

The impact of digital technologies on internal audit

On 21–22 November 2016, members of the European Audit Committee Leadership Network (EACLN) met in Berlin. In one session, they were joined by Jonathan Blackmore, Senior Partner and EMEIA advisory risk leader at EY, and Hans Winters, Chief Audit Officer at Siemens, for a discussion about the ways that technological innovation is changing the internal audit function. For biographies of Mr Blackmore and Mr Winters, see Appendix 1, on page 10. For a full list of participants, see Appendix 2, on page 11.

Executive summary

In conversations before and during the meeting, members and guests discussed three main themes regarding the impact of digital technologies on internal audit:¹

- **Business transformation complicates internal control and risk management** (*page 2*)

Digital advances in areas such as mobile and cloud computing, automation and artificial intelligence are transforming the way companies do business, creating a new landscape of internal controls and risk management. Large-scale digital platforms are changing business processes from end to end, and the boundaries with customers and business partners are becoming blurred. These developments are shifting control points across organizations and demanding more proactive approaches from internal auditors.

- **Digital technologies both strengthen and challenge internal audit** (*page 3*)

Digital technologies such as robotic process automation and advanced analytics are also helping internal audit improve its performance. They allow internal auditors to test an entire population rather than just a sample of transactions, and they can lead to significant cost savings by automating rote tasks. They also allow the internal audit staff to focus on the tasks that require human judgment, deepening insight and enabling internal auditors to provide better advice on business processes as well as improved auditing. Achieving these benefits, however, will require new skills and more flexible approaches to audit planning.

- **Audit chairs are concerned about both innovation and assurance** (*page 6*)

Audit chairs want the internal audit function at their companies to understand and utilize new technologies and techniques. They want chief audit executives (CAEs) who understand the tools and resources required and how these should be integrated into the function and the broader organization. But audit chairs also want to maintain the integrity of assurance, which could be jeopardized as new technologies cause the three “lines of defense” in assurance – line management, compliance and risk management and internal audit – to encroach on each others’ responsibilities. Collaboration among these lines of defense is important, the guests said, but the independence and objectivity of internal audit must be maintained.

For a list of discussion questions for audit committees, see Appendix 3, on page 12.

¹ *ViewPoints* reflects the network’s use of a modified version of the Chatham House Rule whereby comments are not attributed to individuals or corporations. Quotations in italics are drawn directly from conversations with network members, guests and other experts in connection with the meeting.

Business transformation complicates internal control and risk management

Emerging digital technologies are disrupting and transforming enterprises in all sectors and at all levels. This combination of technological and market innovation is fundamentally different from previous industry transformations, as members of the EACLN and the North American Audit Committee Leadership Network (ACLN) discussed at the Audit Committee Leadership Summit in Zurich, highlighting the speed and scale of transformation, the interaction of technologies resulting in “combinatorial innovation,” and changing customer expectations and relationships.² Companies are harnessing new technologies – mobile and cloud computing, the internet of things, automation and artificial intelligence – to replace legacy systems with digital platforms and interact with customers and suppliers in new ways, in some cases even changing the fundamental nature of their business.

At the meeting in Berlin, Mr Winters offered an example from his company, Siemens: *“The transformation for us could be from industrial engineering to digital services. For example, today we’re selling trains. What will the future bring? It could be focused on the mobility of consumers, not the hard product – i.e., trains. With data, we could offer that information, and it would give us the capability to go from train seller to mobility organization.”* He added that boards *“have to understand the new business models to understand risks.”*

These transformations create new challenges for the internal audit team and its task of assessing internal controls and risk management more generally. Network members, guests and other subject matter experts discussed two key developments that will test internal audit:

- **Digital transformation entails new systems and processes.** Stephen Gregory, retired partner and current senior advisor to EY’s EMEIA Financial Services Risk practice, noted in a pre-meeting conversation, *“Big digital platforms will change the way auditing is done. The disruption of moving to new digital systems is huge ... How do you audit that change? How do you audit end-to-end digital processes? You will have to audit something totally different in nature.”* An EACLN member brought up the key issue of controls: *“Audit procedures have changed. Digital processes are overwriting old processes. That has implications for how controls are set up.”* Mr Gregory pointed to a data integrity problem that may emerge when new business processes make use of older data: *“The difficulty is that the data captured years ago is often incomplete, which is now becoming an issue. Now this data might influence things like credit ratings, etcetera. Yet the data captured in the past may not have been as diligently compiled.”*

Some of the necessary controls may not even be in place yet. One member explained, *“Companies are having problems migrating legacy systems to new systems. There is exciting stuff out there, but the practical implications are [worrisome] – I have yet to see internal controls being developed. For both internal financial controls and internal operational controls, there are huge gaps in all of the companies that I work with. We have a long way to go on this.”* At the meeting, a participant from EY made a similar point: *“There is a lack of understanding of end-to-end processes. Control has changed, and some organizations are going back to the basics because they feel that there aren’t controls in place.”*

- **Boundaries with customers and business partners are blurring.** Another element of the challenge is the erosion of company borders. One member simply asked, *“Where are the walls between customers,*

² North American and European Audit Committee Leadership Networks, Digitalization, Disruptive Innovation and the Board, ViewPoints (Waltham, MA: Tapestry Networks, 2016).

vendors and the company?” Members recognized that it is difficult to create an effective control environment when a business process involves third parties in novel ways. Mr Blackmore explained, “The boundaries of organizations are becoming more blurred. There is a more seamless interface with customers. The worry can be a breach not just in your own organization but in the business partners’ organizations.” An EACLN member made a similar point: “There can be a lot of data residing with vendors. How do we control and monitor it? Do we have the right to monitor the potential loss from manipulation of that data? To what extent can we audit for exogenous risk?”

Mr Blackmore elaborated on how these developments are changing the internal control environment: *“As the business model changes, where things are controlled is changing. It used to be close to where [events occurred]. Now the control points may be elsewhere in the world, because where control actually sits is changing. We are moving more toward centralized arrangements, so to audit them is becoming more complex.”* In addition, a member noted that new metrics, such as key performance indicators, that may be especially useful for reporting on new types of businesses will also require changes in controls: *“You have to have a control environment around this information so that it’s accurate.”*

Mr Winters added that auditing will have to become more proactive: *“Machine decision making is going to become more integrated into processes. First, we are going to check that the algorithms are right. We will audit the controls at the beginning, not just at the end of the process.”* Mr Blackmore agreed: *“Robotics will be used to automate many auditing functions, but who audits the robot? Machine learning and decision making will force us to test algorithms and parameters thoroughly in the beginning and force a mind shift in how to do the testing.”*

Another consequence of digital transformation is the generation of large quantities of data, which can create additional challenges for internal auditors. Mr Blackmore said, *“The quality of the data is fundamental, and there is just going to be more and more of it. Think of the number of devices in the room today.”* Mr Winters explained that the increasingly complex systems required to handle this data is causing auditors to focus more deeply on how to protect it: *“One of the biggest threats to digitalization, whether in products or internal processes, is cybersecurity.”*

Digital technologies both strengthen and challenge internal audit

Some of the same technologies that are transforming businesses can also help internal auditors improve their performance, increasing the speed and accuracy of audit processes and enabling more insights about business operations and risks. To best take advantage of these benefits, however, internal audit will need to grow and change in certain ways, particularly in areas of staffing and audit planning. For brief descriptions of some technologies that can help the finance function and internal audit, see the tint box below.

Innovative technologies impacting the finance function and internal audit

Key technologies are changing the game for the finance function and internal audit, each with major implications for advancing an organization's business and operations capabilities:

- **Robotic process automation (RPA).** RPA technology "operates as a virtual workforce controlled by the business operations teams ... It captures and interprets existing applications, manipulates data, triggers responses and communicates with other systems, [and] it can be applied to existing applications (without changing the current IT landscape)."³ Martin Weis, EY partner and robotic process automation leader in EMEIA, explained, "A software robot can be programmed to pretty much do the work of a normal human. Finance teams can program robots to perform standard functions in order to free up the finance staff to focus on more important things."
- **Predictive analytics and data mining.** While businesses have used data analytics for some time, new, advanced analytical tools offer forward-looking capabilities that can help them "improve ability to predict outcomes – and manage strategic risk – through scenario analysis and forecasting" and "better understand the financial impact of key strategic and operational decisions."⁴ Data mining is the process of identifying and analyzing patterns in massive data sets, then simplifying those patterns so humans can learn new things from them.⁵
- **Artificial intelligence (AI).** AI describes technologies that are "capable of ingesting information and instructions, learning from interactions with human beings and responding to new situations and questions in a human-like way."⁶

Benefits of new technologies

New technologies are beginning to change how internal auditors work. Mr Winters noted that new technologies are expanding the type and quantity of data analyzed while at the same time enabling a targeted approach: "We're analyzing massive contracts and complex transactions using unstructured and structured data to identify potential red flags." Mr Blackmore added that these tools eventually will allow for much more automation, creating additional benefits: "As we get into robotics, we will have robotics auditing many functions. It will become more real time as machines are processing so much data very quickly. Absolutely, it's morphing and becoming more automated, becoming built into the function."

These changes in approach brought on by new technology are beginning to yield important benefits:

- **Greater coverage.** Advanced analytics and automation will make it possible to test an entire population of transactions or other events – rather than just a sample – even tracking them in real time rather than retrospectively. In a pre-meeting conversation, Mr Winters mentioned the example of procurement processes: "Before, we could look at 40 transactions out of thousands. With data analytics, we can increase the coverage and the assurance, allowing a more clear statement about overall compliance." At the meeting, he described one of the ways Siemens responded to corruption problems in 2006: "We had

³ EY, *Robotic Process Automation in the Finance Function of the Future* (New York, Ernst & Young Accountants LLP, 2016), page 2.

⁴ EY, *Is the Future of Finance New Technology or New People?* (London: EYGM Limited, 2016), page 5.

⁵ Alexander Furnas, "Everything You Wanted to Know About Data Mining but Were Afraid to Ask," *Atlantic*, 3 April 2016.

⁶ EY, *Is the Future of Finance New Technology or New People?* page 11.

to get cash transactions under control. We started matching bank accounts of transaction recipients and checked them against internal databases to make sure that all the suppliers were legitimate. We brought everything into the electronic environment, so we could start using data analytics to keep track of the information.”

- **Greater efficiency.** Large-scale automation will allow more rote auditing tasks to be done by machine, yielding significant cost savings. An EY leader described the scale of savings he has been witnessing on the external audit side: *“We are using automation around the data consolidation efforts and the results are quite staggering: a 50-60% productivity improvement. For some tasks, we’ve reduced time spent dramatically. Now you have to consider moving activities that are currently offshore back onshore and replacing human labor with software robots.”* With automation, audit teams will turn their attention to testing and auditing the algorithms that drive the process automation, but Mr Blackmore noted that this will require fewer people: *“Internal audit could give assurance that robots are configured correctly and locked properly, but the way you test the control won’t take 50 people.”*
- **Ability to focus human resources on higher-level tasks.** Automation will also allow the internal audit team to focus on the harder tasks that require human judgment. Mr Blackmore explained, *“With new tools, we can free up time to home in on the real risks and provide comfort that these risks are really managed – for example, the risks of going into a new market or launching a new product. We can work with the business on these high risks in a proactive way. Big-ticket risks are related to judgment and can’t be audited by a machine.”*
- **Ability to provide better insights and operational advice.** Advanced analytics and data mining will help the team develop deeper insights. Further, insights about the future – generated with the help of predictive analytics and tools that use AI – could provide opportunities for internal audit to expand its role. *“We have to have the courage to play a role beyond hindsight. We need to be more relevant to the work of management and the audit committee. What if management had the audit function review future risks? I think the audit function needs to move from hindsight to foresight,”* Mr Winters explained.

The guests also mentioned broader benefits for the business of innovation within internal audit. With more sophisticated tools, internal auditors can provide better advice on improving business processes. *“Audit needs to be a part of reviewing how digitalization can challenge current business models,”* Mr Winters said. In addition, the tools themselves may be useful in the business: *“Anything we develop, we turn over to the business to use as well. As soon as the prototype works for audit, we turn it over to the business to use.”*

Many of the enhanced internal audit capabilities are still in the early stages of implementation. For example, neither Mr Winters nor Mr Blackmore saw extensive use yet of more advanced techniques such as AI. In a pre-meeting conversation, Mr Blackmore said, *“Internal audit functions tend to be behind the curve in embracing new technologies. Only in the area of analytics are they beginning to think of what they can do – and it’s only additive, not replacing anything.”* At the meeting, he added, *“AI and machine learning are coming, but they are not seen as much in use yet.”*

Challenges to adoption and implementation

One reason for the slow adoption of new technologies may be the adjustments required in areas such as staffing and audit planning. Mr Blackmore highlighted one of the most important issues: *“There’s a net shortage of skills. The internal audit brand isn’t going to attract top cyber talent to the function. It is a challenge to get those skills into the organization.”* Ideally, members and guests agreed, internal auditors should have skills and knowledge in several areas: auditing, technology and business.

The latter includes not only knowledge of the company’s business but also expertise in areas such as major transactions, Mr Winters said: *“Our team has a group of people with experience in mergers and acquisitions who really understand these kinds of transactions. Their experience helps us stay relevant.”* In a conversation after the meeting, he added that *“you need the right balance between subject matter expertise from outside and in-house business knowledge.”*

Mr Winters described a transformation of the internal audit function that was designed partly to attract talent: *“When I started at Siemens, we had 70 audit departments staffed by over 580 mainly career auditors. We now have a single organization staffed by Siemens employees on multiyear rotational assignments – one large group with 300-plus people and no career auditors. It’s a three- to five-year stint. The question is, how do you make audit attractive to professionals? You need to show that it is a program and point to role models. We have placed 400-plus professionals into the business.”*

Mr Winters also described how the team has strengthened its capabilities in the area of technology: *“We now have 10 hackers on the internal audit team who are constantly probing Siemens’ IT systems and our products. I believe that governance of cybersecurity should be separate from the IT operations. It shows much more where we stand on products, services and internal processes.”* Mr Blackmore said, *“If you don’t have internal audit data scientists, then you’re behind.”*

Given the scarcity of talent, however, Mr Blackmore noted that internal audit functions might need to reach beyond their organizations for help. *“It may involve sourcing outside of audit, sourcing from third parties. Unless you’re a major audit function, the ability to meet that need is difficult, so you need external help. Teams need to be centers of excellence across a global organization, executing across a broad range of skills,”* he said.

New technologies are also necessitating changes to audit planning. Reflecting on how the work of internal audit has changed over the last 10 years, the guests noted the growing prevalence of a more flexible approach. Mr Winters said, *“The traditional way of making a plan and locking it in for 12 to 15 months is becoming more of a historical model. You need to not be married to the audit plan and be responsive instead.”* Mr Blackmore added, *“Risk doesn’t run to a certain month cycle. These traditional plans will become less relevant. I would push the audit function to give an opinion on the control environment. I think coverage plans will also be less relevant. If you sacrifice risk for coverage, you’re in trouble.”*

Audit chairs are concerned about both innovation and assurance

A core responsibility of the audit committee is to oversee the internal audit department, which often reports functionally to the audit committee. How should this oversight address the new digital challenges for internal audit? At the meeting, audit chairs and guests discussed two overall concerns regarding the internal audit function at large companies: innovation and assurance.

Are we keeping up?

Reflecting audit chairs' desire to promote innovation in internal audit, one member asked, *"How can we ensure that we are on the cutting edge?"* Members wondered, for example, if digitalization should be part of the internal audit budget or *"set up as a particular project to ensure forward movement."* In conversations before and during the meeting, the guests offered advice on how the audit committee can determine if the internal audit function is up to speed, addressing both resource needs and organizational issues:

- **The CAE.** Mr Winters highlighted the importance of evaluating the CAE: *"Does the CAE have enough understanding of what it takes to transform the department and enough resources, not only in terms of size but more in terms of expertise?"* A member also raised this issue and mentioned a draconian intervention: *"I've replaced the chief internal auditor because they didn't have the awareness of what they would need."*
- **Integration of analytics into the overall function and organization.** The guests advised that audit committees look for an integrated approach to incorporating new technologies and skills into the function. Mr Blackmore noted, *"It's not about a digital strategy but about how you are integrating digital across a strategy."* In a pre-meeting conversation, Mr Winters explained, *"If you're going to see analytics as just another arm of your procedures, it will not work. It needs to become integrated into the way you work. Are you applying analytics to all the data? How many people would be able to build an app to solve a problem?"* At the meeting, he added, *"I would ask, are there unrestricted opportunities to analyze the data generated by the organization? Also, where does the analytics team sit?"*
- **Culture.** Mr Winters also mentioned more intangible factors that might impede progress: *"I would say, don't underestimate the power of an organizational culture, especially in traditional companies that are today facing a new world. Try to find out what culture internal auditors have to work in and what roadblocks there are in providing digital assurance."*

Is the organizational structure of assurance still sound?

Pushing forward on innovation raises another issue that the audit committee should consider: what impact are new technologies and processes having on the commonly used framework for assurance known as the "three lines of defense" model?

In this framework, line management is the first line of defense, executing controls on a day-to-day basis as part of business operations. The second line consists of functions such as compliance and enterprise risk management, which design the controls and policies and help the business implement them. Internal audit is the third line of defense, providing independent and objective assurance that the other two lines are working as intended. Though the precise allocation of responsibilities varies from company to company, many have found this framework to be a useful baseline.⁷

However, new technologies and approaches may be straining this arrangement, as they allow each line to expand its scope and encroach on the others. This blurring is particularly apparent as internal auditors provide more front-end monitoring. Mr Blackmore explained, *"I think the lines-of-defense model has become weakened, because the third line is seen as first. If the only assurance you're getting is from internal audit, then the system is broken. The second line is struggling with what their role is; they are not internal*

⁷ Stephen Gregory and Mark Watson, *Are We Nearly There Yet? New Challenges ahead for Internal Audit in Financial Services* (London: EYGM Limited, 2016), page 4.

audit, but what are they? You do see the second line taking analytics as their approach, but they must remember that there is also internal audit within the organization.”

An EACLN member also saw a lack of clarity around roles and responsibilities, stemming partly from the introduction of new technology-related processes: *“I agree that it starts with management. In our organization, the hacking team sits with them. But what does the second line do? We want to make sure every line isn’t running separate hacking teams.”*

The guests and audit chairs had few specific recommendations for addressing these issues, beyond making sure that the audit committee considers them and finds an approach that works for the company. Mr Winters did note that even if the first or second line undertakes hacking to test security, the internal audit function should do so as well. Also, while the guests agreed that internal audit must maintain its independence and objectivity as the last line of defense, they saw a continued role for internal audit in supporting, as well as auditing, the other lines – a role that the audit committee could both encourage and monitor. Mr Blackmore said, *“One of internal audit’s roles is strengthening the second line of defense. Creating collaboration among these functions is useful.”*

Mr Winters said that, even with a clear division of responsibilities among the three lines, maintaining professional scepticism and independence will always remain an area of focus, particularly as staff are rotated from the business through the internal audit function. However, he suggested that it was possible with proper training: *“We must make sure that people understand why they are here at the beginning. In my view, client service and independence can remain together – look at the professional accounting firms as an example. We apply the same risk management as the Big Four.”*

Conclusion

New digital technologies are transforming many aspects of business, including internal audit. As these technologies enable innovative digital platforms and new business models, they are presenting fresh challenges for internal audit and its oversight of the control environment and risk management. Yet these same technologies are also allowing internal audit to be more effective. Advanced analytics and automation are enabling greater coverage, efficiency and insight into business processes. The implementation challenges are significant, including a pressing need for expertise and the need to ensure that internal audit remains independent. Nevertheless, as internal audit combines its critical role of providing independent assurance with more consultative roles, it must not shrink from the opportunity to expand its impact. Mr Winters suggested a new benchmark for the function: *“If internal audit doesn’t create waves, it’s not doing its job.”*

About this document

The European Audit Committee Leadership Network is a group of audit committee chairs drawn from leading European companies committed to improving the performance of audit committees and enhancing trust in financial markets. The network is organized and led by Tapestry Networks with the support of EY as part of its continuing commitment to board effectiveness and good governance.

ViewPoints is produced by Tapestry Networks to stimulate timely, substantive board discussions about the choices confronting audit committee members, management and their advisors as they endeavor to fulfil their respective responsibilities to the investing public. The ultimate value of *ViewPoints* lies in its power to help all constituencies develop their own informed points of view on these important issues. Those who receive *ViewPoints* are encouraged to share it with others in their own networks. The more board members, management and advisors who become systematically engaged in this dialogue, the more value will be created for all.

The perspectives presented in this document are the sole responsibility of Tapestry Networks and do not necessarily reflect the views of network members or participants, their affiliated organizations, or EY. Please consult your counselors for specific advice. EY refers to the global organization, and may refer to one or more of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Tapestry Networks and EY are independently owned and controlled organizations. This material is prepared and copyrighted by Tapestry Networks with all rights reserved. It may be reproduced and redistributed, but only in its entirety, including all copyright and trademark legends. Tapestry Networks and the associated logos are trademarks of Tapestry Networks, Inc. and EY and the associated logos are trademarks of EYGM Ltd.

Appendix 1: Guests

Jonathan Blackmore

Mr Blackmore is EMEIA Advisory Risk Leader at EY, leading the firm's governance, risk and control advisory practice in Africa. He has over 10 years of experience as a governance, risk and control subject matter specialist and has worked with a number of South African state-owned enterprises to improve their risk and control environments. He also has extensive experience on both local and international internal audit and risk and control transformation projects, and he has directed large organizational change programs.

Hans Winters

Mr Winters is chief audit officer at Siemens. He is responsible for leading the internal audit group, a global team of approximately 300 professionals providing factual, unbiased assurance to Siemens' managing board, audit committee and executive management. He has held that role since 2007. Prior to joining Siemens, Mr Winters worked at PricewaterhouseCoopers, where he served as lead partner for the securities litigation practice in continental Europe, providing crisis and risk management consulting to companies dealing with compliance matters.

Appendix 2: Participants

Members participating in all or parts of the meeting sit on the boards of about 50 public companies:

- Mr Mike Ashley, Audit Committee Chair, Barclays
- Mr Aldo Cardoso, Audit Committee Chair, ENGIE
- Ms Mary Anne Citrino, Audit Committee Chair, HP Inc.
- Mr Carlos Colomer, Audit Committee Chair, Abertis
- Ms Pam Daley, Audit Committee Chair, BlackRock
- Ms Carolyn Dittmeier, Chairman, Statutory Audit Committee, Generali
- Dr Edgar Ernst, Audit Committee Chair, TUI AG
- Dr Byron Grote, Audit Committee Chair, Tesco, Akzo Nobel and Anglo American
- Mr Lou Hughes, Audit Committee Chair, ABB
- Mr Nasser Munjee, Audit Committee Chair, Tata Motors
- Mr Chuck Noski, Audit Committee Chair, Microsoft
- Ms Guylaine Saucier, Audit Committee Chair, Wendel
- Dr Erhard Schipcoreit, Audit Committee Chair, SAP and RWE
- Mr Lars Westerberg, Audit Committee Chair, Volvo

EY was represented in all or parts of the meeting by the following:

- Mr Andy Baldwin, EMEIA Area Managing Partner
- Mr Jean-Yves Jégourel, EMEIA Assurance Leader
- Ms Julie Linn Teigland, Regional Managing Partner – Germany, Switzerland, Austria

Appendix 3: Discussion questions for audit committees

- ? What are some key changes in how the business operates at your companies? How are digital technologies changing the business?
- ? In what ways do these changes present challenges for internal audit? Is it becoming more difficult to assess controls and risks?
- ? What steps has internal audit taken to address these challenges?
- ? Is internal audit at your company starting to use new digital tools? What kind? What benefits are they seeing?
- ? Have you noticed any implementation challenges for these new tools? What kind of staffing issues, for example, have you heard about?
- ? What kind of interactions with internal audit will the audit committee need? Will the types of meetings or reports need to change?
- ? What does the audit committee need to know in order to oversee the impact of digital transformation on internal audit? What specific issues should the audit committee focus on?
- ? Where might the audit committee need to intervene?