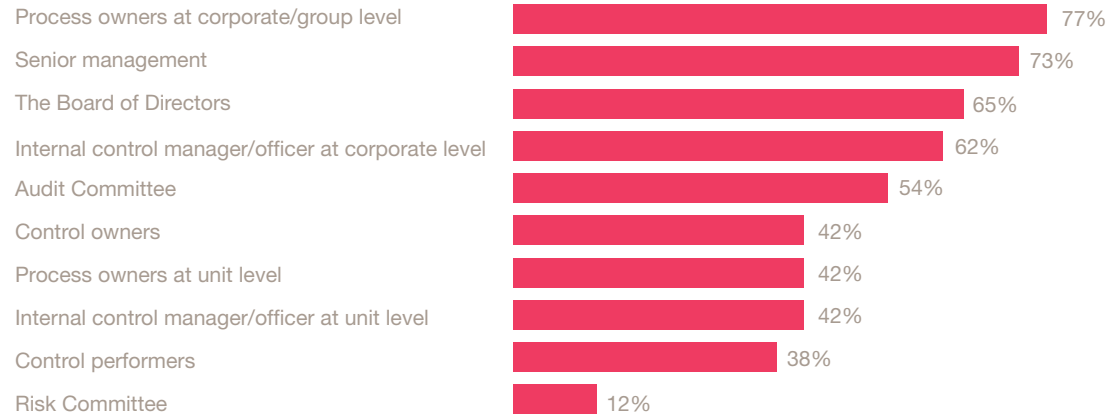
58% enforce roles & responsibilities through status reporting

77% regularly maintain roles & responsibilities

The majority of respondents communicate roles and responsibilities but less than half perform follow-up and maintenance activities.

Figure 6

Q *Roles and responsibilities defined for the following.*



Many respondents have defined roles and responsibilities at the board and group management level, while far fewer have defined roles and responsibilities at the unit level (such as business unit, segment, business area or legal entity)

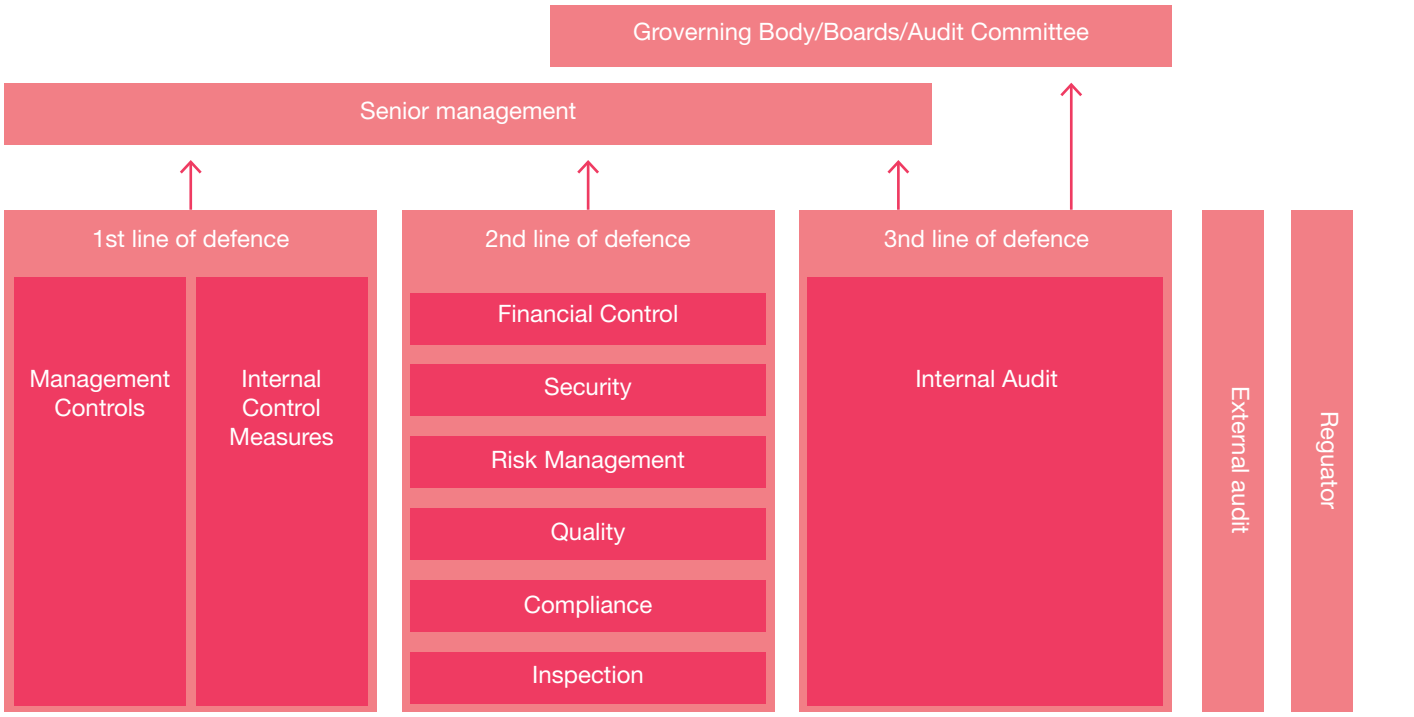
Applications of the Three Lines of Defense model vary

The Three Lines of Defense model is a commonly used model for clarifying roles and responsibilities regarding internal control. The model's underlying premise is that, under the oversight and direction of senior management and the board, three separate lines of defense within the organisation are necessary for effective management of risk and control. The first line of defense (operational management) has ownership, responsibility and accountability for assessing, controlling and mitigating risks and maintaining effective internal controls. The second line of defense often has responsibility for drafting and implementing policies and procedures as well as monitoring the status of internal control and supporting the first line of defense. This is commonly performed by functions put in place by management, such as ICFR Officer, Risk Manager, Compliance Officer etc, which can be placed at both the group and unit level. The third line of defense (typically internal audit) provides independent assurance to the board and senior management concerning the effectiveness of internal control systems, including the manner in which the first and second line of defense operate. See www.ferma.eu for further guidance.

Almost half of the respondents have allocated responsibility for managing ICFR to at least two lines of defense, approximately one third to one line of defense and the remaining have no distinguishable lines of defense. Which lines of defense the responsibilities have been assigned to varies among the respondents.

The responses seem to indicate a higher reliance on the second line of defense than on the first line, which is contrary to the premise of the three lines of defense model, where the primary responsibility rests with the first line. We often experience that the first line of defense has not taken full taken ownership or understood its responsibilities, and important tasks are either picked up by second line functions or are insufficiently managed. Furthermore a number of the companies have placed ICFR management responsibilities within their internal audit function. This practice is not uncommon, especially in companies with small group functions, although in our experience this may result in conflicting roles and responsibilities, within the internal audit.

Figure 7: The Three Lines of Defense model



* Adapted from ECIIA/FERMA Guidance on the 8th Company Law Directive, article 41

How many ICFR employees are involved?

In response to our question regarding how many personnel are involved in managing the ICFR process, the numbers range from zero to five hundred, although the majority are within the range of one to ten. We interpret these responses to mean that the number of employees involved in planning, facilitating and monitoring the ICFR process (i.e. second line of defense responsibilities) most commonly lies between 1 and 10. At the same time, the spread in responses indicates that interpretations of what managing ICFR entails vary.

The level of maturity and organisational structures will impact how organisations define the roles and responsibilities in reation to their ICFR process and this impacts the findings in this survey.

Figure 8

Q *Where in the organisation is ICFR managed?*

54% First line of defense

69% Second line of defense

23% Third line of defense (internal audit)

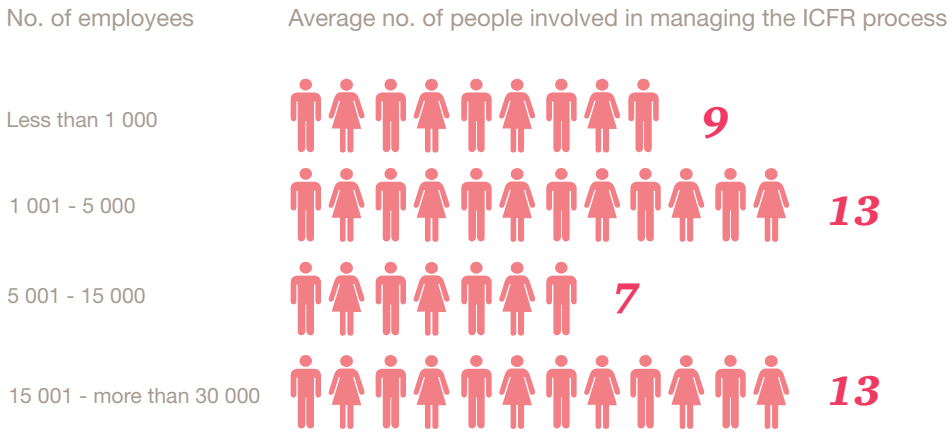
15% No distinguishable lines of defense

The survey indicates a high reliance on the second line of defense

Figure 9

Please estimate how many personnel are involved in managing your company's ICFR process.

** Responses with zero employees or abnormaly high no. of employees involved in managing ICFR have been extracted for the purpose of the analysis.*



There is no clear correlation between the respondents number of employees and the size of the ICFR organization.

Risk

Best practice dictates that ICFR should be top-down and risk-based, meaning that the ICFR system should be designed to address the most significant risks related to financial reporting from top to bottom in the organisation. Risk-based scoping, control design and monitoring require periodical risk assessments and updates.

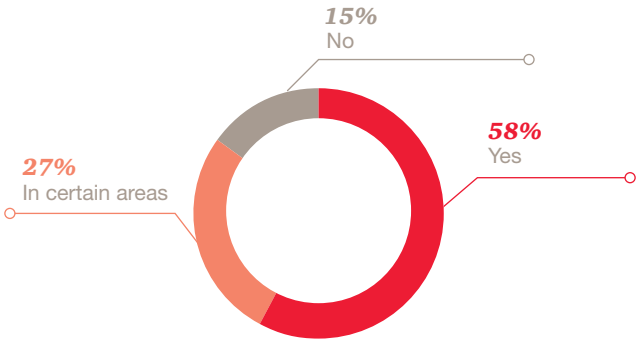
Most companies have an approach for identifying and assessing risks

Risk assessment forms the basis for identifying, understanding, measuring and prioritising risks within an organisation. In order to effectively and efficiently mitigate significant risks of financial reporting misstatements, the scope, design and monitoring of internal controls should be based on comprehensive and thorough risk assessments. The risk assessments should start with the company's financial statement, tracing risks of significant misstatements to significant accounts and the corresponding transaction processes from each entity with the company.

Interestingly, almost half of those who have no defined risk management approach, or only apply it to certain areas, have responded that they use an acknowledged framework and over two thirds that their ICFR maturity is at level 3 or higher. Comprehensive and systematic risk assessments are, in our opinion, prerequisites for building an effective and efficient system for internal control. The companies that lack such an approach are normally unable to identify all the significant risks. Their internal control over financial reporting may as a consequence not be sufficiently risk-based and is most likely incomplete. By definition these companies do not have a fully mature ICFR in place.

Figure 10

Q *Does your company have a defined approach for identifying and assessing inherent risks of significant financial statement misstatements?*



A large majority (85 %) of the companies have a defined approach for identifying and assessing inherent risks of significant financial statement misstatements.

Is ICFR "bolted on" business activities as opposed to "built in"?

ICFR should be an integral part of the way business is conducted and managed, in order to be an efficient and add value. Leading companies take a holistic view on risk management and align or integrate ICFR with their enterprise risk management processes. The findings however supports our experience that ICFR is often perceived as something separate from the regular business activities, which is performed to conform with external and internal requirements.

According to the Norwegian code of practice for corporate governance, boards are required to ensure that the company has sound internal control and systems for risk management that are appropriate in relation to the extent and nature of the company's activities. Boards must form their own opinion on the company's internal controls, based on the information presented to them. Furthermore, they are recommended to carry out an annual review of the company's most important areas of exposure to risk and its internal control arrangements. Where a company has an internal audit function, it must establish a system whereby the board receives routine reports and ad hoc reports as required. Only a little over half of the respondents communicate the risk assessment results to the BoD/Audit Committee, all of which have an internal audit function. We would have expected this number to be higher.

Figure 11

Q *Is the ICFR risk assessment aligned or integrated with other enterprise risk assessments?*

of the survey's respondents who perform ICFR risk assessments have aligned or integrated these activities with other enterprise risk management processes.

Figure 12

Q *Is the outcome of the risk assessment communicated to the BoD/Audit Committee?*

communicate the outcome of the risk assessment to the BoD/Audit Committee.

Risks are assessed at all levels, but few link risks to the financial statements

Internal control risk assessments are the linchpin of the ICFR system, which should be performed at different organisational and financial reporting levels, starting from the top and with the consolidated financial statements. The risk of significant errors in the financial statement should always be the starting point, considering materiality and inherent risk factors for each financial statement line item, significant account and reporting unit within the group. Inherent risks should be assessed for each significant transaction process feeding data into these accounts, initially at a high level and then drilled down into the necessary details per process. We recommend performing an iterative top-down/-buttom-up risk assessment where the result should be a consolidated risk overview at the corporate, reporting unit and process levels. This provides the starting point for scoping the ICFR system and design of risk-based controls.

81 % of the surveyed companies who perform ICFR risk assessments consider risks at the group level and 50 % consider risks at the unit level. Two thirds of the respondents assess risks per significant process, but only one third do the same per financial statement line item. This indicates that although risks are assessed at the process level, the link to the financial statement is less apparent. Hence, the actual consequences of process level risks with regards to the financial statement may not be fully identified and understood.

Nearly all the respondents state that their control activities are specifically designed to mitigate the identified risks. At the same time, only half of these connect the risks to financial statement assertions (objectives for ensuring correct financial reporting, such as completeness, accuracy, existence, presentation and disclosure). Connecting risks to financial statement assertions clarifies the potential consequences errors may have on the financial statement. Furthermore it ensures that the controls are designed to focus on activities that effectively target the most relevant risks.

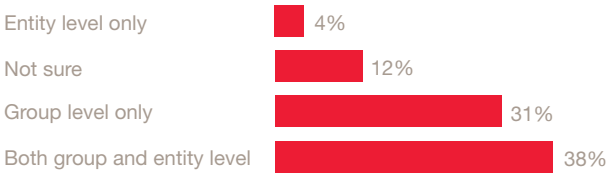
Figure 13

Q *Are control activities specifically designed to mitigate the identified risks?*

of the respondents who have a defined approach to risk assessment also design controls to specifically mitigate the identified risks.

Figure 14

Q *Where are ICFR risk assessments performed?*



15% of respondents do not have a defined approach to risk assessment and are therefore not a part of this analysis.

Figure 15

Q *At which financial reporting levels are ICFR risk assessments performed?*

Respondents perform and document their risk assessments per process, but only about a third per financial statement line item.

There are several risk assessment approaches. In our survey the approach of assessing risk by evaluating the likelihood and impact of an event occurring that has an adverse impact on the financial statement is widely applied among the participants. Reports from internal and external auditors and historical events are also considered during risk assessments, but not to the extent that we would expect. All relevant and available information should be utilised in risk assessments, including learnings devived from historical events and audit findings.

Risk assessments run the risk of being outdated

In a rapidly changing business and regulatory environment, risks are constantly emerging and changing. Risks should be re-assessed at least annually, or more often if significant events occur. Of the respondents who have defined a risk assessment approach, more than half of the respondents revise their risk assessments annually. 27% either revise every two to three years or have replied that this is not applicable to their company, which we interpret to be never. The few respondents who revise their risk assessments when something happens, may have the most up-to-date risk picture, provided that all relevant events are captured and assessed on a timely basis.

Figure 16

Q *Is the likelihood and impact of the individual risks a part of the evaluation?*

Of the respondents who have a defined approach to risk assessment document the likelihood and impact as part of the risk evaluation.

Figure 17

Q *Events considered during risk assessments?*

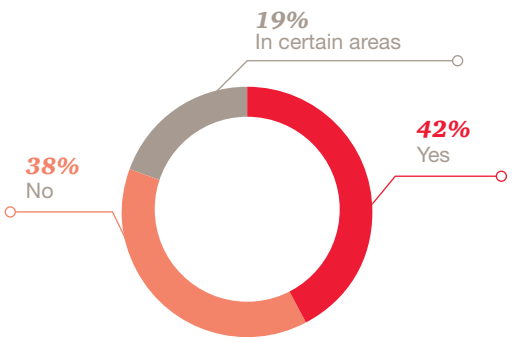
Scoping is an underutilised tool for establishing an efficient ICFR system

Systematic high level risk assessments should form the basis for ICFR scoping. By scoping we mean deciding which units, processes and financial statement line items are to be prioritised in the ICFR system, and to which extent. Risk-based scoping is essential to an effective and efficient ICFR system, in that it ensures that ICFR controls are designed to mitigate the most significant risks.

In the survey, only 42% of the respondents use a comprehensive risk-based approach for scoping ICFR, while 19% use the approach in certain areas. Of the remaining 38 %, half report that ICFR is applied to all processes and entities regardless of risk. These findings indicate that many companies may benefit from a more structured planning and scoping process, in order to increase efficiency and effectiveness and prioritise ICFR activities that provide the most benefit.

Figure 18

Q *Does your company use a risk-based approach for defining the scope of ICFR?*



Less than half base their scope of ICFR on the assessment of risks of errors in the financial statement.

Figure 19

Q *How do you apply your scoping regarding entities and processes?*

63% exclude low-risk processes and entities from the ICFR design requirements.

75% monitor low-risk processes less rigorously

56% monitor low-risk entities less rigorously

94% have a minimum level of controls for all entities.

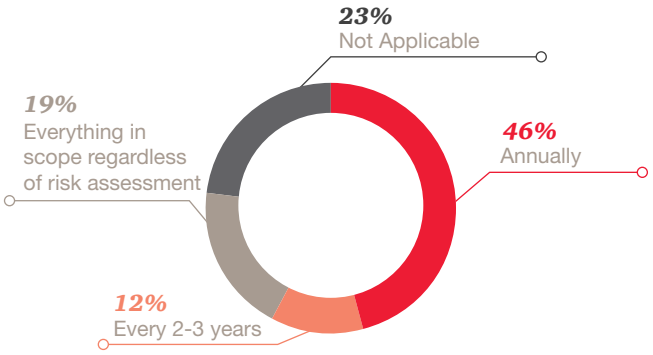
The respondents who have a defined risk-based approach to scoping utilise their risk assessments to focus their control design and monitoring activities on important risk areas.

The companies who perform risk-based scoping were asked how they apply their scoping to the design and monitoring of internal controls. Almost all have defined a minimum set of controls that are applied to all entities regardless of scope. This is a common practice and typically involves governing documents such as the code of conduct, authority matrix and policies, and entity level financial reporting controls. Most of the respondents scope ICFR at both entity and process level.

Given the increasing pace of change businesses are exposed to, the ICFR scope should be revised annually or more often if significant events occur, such as mergers or divestments (aligned with the risk assessments). Less than half of the respondents revise their scope annually, and those also revise risk assessment annually or upon events. This is in line with best practice and indicates that the scoping is performed based on an updated risk picture. The others who have a defined approach to ICFR scoping revise their scope every two to three years, possibly because they experience few changes impacting their scope in the shorter term.

Figure 20

Q *How often do you revise your scope?*



Most of those who perform scoping update their scope annually.

Design

Best practice companies have designed their internal controls to specifically mitigate defined risks in an efficient manner and in alignment with the needs and nature of the business.

Governing documents are widely used as entity level controls

The top-down design of internal control should begin with relevant governing principles and policies. These can be powerful entity level controls designed to communicate the tone from the top, and direct behaviour, decisions and culture at all levels in the organisation. Less than half of the respondents revise their scope annually, most of whom reassess their ICFR risks annually. Such risk reducing measures at entity level provide the necessary control environment that may reduce the need for, or at least strengthen and supplement, detailed ICFR process level controls and documentation. A robust internal control structure depends on a strong linkage between governing documents and processes and transaction process level controls that in aggregate address significant risks over financial reporting. The participants in the survey indicate an extensive use of policies as part of their ICFR framework.

The majority of the respondents have a number of policies, where the most common cover areas of Financial Close and Reporting, Procurement, Anti-Fraud and -Corruption and Delegation of Authority. Fewer have policies for Treasury, Sales and Legal. Treasury is often centralised and sufficiently covered by Delegation of Authority, while Legal may overlap with Anti-Fraud and -Corruption. It is not uncommon to lack a sales policy, as this process is often highly operational and fragmented across many departments, making it difficult to define a comprehensive and standardised policy with one established owner. In our view, this, and the fact that ICFR risks over revenue processes are typically high, only increases the need for a sales policy, which outlines roles, responsibilities and guiding principles across the process.

Interestingly, almost half of the respondents have local policies, the majority in addition to group policies, indicating that they allow for local flexibility and possibly also local monitoring of compliance. Such structures are often a consequence of the company's operating model, (autonomous units tend to have their own policies,) which may result in deviations in content and interpretations between group and local policies.

Figure 21: Example of a top-down internal control pyramid

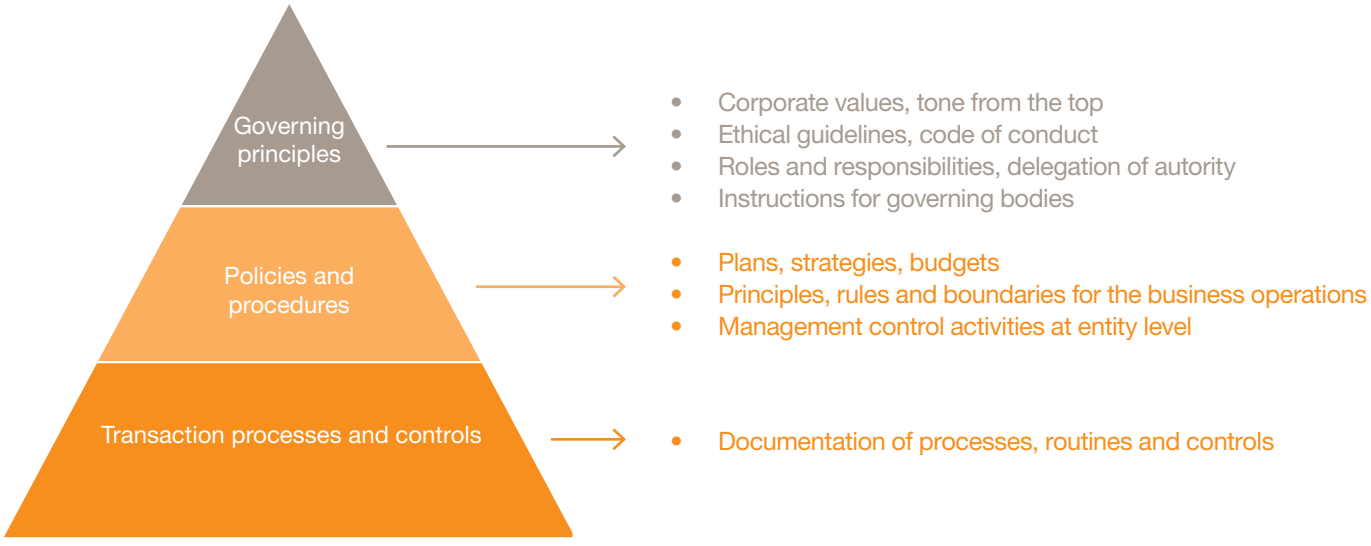
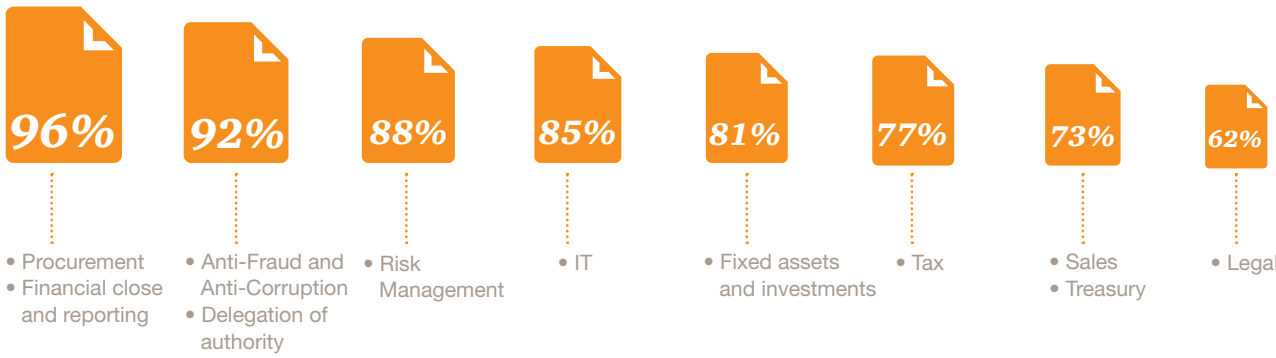


Figure 22

Q *Does the organization have documented policies in place for the following processes / policy areas:*



The most common policies are related to ICFR, fraud and risk management.

We observe a trend where corporations are looking to centralise and standardise their policy management across countries and units in order to gain a tighter control over compliance with laws, regulations and internal requirements. This is in many cases due to the fact that corporate headquarters are increasingly being held responsible for the operations of their local subsidiaries. A top-down approach with clear and concise information that trickles down from top management to the lower levels of the business with a holistic monitoring of compliance, is in our view essential to good internal control. A clearly defined top-down structure should have group policies and procedures that apply to all parts of the organisation (with any necessary adaptations for different types of businesses or local conditions) with locally developed handbooks, guidelines and tools catering to the specific needs of the local units.

Figure 23

Q *Do the policies encompass the whole group or are there local policies for each unit?*

of the respondents have standardised policies across all units.

Flowcharts are commonly used, but some types are more common than others

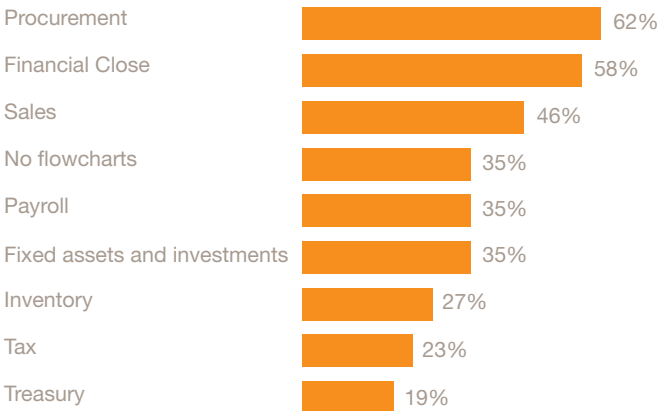
A commonly used method to gaining understanding of a process and its inherent risks is to map flowcharts. In our experience, flowcharts that are kept up-to-date can be a useful tool for discussing and gaining a common understanding in the organisation of what the inherent risks are and where there is a need for implementing risk reducing measures. When our clients are in the process of establishing or improving their ICFR, our advice is often to investigate ways of reducing inherent risks over the process before internal controls are added or redesigned. For instance, if a process is highly manual with many interfaces, trying to mitigate the risks only through internal controls, may be insufficient. Ways to automate and simplify the process should in this case be investigated before internal controls are to be introduced.

Flowcharts are also valuable in assessing where and how processes and internal controls can be standardised and streamlined across organisational units, in order to develop an efficient and lean internal control design and reap other operational benefits.

65% of the participants in the survey utilise process flowcharts in their ICFR, of which half use standardised flowcharts across units. Flowcharts are most commonly utilised for procurement, Financial Close and Sales. 58% document Financial Close, which is often a more standardised and "easier" process to document in a flowchart. Tax and Treasury are the least common, and are areas that are typically more to flowchart. More surprising is the limited use of flowcharts for Payroll, Fixed Assets and Inventory challenging, since they often involve significant inherent complexity and risk. However, this may in part be due to low financial impact for the responding companies in question.

Figure 24

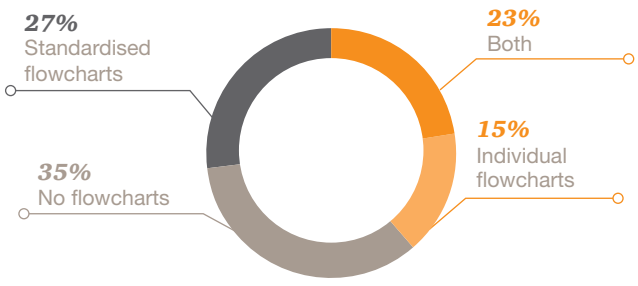
Q *Are flowcharts documented for the following processes?*



62% of the respondents document flowcharts for procurement, which is often considered a complex process. 58% document Financial Close, which is often a more standardised and "easier" process to document in a flowchart.

Figure 25

Q *Are the flowcharts / process descriptions standardised for the whole Group or do local units have individual flow charts?*



The majority have standardised process flow or a combination of standardised and individual.

Surprisingly many have an incomplete control design

A defined and formally documented design of controls that addresses all critical risks and is regularly maintained is a prerequisite for effective internal control. Documentation is critical to ensure that internal controls are correctly and consistently understood and carried out and that performed activities can be evidenced and monitored. The majority of the respondents have defined and formally documented controls. However, only half of the respondents state that they have built a complete design of controls (entity level controls, IT general controls and process level controls) that in total addresses all critical risks. Half of the remaining respondents with incomplete control design have assessed their overall maturity to be at level 4, which is inconsistent with these results.

Incomplete control design provides a dubious sense of security.

Figure 26

Q *Have you built a complete control design that addresses all critical risks and which is formally documented?*

50% of the respondents have a documented design that covers the most critical risks, although 35% of these have only controls documented in certain areas.

Financial close controls are the most common, and controls are both standardised and locally tailored

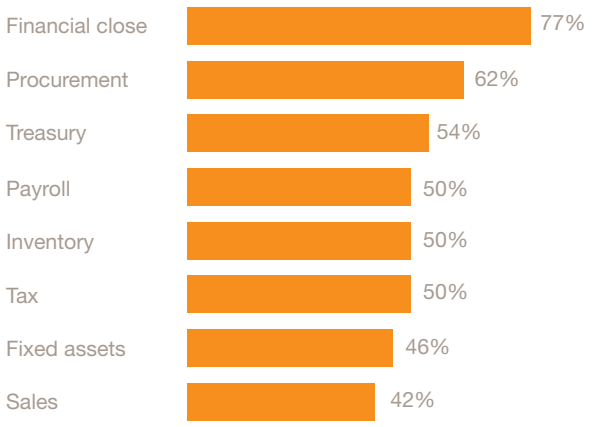
The majority of the respondents have designed and formally documented process level controls, most commonly for Financial Close and Procurement and least commonly for Sales. In our experience, this may be explained by some of the same factors as for policies. Financial close and procurement are close to financial reporting, while the sales process is often highly operational and fragmented across many departments, making it difficult to define ICFR controls under one process owner. The fact that ICFR risks over revenue processes are typically high (e.g. revenue recognition), only increases the need for internal controls over the sales process.

Similar to the policy area, we observe a trend where corporations are standardising their processes and internal controls across units in order to reap efficiency benefits and to improve the effectiveness of their internal controls. The most favoured approach among the survey respondents is using a combination of standardised controls and locally tailored controls.

A top-down standardised control design is usually owned at corporate level, meaning that controls are documented and maintained centrally and local units are required to adhere to the control design. Not surprisingly, since many respondents favour a combination of standardised and locally tailored controls, their companies have chosen a combination of centralised and local design ownership.

Figure 27

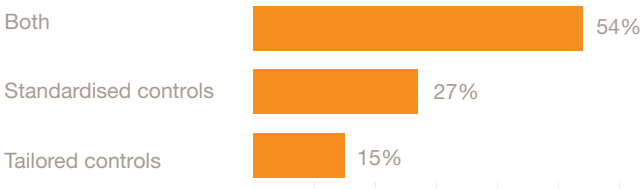
Q *Are ICFR controls designed (formally documented) and maintained for the following processes?*



Financial Close controls are most common while sales are the least common.

Figure 28

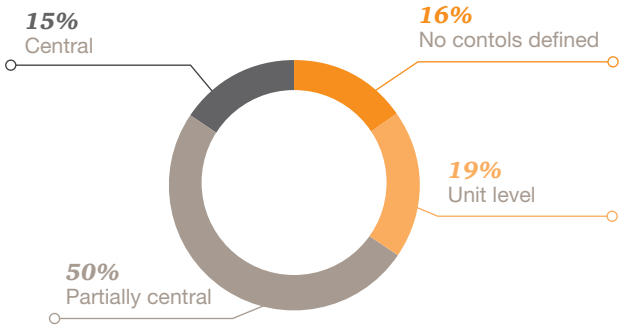
Q *Are the controls in general standardised across the group or are there individual controls tailored to the units?*



Most apply a combination of standardised and locally tailored controls.

Figure 29

Q *How is the ownership of the overall ICFR control design distributed in the organisation?*



Most have partially centralised control design ownership.

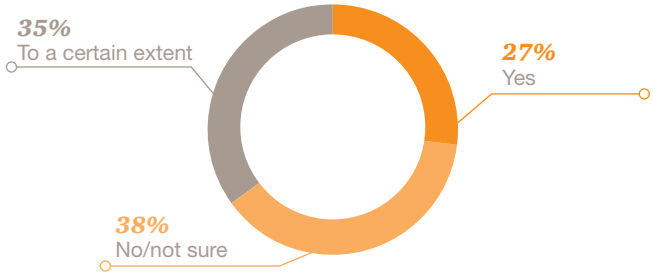
Few consider the dependency on IT-related risks, but access controls are commonly used

Increasing digitalisation and automation of business processes and internal controls increases the dependence on IT and hence IT controls. IT general controls (such as controls over programme changes, system access controls, incident management and IT operations continuity) should be taken into consideration in the design of process level controls that rely on the relevant IT systems. A common challenge today is a lack of awareness and dialogue around the interdependencies between IT general controls level and process controls, and they are typically designed and implemented separately. This can result in unreliable process controls, an inefficient control structure with duplicate controls and control gaps.

There is, however, a high awareness regarding the importance of system access controls. These controls are not exclusive for information security purposes, as they serve to ensure the reliability of automated and IT-dependent controls, such as segregation of duties, automated approval flows, input data validations and system blocks. The majority of the respondents are aware of the importance of access controls and state that they have established system access controls and that these are based on authorisation matrices.

Figure 30

Q *Is the dependence on IT general controls taken into consideration in the design of process level controls?*



Our experience is supported by the survey, where less than a third of the participants have taken IT general controls into consideration in their process level control design.

Figure 31

Q *Are security and segregation of duty risks mitigated by system access controls? Are these controls reconciled with group and/or local authorisation matrices?*

have established system access controls and reconcile these to the relevant authorisation matrices.

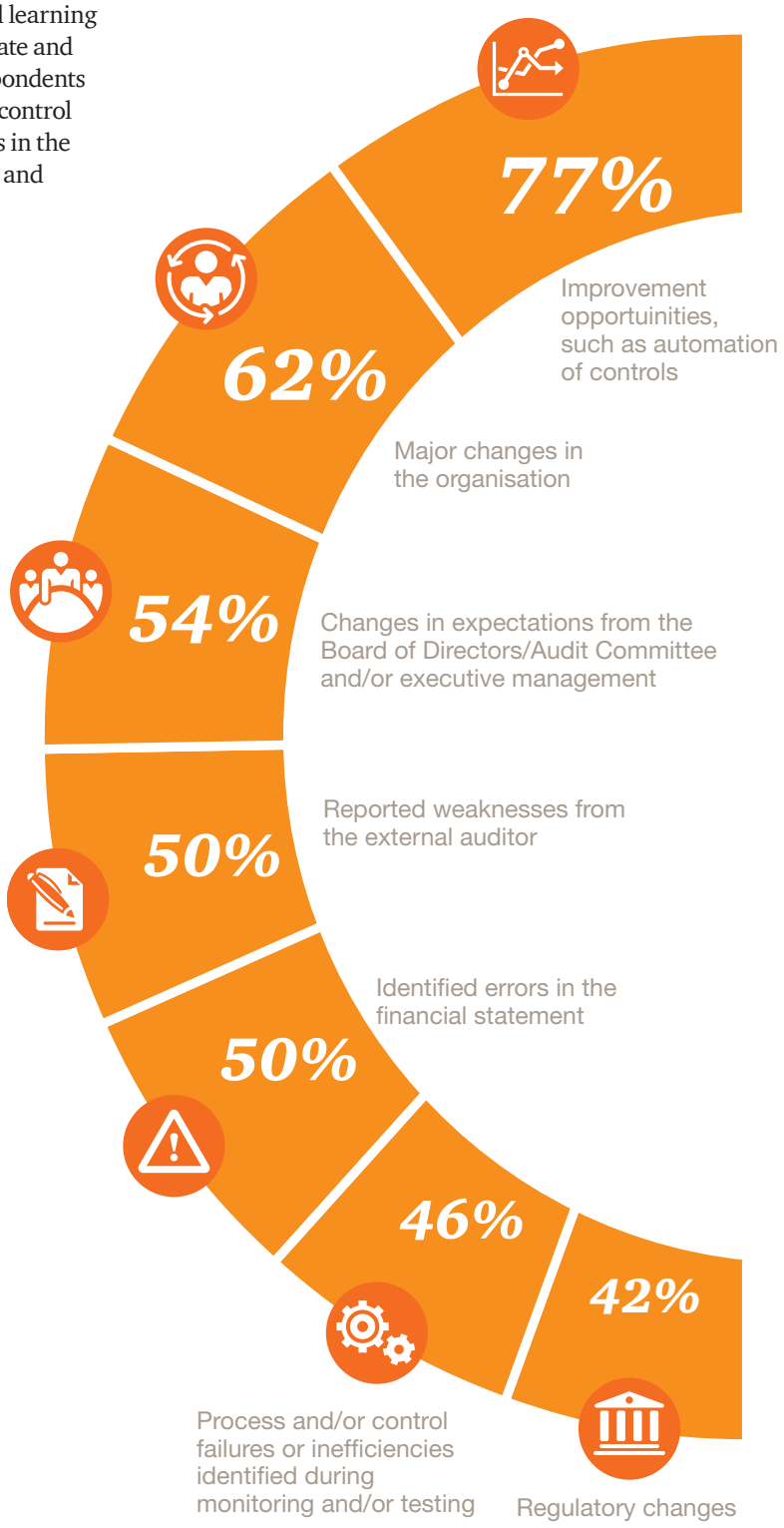
Most respondents have a structured approach for maintaining their control design

The control design should be regularly updated to avoid that it becomes obsolete and ensure that it continues to mitigate critical risks. Leading companies recognise the need for a structured approach to capture external and internal changes and learning from ICFR activities and incidents to continuously update and improve their internal control. The majority of the respondents have a structured approach in place for updating their control design. The most common triggers are identified errors in the financial statement, major changes to the organisation and reported weaknesses from the external auditor.

Never pass up an opportunity to learn from failures and errors!

Figure 32

Q *Do you have a structured approach for updating the ICFR control design, which would be triggered by one of the following events?*



The majority have a structured process in place for updating their control design.

How many controls is the norm?

A popular topic of discussion is how many controls companies typically design for each process. Based on the data collected in this survey, we are unable to determine clear correlations between the number of process controls and company characteristics (such as size, type of industry, number of business units or centralised versus local control design). However, these are all variables impacting the number of controls that are deemed optimal for an organisation. Not all the respondents were able to estimate the number of designed controls and the answers vary from 5 to 400, the median being 135 controls in total. Interestingly, a number of the respondents lack formalised controls for one or more processes, which we would expect to be quite common, such as Procurement and Sales. Although some of the listed processes may not be relevant or material to all, we find this surprising, especially since many of these respondents have assessed their ICFR maturity to be at level 3 or 4.

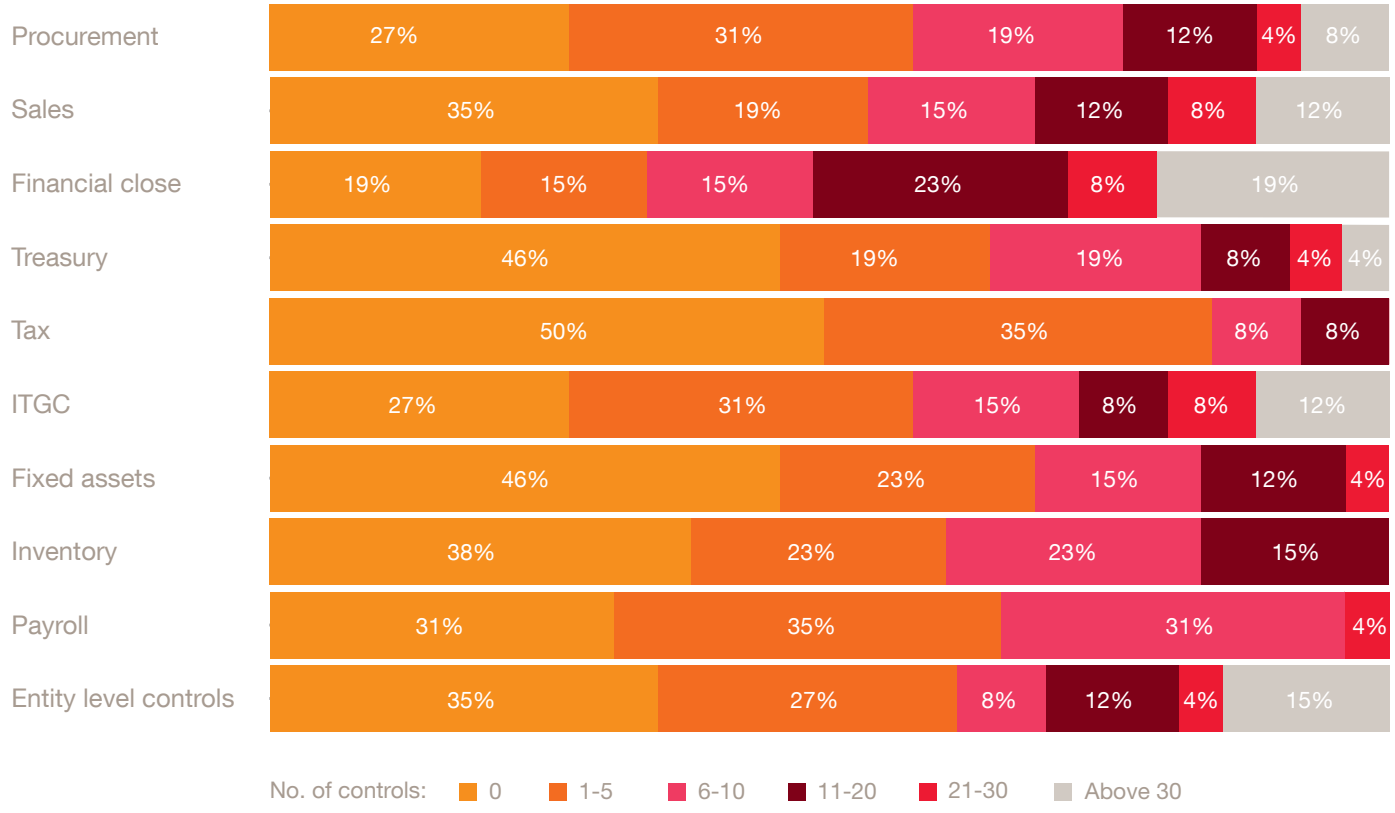
We have taken a closer look at two processes where we would expect to find some commonality regardless of industry and type of organisation, i.e. financial close and entity level controls. The majority of those who have designed financial close controls either have 11 to 20 controls or more than 30 controls.35 % of the respondents have not designed any entity level controls (ELCs). Those with ELC controls have a large variation in number of controls and it is difficult to derive a standard number. The processes Procurement, Inventory, Fixed Assets and Payroll have similar control number distributions, the majority have 1-5 controls and the median is 6-10 controls. The numbers for the Tax process have a similar distribution with the median being 1-5 controls.

? How to read the graph?

27% of respondents have 0 controls in the procurement process while 31% have between 1 and 5 controls..

Figure 33

Q *Estimate the no. of controls in each of the process below.*



It is important to take into account that all processes are not relevant or are low risk. However it is still surprising that large organisations have rated themselves as high maturity have low number of processes formalised.

Monitoring

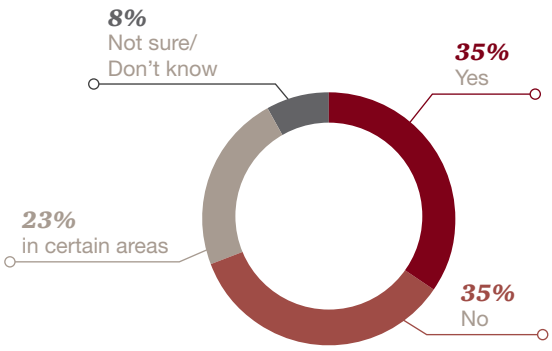
Monitoring is a crucial element of internal control over financial reporting that provides timely information regarding the effectiveness of internal controls and enables companiess to act on deviations and respond to new risks. Monitoring ensures that ICFR is implemented and operating as designed and that improvement needs and learning opportunities are captured in order to continuously improve the ICFR system.

A stricter approach to defining key controls would enable more efficient monitoring

To secure efficient use of resources, the most critical controls upon which the ICFR system relies should be identified, ie. the key controls. The concept of key controls is often used to establish which controls would provide sufficient assurance that the ICFR system is functioning as intended when monitored and/or tested. A little over half of the respondents distinguish between key controls and other controls, although a number of these seem to have defined all their controls as key. This finding indicates that a number of companies may benefit from more efficient monitoring and more focus on the most critical activities by taking a stricter approach to defining key controls.

Figure 34

Q *Do you distinguish between key controls and other controls based on risk assessments and/or for monitoring / testing purposes?*



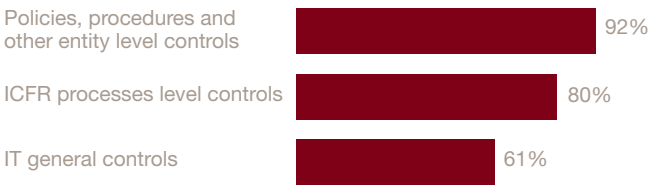
Many respondents do not consistently distinguish between key controls and other controls.

Monitoring of IT general controls seems under-prioritised

The survey shows that most respondents have some form of monitoring in place for entity level controls (policies) and process level controls. However, more than a third of the respondents do not have, or do not know if they have, any monitoring of IT general controls (ITGs). Almost two thirds of these have outsourced their IT operations, supporting our experience that controls over outsourced IT operations are often weaker than when they are retained in-house.

Figure 35

Q *Which processes are monitored and reported?*



IT general controls are the least monitored.

Periodic self assessments are widely used, but provide low levels of assurance

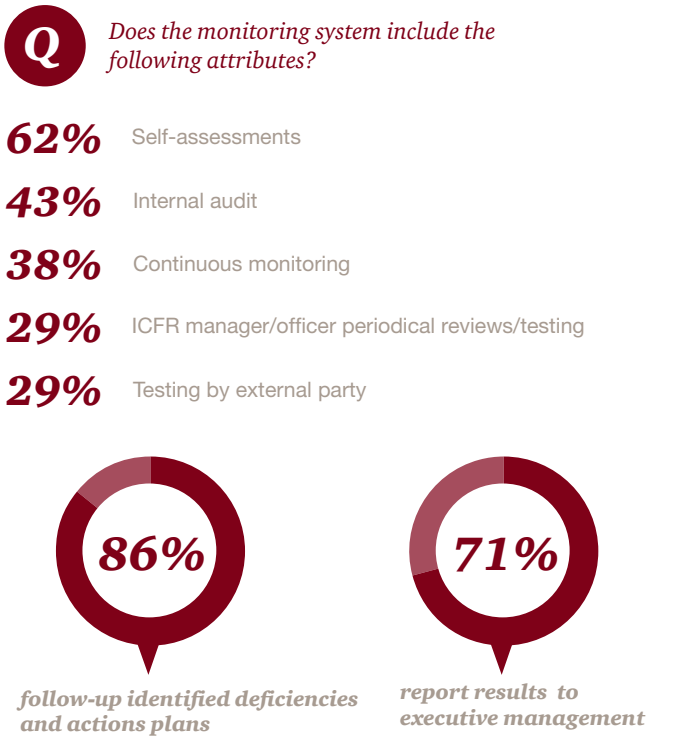
Monitoring should be performed periodically and as often as necessary, depending on the nature of the business, level of risks and internal control maturity. In our experience, the most effective monitoring systems build on a combination of specifically designed monitoring activities, where automated or manual gathering and evaluation of evidence provides the strongest assurance, and self assessments unaccompanied by documentation provides the weakest assurance. The latter are typically used for reporting compliance with policies.

Our survey shows that the most common way to monitor ICFR compliance is through periodic self-assessments, performance reporting and internal audit. Less than one third conduct continuous management monitoring. Most state that the monitoring of ICFR includes follow-up of identified deficiencies and action plans.

Testing is mainly performed by internal audit, but also by the ICFR manager in some companies. No companies report that testing is performed by both. Of those who use external parties, only a few have outsourced their internal audit functions, indicating that this may refer to external audit, such as an ISAE3402 report (Assurance Report on Controls at a Service Organization).

Interestingly, only a little more than half of the respondents report results from the monitoring process to senior management and/or the Board or Audit Committee. Amongst those who do not perform such reporting, some have an internal audit function, indicating that this result may be somewhat unreliable and due to some respondents' possible lack of insight into reporting lines to senior management and the board. However, there seems to be room for improvement regarding keeping management and oversight bodies informed on the status of internal control.

Figure 36



Self-assessments is the most commonly used method for monitoring ICFR.

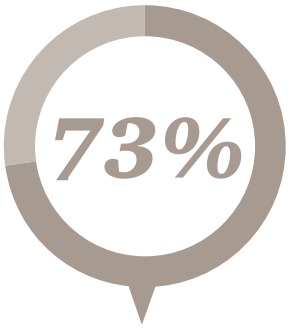
Self assessments are simple monitoring tools, but provide limited value on their own.

ICFR technology support

The size and complexity of internal control systems should reflect the nature of the business. Large and complex ICFR systems, involving many controls, organisation units and personnel, are often challenging to manage and oversee. Many organisations use technology to support parts or the entire internal control process. Examples are GRC software, ERP system functionality and workflow support. However, the market in Norway for GRC systems is still immature relative to other European countries. In particular, using system support for continuous monitoring of control performance is still relatively uncommon.

Figure 37

Q *Do you use technology to support the ICFR system?*



use technology to support the ICFR system

Q *What type of system do you use?*

50% Document repository

38% Systems for self-assessment surveys

31% Built in monitoring functionality and workflows in ERP systems

19% GRC system with functionality for supporing parts of the ICFR process

8% GRC system with functionality for supporting the entire ICFR process

27% have implemented GRC system functionality, but only 8% have a GRC system with complete functionality for supporting all ICFR processes.

System support for ICFR is relatively immature

A majority of the respondents use IT to support their ICFR, beyond the use of spreadsheets. The most common is to use a document repository system. Less than half of the largest companies in the survey use a GRC system to support their ICFR.

The need for document repository and management is obvious due to the large number of documents typically required to manage ICFR. However, the additional benefits from using GRC software, such as risk assessment and scoping support, consistent ICFR implementation, efficient communication, maintenance and enforcement of roles and responsibilities, management of policies, processes and control design, continuous monitoring and value adding reporting, are often difficult to gage and measure. We believe this to be a key reason for the relatively low utilisation of GRC software in Norway, together with the relatively immature internal control environment.

What are your ICFR system support needs?

There are many types of ICFR systems on the market. Before you start exploring the various options, it is often a useful excercise to assess what your needs are.

Questions to ask should include:

- Are our needs limited to ICFR, or should the system support integration with other processes? (e.g. compliance management, internal audit and enterprise risk management).
- Do we need support for all or selected parts of the ICFR process? (see figure).
- Do we need support for all or selected policy areas, IT controls and transaction processes?
- What are our automation and system integration requirements?
- Who are main user groups and their roles and needs? Think 3 lines of defense.
- Can our existing systems provide ICFR support functionality?
- Do we need a high degree of flexibility, or can we use a standardised system?

Figure 38: ICFR process illustration

Conclusion

We hope this benchmark survey has provided some useful insights into ICFR practices among large Norwegian corporations. In general, we have found that many companies would benefit from investing in a more effective and efficient internal control system. However, we did find some leading practices among the survey respondents, which we have summarised below:

Leading companies

- ☐ Use an acknowledged internal control framework and have implemented a structured annual ICFR process with clearly defined roles and responsibilities for first, second and third lines of defense functions involved in managing and overseeing ICFR.
- ☐ Perform and regularly update top-down risk assessments, upon which they base their scoping of units and processes, design of mitigating controls and monitoring activities.
- ☐ Have documented and implemented a top-down design of internal controls, including entity level controls, IT general controls and process level controls, which in total address the most critical risks.
- ☐ Monitor the effectiveness of the most critical controls and of the ICFR system, using a variety of methods across all lines of defense.
- ☐ Utilise technology to increase effectiveness, efficiency and ease of oversight regarding their ICFR activities.

To summarise some of the key findings from the report, we would like to end with five tips to remember when establishing or improving the company's ICFR

1. Focus on ***material risks*** - plan and scope your ICFR efforts accordingly.
2. Use a ***structured approach*** for planning, updating, improving, monitoring and reporting on ICFR - and stick to it.
3. ***Monitoring*** is key - what gets monitored gets managed.
4. Aim to ***integrate*** ICFR into the overall governance and operations of the business - for instance by aligning with your enterprise risk management, business performance processes and operational procedures.
5. ***Communicate*** - when roles, responsibilities and how to perform tasks are understood and agreed, ICFR is more likely to survive and thrive in the business.

Contacting PwC

If you wish to benchmark your company's internal control against our database and/or have a deeper conversation about how you may improve the effectiveness and efficiency of your company's internal control, please contact:

Aase Lindahl
Partner, RISK Advisory Services
Tlf: 952 60 135
aase.lindahl@pwc.com

Ine Jacobsen
Manager, RISK Advisory Services
Tlf: 952 60 560
ine.jacobsen@pwc.com

Liubov Kokorina
Manager, RISK Advisory Services
Tlf: 952 16 190
liubov.kokrina@pwc.com

By spring 2017 an online benchmark tool will be available on www.pwc.no

Foto: Anette Larsen.