The world is evolving - is ICFR keeping up?

PwC's 2019 ICFR Benchmarking Survey

pwc

Table of content

Introduction

Welcome to PwC Norway's 2019 report on Internal Control over Financial Reporting (ICFR) benchmarking survey, where we provide insights into the following questions:

- **How effective and future proof is your internal control over financial reporting (ICFR)?**
- **How are your peers managing their ICFR frameworks?**

The first PwC ICFR benchmark survey was published in 2016, with the aim to capture the current status of ICFR among large Norwegian companies. The report received widespread positive feedback from ICFR leaders, for the valuable insights the report provided into good and common practices among their peers in the field of ICFR.

Since 2016 we have made the benchmark survey available as an online questionnaire (see www.pwc.no), allowing companies to benchmark themselves directly against good practices and gain immediate feedback on the overall maturity of their ICFR.

In this report we present our analysis of benchmark data collected throughout 2019. The data represents survey responses from 29 large Norwegian companies across a wide variety of industries, 13 of which are listed on Oslo Stock Exchange.

According to the 2016 benchmark the participating companies had an overall low level of ICFR maturity:

- More than half reported that they lacked sufficient controls to address critical risks
- Almost a third reported that their ICFR did not satisfy the minimum requirements for Norwegian listed companies

Were we expecting to see improvements since 2016? The short response is yes, our expectation was to see a general increase in ICFR maturity due to certain key trends evolving over the past three years. Our expectation was that this would affect companies' focus on and willingness to invest in ICFR.

Increased expectations from stakeholders - authorities, owners, customers, third parties etc. are requiring companies to implement transparent and formalised risk management and compliance programs, including ICFR.

More accessible digital tools - data analytics and process mining tools, RPA, niche GRC/risk management systems etc. makes it possible to automate processes, controls, monitoring and ICFR management activities.

A number of high profile fraud incidents in the media - leading to a heightened awareness regarding fraud risks and the pivotal role of ICFR in the prevention and detection of internal and external fraud.

Opportunities for added business value from investments in ICFR - e.g. process optimisation, improved internal reporting and business information, reduced reliance on key personnel and enhanced revenue assurance.

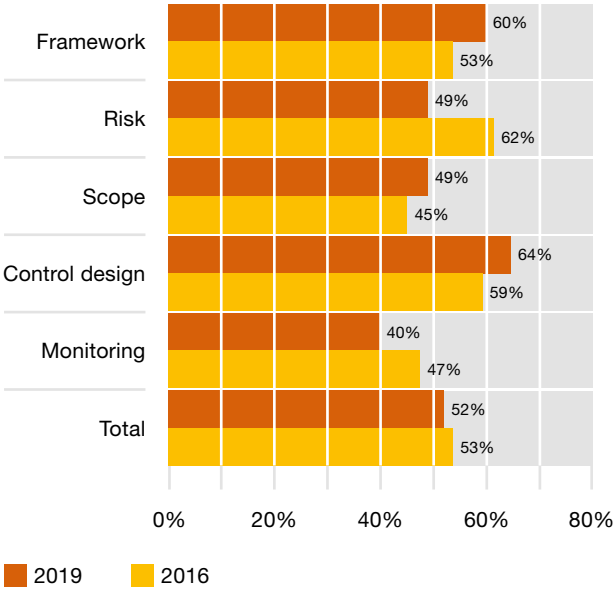
The 2019 survey goes beyond comparing maturity levels with prior years responses. We have added additional questions in order to gain insight into the respondents' use of digital tools to further advance their ICFR frameworks and how ICFR is utilised to manage fraud risk.

Do our findings support our hypotheses and provide new insights?

Has the overall ICFR maturity increased?

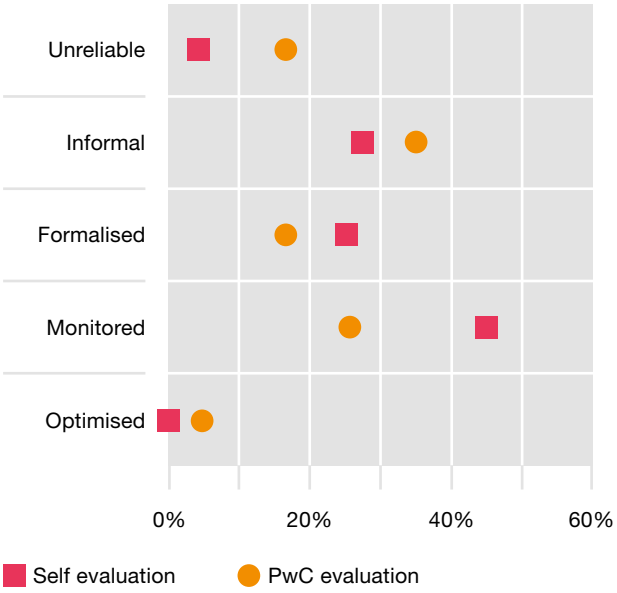
In short, the results from the survey provide little evidence supporting a general increase in overall ICFR maturity. The overall maturity is largely unchanged, and monitoring continues to be the area with the highest improvement potential.

Total average score per internal control area



Average scores for each internal control area indicate minor variations compared to 2016. The largest decline in maturity is related to risk and monitoring. These are also the areas with the most significant opportunities for improvements.

Self evaluation of ICFR maturity



Respondents rate their respective ICFR frameworks as less mature than in 2016. Nevertheless, they generally rate themselves higher than what is evidenced by their subsequent detailed responses to the survey questions.

Filtering the data gives a better understanding of the holistic picture. New respondents on average rate themselves as having a lower maturity than the participants of both the 2016 and 2019 surveys. Participants of both surveys have an increase in maturity since 2016. Throughout the report we will dissect this further and elaborate on the detailed results.

Furthermore, mature companies address fraud risk and use technology to support their ICFR work. The survey indicates that the majority of our respondents have a good understanding of the different types of fraud and fraudulent behavior impacting their financial reporting, but few address them in a holistic and systematic way across the business.

The survey indicates the use of technology and digital tools for ICFR is still in its infancy, despite obvious advantages presented by an array of tools, many of which are becoming increasingly available and easy to use.

Maturity model

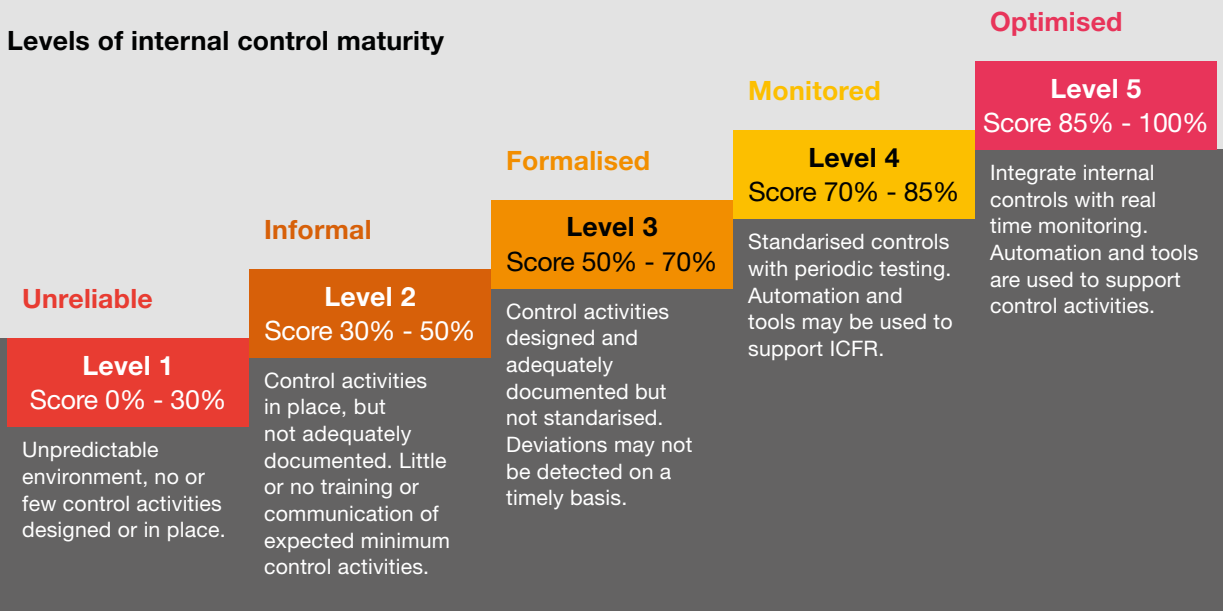
The ICFR maturity model is widely used among audit firms and other companies to assess the maturity of internal control frameworks. Although there may be nuances between the various maturity models, overall levels and categorisations are built on a similar logic. A maturity framework normally ranges from level 1 to 5, where level 1 represents an unpredictable environment with no or few controls and level 5 represents integrated controls with real time monitoring and automatisation. The lowest acceptable and most common level of ICFR for Norwegian listed companies is assumed to be level 3.

Technology enables a faster climb up the maturity ladder

Advancements in technology are driving cost efficient ICFR maturity improvements, such as automation and streamlining of control performance, monitoring and testing. However, the effective use of digital ICFR tools often requires that the underlying processes and available data are stream- lined and automated. Hence, as companies continues to digitalise their business processes we expect them to rapidly move up the maturity scale. In addition, this might allow them to leapfrog traditional testing and periodic monitoring entirely, moving straight to the highest maturity level with real time monitoring and internal control embedded into business processes.

This benchmark survey lists some of the most common factors impacting the level of a company's internal control maturity and asks 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 against our understanding of an Optimised level of internal control over financial reporting.

Levels of internal control maturity



Survey results at a glance - Minor developments in responses since 2016

	2019	2016
Calculated internal control maturity based on responses	52%	53%
Self-assessment of maturity	Level 3	Level 3
Use an acknowledged internal control framework	55%	69%
Have defined an annual process for governing ICFR	81%	85%
Have a process for identifying and assessing inherent risks of significant financial statement misstatements	86%	85%
Have a process for scoping (e.g. of business units and processes) to identify to which extent and level the ICFR framework is applied	59%	62%
Have defined and formally documented their ICFR control design	66%	88%
Have designed specific controls to mitigate one or more of the identified risks	89%	96%
Distinguish between key controls and non-key controls for monitoring and/or testing purposes	56%	58%

One might speculate whether companies with clear opportunities for improvement (low or medium maturity) have a higher motivation for participating in a benchmark survey, causing a skewed population. For these companies, benchmarking towards good practice and other companies helps them assess their current situation, areas of improvement and direction for further ICFR work. The same rationale may also explain why the most mature companies from the 2016 survey chose not to participate in 2019.

ICFR framework

About half of the companies use an acknowledged ICFR framework. This is a significant decline compared to the results from the 2016 survey.

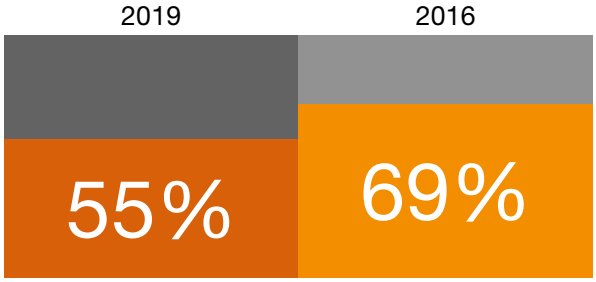
A commonly used framework provides structure and guidance for management on how to design, implement and maintain internal controls that effectively and efficiently address financial reporting risks. Interestingly, we see a decline in the number of respondents using an acknowledged framework and having a defined annual process to implement ICFR.

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

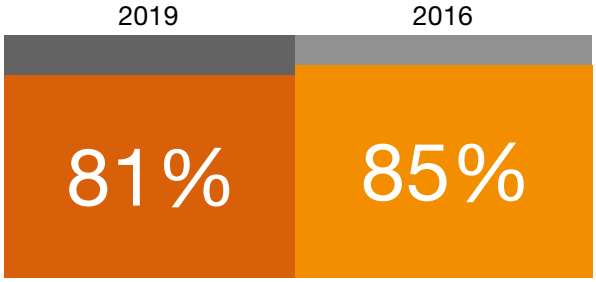
Internal control is «a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and Committee on Sponsoring Organisations (COSO) of the Treadway Commission».

Source; Committee of Sponsoring organisations of the Treadway Commision

Companies using an acknowledged framework



Companies with a defined annual process to implement ICFR



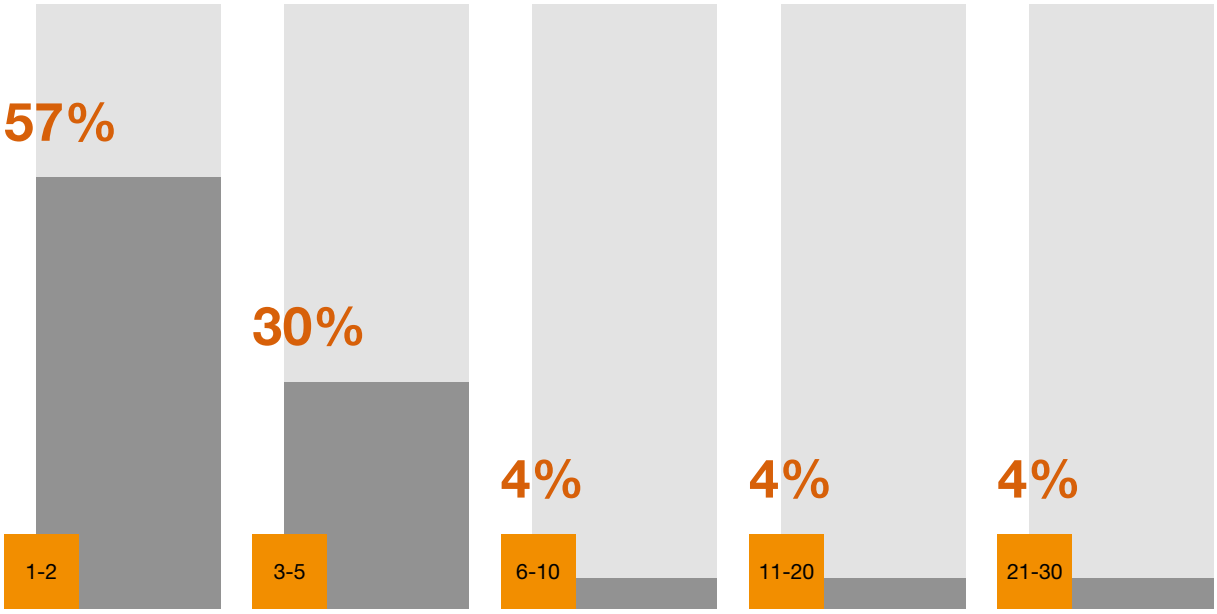
In less than half of the participating companies the responsibility for managing ICFR is defined as a separate role or function. In one fifth of the companies the role has not been established. These ratios supports the observation claiming that many companies are still under development when it comes to establishing a mature and well-organised internal control framework and methodology.

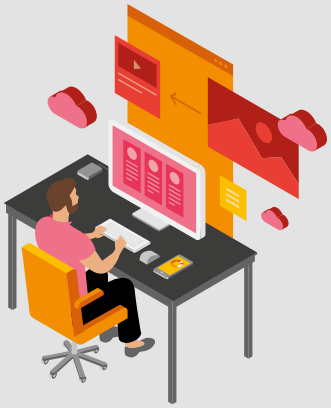
Has the company established a centralised ICFR function/role in charge of the ICFR framework?

41%	Separate designated function	**38%**	Accounting/finance department	**21%**	Not established a function/role

ICFR Personnel

The number of personnel involved in the managing of ICFR varies. Most have employed between 1 and 5 people.





Digitalising the ICFR framework

A GRC system or software is designed to support management in effectively integrating the internal control framework in everyday business. GRC systems contain sets of tools supporting periodic and ongoing activities, such as scoping, risk assessments, control design maintenance, control performance and documentation, control monitoring, assessments and reporting. Such systems typically provide task and approval workflows, structured documentation storage and audits trails, as well as status and dashboard reporting.

There are different types of GRC systems available, including large systems integrating all aspects of GRC with common risk universes (such as internal audit, enterprise risk management, operational risk management, governing documents, GDPR, ICFR etc.) and smaller niche systems geared towards specific risk areas, such as Financial Reporting or elements of ICFR (such as balance sheet reconciliations, monitoring or testing).

The main benefit of large integrated GRC systems is that they enable a holistic and integrated approach towards risk management, across silos and business boundaries. However, the market for GRC systems is changing, moving away from large scale GRC systems, and towards providers of smaller niche systems. Full scale GRC systems are not only costly and complicated to implement, they also tend to involve significant compromises leading to a

"one size fits no one" situation. Niche systems are less costly and easier to implement. Implementation becomes less of a turn-around and eases the implementation for smaller companies, making them more desirable. In addition, they usually provide the benefits of offering more tailored solutions to specific needs.

Few companies have adopted GRC systems to manage their ICFR

The maturity of the Norwegian market regarding the use of GRC systems seems to be lagging behind other European markets. Our findings support this observation, showing that only one third of the respondents have implemented a GRC system for managing their ICFR. The main reasons cited for implementing a system are storage of documentation, efficiency and real-time monitoring and reporting.

More than half of the respondents share that they have not implemented a GRC system, either due to lacking appropriate maturity level or size. Furthermore, one fifth state it is due to uncertainty regarding whether the system will provide added business value.

The company has implemented a GRC-system for managing ICFR

What was the main reason(s) for implementing GRC system(s)?

75%	Efficiency reasons, such as process automation and workflow enablement
73%	Centralised documentation and audit trail
63%	Real-time reporting and monitoring
25%	Possibility to integrate systems for risk management, internal controls, internal audit etc.
25%	Improve intelligence data and reporting

What was the main reason(s) for not implementing GRC system(s)?

53%	We are not mature/big enough
18%	Unsure if they provide value
12%	Cost
6%	We have too many systems already

Which ICFR processes does the GRC system support?

100%	Reporting
88%	Control testing
88%	Monitoring of control performance
88%	Follow up on issues
75%	Development and maintenance of control design
25%	Scoping and risk assessment
38%	Process mapping
13%	Automated control performance

Which modules (functionalities) in the GRC system does the company use?

100%	Internal control
25%	Compliance
13%	Enterprise risk management
13%	Operational risk management
13%	Governing documents
13%	Internal audit
0%	Information security/GDPR

Risk

There has been a negative development in the overall risk maturity score. If a company's ICFR is not based on holistic risk assessments, this could lead to a lack of focus on the most critical risks and potential gaps and overlaps in the control design.

A large majority of the companies have a defined approach for identifying and assessing inherent risks of significant financial statement misstatements. This is in line with the results from the 2016 survey.

Efficient and effective internal control should be top-down, risk based and systematic, meaning that the ICFR framework should be designed to address the most significant risks related to financial reporting from top to bottom in the entire organisation.

The company has a defined approach for identifying and assessing inherent risks of significant financial statement missatements

Nevertheless, approximately one third perform the risk assessment per financial statement line item, connecting it to the financial statement. Connecting risks to financial statement assertions clarifies the potential impact errors may have on the financial statement. Furthermore, it ensures that controls are designed to focus on activities that effectively target the most relevant risks of material misstatements.

The risk assessment is performed and documented

77%	At group level
68%	Per significant process
45%	Per unit
39%	Per financial statement line item

The following factors were considered during the risk assessment

84%	Historical events
83%	Likelihood and impact of the individual risks
79%	Reports from the internal or/and external auditor
68%	Per significant process

"Best in class" companies align or integrate ICFR and fraud management with their enterprise risk management processes in order to understand the full risk picture across the business and prioritise risk mitigating activities accordingly.

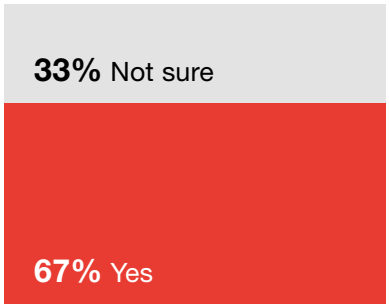
Less than half of the respondents confirm that their ICFR risk assessments have been aligned or integrated with other enterprise risk management processes. A similar proportion states that they have aligned their fraud risk management with their compliance risk management.

Most respondents would benefit from a more integrated and holistic approach to risk management, ensuring that all significant risks are identified and consistently managed throughout the business.

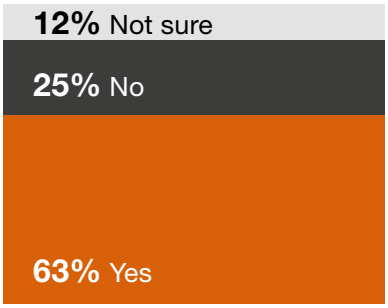
Fraud risks

Most respondents seem to be aware of the critical role ICFR plays when managing fraud risk. Two thirds say that they have a good understanding of the types of fraud and fraudulent behavior that could have an impact on their financial reporting...

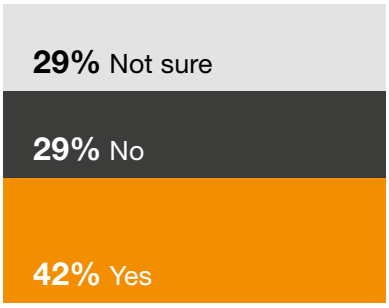
The company understands the types of fraud and fraudulent behavior that could impact the financial reporting



The company has defined which fraud risks that are most relevant to ICFR in terms of likelihood and potential impact



Fraud risk assessments are aligned with the company's compliance assessment



...while close to two thirds have defined the fraud risks they find most relevant to ICFR in terms of likelihood and potential impact.

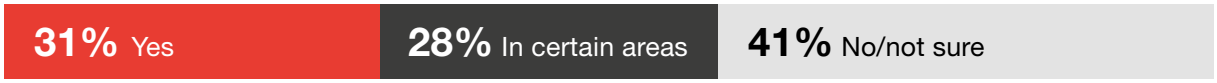
However, less than half of the respondents states that their fraud risk assessments are aligned with the company's compliance risk assessment. Fraud risk management is most efficient when integrated in the ICFR, compliance, and business operation functions. This is because different functions play different roles in the prevention of fraud. The use of GRC systems and more digital tools can facilitate the integration of ICFR activities and fraud management, making them more integrated in the business activities and way of working.

Scoping

The use of scoping to build a focused and cost efficient ICFR framework continues to be an area of improvement for most respondents.

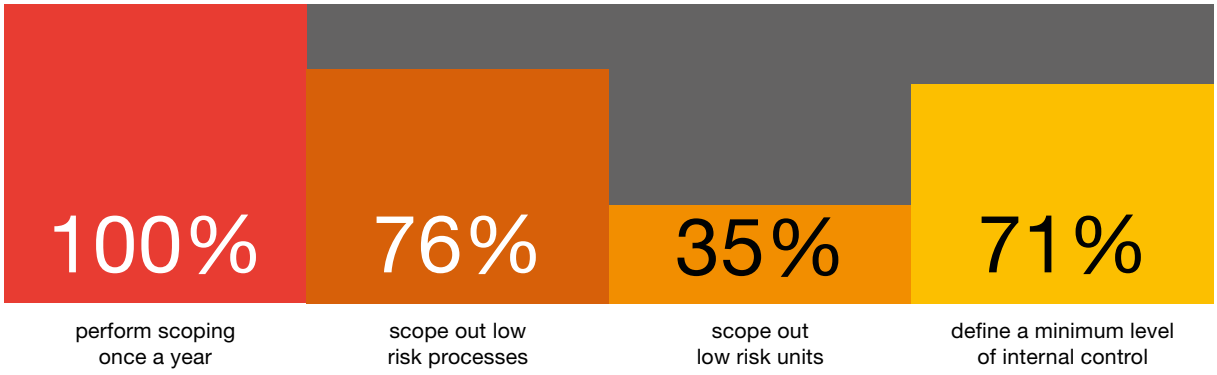
Risk-based scoping is essential for an effective and efficient ICFR framework. By scoping, we refer to deciding which processes, business entities and financial statement line items to include in the ICFR framework and to which extent. This is done by assessing materiality to the financial statement and the overall risk of material misstatements occuring.

The company has a process for scoping (e.g. of business units and processes) to identify to which extent and level the ICFR framework is applied



All participants performing scoping as part of their ICFR framework share that scoping is done once a year. In 2016 only 75 percent performed scoping on an annual basis, and the remainder every 2-3 years. Considering how businesses are constantly required to adapt to more rapidly changing environments and expectations, we consider this to be a healthy development.

How is scoping employed in your company?



According to our survey, companies performing scoping scope out low risk processes and low risk entities, leading to more efficient and focused internal control. However, it is more common to scope out processes than entities. Over two thirds of these companies have defined a minimum level of internal control all units must comply with, regardless of size and risk. This is in accordance with our general recommendation. For most companies, an effective and cost-efficient approach involves defining a standard set of controls, with which all in-scope entities must comply, but which may be tailored to local needs and risks where necessary.

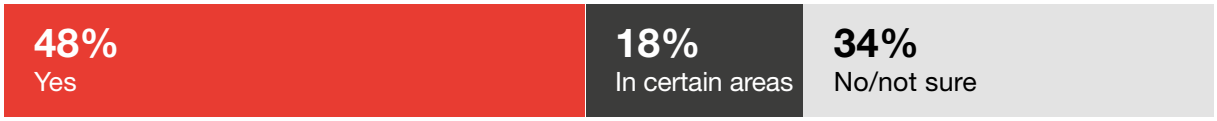
Control design

Control design maturity has improved slightly, indicating that companies are increasingly focusing on formalising their controls.

Less than half of the respondents have a complete control design. More than a third share that they do not know or have not defined and documented their ICFR control design. This is a significant increase compared to the 2016 survey, with only 12 percent stating the same. This increase is mostly due to a number of new respondents having less mature control frameworks.

Good practice is that internal control is an integrated part of business as usual and everyday routines. In leading companies internal control is designed to mitigate defined risks in an efficient manner and in alignment with the underlying business processes.

The company has built a complete set of controls which in total addresses the most critical risks of financial statement misstatements



Focusing on the companies with defined and formally documented ICFR control design, most companies report that they have built a complete set of controls that in total addresses the most critical risks of financial statement misstatements.

Types of controls used by the companies:

79%	Process level controls	66%	Entity level controls
72%	Analytical controls	10%	Roboticised controls
72%	IT general controls	7%	Other

Our recommendation is to continuously update internal control frameworks. Up-to-date systems ensures relevant content and keeps the framework top of mind in the business. Furthermore, having a well-structured approach to maintain control design is highly recommended. According to our respondents the most common reasons for updating internal control systems were the following: Reports of weaknesses from the internal and/or external auditor, major changes in the company, identification of process and/or control failures during monitoring and/or testing.

Events that trigger update of the ICFR control design:

85%	Reported weaknesses from the internal and/or external auditor
78%	Process and/or control failures or inefficiencies identified during monitoring and/or testing
74%	Major changes in the company
70%	Improvement opportunities, such as automation of controls
70%	Identified errors in the financial statement
56%	Regulatory changes
52%	Changes in expectations from the Board of Directors/audit committee and/or executive management

Fraud controls

According to our results ICFR is a key component when managing fraud risk. More than two thirds of the respondents design internal control aiming to prevent and detect fraudulent behavior.

Efficient ICFR controls have multiple purposes. They prevent, detect and identify unintentional and intentional errors. Therefore, we recommend incorporating fraud controls into ICFR frameworks, systems and controls. A common challenge is aligning efforts and activities between those responsible for managing ICFR and those responsible for anti-fraud/ compliance. Consequences include increased strain on the organisation, duplicate efforts and heightened possibility of overlooked risks.

Internal controls are designed to prevent and detect fraudulent behavior

Governing documents

According to the survey there is an increasing trend of companies having a more centralised design for governing documents and controls. Large companies centralise their policy management across countries and entities in order to gain better control of compliance with laws, regulations and internal requirements. Furthermore, good practice includes standardising the control design across the group, moving away from a dual design combining standardised and tailored controls.

Do the policies encompass the whole group or do local policies exist?

- 57% Group policies
- 0% Local policies
- 43% Group and local policies

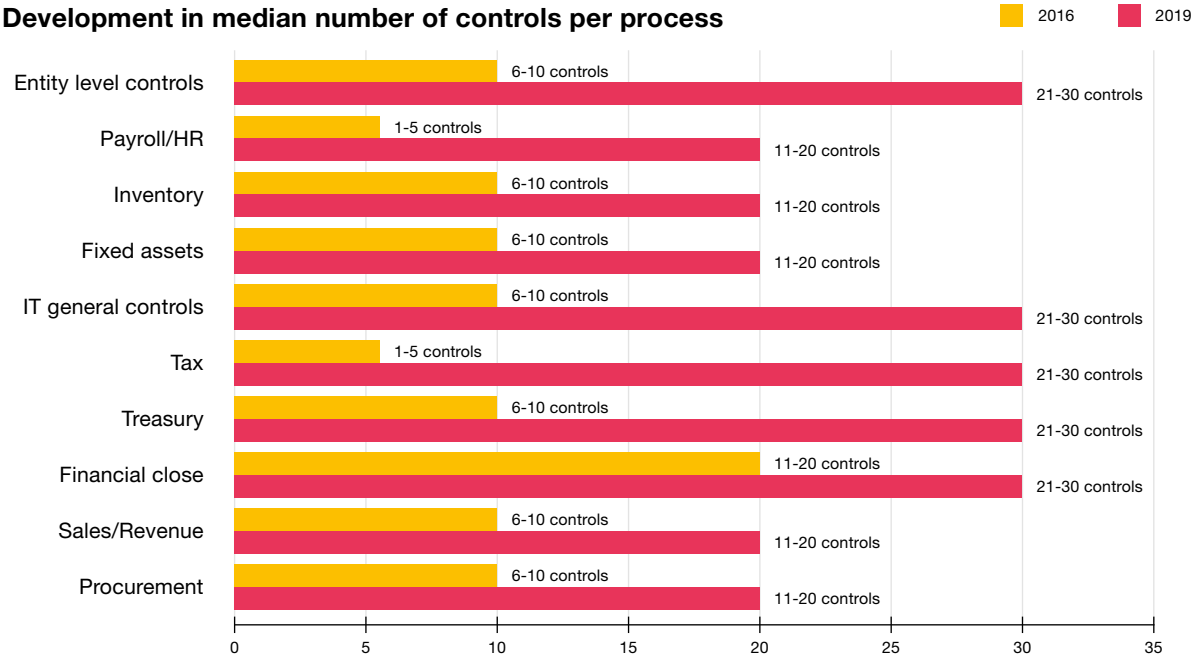
Are the controls standardised across the group or are there tailored controls at entity level?

- 37% Standardised controls across the group
- 33% Both standardised and tailord controls
- 19% Tailored controls at entity level
- 11% Not sure

Controls

Clients frequently ask us how many controls it is normal to have in place. The 2019 survey indicates a general increase in the number of key controls per process. The growth is mostly related to formalisation of entity level controls, IT general controls, financial close controls and treasury controls. Interestingly, only half of the companies differentiate between key and non-key controls, indicating that many could benefit from a tighter focus on the most critical risks.

Development in median number of controls per process



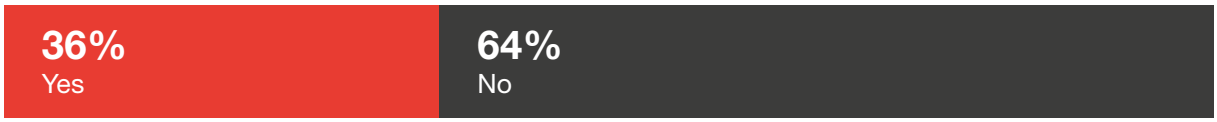
We asked: What situation or new and emerging risks trigger the need to design new controls?

The respondents replied: Entering new markets, buying new business or changes in operating model, new changes in accounting standards and the use of robotics.

Digital controls and tools

Using digital tools for a more efficient and effective ICFR framework is still not a widespread practice. One third of the respondents use digital tools to support their ICFR activities. Data analytics is the preferred digital tool and there is limited use of RPA and process mining to streamline processes and automate controls and monitoring. The most common reasons for using data analytics and process mining are to conduct detective controls and to monitor transaction flows.

The company applies digital tools to support the ICFR process



Digital tools used by the companies to support ICFR activities

89%	Data Analytics	11%	Robotic Process/Automation (RPA)
22%	Process Mining/Process Analytics	11%	Other

Business processes for which data analytics is applied

75%	Procurement	25%	Inventory
63%	Sales/revenue	13%	Fixed assets and investments
63%	Financial close and reporting	13%	Treasury
25%	HR/payroll		

Standardised processes with a high number of transactions are well suited for applying data analytics. Hence, it is not a surprise that our respondents most commonly apply data analytics to processes within procurement and sales. Furthermore, we observe a high use of data analytics within processes related to financial close and reporting. Typically, data analytics is then applied in the reconciliation process and the elimination of intercompany transactions.

Despite the current limited use of digital tools, the majority of the respondents state that the company plans to increase the use of RPA, data analytics and/or process mining going forward. Digital tools are relevant within several areas of the internal control framework providing support and enhancing the level of assurance. Nevertheless, it is key to have a good understanding of which tools are suitable for which purposes ensuring an efficient and desired outcome.

Data analytics

Use of data analytics is commonly integrated in the control design. There are two purposes for doing this:

- providing assurance for the financial statement by detecting anomalies or deviations for further investigation and follow-up
- providing insights and information for decision making

Furthermore, data analytics can be used for monitoring purposes, e.g. identifying whether controls are working as intended and effectively mitigating risks.

Process mining

Process mining is useful when identifying incidents failing to follow the standard process flow, including controls. Making these observations enable further inspection and remediation of failures and root causes. Process mining is a useful tool for tracking:

- mapping the as-is process
- reviewing risks, controls, bottlenecks, rework, segregation of duties etc.
- monitoring the flow of transactions

Robotic process automation

Robotic process automation (RPA) can efficiently reduce inherent risk in transaction processes by automating manual activities. RPA is particularly applicable where full automation using e.g. the ERP system is too complicated or expensive. Additionally, RPA can automate control testing by e.g. testing whether a control is performed or not. Applying artificial intelligence (see below) and RPA together can in addition enable interpretation of control documentation and testing of control performance.

Artificial intelligence

Artificial intelligence (AI) is a tool for performing activities physically or digitally and interpreting and assessing data. E.g. detecting unusual transactions in the General Ledger and selecting transactions for further investigation. Together with PRA, AI allows for more efficient testing and can be built into the control design for automated controls.

IT general controls - ITGCs

ITGCs are controls over access to programs and data, changes to programs and data, computer operations and program development. ITGCs include controls over transaction processes relying on IT systems or other digital tools (eg. RPA). As it is less common and not recommended to only have manual controls, ITGCs are of increasing importance to ICFR. Well-functioning ITGCs are critical for ensuring effectiveness of controls relying on systems and system generated reports.

Digitalisation and automation of business processes and internal controls increase the reliance on IT and ITGCs. In the 2016 benchmark 38 percent of the respondents had not taken, or were not aware of having taken, the reliance of ITGCs into consideration when designing the process level controls. In this year's survey this percentage has dropped significantly, indicating that companies are recognising the interdependencies between ITGCs and process level controls and are taking action accordingly.

Dependence in ITGC is taken into consideration in the design of process level controls

32%	56%	12%
Yes	To a certain extent	Not sure

Access management controls and system-implemented segregation of duties are critical ITGCs. These controls are fundamental to any internal control framework and to mitigating the risk of fraud. This is widely recognised among the respondents. Almost all respondents have implemented system access controls and reconcile these with the company's authorisation matrix.

Security and segregation of duty risks are mitigated by system access controls **92%**

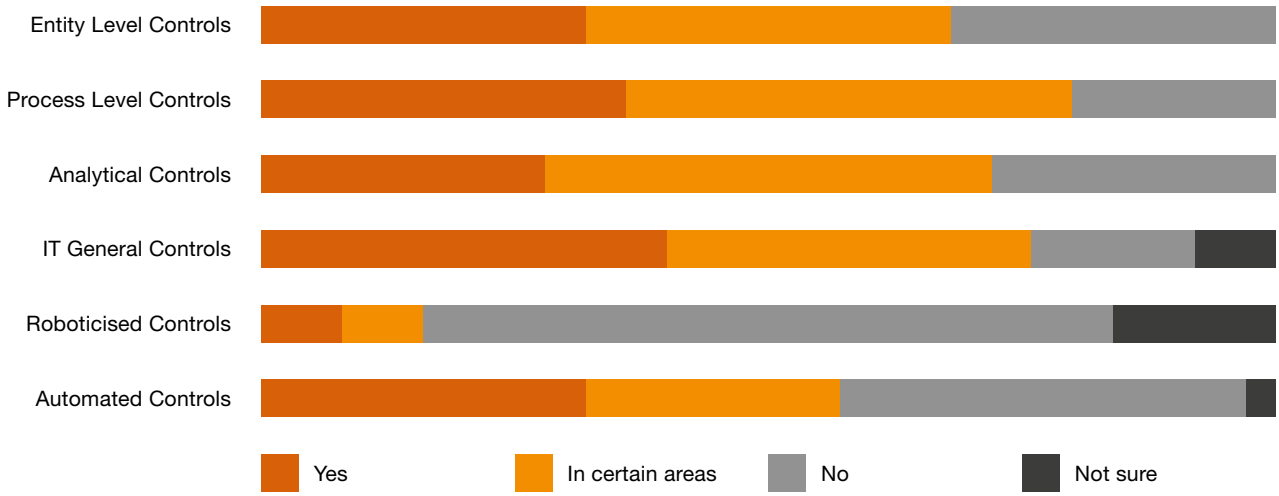
Monitoring

The survey shows that little has changed with regards to monitoring. Most respondents have some form of monitoring in place for entity level (policies), process level, analytical and IT general controls (ITGC). Interestingly, we see that only approximately half of the respondents conduct monitoring of their automated controls.

There has been little change since 2016 in our survey results related to monitoring. Approximately one fifth to a third of the respondents report that they do not conduct any type of monitoring. According to our results it is common to have limited monitoring in place.

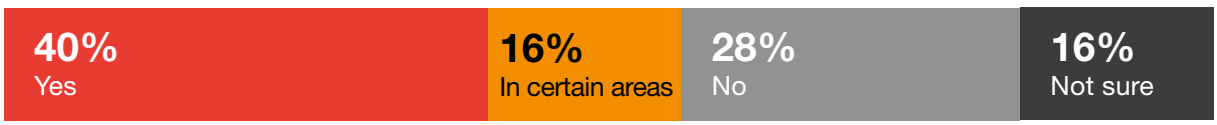
Monitoring is a key element of ICFR, ensuring that the control framework is implemented and that it is functioning as intended. Furthermore, monitoring is an efficient method to identify needs for improvements and learning opportunities.

Are there processes in place to monitor effectiveness of the following control types?



Identifying the most critical controls of the ICFR system is important to ensure efficient use of resources. Half of the respondents distinguish between key and non-key controls, indicating that many could improve their cost effectiveness by focusing their ICFR activities on key risks and controls. The most mature respondents use scoping to consciously prioritise their monitoring activities, monitoring low risk entities and processes less rigorously than areas with higher risk.

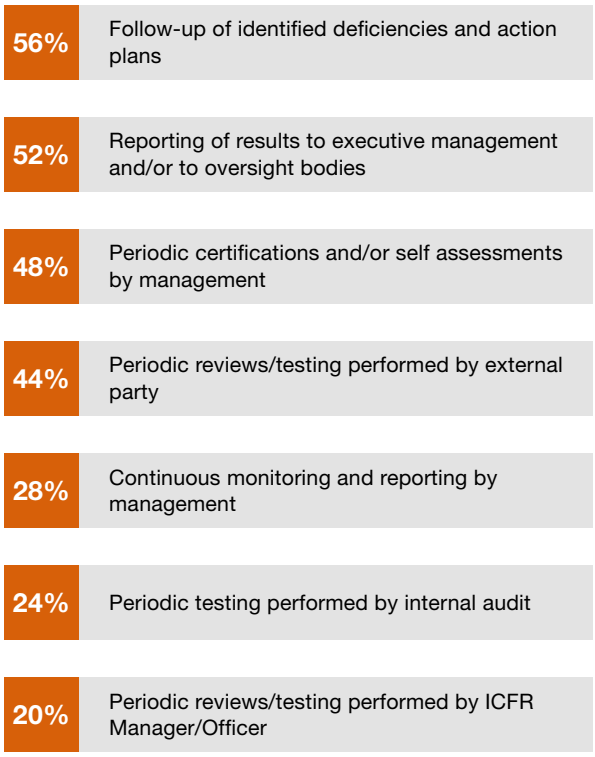
Do you distinguish between key controls and other controls on risk assessments and/or for monitoring/testing purposes?



Monitoring and/or testing of controls performance is performed less rigorously for:

There are different ways to perform monitoring. The figure below illustrates how the survey respondents perform their monitoring. Self-assessments and testing performed by external parties are the most common ways to perform monitoring. These two methods provide the lowest and highest level of assurance. Less than a third of the respondents perform continuous monitoring.

The monitoring system includes these following elements:



Fraud

Fraud is a continuous threat, which is becoming ever more complex and costly to manage. A right mix of preventive and detective anti-fraud controls can lower the risk and vulnerability to fraud significantly.

According to PwC's 2018 Global Economic Crime and Fraud Survey, close to half of global corporations report experiencing economic crime during the past two years. The most common types of fraud being asset misappropriation, cybercrime and fraud committed by consumers. Almost two thirds of the respondents share their losses resulting from fraud reaching up to $US1 million, while 16 percent share having experienced losses between $US1 million and $US50 million.

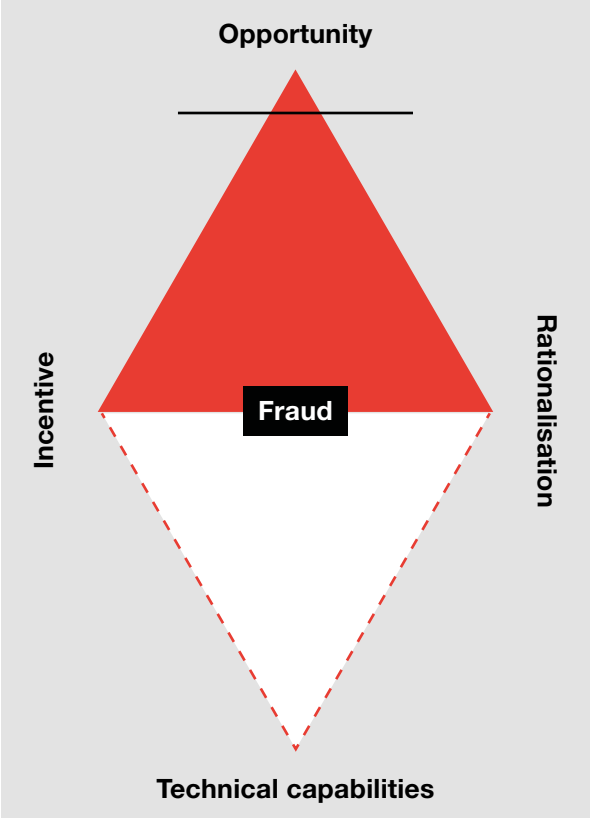
Fraud is defined as an intentional act by those charged with governance, employees, or third parties, involving the use of deception to obtain an unjust or illegal advantage. In a rapidly changing environment, fraud risks are emerging and changing both externally and internally. Regulatory regimes are getting more robust, the digitally enabled world allows for fraud to be more advanced and public expectations around transparency and accountability are increasing. To become fully aware of the fraud risks companies are facing can therefore be a challenging task.

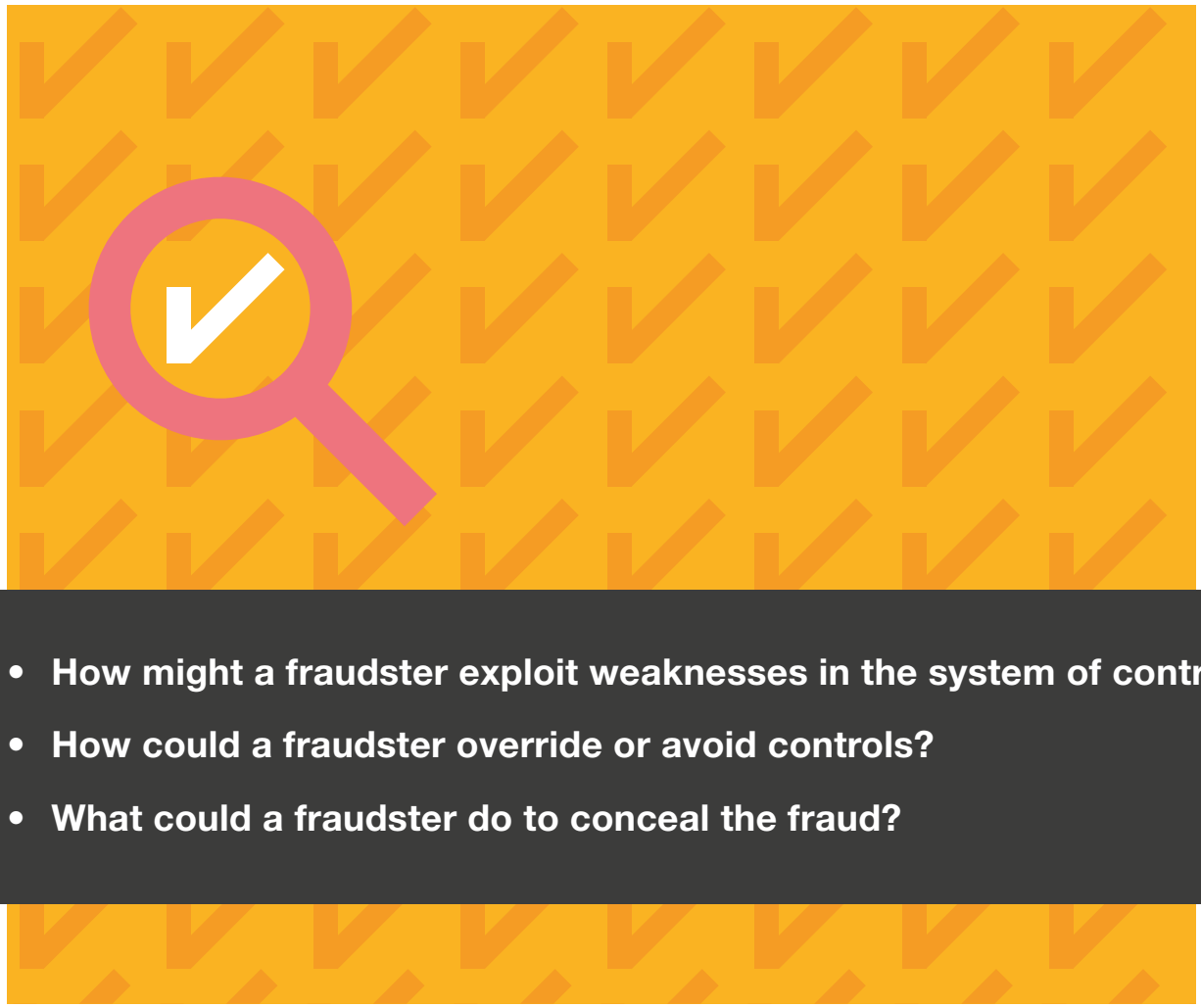
Mitigating fraud risk through internal control

According to the fraud triangle theory, there are three factors that have to be present for fraud to occur: Incentive, Rationalisation and Opportunity. The triangle has in recent times been extended to a diamond with a fourth factor, Technical Capabilities.

No system of internal controls can fully eliminate all risks of fraud, but well-designed and effective internal controls can reduce the opportunities for committing fraud and deter the average fraudster by increasing the perception of detection. A right mix of preventive and detective controls can therefore lower the risk and vulnerability to fraud significantly.

The main distinguishing factor between a fraud and an error is whether the underlying act is intentional or unintentional. Due to this fundamental difference it is necessary to assess fraud risks differently and anticipate the behavior of a potential fraud perpetrator.





- **How might a fraudster exploit weaknesses in the system of controls?**
- **How could a fraudster override or avoid controls?**
- **What could a fraudster do to conceal the fraud?**

Examples of fraud mitigating ICFR controls and activities

Control environment:	Process controls:	ITGCs:
• Purchasing policy • Code of Conduct • Delegation of Authority policy	• Timely reconciliation of cash balance • Review and authorisation of reimbursements from expenses • Review of estimates and discretionary records • Salary calculations inc. bonus and payment approval • Review of manual recordings • Vendor registration control • Contract approvals	• System access controls • Segregation of duties

Digitalisation

Using technology to digitise activities can lead to higher quality at lower cost by obtaining greater assurance over control effectiveness, performing analytically based risk assessments and decision making and by streamlining and automating processes.

Digital tools are becoming more available, but are companies utilising them?

According to PwC's 23rd Global CEO Survey the speed of technological change is still one of the top concerns among CEOs. Risk professionals have an obligation to help their organisations ensuring effective processes and controls. Today, performing ICFR manually or having inefficient, resource-intense processes is common in many organisations. This may lead to a reducing employee engagement over time. As the Norwegian market is still relatively immature when it comes to digitalisation, we have to look abroad to predict future trends and possibilities. As the ICFR survey confirms, Norwegian companies are to a limited extent utilising technology to improve efficiency and effectiveness of their ICFR frameworks.

Evolvers
Advanced in their technology adoption

Followers
Taking note and following Evolvers technology adaption, but at a slower pace

Observers
Have basic or no technology use

Leading companies, defined as evolvers, are advanced in their adoption of technology by means of usage and utilisation of collaboration tools, analytical and monitoring tools and by means of experimenting with predictive risk indicators. They invest in their employees creating a tech savvy culture.

Advanced technology and collaboration tools include GRC systems.GRC systems could help organisations systemise and automate risk and controls processes, by making use of data from transactional systems / ERP systems into a standard tool with predefined controls. GRC systems and re-usable data analytics solutions could enable continuous monitoring within the business processes, which is useful both for monitoring and risk assessment purposes.

Taking advantage of digital tools

Technology is evolving rapidly and has at the same time become more accessible and user

friendly. The individual employee can to a higher degree develop and use data analysis and robotisation to perform internal control activities. Leading companies use GRC systems for monitoring and managing ICFR, robotisation for automation of work processes, and data analysis to prevent errors from occurring (proactive controls) and to provide more thorough and detailed analyses (reactive controls).

An immature internal control system may not be ready for the use of new technology, but if the company has an ambition to increase their maturity level, technology can enhance speed and efficiency to achieve the desired level.

Benefits of automation programs depend on whether there are scalable mechanisms and standardised, streamlined and consolidated processes. Furthermore, it is key to ensure the digital tools are not stand alone. Being integrated into the system allows them to be a part of the core business processes and enables a new way of working. Integration allows companies to further develop the capability to automate new processes and continuously improve. Moreover, it is important to ensure that the organisation has the capacity and capability to implement automation programs into the overall internal controls framework in a sustainable way.

Automation of control testing

Automation of control testing is one way to improve productivity, quality, consistency and insights through technology enablement. We recommend starting with an initial assessment of all workstreams ensuring they are standardised and streamlined, and that all internal controls are identified. Then performing an opportunity assessment measuring the suitability and complexity of each control. Controls with high suitability and low complexity are the best fit for control testing automation (e.g. highly digital controls and amount of current manual effort involved). Based on the outcome of the opportunity assessment, controls are grouped together into key automation themes. The automation themes can then be prioritised for piloting and the development of supporting business cases.

Productivity

- Filter out - focus on less
- Reduce volume of manual testing activity
- Release capacity to focus on the judgemental control testing activities

Consistency

- Removal of human error and bias
- Automation e.g. evidence capture and storage
- Scalable and easily replicable

Quality

- Greater precision on the anomalies
- Improved quality of evidence capture

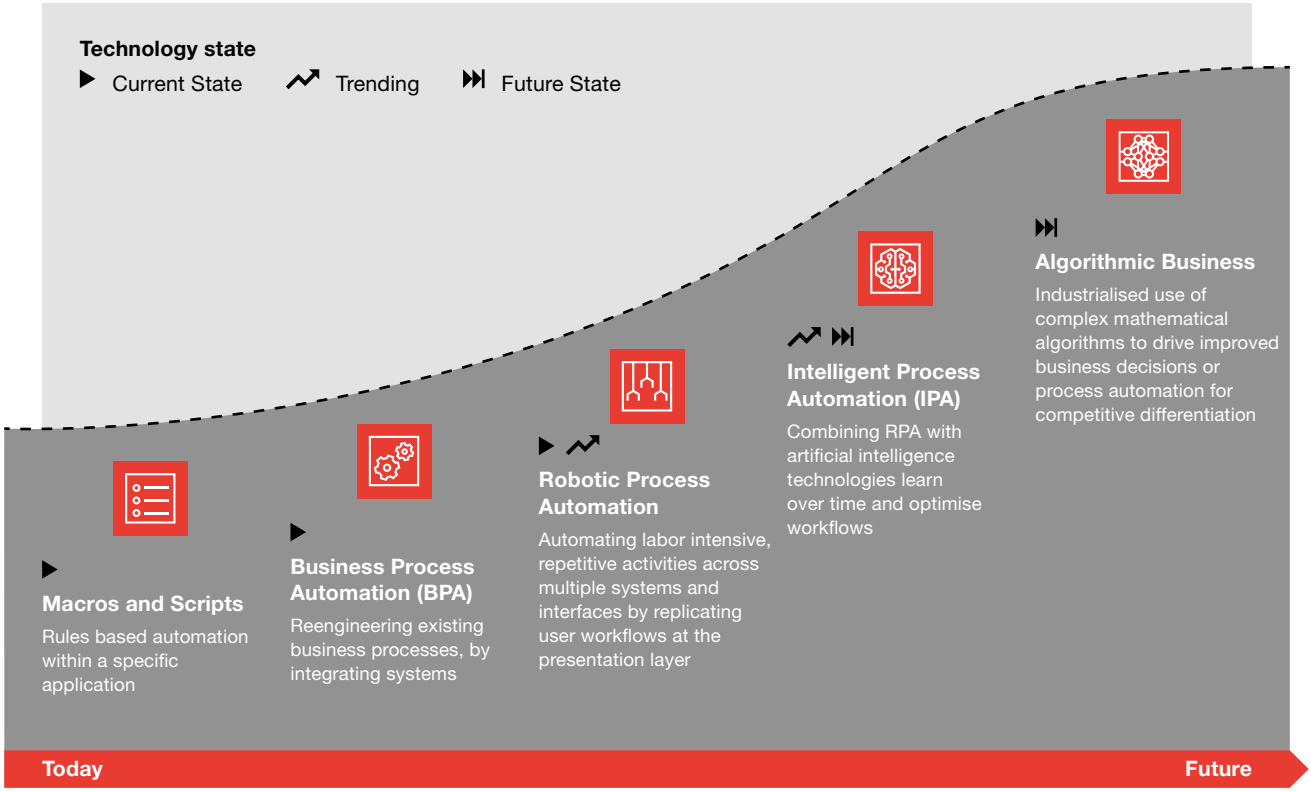
Insight

- Deeper insights through 100% populations
- Increased time to challenge outcomes and perform root cause analysis

Robotic Process Automation

Process automation is a leading factor in driving productive growth in organisations, with Robotic Process Automation (RPA) and Intelligent Process Automation (IPA) emerging as next evolution steps. The figure below illustrates a forward-looking perspective on the evolution of automation capabilities over time. The continuum extends from common technologies in use today to potential replacement technologies to be adopted in the future.

The process automation landscape is rapidly changing towards Intelligent Process Automation



The use of RPA undoubtedly has several benefits to organisations. Beyond cost saving it has become critical for competitiveness due to its efficiency advantages such as response time, scalability and precision. Keep in mind that it is important to have a standardised process before automating controls, as automation of non-standardised processes would introduce errors in the execution of the controls.

The RPA software follows a rule-based logic to perform manual, time-consuming office tasks more efficiently. The RPA operates on top of existing software, potentially across different systems, mimicking interactions of users. The application can aggregate data from multiple sources and develop an integrated single view for all business processes, thereby reducing the requirement of human intervention in complex business processes. RPA may be used with any application, such as an ERP system, databases, MS suite, Business Warehouses or other RPA is perfect for automating highly manual processes that are streamlined and require a limited amount of judgement.

As an example of usage of RPA within automatic control testing, we have seen efficient RPA implementation within testing of IT general controls. Testing of certain controls within access to programs and data often requires manual trailing of tickets in Case Management systems, for instance to verify whether access to an ERP system has been appropriately approved before it is provisioned to the user. A robot could easily fetch the time stamps of the approval and user provisioning from the case management and the ERP systems, compile it into a worksheet, and draw the conclusion whether approval was obtained before user provisioning. Furthermore, the robot could add the name and title of the approver. The only manual task is for a person to verify the appropriateness of the approver. Hence, while a person would normally only be able to manage testing of relatively small samples, for the robot there is virtually no limitation in terms of sample size.

RPA can also be used to automatically initiate and execute activities based on pre-configured rules, to compile data from different sources through data scraping, to perform data entry and data transfers across different systems, to identify specific fields and words in images through optical character recognition and to review/identify data in long audit logs and audit trails.

Examples where RPA can be used is for automatic control testing:

Rules-based triggers: Automatically initiate and execute activities based on pre-configured rules

Data scraping: Capture content and simulation of key strokes and mouse clicks from various systems including webpages and desktop applications

Data entry: Automated data entry and transfer across different systems

Document image capture: Optical Character Recognition functionality with the ability to identify specific fields and words

Audit trail and metrics: Log and review by key stroke audit trail of a robot

Implications for the control environment?

The RPA does not exercise judgement, nor can it detect errors or changes to source systems. The robot only acts upon pre-defined rules. It is important that this is taken into consideration when deciding where to apply RPA.

It is also crucial to ensure that the control environment reflects the use of RPA. This implies that organisations need to include RPA as part of their IT Governance, update process descriptions and routines to follow up on data quality and deficiencies, and perform system validation checks among other measures. In addition, ownership of RPA is a possible pitfall. An important consideration is whether RPA should be owned by the IT department or by the process owner.

Data analytics

Data analytics is the science of analysing raw data in order to make conclusions about that information. Many of the techniques and processes of data analytics have been automated into mechanical processes and algorithms that work over raw data. Data analytics techniques can reveal trends and metrics that would otherwise be lost in the mass of information. This information can be used to perform controls, monitor control performance, perform risk assessments, planning and scoping, reporting all areas within the ICFR Annual wheel. Due to a substantial increase in processing power and more advanced ERP and Business Intelligence solutions in the marketplace, the potential to take advantage of analytical controls is substantial.

There are several different data sources that can be used to optimise processes and to increase the overall efficiency of control, business or system.

1 Externally reported data and management information (MI)

Data and information used as a basis for critical decision making, fincancial statements, regulatory reports etc.

2 Master/standing data

Data and information used as a basis for critical decision making, fincancial statements, regulatory reports etc.

3 Process and transactional data

E.g. which illuminates how processes and controls are operating in practice.

4 Access data

E.g. data which highlights who is doing what activities and in what ways.

5 Configuration and interface data

Data which shows how systems are architected and how data flows and is reconciled between systems.

6 Control Performance

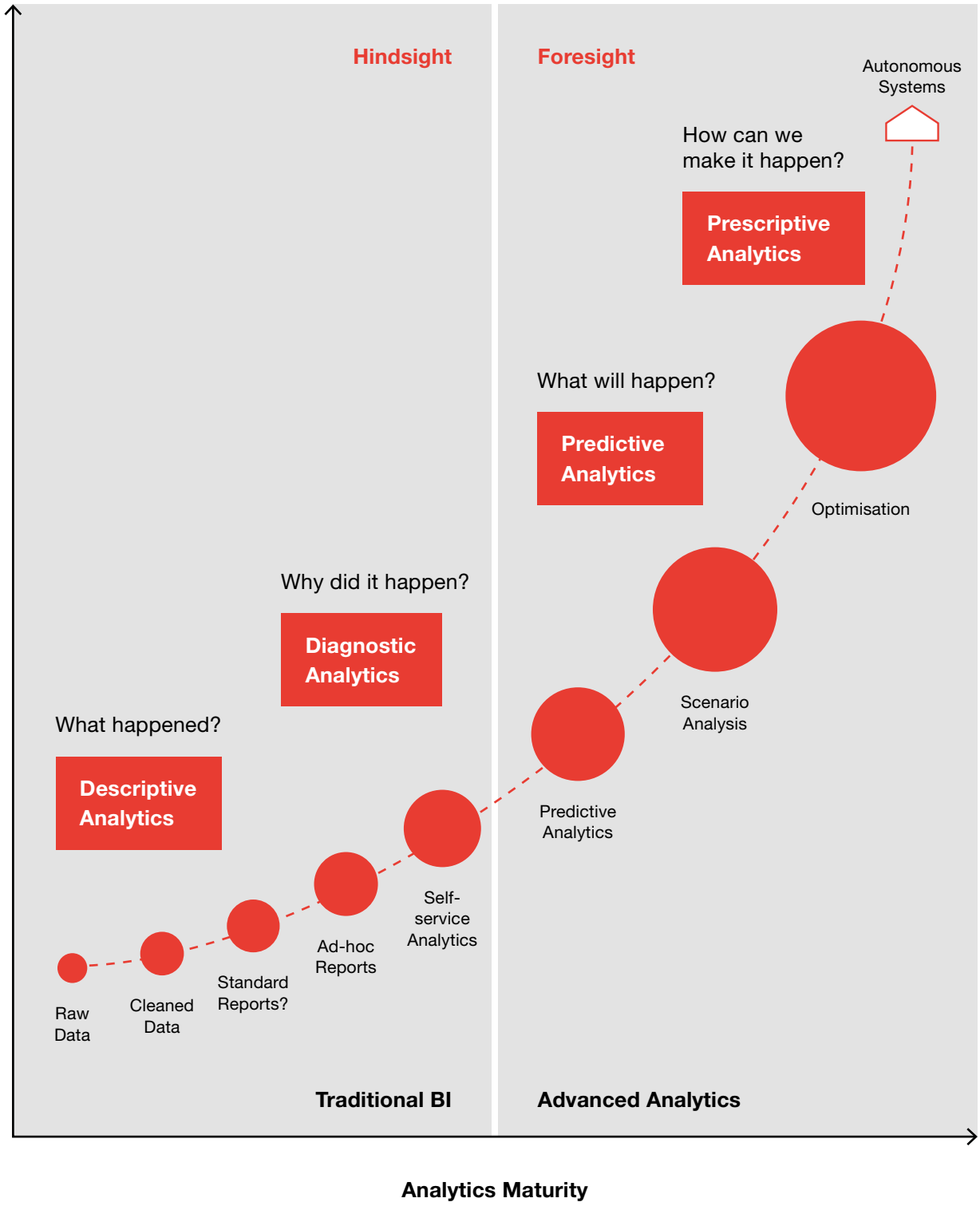
E.g. data relating to historical performance by operating division and process domain.

Financial Data | **Operational Data** | **People Data**

Structured Data

Unstructured Data

Areas that are right for data analytics are areas where you get a high level of insight and impact that are linked to the organisation's strategy and objectives. It is also easier to implement data analytics solutions within processes that are relatively easy to understand, such as for example the Purchase-to-Pay process. To build and mature in this area companies are likely to start with reactive and detective analyses before they are moving towards predictive analyses that are giving more value to the organisation and effects the inherent risk assessment.



Types of data analytics

Data analytics is broken down into four basic types:

1 Descriptive analytics

Descriptive analytics describes what has happened over a given period of time, using observation, walkthrough, hard copy documents. Analytics are sample based and statistical or judgemental. Has the salary cost increased relative to the number of employees? Are sales stronger then expected based on approved sale contracts? There is a lot of potential to implement descriptive analyses adding value to the organisation. While less complex than the other types of data analyses, descriptive analyses often provide valuable insight into controls and business processes.

2 Diagnostic analytics

Diagnostic analytics focuses more on why something happened. This involves more diverse data inputs and a bit of hypothesising. For example, analytical tools such as ACL and AIDA are run on a one off basis addressing a specific question. Automated and standardised scripts are used for specific reviews and specialist staff support extract and analysis of data. Did the weather affect sales? Did that latest marketing campaign impact sales?

3 Predictive analytics

Predictive analytics revolve around what is likely going to happen in the near term. Extensive data structures are dissected and normalised. Normality is learned and relearned on demand using stylised scenarios including introduction of false positives and incorporation of new scenarios and variables as required to train the tool. Exceptions in patterns and risks are exposed so that proactive and predictive actions can be taken. What happened to sales the last time we had a hot summer? How many weather models predict a hot summer this year?

4 Prescriptive analytics

Prescriptive analytics suggest a course of action, given a particular outcome. For example, the model could prescribe that if the likelihood of a hot summer is measured as above 58% based on an average of five weather models, we should add an extra shift and rent an additional production unit and storage.

Process Intelligence / Process Mining

Process Intelligence is based on the technology of process mining. When employees perform activities in one of the company's applications, the activities performed, series of events, and user data are logged.

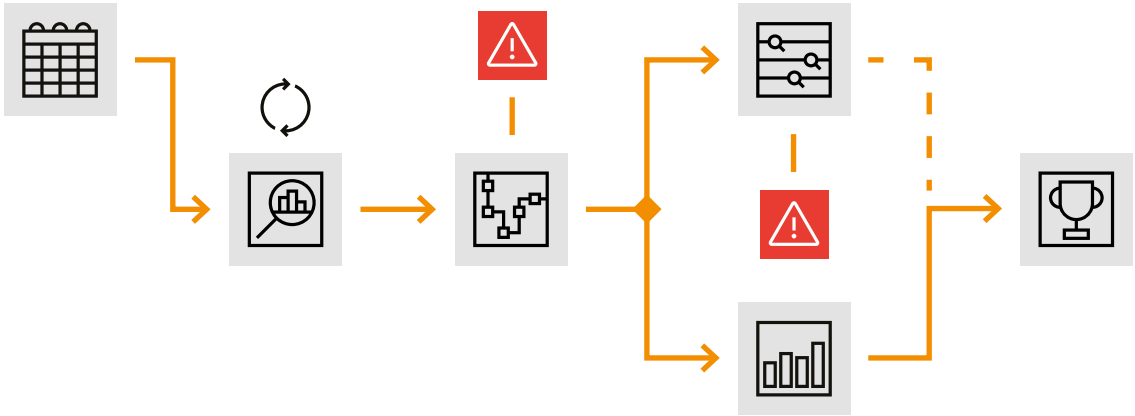
Process Intelligence tools can be used to visualise the event logs and life cycle of business processes. Regardless of the business area there is often a gap between how processes are intended to be and what they are in reality.

The most common processes to analyse using process mining tools are Purchase-to-Pay and Order-to-Cash. This technology enables organisations to analyse 100 percent of all transactions within the process, exposing bottlenecks, compliance issues, segregation of duties, level of automation, cycle times, etc.

The tool can be used both as a mapping tool to get an overview of the actual process and as a monitoring control, ensuring all transactions follow the intended work flow and internal controls.

Expectation:

Reality:



Traditionally, monitoring of controls has been performed manually, often with a sample that is tested. With increasing digitisation more process data are being registered, which also provides the opportunity to use analytical tools to perform monitoring of not only a sample, but the complete population.

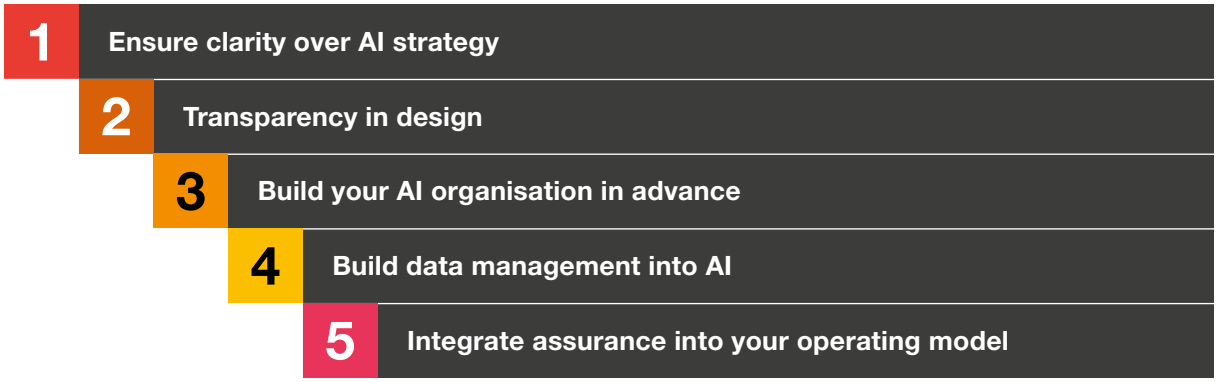
Artificial Intelligence

Artificial Intelligence (AI) is defined as the theory and development of computer systems that perform tasks that normally require human intelligence. It is a tool which can perform activities physically or digitally, based on an interpretation and assessment of structured or unstructured data. Some AI systems can also adapt through analyses and continuous learning from previous actions and results. As an example, PwC has developed the tool GL.ai for anomaly detection in the General Ledger. GL.ai is a bot that detects anomalies in a company's general ledger through the combination of advanced AI technology and the knowledge and experience of auditors.

If a company wants to implement AI it needs to consider the risks associated in order to realise their benefits and ensure it is used responsibly. As an example, AI is bias-prone, meaning it is difficult to explain/ perceived as 'black box'. This can make it difficult to understand or accept decisions, especially if there is an implication of bias. Furthermore, AI has no sense of morality or ethical considerations and is not aware of the impact to workers and society.

The adoption of AI demands a new way of thinking about technology, business development and strategic execution. Assurance over AI requires business-wide evaluation to gauge outcomes, identify emerging risks and look out for opportunities.

The following steps must be considered in order to adopt AI in a business context:

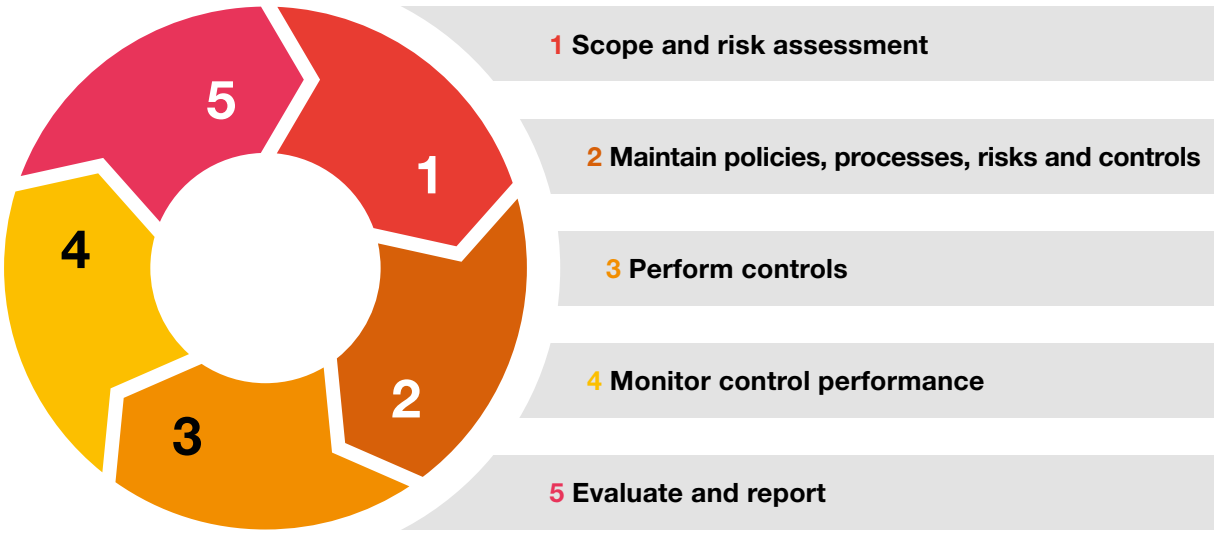


Conclusion

The aim of this survey is to provide useful insights into ICFR practices. The conclusion from 2016 remains in 2019 – companies would benefit from investing in a more effective and efficient internal control system. In addition, our report has taken a deeper dive into fraud and the possible uses of technology. These are areas of increasing focus going forward and we hope that by sharing good practices we can have provided you with some inspiration on how you can be ahead of the curve.

When establishing or improving your company's ICFR framework, we recommend you to:

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.
6. **Align your ICFR and Compliance frameworks,** utilising your ICFR control design to contribute to an effective and holistic management of fraud risk.
7. **Use technology** to reduce manual tasks, increase productivity and precision and facilitate your ICFR work.
8. To **continuously improve** and maintain the ICFR framework, establish an annual process that should be managed by a designated role or function. Monitoring, evaluation and reporting can be used to ensure continuous learning and improvement of the ICFR process and framework.



Contact

Aase Lindahl
Partner
+ 47 95 26 01 35
aase.lindahl@pwc.com

Tanja Sæland
Director
+ 47 95 26 06 30
tanja.saeland@pwc.com