Current trends in outsourcing and addressing third party risk

KEVIN F. MCCLOSKEY
CISA, CIA, CRMA, Deloitte AS

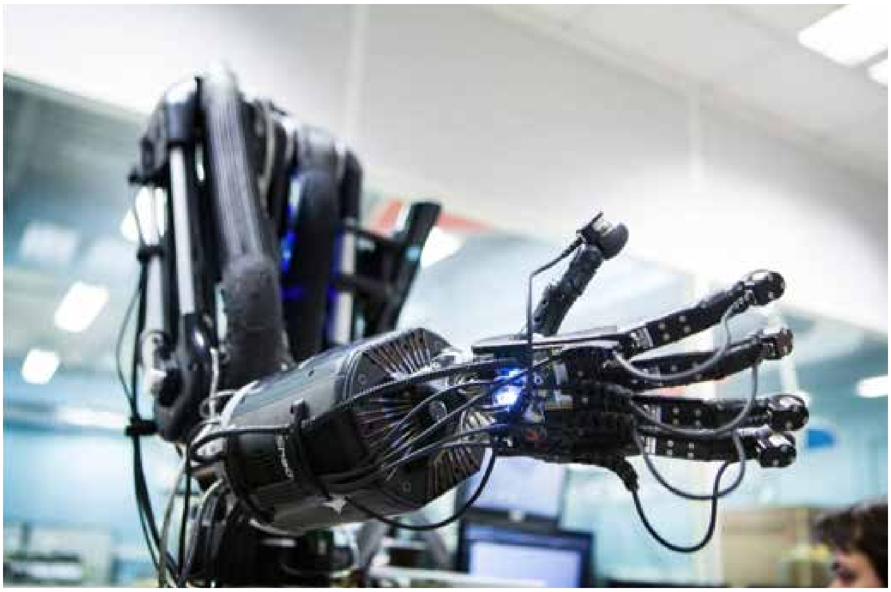


Figure 1: Source - Deloitte

Outsourcing – A growing trend

Businesses are increasingly dependent on third parties to provide mission-critical services. This may include services related to information technology (e.g., managed IT services, SaaS, security-monitoring services), finance and accounting (e.g., payroll processing and accounting services), customer service support and human resources administration, to name a few. Outsourcing has gone from being a value-protecting measure to becoming a value-creating measure.

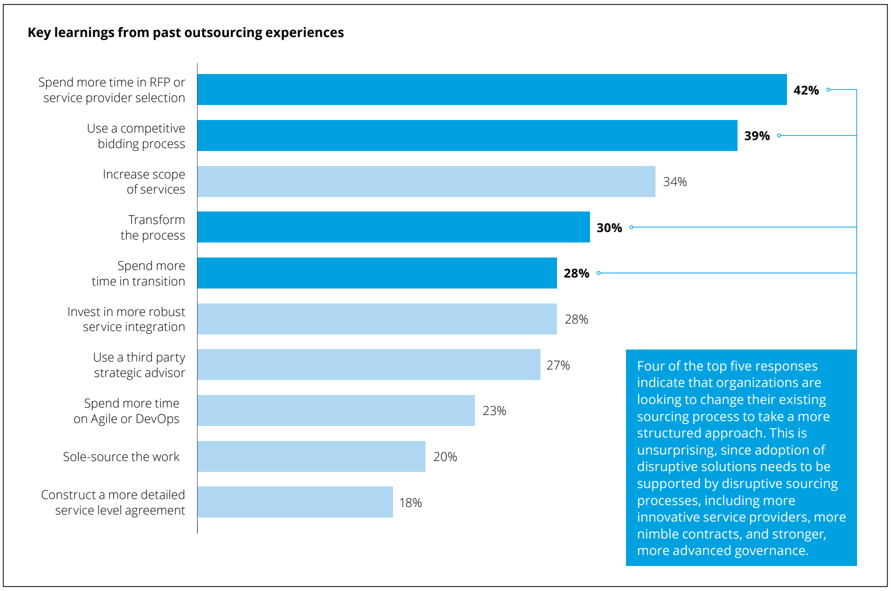
> Outsourcing has gone from being a value-protecting measure to becoming a value-creating measure

What drives this? Simply put, companies must accept that outsourcing is sometimes required to be competitive on a global basis, to grow in the market or to reduce costs and increase quality. The increasing use of outsourcing in today´s market has made companies more dependent on a complex network of third-party suppliers. From a risk perspective, it is important that the companies themselves have an overview of the risks that affect them and manage and monitor these in a satisfactory manner. You can outsource a task but you cannot outsource the risk related to it.

The Deloitte Global Outsourcing Survey

Deloitte recently surveyed over 500 leaders from organizations of all sizes and with operations in Europe, the Americas and Asia in regards to their experiences and thoughts related to outsourcing. The survey found that while in the past organizations typically used outsourcing to improve back-office operations through cost reduction and performance improvement, today's organizations are looking to disruptive outsourcing solutions to enable competitive advantage by accelerating changes within those organizations. For these organizations, outsourcing can bring quick wins to top line growth, as well as to a more agile, effective back office. The focus has shifted from traditional 'work transfer' to upfront transformation and automation. Organizations are recognizing that disruptive solutions can revolutionize the way they do business, and that "buying" capabilities in the marketplace is generally faster and more scalable than developing capabilities internally. Emerging solutions incorporating cloud and automation are empowering organizations to work smarter, scale faster, reach new markets, increase productivity and, ultimately, to gain competitive advantage.

As with many initiatives, organizations are finding that delivering competitive advantage through disruptive outsourcing



Four of the top five responses indicate that organizations are looking to change their existing sourcing process to take a more structured approach. This is unsurprising, since adoption of disruptive solutions needs to be supported by disruptive sourcing processes, including more innovative service providers, more nimble contracts, and stronger, more advanced governance.

Figure 2: Source - The Deloitte Global Outsourcing Survey 2018

solutions is anything but simple; effort and expertise are needed to address security and cyber risks, changing regulations, organizational resistance, skill gaps, and to help flatten fragmented processes.

The survey itself can be found here: https://deloi.tt/2ZPd9A8

Technology drivers for disruptive outsourcing?

What are the technologies driving disruptive outsourcing? The survey found that there were three main technologies that are driving this focus on disruptive outsourcing. These are cloud computing, robotic process automation (RPA) and cognitive automation.

- **Cloud computing** is a model for providing customers access to a shared pool of computing resources (e.g., networks, servers, storage, applications and services). The model for these resources is that the ultimate user of the resource can do so with minimal management effort or service provider interaction.
- **Robotic process automation (RPA)** is basically a software that performs repetitive rules-based tasks to improve efficiency, quality and accuracy of process outcomes.
- **Cognitive automation** adds additional capabilities to RPA, including learning, judgment and 'reading' of unstructured text (e.g., handwriting, photographs, etc.).

What does this look like in Norway?

My vantage point is that of a third party assurance specialist/external and internal IT auditor. I base my observations on what I see at my clients, who are managed IT service providers, Software as a service providers, data center management providers, multinational telecom companies, financial institutions and public sector institutions, among others. What I am seeing is a clear increase in the use of all of these technologies.

- **Cloud computing**, of course, has been a hot topic for some time now and many of us use some form of cloud computing resource whether we know it or not. Cloud is one of the top-of-mind subjects when discussing areas such as IT strategy, budget and performance. It is also one of the 'black holes' in the IT auditor world. Where are my documents actually stored?
- **RPA** is very prevalent in, among others, the financial services industry, the healthcare sector, manufacturing and even agriculture sectors. These types of programmed routines present advantages for the users of the service due to the lower margin of error they provide. They also present challenges for us auditors and those tasked with managing internal control programs in user companies as to how to gain confidence in the functionality and reliability of the programmed routines themselves. Have you tried to interview a robot?
- Being the logical extension of RPA and providing true automation possibilities, **cognitive automation**, to me, can be seen as the culmination where we want to go with robotics. In my experience, this has been highly present in the financial services sector, but also in the consumer business, healthcare and pretty much all sectors when considering opportunities for automating repetitive and standard processes. Cognitive automation, also known as smart or intelligent automation, includes such exciting areas as Natural language processing (NLP) and machine learning. That 'person' answering your questions on the hotline sounds a bit metallic do they?

What does this mean from an internal control perspective?

In general, more outsourcing means more situations where someone at a user organization needs to understand controls that are outside of their company in order to fulfill their obligation to have an end-to-end understanding of internal control processes. Limited insight into the functionality and internal controls at outsourcing organizations due to contractual constraints, time and budget constraints and / or limitations in competence to understand and analyze the risks related to the use of the outsourced services can hinder a company's ability to have the right amount of control over their internal control processes from start to finish.

There is a growing need for more assurance from those providing the services and this need is being evidenced to me by numerous requests for third party assurance reports. I have seen a lot of recent requests for something called SOC2 reports (which basically provide assurance in regards to security, availability, confidentiality, processing integrity and privacy of information). I have also seen an increase in requests for ISAE3402/SOC1 reports (focused on the areas addressing the internal control related to processing of financial information and meeting the needs of, among others, external auditors) as well as specific

ISAE3000 reports designed to meet the needs of an individual customer of the service provider.

GDPR is a hot topic these days and is getting a lot of attention from us in the audit and assurance crowd due to the drastic penalties of non-compliance. These other areas like cloud computing and RPA also present clear 'issues' for auditors and the companies they audit. The availability of third party attestation reports is currently somewhat limited but I am seeing an increase in requests for these, even from some companies I had assumed to have had such reports in place for several years based on their services and customer portfolio.

The survey found that most organizations with outsourcing initiatives that have been reviewed by internal or third party auditors in the last 12 months have completed and passed their audits. There were few completing their audits with material issues. This is promising and in my experience from the companies I have worked with this development is a natural result of the work of both the auditor performing the work and providing the opinion as well as the company being audited through their receptiveness to take advice and remediate weak controls or implementing new controls where there are gaps.

Does auditing/attestation contribute to the quality of and focus on internal control?

As a specialist in providing third party attestation services I may be biased in my opinion as to the reasoning for these good results. Of course there is an extraordinary amount of money and resources spent on security each year. My bias here would be to say that those companies that undergo a significant audit of the type required to issue a third party report or independent opinion as to the design and implementation of security controls have a tendency to learn from the audit and 'clean up' their reportable issues under the audit and, if findings are issued, afterwards. These audits generally subject the auditee to measurement against formal criteria such as the SOC2 Trust Criteria or COBIT or ISO27001 for an ISAE3402 / SOC1 report using one of those standards as measurement criteria. The criteria are designed to measure a company's maturity against a set of best practice standards and when performing the audit, the auditee receives a set of control 'gaps' or weaknesses that they need to either clear or they turn into findings in the report, which will go to their customers.

In my experience, most organizations that take the step to initiate such an attestation project are receptive to observations and take them as 'constructive criticism'. This is dependent on us as the auditors and how we present our findings. If we can present findings in a manner that clearly highlights the risks the gap or weakness in controls presents to them and, if possible, come with good and constructive feedback and suggestions as to how they can remediate the issues, then the recipient of the 'bad news' has a tendency to look at the findings as positive opportunities for improvement. Through the iterative process of auditing and remediating issues, companies improve their overall internal control structure and often improve their IT Governance maturity in regards to internal control and information security.

How do companies address cyber risks with their vendors?

Based on the survey results, companies rely heavily on a regime of contractual commitment and periodic evaluation. This most likely reflects the uncertainties in the market these days in regards to various regulatory requirements and, in general, the difficulties involved in transferring some of your internal functions to an external party. Companies basically get

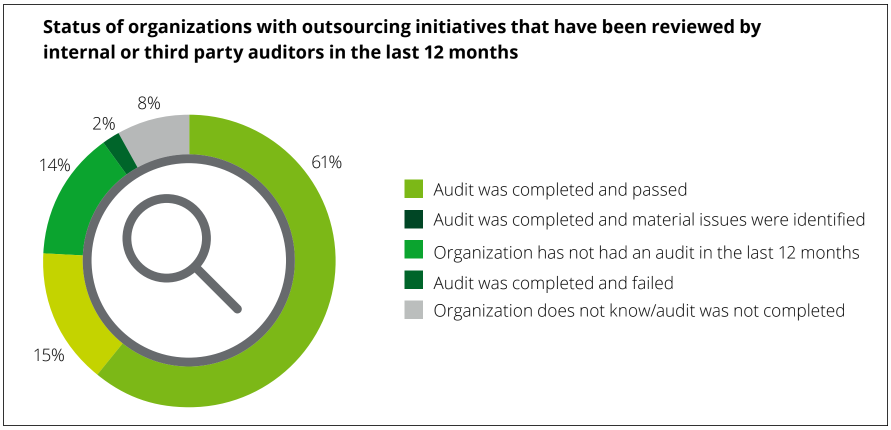


Figure 3: Source - The Deloitte Global Outsourcing Survey 2018

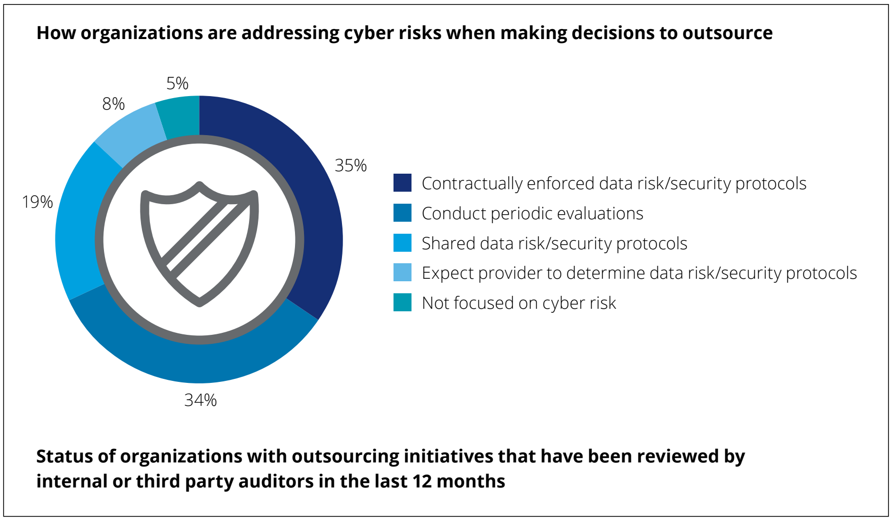


Figure 4: Source - The Deloitte Global Outsourcing Survey 2018

vendors to contractually commit to a form of behavior / provide a specific level of service and they follow-up that commitment with periodic assessments. There are basically 3 types of 'assessments':

1) Self-assessment by the vendor (low level of security / reliance)
2) Assessment of the vendor by the customer itself (high level of security but dependent on the scope and depth of the review and also the competence and time commitment from the team performing the audit), and
3) Independent review by a specialized third party (high level of security but the receiver of any report needs to be aware of the scope of the audit performed to ensure the areas significant to them are included).

More complex organizations will most likely use a mix of these methods based on a risk-based analysis of their vendors and business partners to obtain a balanced approach to gaining assurance.

Security is foremost when choosing a cloud provider

Cloud is enabling competitive advantage by providing access to innovative technologies at the touch of a button, while avoiding many traditional roadblocks, including extensive up-front planning, capital expenditure, lengthy implementation times, and long term contracts. This is helping organizations be more agile, rapidly expand their offerings, enter new markets, and transform their internal operations.

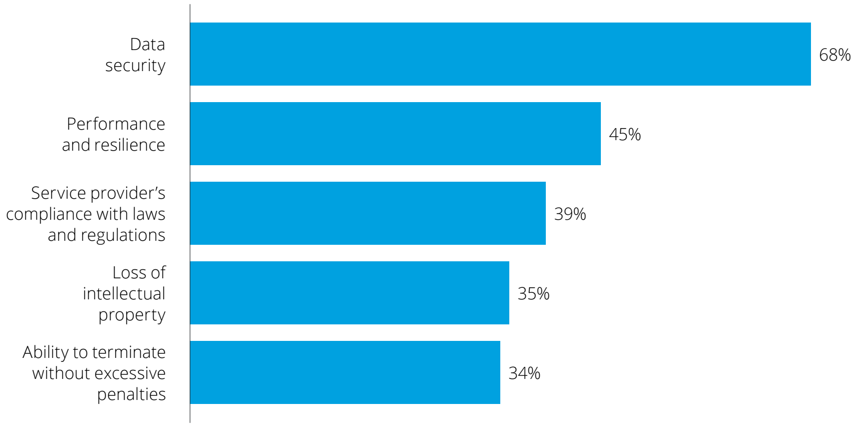
When selecting a cloud service provider and designing solutions, executives' primary contractual concern is data security (68 percent), followed by performance/ resilience (45 percent), and providers' compliance with laws and regulations (39 percent). Data security and compliance issues can make organizations wary of adopting public cloud solutions, but this can cause them to miss out on its many benefits. A well considered cloud strategy must strike the right balance between achieving cloud's benefits and maintaining the appropriate levels of security.

CYBER RISKS WHEN MAKING OUTSOURCING DECISIONS

Nearly all respondents to the survey (95 percent) have cyber risk measures in place. About one-third (35 percent) of organizations contractually enforce data risk and security protocols with their providers and conduct period evaluations/audits. Clearly, organizations recognize the importance of proactive monitoring of cyber risk, and increasingly they are being proactive in its management.

In 2018, 78 percent of organizations reported that their outsourcing engagements were audited within the past 12 months; this is in line with 77 percent reported in an earlier survey from 2016. More audits were completed and passed (61 percent in 2018 vs. 53 percent in 2016), and fewer material issues were identified (15 percent in 2018 vs. 22 percent in 2016).

Top five concerns with cloud services contracting



Source: The Deloitte Global Outsourcing Survey 2018.

Figure 5: Source - The Deloitte Global Outsourcing Survey 2018

Security is also foremost when considering an RPA service provider

Digital labor is increasingly replacing repetitive, rules-driven tasks through automation, enabling faster, more efficient, and more accurate work at reduced costs, and fundamentally disrupting the old mantra of driving change through incremental improvements and labor arbitrage.

According to the survey, when selecting an RPA service provider and designing solutions, executives' primary contractual concern is data security (62 percent), followed by performance/ resilience (48 percent), and the providers' compliance with laws and regulations (42 percent). Approximately half of them see organizational resistance, process fragmentation, and regulatory constraints as their biggest implementation challenges. Of respondents using RPA, approximately one-third are also implementing cognitive automation, while another 59 percent plan to do so within the next 18 months.

What do the survey respondents plan to do differently in the future?

The survey asked respondents what they would do differently when launching their next outsourcing initiative based on their past experiences. The top responses were focused on the selection of providers as well as taking a more strategic planning approach.

- Service provider selection. The top responses were related to the selection process: spend more time in RFP or service provider selection (42 percent), and use a competitive bidding process (39 percent). This may be due to the increasing maturity of both the procurement and vendor management functions within organizations.

- Strategic planning approach. Other popular answers involved taking a more strategic approach to planning a new outsourcing initiative: increase the scope of service (34 percent); transform the process rather than simply lifting and shifting (30 percent); invest in more robust service integration and transition (28 percent); and use a third-party advisor (27 percent).

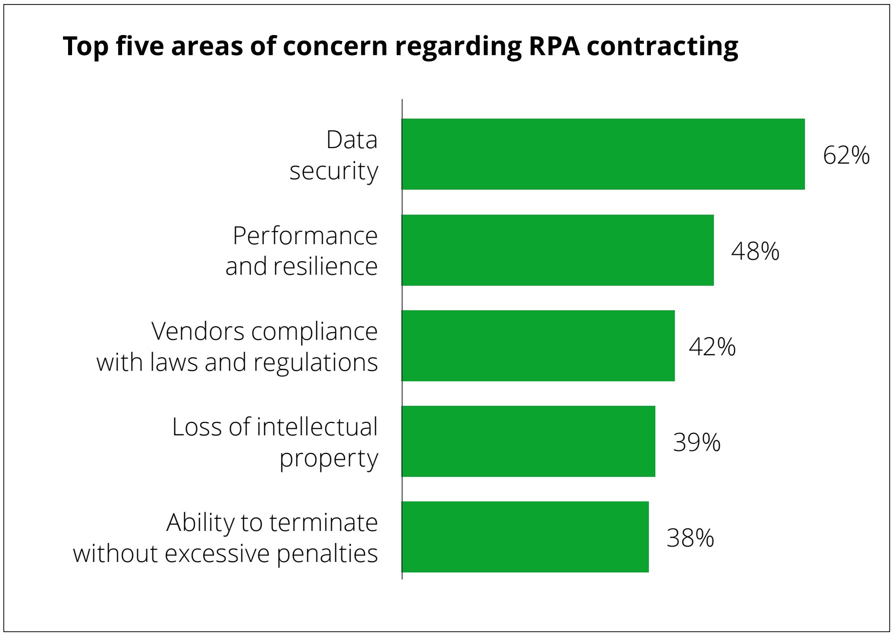


Figure 6: Source - The Deloitte Global Outsourcing Survey 2018

What does this all mean?

My work experience is focused on the internal control aspects of outsourcing, performing third party attestation engagements (e.g., ISAE3402, SOC1, SOC2, ISAE3000), assisting clients in evaluating their maturity in regards to their vendor governance programs, performing individual vendor audits and reviewing the results of vendor audits. In the past years I have seen a drastic increase in the number of requests for independent verification / attestation of internal controls at outsourced vendors. SOC1, SOC2, ISAE3000 and ISAE3402 reports are becoming more commonplace in Norway as more companies are being required to provide them to their customers.

With global expansion for many service providers, we see that they are running into international customers that bring with them the contractual requirement of providing third party attestations and other forms for confirmation of good security or internal control. I currently deliver a number of SOC2 reports which focus on the areas of Security, Availability, Processing Integrity, Confidentiality and Privacy. The requests for these reports and the standard ISAE3402 / SOC1 reports that we generally issue are increasingly being driven by the larger, more influential and often international customers of the outsourcing service providers. This will only grow as our local Norwegian providers either expand their operations internationally through their own devices or through their being acquired by companies with an international footprint.

I fully expect the focus on outsourcing and the risks involved will be on the agenda for many years to come. One of the main areas that will continue to be in focus will be the area of information security and becoming comfortable with the vendor's internal control maturity in regards to the services being provided. Of course, GDPR trust issues between companies and security measures such as liability caps in regards to GDPR compliance risk in contracts will be driving many companies to want to prove to their customers and business partners that they are compliant. Independently produced third party attestation reports will be one of the most logical and useful methods for companies to show their compliance.

Exciting times ahead

I think that the recent developments in outsourcing outlined in the survey provide exciting opportunities for all involved parties. These new technologies present new risks and new challenges for us auditors. But if it was easy, it wouldn't be fun! Is suggest you take a look at the survey itself for more details than I have summarized here. The link is provided early in this article.

More organizations are conducting and passing audits with fewer material issues

76% of respondents indicated that regulations around data privacy and protection are affecting their disruptive outsourcing decisions

62% of respondents adopting RPA, and 68% of respondents adopting cloud indicated data security as an area of concern during contracting